TPM Vol. 32, No. S4, 2025
ISSN: 1972-6325
https://www.tpmap.org/

CYBER SECURITY DISCLOSURE OF BANK SYARIAH INDONESIA: A COMPARATIVE STUDY

LIA SARI
SRIWIJAYA UNIVERSITY INDONESIA.
EMAIL: liasari1505@gmail.com

MOHAMAD ADAM
SRIWIJAYA UNIVERSITY INDONESIA.
EMAIL: mr_adam2406@yahoo.com

LUK LUK FUADAH
SRIWIJAYA UNIVERSITY INDONESIA.
EMAIL: lukluk_fuadah@unsri.ac.id

YUSNAINI
SRIWIJAYA UNIVERSITY INDONESIA.
EMAIL: yusnaini@fe.unsri.ac.id

ABSTRACT

This current study investigated cyber security disclosures at Bank Syariah Indonesia (BSI) during 2022 and 2023 using a qualitative exploratory approach. This period was chosen because in 2023 there a cyber security breach or incident to BSI. Previous research had shown that cyber security incident could affect bank's cyber security disclosure. This current study used the cyber security disclosure index to analyze the content of cyber security disclosures in the information technology chapter in the bank's annual report. This study compared cyber security disclosures before and after the 2023 BSI cyber security breach/incident, compared BSI's cyber security disclosures with Islamic banks listed on the IDX in 2022 and 2023, and also compared with 2 conventional commercial banks as a benchmark for cyber security disclosure in Indonesia. This study concludes that the cyber security incidents experienced by BSI in mid-2023 have had a positive effect on the extent of cyber security disclosure of BSI, Islamic banking in Indonesia, as well as conventional commercial banks in Indonesia. This research contributes to providing an overview of the level of cyber security disclosure in BSI before and after the cyber incident, as well as peer industry.

Keyword: cyber security disclosure, cyber incident, voluntary disclosure, bank, shariah bank.
JEL Classification : G21, G34, M41, M480

INTRODUCTION

Digitalization has happened globally over the past decade, including in banking sector. The development of digitalization is taking place very quickly which offers convenience and practicality in financial activities. Banking digitalization involves the use of digital technology in banking activities. Digitalization and digital technology also pose a threat in the form of cyber threats. One of the largest dangers for businesses that rely on information technology systems for their daily operations is cyber risk. The 2022-2023 Global Risks Perception Survey (GRPS) perform by the World Economic Forum shows that "Cyberattacks on critical infrastructure" as one of the top 5 risks in 2023 with the largest risk of their potential impact on a global scale [1].

[1] World Economic Forum WEF, "The Global Risks Report 2023 18th Edition," *World Economic Forum*, 2023, https://www.weforum.org/reports/global-risks-report-2023.

The global financial system is undergoing an unprecedented digital transformation, and this is accelerated by the COVID-19 pandemic [2]. Banks are increasingly intensively using information technology in their operations. Currently, the transformation to digital currency and the modernization of payment systems are rampant, where cyber security is becoming increasingly important. A new aspect of risk management is cyber security [3]. Cyber security can be defined as

"the approach and actions associated with security risk management processes followed by organizations and states to protect confidentiality, integrity and availability of data and assets used in cyber space. The concept includes guidelines, policies and collections of safeguards, technologies, tools and training to provide the best protection for the state of the cyber environment and its users" [4].

In order to effectively manage cyber hazards, banks awareness must be raised. Banks are concerned about safeguarding their digital assets because cyber attacks have the potential to impair their operations.

The rapid development of information technology, followed by the high number of cyber attacks, encourages stakeholders to obtain certainty that the company has implemented management related to cyber security properly.

A relatively recent corporate disclosure goal is cyber security disclosure. The necessity for stakeholders to have access to sufficient information on cyber security is increased by the growing frequency of cyber attacks. Stakeholders will expect public businesses to address cyber security risks transparently. Any publicly traded firm must guarantee robust cyber security governance and offer sufficient disclosure regarding the prioritization and management of cyber security in order to allay these growing worries. It is imperative that public companies comprehend the significance of cyber security and make adequate disclosures for this issue. Such disclosures will allow companies to demonstrate their accountability and involvement in the matter and build stakeholder trust. Public corporations ought to put in place more than just efficient cyber risk management initiatives but also provide timely and useful information about the initiative to stakeholders through cyber security disclosures.

Research about cyber security disclosure in Indonesia is rare. In fact, Indonesia is one of the developing countries where cyber risks are relatively higher than cyber risks in developed countries. There is no specific regulation on the obligation to make cyber security disclosure by companies in Indonesia. It's make cyber security disclosure as one of the voluntary disclosures in Indonesia. In the next section, the research background will be presented. Literature review, methodology, results, and conclusions subsequently.

RESEARCH BACKGROUND

In recent years, regulatory bodies in the United States and Canada have highlighted the importance of cyber security disclosure and published detailed guidance [5]. Cyber security disclosure had been a concern for accounting researchers lately. However, most of the previous research was conducted in the context of the United States, where cyber security disclosure is Quasi-Compulsory [6]. Previous research has shown the rarity of cyber security disclosure research in the context of developing countries, which are at higher risk of being targeted by cyber attacks. Therefore, this research was conducted in the context of Indonesia, which is a developing country, where cyber security disclosure is a voluntary disclosure option for companies.

The phenomenon of increasing the use of digital technology in Indonesia is also followed by increasing cyber security threats. Based on data from the 2022 X-Force Threat Intelligence Index, IBM Security, 22.4% of cyber attacks

[2] Tim Maurer and Arthur Nelson, "The Global Cyber Threat Cyber Threats to the Financial System Are Growing, and the Global Community Must Cooperate to Protect It," *Finance and Development*, 2021.

[3] He Li, Won Gyun No, and Tawei Wang, "SEC ' s Cybersecurity Disclosure Guidance and Disclosed Cybersecurity Risk Factors," *International Journal of Accounting Information Systems* xxx, no. xxxx (2018): 1–16, https://doi.org/10.1016/j.accinf.2018.06.003.

[4] **(Schatz & Wall, 2017, p 66)**

[5] Lei Gao, Thomas G Calderon, and Fengchun Tang, "Public Companies ' Cybersecurity Risk Disclosures," *International Journal of Accounting Information Systems* 38, no. 100468 (2020): 1–22, https://doi.org/10.1016/j.accinf.2020.100468; Sylvie Héroux and Anne Fortin, "Cybersecurity Disclosure by the Companies on the S & P / TSX 60 Index," *Accounting Perspectives* 19, no. 2 (2020): 73–100, https://doi.org/10.1111/1911-3838.12220.

[6] Mohammed Mehadi Masud Mazumder and Dewan Mahboob Hossain, "Voluntary Cybersecurity Disclosure in the Banking Industry of Bangladesh : Does Board Composition Matter ?," *Journal of Accounting in Emerging Economies* 13, no. 2 (2022): 1–23, https://doi.org/10.1108/JAEE-07-2021-0237.

that occurred in the top 10 industries in 2021 occurred in the financial and insurance industry with details of 70% of attacks aimed at banks, 16% of insurance companies, and 14% of other financial sectors [7]. The case of the Bank Syariah Indonesia (BSI) cyber attack in early May 2023 shows that cyber risks are real. On Saturday, May 13, 2023, the LockBit ransomware gang claimed responsibility for the disruption of all services at BSI, and stated that the down incident at the bank was their doing. In the attack, 15 million customer records, employee information, and about 1.5 terabytes of internal data had been stolen. In the end, the data was found to have been released on the internet due to failed negotiations [8]. The financial impact of ransomware attacks is in the form of ransoms, response and recovery costs, legal fees, monitoring, and other unexpected additional costs. In addition, BSI as a victim also has to bear the potential loss of reputation. This attack became one of the largest incidents in the Islamic banking sector in Indonesia and highlighted the importance of cybersecurity in the increasingly digitally connected banking industry.

Currently, banks use various financial technologies, such as mobile banking, internet banking, paperless loan procedures, digital currencies, blockchain, etc. Deputy Director of Basel & International Banking, OJK Banking Research and Regulation Department said that cyber attacks that are often experienced by banks involve five things, including unencrypted data, malware, unsecured third party services, manipulated data, and website or application spoofing. It is predicted that the probability of cyber attacks in the financial sector in the future can increase if banks are not ready to mitigate cyber security [9]. Cyber attacks have the potential to cause data and financial losses as well as business disruption.

Regulations regarding risk disclosure in annual reports refer to the Otoritas Jasa Keuangan Circular Letter Number 16/SEOJK.04/2021 concerning the Form and Content of Annual Reports of Issuers or Public Companies. Companies are required to disclose the type and level of risk. For banks, regulations regarding information technology risk management are regulated in POJK Number 38/POJK.03/2016 as amended to POJK Number 13/POJK.03/2020. In 2022, OJK has issued OJK Regulation No.11/POJK.03/2022 regarding the implementation of information technology by commercial banks. This regulation replaces POJK Number 13/POJK.03/2020. Currently, this regulation only covers aspects of data, technology, risk management, collaboration and institutional order of commercial banks in order to increase the resilience and operational maturity of commercial banks. The new regulation developed by the Otoritas Jasa Keuangan (OJK) is the first cyber security regulation in Indonesia that is specifically for the financial sector, especially banking. The OJK describes the rules in circular letter Number 29/SEOJK.03/2022 (SEOJK 29) dated December 27, 2022. The circular contains details of the implementation of Regulation Number 11/POJK.03/2022 concerning the Implementation of Information Technology by Banks. From those existing rules, cyber security disclosure has not become mandatory for companies in Indonesia.

Public companies must be able to provide the best information as a proxy for their performance. Investors will use this information in assessing, predicting, and making decisions on a company's stock. Important information about the company's performance is reflected in the annual report. In addition to financial information, investors also need non-financial information to make investment decisions. Information in the form of voluntary disclosure is considered to increase the company's value because the company is considered more transparent. The cyber incident that occurred at BSI can encourage BSI, as well as peer Islamic banks in Indonesia, as well as conventional banks to carry out higher and more complete cyber security disclosures. Extensive and complete cyber security disclosure is one of the bank's communication tools to stakeholders. Banks communicate their readiness and responsibilities related to cyber security. It is interesting to examine how cyber incidents at BSI affect the extent of BSI's cyber security disclosure after cyber incidents, how the extent of BSI's cyber security disclosure compares to the extent of cyber security disclosures of Islamic banks (as peer industries), and how the extent of BSI's cyber security disclosure compares to the extent of cyber security disclosures of BM and BRI as a benchmark for banking cyber security disclosure in Indonesia.

In this study, the author restricting the measurement of cyber security disclosure items to chapter or sub-chapter with the title Information Technology in the annual report. The author did this restriction because information technology is closely related to cyber and cyber security. In addition, the restriction is expected to increase the focus of this research that uses content analysis. 6 banks listed on the Indonesia Stock Exchange in 2022 and 2023 that chosen as the objects research are Bank Syariah Indonesia (BSI), Bank Panin Dubai Syariah (BPDS), Bank Aladin, Bank Tabungan Pensiunan Nasional Syariah (BTPNS), Bank Mandiri, and Bank Rakyat Indonesia.

[7] OJK, "Best Practices: Penanganan Insiden Keamanan Siber Di Sektor Jasa Keuangan," 2022.
[8] Egidius Patnistik, "BSI, Bisnis Ransomware, Dan Negosiasi Pemerasan," money.kompas.com, 2023.
[9] Novita Intan, "OJK : Sektor Keuangan Paling Banyak Mendapat Serangan Siber Pada 2021," Republika.co.id, 2022.

LITERATURE REVIEW

SIGNALING THEORY

From the point of view of the signaling theory, cyber security disclosure in the annual report allows public companies to signal to the market that companies are actively involved in preventing, detecting, and remediating the impact of cyber incident. Cyber security disclosure serve to reduce potential litigation costs due to reduced liability due to increased transparency associated with disclosure. [10] found a positive relationship between cyber security awareness and market value. From the point of view of the signaling theory, cyber security disclosure in the annual report allows public companies to signal to the market that companies are actively involved in preventing, detecting, and remediating the impact of cyber incident. From the point of view of the signaling theory, companies with larger assets have a higher incentive to conduct cyber security disclosure and give a positive signal to the market that the company has a high commitment to cyber security. Large listed companies are more likely to attract investor interest, so they should be more willing to comply with disclosure practices [11].

INSTITUTIONAL THEORY

Institutional theory support the peer effects, that implies that businesses' decisions and actions are frequently impacted by how other businesses in their field behave [12]. In the study of institutional theory, external factors or industry-level demands have been described as a type of institutional pressure [13]. The author took industry peers' violations as an example of institutional pressure for banks cyber security disclosure decisions. The actions of industry peers (in this case, cyber incident of BSI) are institutional influences on the decisions of islamic banks as well as common banks in Indonesia. From the perspective of the new institutional theory, large companies tend to receive more pressure from stakeholders to conduct cyber security disclosures and the size of their assets makes them able to afford additional costs for such disclosures [14]. In addition, the annual reports of leading companies are a benchmark for disclosure best practices.

CYBER SECURITY DISCLOSURE

Cyber security is a condition for maintaining confidentiality, integrity, and availability of information and/or information systems that are interconnected with each other through cyber media, from cyber attacks. Cyber security can also include other aspects, such as authenticity, accountability, non-repudiation, and reliability (Copy of the Circular Letter of the Otoritas Jasa Keuangan of the Republic of Indonesia Number 29/POJK.03/2022 concerning Cyber Resilience and Security for Commercial Banks, 2022). Cyber security is information security and the protection of electronic systems, networks, devices, programs or data from theft or damage [15]. So, cyber security disclosure can be defined as disclosure addressed to stakeholders regarding information security and protection of electronic systems, networks, devices, programs or data from theft or damage.

---

[10] Berkman et al. (2018)
[11] Ahmad Ibrahim and Said Karajeh, "Voluntary Disclosure and Earnings Quality : Evidence from Ownership Concentration Environment," *Management Research Review* 43, no. 1 (2020): 35–55, https://doi.org/10.1108/MRR-11-2018-0447.
[12] Paul J DiMaggio and Walter W Powell, "Introduction," in *New Institutional Theory*, 1983, 1–38.
[13] John D Arcy and Asli Basoglu, "The Influences of Public and Institutional Pressure on Firms ' Cybersecurity Disclosures," *Journal of the Association for Information Systems* 23, no. 3 (2022): 779–805, https://doi.org/10.17705/1jais.00740.
[14] Mazumder and Hossain, "Voluntary Cybersecurity Disclosure in the Banking Industry of Bangladesh : Does Board Composition Matter ?"; Camélia Radu and Nadia Smaili, "Board Gender Diversity and Corporate Response to Cyber Risk : Evidence from Cybersecurity Related Disclosure," *Journal of Business Ethics* 177 (2022): 351–74, https://doi.org/10.1007/s10551-020-04717-9.
[15] Schatz and Wall, "Towards a More Representative Definition of Cyber Security."

The measurement of the cyber security disclosure variable in previous studies was quite varied, namely as an indicator/dummy variable [16] measured by word count [17], tone [18], readability/fog [19], boilerplate [20], specificity [21], number of keywords related to cyber security [22], use of litigious language [23], and cyber security disclosure index [24].
From the results of a literature review of previous studies, the author found that there are four previous studies that have developed a cyber security disclosure index, namely research by [25], [26], [27], and [28]. This current research will use the cyber security disclosure index that had developed by [29]. This index was chosen because it is a latest cyber security disclosure index. In addition, this index is a bank-specific cyber security disclosure index, appropriate for this study. The index is presented in Table 1. The banking-specific cyber security disclosure index used in this study consisted of 62 disclosure items categorized in cyber risk factors (9 items), potential impacts of cyber security incidents (13 items), cyber security risk management (7 items), cyber security risk mitigation (15 items), cyber security incidents (15 items), and other categories (3 items). This cyber security disclosure index is built on cyber security disclosure guidelines and best practices in the United States and Canada. The index is expected to be a guide for best practices for cyber security disclosure in Indonesian Banking.

The author compared cyber security disclosures before and after BSI cyber incident, compared BSI's cyber security disclosures with Islamic banks listed on the IDX in 2022 and 2023, as well as comparisons with 2 conventional

[16] Najeb Masoud and Ghassan Al-utaibi, "The Determinants of Cybersecurity Risk Disclosure in Firms ' Financial Reporting : Empirical Evidence," *Research in Economics* 76, no. 2 (2022): 131–40, https://doi.org/10.1016/j.rie.2022.07.001; Li, No, and Wang, "SEC ' s Cybersecurity Disclosure Guidance and Disclosed Cybersecurity Risk Factors."
[17] Thomas G Calderon and Lei Gao, "Cybersecurity Risks Disclosure and Implied Audit Risks : Evidence from Audit Fees," *International Journal Audit* Special Is, no. October (2020): 1–16, https://doi.org/10.1111/ijau.12209; Li, No, and Wang, "SEC ' s Cybersecurity Disclosure Guidance and Disclosed Cybersecurity Risk Factors"; Orry Swift, Ricardo Colon, and Kelly Davis, "The Impact of Cyber Breaches on the Content of Cybersecurity Disclosures," *Journal of Forensic and Investigative Accounting* 12, no. 2 (2020): 197–212.
[18] Swift, Colon, and Davis, "The Impact of Cyber Breaches on the Content of Cybersecurity Disclosures."
[19] Calderon and Gao, "Cybersecurity Risks Disclosure and Implied Audit Risks : Evidence from Audit Fees"; Swift, Colon, and Davis, "The Impact of Cyber Breaches on the Content of Cybersecurity Disclosures."
[20] Swift, Colon, and Davis, "The Impact of Cyber Breaches on the Content of Cybersecurity Disclosures."
[21] Swift, Colon, and Davis.
[22] Arcy and Basoglu, "The Influences of Public and Institutional Pressure on Firms ' Cybersecurity Disclosures"; Jing Chen, Elaine Henry, and Xi Jiang, "Is Cybersecurity Risk Factor Disclosure Informative ? Evidence from Disclosures Following a Data Breach," *Journal of Business Ethics* 187, no. September (2023): 199–224, https://doi.org/10.1007/s10551-022-05107-z; Mazumder and Hossain, "Voluntary Cybersecurity Disclosure in the Banking Industry of Bangladesh : Does Board Composition Matter ?"
[23] Calderon and Gao, "Cybersecurity Risks Disclosure and Implied Audit Risks : Evidence from Audit Fees."
[24] Ernst & Young, "Board Agenda 2017 - Top Priorities for European Boards," 2019, https://www.ey.com/Publication/vwLUAssets/ey-board-agenda-top-priorities-for-european-boards-in-2019/$FILE/ey-board-agenda-top-priorities-for-european-boards-in-2019.pdf; EY, "How Cyber Governance and Disclosures Are Closing the Gaps in 2022," 2022; Ey and CPA Canada, "CPA Canada and EY: Cybersecurity Disclosure Report," no. May (2020), https://www.cpacanada.ca/en/business-and-accounting-resources/other-general-business-topics/information-management-and-technology/publications/cybersecurity-disclosure-study-key-highlights; Maryam Firoozi and Sana Mohsni, "Cybersecurity Disclosure in the Banking Industry: A Comparative Study," *International Journal of Disclosure and Governance* 20, no. July 2023 (2023): 451–77, https://doi.org/10.1057/s41310-023-00190-8; Héroux and Fortin, "Cybersecurity Disclosure by the Companies on the S & P / TSX 60 Index"; Maricela Ramirez et al., "The Disclosures of Information on Cybersecurity in Listed Companies in Latin America — Proposal for a Cybersecurity Disclosure Index," *Sustainability* 14, no. 1390 (2022): 1–23, https://www.mdpi.com.
[25] Héroux & Fortin (2020)
[26] Ernst & Young (2019, 2022, 2020)
[27] Ramirez et al. (2022)
[28] Firoozi & Mohsni (2023)
[29] Firoozi and Mohsni.

commercial banks as a benchmark for cyber security disclosure in Indonesia, Bank Mandiri and Bank Rakyat Indonesia.

METHODOLOGY

RESEARCH QUESTION

This current study aims to investigating the following issue:
1. What is the level of BSI's cyber security disclosure before and after BSI's cyber incident ?
2. What is the level of BSI's cyber security disclosures compared to the level of Indonesian Islamic banks cyber security disclosures before and after BSI's cyber incident ?
3. What is the level of BSI's cyber security disclosure compared to to the level of BM and BRI cyber security disclosures before and after BSI's cyber incident ?

RESEARCH OBJECT

The object of this study are chapters/sub-chapters of information technology in the annual report of Islamic banking listed on the IDX in 2022 and 2023 and 2 conventional commercial banks which used as a benchmark for bank cyber security disclosure in Indonesia. There are 4 Islamic banks listed on the Indonesia Stock Exchange in 2022 and 2023, namely Bank Syariah Indonesia (BSI), Bank Panin Dubai Syariah (BPDS), Bank Aladin (BA), and Bank Tabungan Pensiunan Nasional Syariah (BTPNS). As a benchmark for bank cyber security disclosure in Indonesia, Bank Mandiri (BM) and Bank Rakyat Indonesia (BRI) had chosen. In this study, the author chose BM and BRI as the benchmark for cyber security disclosure, because BM and BRI have the annual reports with the most page lengths compared to the average annual reports of banks in Indonesia. The author assumes that the page length in a bank's annual report will be directly proportional to the extent of its cyber security disclosures.

RESEARCH METHODS

This research will use a comparative method based on the content analysis. The content analysis is carried out on the chapter or sub-chapter of information technology in the bank's annual report for the 2022 and 2023 periods. The chapter or sub-chapter on information technology will be analyzed based on a cyber security disclosure index developed specifically for banking by [30]. This index consist of 62 items of disclosure related to cyber security (see appendix 1). A comparison made to BSI's cyber security disclosures in 2022 and 2023, namely before and after the BSI's cyber incident. A comparison also made for the cyber security disclosures between BSI and Islamic banks in Indonesia listed on the IDX in 2022 and 2023. Another comparison also made among the cyber security disclosure of BSI, BM and BRI in the 2022 and 2023 annual reports.
For this research, the author took some steps. First, the author collected annual reports of 6 banks, consist of Islamic banks listed on the Indonesia Stock Exchange in 2022 and 2023 as well as annual reports of BM and BRI in 2022 and 2023. Next, the author sorted out the chapter/sub-chapter entitled information technology from the bank's annual report. Next, the chapter/sub-chapter on information technology analyzed using a cyber security disclosure index. Each item of disclosure made is given a value of 1, otherwise 0. The total items disclosure of each banks are then summed up. And then, these total amount cyber security disclosures were then compared between 2022 and 2023, compared among Islamic banks, and also compared among BSI, BM and BRI.

RESULT AND ANALYSIS

The appendix 1 shows the results of coding cyber security disclosure items in the chapter/sub-chapter of information technology in the 2022 and 2023 annual reports of 6 banks that are the object of this research, namely BSI, BPDBS, BA, BTPNS, BM, and BRI. Content analysis shows that in general, there has been an increase in the number of items disclosed related to cyber security disclosures. The number of BSI cyber security disclosures increased from a total of 5 cyber security disclosure items in 2022 to a total of 10 cyber security disclosure items in 2023, increasing 5 items compared to 2022.

[30] Firoozi & Mohsni (2023)

The number of cyber security disclosures of BA increased from a total of 7 cyber security disclosure items in 2022 to a total of 9 cyber security disclosure items in 2023 or increasing 2 items compared to 2022. The number of BTPNS cyber security disclosures increased from a total of 4 cyber security disclosure items in 2022 to a total of 12 cyber security disclosure items in 2023, increasing 8 items compared to 2022. The number of BM cyber security disclosures increased from a total of 17 cyber security disclosure items in 2022 to a total of 19 cyber security disclosure items in 2023, increasing 2 items compared to 2022. The number of BRI cyber security disclosures increased from a total of 13 cyber security disclosure items in 2022 to a total of 15 cyber security disclosure items in 2023, increasing 2 items compared to 2022. Only BPDBS cyber security disclosure shows that there has been no change in the extent of cyber security disclosure because the number of disclosure items in 2022 and 2023 is similar (see table 1).

THE LEVEL OF BSI'S CYBER SECURITY DISCLOSURE BEFORE AND AFTER CYBER INCIDENT

Content analysis of the information technology chapter in BSI 2022 annual report shows that only 5 items out of 62 cyber security disclosure items were disclosed by BSI. The category of disclosure items consist of the category cyber security risk governance (2 items) and cyber security risk mitigation (3 items). BSI does not make any disclosures for the potential impact of a cyber security incident (impact) category, cyber security incidents (incident) category, and other category. Cyber security disclosure in the information technology chapter of BSI annual report for 2022 is 5 out of 62 items, or less than 10%, it is categorized a low level of disclosure.

These following items are the cyber security disclosures in BSI's annual report 2022 ([31] :

1. Item C.1 in the cyber security disclosure index, BSI reveals that a committee or individual has been designated as in charge of managing risk mitigation and cyber security.
2. Item C.3 in the cyber security disclosure index, BSI reveals that it has extensive cyber security policies and procedures (cyber security risk management program)
3. Item D.7 in the cyber security disclosure index, namely BSI reveals that all of its employees participate in a training or educational program aimed at raising their understanding of cyber risks.
4. Item to D.9 in the cyber security disclosure index, in the event of a cyber incident, BSI discloses that it has a disaster (incident) recovery (reaction) plan.
5. Item to D.11 in the cyber security disclosure index, BSI reveals that it has data protection procedures in place.

Content analysis of the information technology chapter in BSI annual report in 2023 shows that there are 10 items out of 62 cyber security disclosure items that disclosed by BSI. The total disclosure in 2023 is higher than the disclosure in 2022. The disclosure items category carried out by BSI are the same as in 2022 plus 5 other disclosure items. The category of disclosure items consist of the category of cyber risk factor (1 item), the category of cyber security risk governance (2 items), the category of cyber security risk mitigation (6 items) and the category of Other (1 item). It is interesting to know that despite the fact that BSI experienced a breach/cyber incident in 2023, BSI did not make any disclosures for the potential impact of a cyber security incident (impact) and cyber security incidents (incident) categories in the information technology chapter in the 2023 annual report.

Just like the 2022 cyber security disclosure, in 2023 BSI reveals that a committee or individual has been designated as in charge of managing risk mitigation and cyber security, reveals that it has extensive cyber security policies and procedures (cyber security risk management program), reveals that all of its employees participate in a training or educational program aimed at raising their understanding of cyber risks, revealing the existence of a disaster recovery plan (incident) in the case of cyber incidents, also reveals that it has data protection procedures in place.

In addition to the 5 items disclosed above, the 5 cyber security disclosure items added to BSI's 2023 annual report include [32]:

1. Item A.7 in the cyber security disclosure index, cyber risk is reported as a priority risk by BSI.
2. Item D.8 in the cyber security disclosure index, BSI reveal that the entity has controls in place to prevent unauthorized access to its data.
3. Item to D.5 in the cyber security disclosure index, BSI reveal evaluating the adequacy of their cyber security disclosure controls and processes.
4. Item to D.14 in the cyber security disclosure index, BSI reveal that the organization has the human resources to develop, set up, and test its cyber security systems.

[31] BSI, "Bank Syariah Indonesia Annual Report 2022," 2022.
[32] BSI, "Bank Syariah Indonesia Annual Report 2023," 2023.

5. Item to F.1 in the cyber security disclosure index, BSI have a communication strategy in place in case of an attack or breach.

The level of BSI's cyber security disclosures in 2023 increased by 5 items compared to BSI's cyber security disclosures in 2022. The total items disclosed were 10 items out of 62 cyber security disclosure items. It can be interpreted that the occurrence of a cyber incident in 2023 at BSI has a positive effect on the level of BSI's cyber security disclosure. It can be seen that BSI disclosed more items in the cyber security risk mitigation category (6 items, from the previous 3 items) and added disclosures in Other category (1 item) and cyber risk factor category (1 item) that were not previously carried out. BSI seeks to signal to stakeholders that BSI is taking important steps related to cyber security. Although there has been an increase in the number of cyber security disclosure items compared to 2022, this number is still categorized the low-level disclosure category.

THE LEVEL OF CYBER SECURITY DISCLOSURE OF BSI COMPARED TO THE LEVEL OF CYBER SECURITY DISCLOSURE OF ISLAMIC BANKS IN INDONESIA BEFORE AND AFTER BSI CYBER INCIDENT

Content analysis of the chapter/sub-chapter of information technology in the annual report of Islamic banks in Indonesia for 2022 and 2023 shows that there is similar effect, where the level of cyber security disclosure of Islamic banking in Indonesia shows an increase. The category of disclosure items is dominated by the cyber security risk governance category and the cyber security risk mitigation category.

Table 1 Comparison of the Level of Cyber Security Disclosure in Islamic Banks in Indonesia

No.	Bank	Cyber Security Disclosure														Desc.
		2022							2023							
		A	B	C	D	E	F	Total	A	B	C	D	E	F	Total	
1.	BSI	0	0	2	3	0	0	5	1	0	2	6	0	1	10	Enhanced
2.	BPDS	1	0	2	2	0	0	5	1	0	2	2	0	0	5	Still
3.	BA	1	0	4	2	0	0	7	1	0	4	4	0	0	9	Enhanced
4.	BTPNS	1	0	2	1	0	0	4	1	0	4	7	0	0	12	Enhanced

Description :
A : Cyber Risk Factors (Risk)
B : Potential Impact of a Cyber security Incident (Impact)
C : Governance of Cyber security Risk (Governance)
D : Cyber security Risk Mitigation (Mitigation)
E : Cyber security Incidents (Incident)
F : Other
Desc : Description

Source : data processed (2024)

Table 1 shows the results of content analysis of the cyber security disclosure of Islamic banks in Indonesia in 2022 and 2023. There is a trend of increasing the level of cyber security disclosure in the chapter/sub-chapter of the information technology annual report of Islamic banks in Indonesia. The number of cyber security disclosure items in BSI in 2022 is 5 items, to 10 items in 2023. The similar effect is also seen in the level of cyber security disclosure at BA and BTPNS. BA cyber security disclosure items in 2022 were 7 items, increasing to 9 items in 2023. BTPNS cyber security disclosure items in 2022 were 4 items, tripling to 12 items in 2023. BPDS did not have the similar effect, because the number of BPDS cyber security disclosure items in 2022 and 2023 similar, consist of 5 disclosure items.

This research support the peer effects, within institutional theory, firms' actions and decisions are often influenced by the behavior of other firms in their industry. The cyber incident of industry peers as a form of institutional pressure that encourages banks's cyber security disclosure decisions. The actions of industry peers (in this case, the cyber incident of BSI) are institutional influences on the decisions of islamic banks in Indonesia. Furthermore, when viewed by item category, cyber security disclosure is dominated by category C, Governance of Cyber Security Risk (Governance) and category D, Cyber Security Risk Mitigation (Mitigation). No bank has disclosed category B, Potential Impact of a Cyber Security Incident (Impact) and category D, Cyber Security Incidents (Incident). Only BSI added a disclosure for category F, i.e. Other.

If compared the level of cyber security disclosure among BSI and Islamic banks in Indonesia, it can be seen that in 2022 and 2023, the level of BSI's cyber security disclosure is relatively similar compared to the other 3 Islamic banks (BPDS, BA, and BTPNS). Overall, the number of cyber security disclosure items of Islamic banks in Indonesia is very low. In 2022 it averaged only 5.25 out of 62 items of cyber security disclosures, and an average of 9 out of 62 items of cyber security disclosures in 2023. Despite an increase of almost 40% (5.25 to 9 items) cyber security disclosures, this number classified as a low level of cyber security disclosure.

THE LEVEL OF CYBER SECURITY DISCLOSURE OF BSI COMPARED TO THE LEVEL OF CYBER SECURITY DISCLOSURE OF BANK MANDIRI AND BRI BEFORE AND AFTER BSI CYBER INCIDENT

Content analysis of the information technology chapters/sub-chapters in the annual reports of BSI, BM, and BRI for 2022 and 2023 shows that there is similar effect, an increase in the level of cyber security disclosure.

Table 2
Comparison of the Level of Cyber Security Disclosure at BSI, Bank Mandiri, and BRI

No.	Bank	Cyber Security Disclosure														Description
		2022							2023							
		A	B	C	D	E	F	Total	A	B	C	D	E	F	Total	
1.	BSI	0	0	2	3	0	0	5	1	0	2	6	0	1	10	Enhanced
2.	BM	3	0	5	9	0	0	17	3	0	5	11	0	0	19	Enhanced
3.	BRI	0	0	4	8	0	0	13	0	1	5	9	0	0	15	Enhanced

Description :
A : Cyber Risk Factors (Risk)
B : Potential Impact of a Cyber security Incident (Impact)
C : Governance of Cyber security Risk (Governance)
D : Cyber security Risk Mitigation (Mitigation)
E : Cyber security Incidents (Incident)
F : Other

Source : data processed (2024)

Table 2 shows the results of content analysis of cyber security disclosures of BSI, BM, and BRI in 2022 and 2023. There is a trend of increasing the leve of cyber security disclosure in the chapter/sub-chapter information technology of the annual report. The number of cyber security disclosure items in BSI in 2022 is 5 items, to 10 items in 2023. The BM and BRI cyber security disclosure show the similar effect. BM cyber security disclosure items in 2022 were 17 items, increasing to 19 items in 2023. BRI cyber security disclosure items in 2022 were 13 items, increasing to 15 items in 2023. Furthermore, when viewed by item category, cyber security disclosure is dominated by category C, Governance of Cyber Security Risk (Governance) and category D, Cyber Security Risk Mitigation (Mitigation). BRI disclosed 1 category B item, Potential Impact of a Cyber Security Incident (Impact). BSI, BM and BRI did not disclose category D, Cyber Security Incidents (Incidents). Only BSI added a disclosure for category F, namely Other.
If compared the level of cyber security disclosure between BSI, BM and BRI, it can be seen that in 2022 and 2023, the level of BSI's cyber security disclosure lower than BM and BRI. 6 items BSI cyber security disclosure compared to 17 items BM cyber security disclosure and 13 items BRI cyber security disclosure in 2022. In 2023, 10 items BSI cyber security disclosure compared to 19 items BM cyber security disclosure and 15 items BRI cyber security disclosure. BM and BRI as a benchmark of cyber security disclosure, have higher level or more extent of cyber security disclosure than BSI cyber security disclosure.

DISCUSSION

The level of BSI's cyber security disclosure before and after cyber incident shows a significant increase from 5 items to 10 items or increasing twice after the event. This research support the signaling theory that suggest that the bank is trying to signal to stakeholders that the bank has taken the necessary steps related to cyber security. This communication is carried out in the cyber security disclosure in the bank's annual report. BSI disclosed more items in the cyber security risk mitigation category (6 items, from the previous 3 items) and added disclosures in Other category (1 item) and cyber risk factor category (1 item) that were not previously carried out. BSI explains in more detail about

cyber security risk mitigation in BSI, BSI have a communication strategy in place in case of an attack or breach, and BSI declare about cyber risk factor.

This research substantiates the concept of peer effects, within institutional theory, the actions and decisions of enterprises are frequently influence by the behaviors of their industry counterparts. The cyber incident involving industry peers serves as a sort of institutional pressure that influences Banks' actions regarding cyber security disclosures. The actions of industry peers (in this case, the cyber incident of BSI) are institutional influences on the decisions of banks cyber security disclosure in Indonesia. The level of cyber security disclosure of BSI compared to the level of cyber security disclosure BPDS, BA, BTPN, BM and BRI shows similar effects. There has been an increase in cyber security disclosures after BSI cyber incident.

If compared the level of cyber security disclosure between BSI, BM and BRI, it can be seen that in 2022 and 2023, the level of BSI's cyber security disclosure lower than BM and BRI. BM and BRI as a benchmark of cyber security disclosure, have higher level or more extent of cyber security disclosure than BSI cyber security disclosure. Comparison the level of cyber security disclosure among BSI and Islamic banks in Indonesia, it can be seen that in 2022 and 2023, the level of BSI's cyber security disclosure is relatively similar compared to the other 3 Islamic banks (BPDS, BA, and BTPNS). Overall, the number of cyber security disclosure items of Islamic banks in Indonesia is classified as a low level of cyber security disclosure.

CONCLUSION, LIMITATION AND RECOMMENDATION

CONCLUSION

This study concluded that

1. The cyber incidents experienced by BSI in mid-2023 have a positive effect on the level of BSI's cyber security disclosures. BSI's cyber security disclosures 2023 higher than BSI's cyber security disclosures 2022.
2. The similar effect is also seen in the level of cyber security disclosure of Islamic banks in Indonesia. This effect could be seen as the influence of peer cyber security incidents on the level of cyber security disclosure in Indonesian islamic banks. In 2022 and 2023, the level of BSI's cyber security disclosure is relatively similar compared to the other 3 Islamic banks (BPDS, BA, and BTPNS). Overall, the level of cyber security disclosure items of Indonesian islamic banks are low.
3. BM and BRI as members in the same industry, Indonesian banks, also showing the similar effect. This effect can be seen as the influence of peer cyber security incidents on the level of cyber security disclosure in Indonesian banks industry. Cyber security disclosure among BSI, BM and BRI, in 2022 and 2023, the level of BSI's cyber security disclosure is lower than BM and BRI. BM and BRI as a benchmark of cyber security disclosure, have higher level of cyber security disclosure.
4.

LIMITATION

Limitations of this study are :

1. Content analysis is limited to only chapters/sub-chapters on information technology, whereas other sections of the annual report may contain information related to cyber security disclosures.
2. Content analysis using a cyber security disclosure index developed abroad, which of course does not include OJK rules on cyber security, and disclosure practices in Indonesian banks.

RECOMMENDATION

The author recommends the following two things :

1. Banks should take into consideration cyber security disclosure index that has been developed by researchers as a guide in compiling cyber security disclosures for Indonesian banks industry.
2. Subsequent research must develop cyber security disclosures that appropriate for Indonesia based on guide, rules, and best practice Indonesian banks.

REFERENCE

1. Arcy, John D, and Asli Basoglu. “The Influences of Public and Institutional Pressure on Firms ’ Cybersecurity

Disclosures." *Journal of the Association for Information Systems* 23, no. 3 (2022): 779–805. https://doi.org/10.17705/1jais.00740.
2. Berkman, Henk, Jonathan Jona, Gladys Lee, and Naomi Soderstrom. "Cybersecurity Awareness and Market Valuations." *Journal of Accounting and Public Policy* xxx, no. xxxx (2018): 1–19. https://doi.org/10.1016/j.jaccpubpol.2018.10.003.
3. BSI. "Bank Syariah Indonesia Annual Report 2022," 2022.
4. ———. "Bank Syariah Indonesia Annual Report 2023," 2023.
5. Calderon, Thomas G, and Lei Gao. "Cybersecurity Risks Disclosure and Implied Audit Risks : Evidence from Audit Fees." *International Journal Audit* Special Is, no. October (2020): 1–16. https://doi.org/10.1111/ijau.12209.
6. Chen, Jing, Elaine Henry, and Xi Jiang. "Is Cybersecurity Risk Factor Disclosure Informative ? Evidence from Disclosures Following a Data Breach." *Journal of Business Ethics* 187, no. September (2023): 199–224. https://doi.org/10.1007/s10551-022-05107-z.
7. DiMaggio, Paul J, and Walter W Powell. "Introduction." In *New Institutional Theory*, 1–38, 1983.
8. Egidius Patnistik. "BSI, Bisnis Ransomware, Dan Negosiasi Pemerasan." money.kompas.com, 2023.
9. Ernst & Young. "Board Agenda 2017 - Top Priorities for European Boards," 2019. https://www.ey.com/Publication/vwLUAssets/ey-board-agenda-top-priorities-for-european-boards-in-2019/$FILE/ey-board-agenda-top-priorities-for-european-boards-in-2019.pdf.
10. EY. "How Cyber Governance and Disclosures Are Closing the Gaps in 2022," 2022.
11. Ey, and CPA Canada. "CPA Canada and EY: Cybersecurity Disclosure Report," no. May (2020). https://www.cpacanada.ca/en/business-and-accounting-resources/other-general-business-topics/information-management-and-technology/publications/cybersecurity-disclosure-study-key-highlights.
12. Firoozi, Maryam, and Sana Mohsni. "Cybersecurity Disclosure in the Banking Industry: A Comparative Study." *International Journal of Disclosure and Governance* 20, no. July 2023 (2023): 451–77. https://doi.org/10.1057/s41310-023-00190-8.
13. Gao, Lei, Thomas G Calderon, and Fengchun Tang. "Public Companies ' Cybersecurity Risk Disclosures." *International Journal of Accounting Information Systems* 38, no. 100468 (2020): 1–22. https://doi.org/10.1016/j.accinf.2020.100468.
14. Héroux, Sylvie, and Anne Fortin. "Cybersecurity Disclosure by the Companies on the S & P / TSX 60 Index." *Accounting Perspectives* 19, no. 2 (2020): 73–100. https://doi.org/10.1111/1911-3838.12220.
15. Ibrahim, Ahmad, and Said Karajeh. "Voluntary Disclosure and Earnings Quality : Evidence from Ownership Concentration Environment." *Management Research Review* 43, no. 1 (2020): 35–55. https://doi.org/10.1108/MRR-11-2018-0447.
16. Intan, Novita. "OJK : Sektor Keuangan Paling Banyak Mendapat Serangan Siber Pada 2021." Republika.co.id, 2022.
17. Li, He, Won Gyun No, and Tawei Wang. "SEC ' s Cybersecurity Disclosure Guidance and Disclosed Cybersecurity Risk Factors." *International Journal of Accounting Information Systems* xxx, no. xxxx (2018): 1–16. https://doi.org/10.1016/j.accinf.2018.06.003.
18. Masoud, Najeb, and Ghassan Al-utaibi. "The Determinants of Cybersecurity Risk Disclosure in Firms ' Financial Reporting : Empirical Evidence." *Research in Economics* 76, no. 2 (2022): 131–40. https://doi.org/10.1016/j.rie.2022.07.001.
19. Maurer, Tim, and Arthur Nelson. "The Global Cyber Threat Cyber Threats to the Financial System Are Growing, and the Global Community Must Cooperate to Protect It." *Finance and Development*, 2021.
20. Mazumder, Mohammed Mehadi Masud, and Dewan Mahboob Hossain. "Voluntary Cybersecurity Disclosure in the Banking Industry of Bangladesh : Does Board Composition Matter ?" *Journal of Accounting in Emerging Economies* 13, no. 2 (2022): 1–23. https://doi.org/10.1108/JAEE-07-2021-0237.
21. OJK. "Best Practices: Penanganan Insiden Keamanan Siber Di Sektor Jasa Keuangan," 2022.
22. Radu, Camélia, and Nadia Smaili. "Board Gender Diversity and Corporate Response to Cyber Risk : Evidence from Cybersecurity Related Disclosure." *Journal of Business Ethics* 177 (2022): 351–74. https://doi.org/10.1007/s10551-020-04717-9.
23. Ramirez, Maricela, Lázaro Rodríguez Ariza, María Elena Gómez Miranda Miranda, and Vartika. "The Disclosures of Information on Cybersecurity in Listed Companies in Latin America — Proposal for a Cybersecurity Disclosure Index." *Sustainability* 14, no. 1390 (2022): 1–23. https://www.mdpi.com.
24. Schatz, Daniel, and Julie Wall. "Towards a More Representative Definition of Cyber Security." *Journal of Digital Forensics, Security and Law* 12, no. 2 (2017): 53–74. https://doi.org/10.15394/jdfsl.2017.1476.

25. Swift, Orry, Ricardo Colon, and Kelly Davis. "The Impact of Cyber Breaches on the Content of Cybersecurity Disclosures." *Journal of Forensic and Investigative Accounting* 12, no. 2 (2020): 197–212.
26. WEF, World Economic Forum. "The Global Risks Report 2023 18th Edition." *World Economic Forum*, 2023. https://www.weforum.org/reports/global-risks-report-2023.

Appendix 1

The following cyber security disclosure index developed by Firoozi & Mohsni (2023). Data obtained from Bank Annual Report, Information Technology chapter/sub-chapter BSI, BPDS, BA, BTPNS, BM, and BRI 2022-2023.

Table A

BSI Cyber Security Disclosure Compared to Indonesian Banks

		BSI[1]		BPDS[2]		BA[3]		BTPNS[4]		BM[5]		BRI[6]	
Cyber Risk Factors (Risk)		**2022**	**2023**	**2022**	**2023**	**2022**	**2023**	**2022**	**2023**	**2022**	**2023**	**2022**	**2023**
A.1	The entity describe cyber security risk	-	-	-	-	-	-	-	-	√	√	-	-
A.2	The entity discuss cyber risk specific to banking industry	-	-	-	-	-	-	-	-	-	-	-	-
A.3	The entity discuss cyber risk specific to the bank	-	-	-	-	-	-	-	-	-	-	-	-
A.4	The entity report on outsourcing functions that have material cyber risks	-	-	√	√	-	-	-	-	√	√	-	-
A.5	For an entity that has had a prior material cyber security incident, there is any discussion on the effects of the incident on the entity's cyber risk	-	-	-	-	-	-	-	-	-	-	-	-
A.6	The entity report on risks related to cyber incidents that may remain undetected for an extended period	-	-	-	-	-	-	-	-	-	-	-	-
A.7	The entity report cyber risk as a priority risk	-	√	-	-	√	√	√	√	√	√	-	-
A.8	The entity report risk related to social media	-	-	-	-	-	-	-	-	-	-	-	-
A.9	The entity report on aspects of its business or operations that give rise to material cyber security risks	-	-	-	-	-	-	-	-	-	-	-	-
Potential Impact of a Cyber security Incident (Impact)													
B.1	The entity discuss the potential impact of cyber risks on the entity's reputation and customer confidence	-	-	-	-	-	-	-	-	-	-	-	-
B.2	The entity discuss the effects of cyber risks on stakeholders (other than customers)	-	-	-	-	-	-	-	-	-	-	-	√

B.3	The entity discuss the costs of remediation after a breach	-	-	-	-	-	-	-	-	-	-	-	-
B.4	The entity discuss potential litigation cost, fines and related liabilities brought by parties seeking damages against the entity	-	-	-	-	-	-	-	-	-	-	-	-
B.5	The entity discuss potential litigation cost brought by the entity against third parties	-	-	-	-	-	-	-	-	-	-	-	-
B.6	The entity discuss the effects of cyber risks on the issuer's internal and disclosure controls	-	-	-	-	-	-	-	-	-	-	-	-
B.7	The entity discuss the potential impact of cyber risks and cyber incidents on the entity's financial statements	-	-	-	-	-	-	-	-	-	-	-	-
B.8	The entity discuss lost revenues due to a disruption of activity (delays) as a result of a potential cyber security incident	-	-	-	-	-	-	-	-	-	-	-	-
B.9	The entity discuss compromise of confidential data of customers and employees or unauthorized access to proprietary or sensitive information as a result of a potential cyber security incident	-	-	-	-	-	-	-	-	-	-	-	-
B.10	The entity discuss corruption or destruction of data because of a potential cyber security incident	-	-	-	-	-	-	-	-	-	-	-	-
B.11	The entity discuss decreased competitive advantage as a result of a potential cyber security incident	-	-	-	-	-	-	-	-	-	-	-	-
B.12	The entity discuss regulatory investigations as a result of a potential cyber security incident	-	-	-	-	-	-	-	-	-	-	-	-
B.13	The entity discuss higher insurance premiums as a	-	-	-	-	-	-	-	-	-	-	-	-

	result of a potential cyber security incident												
Governance of Cyber security Risk (Governance)													
C.1	The entity disclose having a committee or person identified as responsible for cyber security and risk mitigation strategy at the management level	√	√	√	√	√	√	√	√	√	√	√	√
C.2	The entity disclose having any committee at the board level in charge of cyber security	-	-	-	-	√	√	-	-	√	√	-	-
C.3	The entity disclose having comprehensive policy and procedures related to cyber security (cyber security risk management program)	√	√	√	√	√	√	√	√	√	√	√	√
C.4	The entity disclose assessing the compliance of the cyber security policy on a regular basis	-	-	-	-	√	√	-	√	√	√	√	√
C.5	The entity disclose auditing (internal or external) its cyber security risk management program	-	-	-	-	-	-	-	√	√	√	√	√
C.6	The entity report on insider trading restrictions for directors, officers and other corporate insiders (from trading on the basis of material nonpublic information about cyber security risks and incidents)	-	-	-	-	-	-	-	-	-	-	-	-
C.7	The entity disclose board members who have expertise in IT and/or cyber security	-	-	-	-	-	-	-	-	-	-	√	√
Cyber security Risk Mitigation (Mitigation)													
D.1	The entity disclose maintaining insurance covering cyber attacks	-	-	-	-	-	-	-	-	-	-	-	-
D.2	The entity disclose to what extent they maintain insurance covering cyber attacks (or mention their insurance may be insufficient)	-	-	-	-	-	-	-	-	-	-	-	-

D.3	The entity disclose relying on third-party experts for their cyber security strategy	-	-	-	-	-	-	-	√	-	√	√	√
D.4	The entity disclose relying on third-party experts to remediate prior or future cyber attacks	-	-	-	-	-	-	-	-	-	-	-	-
D.5	The entity disclose assessing sufficiency of their disclosure controls and procedures related to cyber security	-	√	-	-	-	-	-	-	√	√	-	-
D.6	The entity disclose having training or an education program that targets cyber risk awareness among board members	-	-	-	-	-	-	-	-	√	√	-	-
D.7	The entity disclose having a training or an education program that targets cyber risk awareness among all employees	√	√	√	√	-	-	-	-	√	√	√	√
D.8	The entity disclose having controls over unauthorized access to the entity's data	-	√	-	-	-	-	-	√	√	√	√	√
D.9	The entity disclose having a disaster (incident) recovery (response) plan in case of a cyber incident	√	√	-	-	√	√	-	√	√	√	√	√
D.10	The entity disclose testing their recovery plan	-	-	-	-	-	-	-	√	-	√	-	√
D.11	The entity disclose having data protection mechanisms in place	√	√	√	√	-	√	√	√	√	√	√	√
D.12	The entity disclose making adjustments in their firm based on previous cyber attacks	-	-	-	-	-	-	-	-	-	-	-	-
D.13	The entity disclose regularly conducting penetration testing on their infrastructure	-	-	-	-	√	-	-	√	√	√	√	√
D.14	The entity disclose having sufficient human talent to design, configure and test their	-	√	-	-	-	√	-	-	√	√	√	√

	cyber security systems (entity's expertise)												
D.15	The entity disclose having sufficient tools to design, configure and test their cyber security systems (investment in cyber defense and security)	-	-	-	-	-	√	-	√	√	√	√	√
Cyber security Incidents (Incident)													
E.1	The entity disclose the cyber incidents experienced that are individually or in the aggregate, material	-	-	-	-	-	-	-	-	-	-	-	-
E.2	The entity disclose the size of the attack	-	-	-	-	-	-	-	-	-	-	-	-
E.3	The entity disclose the source of the attack	-	-	-	-	-	-	-	-	-	-	-	-
E.4	The entity discuss how materiality of an attack would be assessed in any cyber attack remediation plan to determine whether to disclose the attack (its timing and how to disclose it)	-	-	-	-	-	-	-	-	-	-	-	-
E.5	The entity discuss the impact of the incident on the company's operations and reputation, its customers, employees and investors	-	-	-	-	-	-	-	-	-	-	-	-
E.6	The entity disclose the overall financial cost of a cyber incident (including loss of intellectual property)	-	-	-	-	-	-	-	-	-	-	-	-
E.7	The entity disclose the immediate costs of the incident	-	-	-	-	-	-	-	-	-	-	-	-
E.8	The entity disclose the costs associated with implementing preventative measures after an incident	-	-	-	-	-	-	-	-	-	-	-	-
E.9	The entity disclose the cost of maintaining insurance after an incident	-	-	-	-	-	-	-	-	-	-	-	-
E.10	The entity disclose the cost of responding to litigation and regulatory	-	-	-	-	-	-	-	-	-	-	-	-

	investigations after an incident												
E.11	The entity disclose the cost of preparing for and complying with proposed or current legislation	-	-	-	-	-	-	-	-	-	-	-	-
E.12	The entity disclose the cost of engaging in remediation efforts	-	-	-	-	-	-	-	-	-	-	-	-
E.13	The entity disclose the cost of addressing harm to reputation and the loss of competitive advantage	-	-	-	-	-	-	-	-	-	-	-	-
E.14	The entity disclose the incident timely	-	-	-	-	-	-	-	-	-	-	-	-
E.15	The entity disclose a material pending legal proceeding involving a cyber incident, in its legal proceedings	-	-	-	-	-	-	-	-	-	-	-	-
Other													
F.1	The entity disclose having a communication plan in case of a breach or attack	-	√	-	-	-	-	-	-	-	-	-	-
F.2	The entity disclose that they have not experienced a cyber incident (or have experienced no loss from cyber attacks)	-	-	-	-	-	-	-	-	-	-	-	-
F.3	The entity disclose that they have not experienced a material cyber incident	-	-	-	-	-	-	-	-	-	-	-	-
Total		6	10	5	5	7	9	4	12	17	19	13	15

1 BSI Annual report 2022 and 2023
2 BPDBS Annual report 2022 and 2023
3 BA Annual report 2022 and 2023
4 BTPNS Annual report 2022 and 2023
5 BM Annual report 2022 and 2023
6 BRI Annual report 2022 and 2023

Appendix 2
These following items are the cyber security disclosures in BSI's annual report 2022 :

6. Item C.1 in the cyber security disclosure index, BSI reveals that a committee or individual has been designated as in charge of managing risk mitigation and cyber security.

"The IT management organization at BSI is under the IT directorate, which oversees the following support structures: IT Strategic Planning Grup (ISG), IT Operation Group (IOG), IT Development Group (IDG), and Chief Information Security Officer Group (CSO). IOG carries out IT operational tasks, while strategic planning activities are carried out by the ISG. Meanwhile, IT development is carried out by IDG and information security is carried out by CSO."
(BSI, 2022, p.251)

7. Item C.3 in the cyber security disclosure index, BSI reveals that it has extensive cyber security policies and procedures (cyber security risk management program)

"In support of this strategy, BSI implements the programs listed in the "7 IT Stars" (Strategic Actions and Programs) including:

1. Security, Risk and Fraud Establish and improve security perimeter, risk management, and fraud & AML in order to protect the customers and banking transaction processes.
2. Core system modernization Implementation of core banking modernization initiative to simplify the core banking system, improve core functions, and enable the next generation of core banking to support diverse baking products and services.
3. Infrastructure & Connectivity Establishment and improvement of infrastructure and connectivity tools, applications, and hardware that combines various technologies to support the bank's business.
4. Integrated data management monitoring and reporting Establishment and improvement of enterprise data warehouse and bigdata analysis to activate data as-a-service as well as information management tools that can be used by employees to perform independent monitoring and reporting.
5. Organization, Corporate Support & Internal Improvements Establishment and improvement of the Company's core functions to support the bank's operations and internal processes, as well as organizational improvement.
6. Unified Platform & Customer 360 The use of a single main platform to accommodate all work flow capabilities assisted by the improvement of the data center and integrated customer service (customer relationship) in sales, marketing, and campaign management areas to increase engagement with customers
7. Digital Expansion & Open Banking Improvement and expansion of digital distribution network, sales, and omni-channel, including by increasing integration capabilities with various methods and strategies to allow open banking with seamless and secure connectivity, internally and externally.
8. Environment, Social & Governance (ESG) Implementation of the company's sustainable strategy in carrying out development (investment) that provides added value in environmental, social, governance (corporate governance) aspects and able to become a pioneer (agent of change) for sharia economics in Indonesia."

(BSI, 2022, p.252)

8. Item D.7 in the cyber security disclosure index, namely BSI reveals that all of its employees participate in a training or educational program aimed at raising their understanding of cyber risks.

"The following is a list of HR development that has been realized throughout 2022.

…

3 Training and Certified Information Security for Manager (CISM)
4 Change & Release Management training
5 COBIT 2019 Foundation & Certification training
6 ISOIEC 27001 2013 Information Security Management Systems training
7 ITIL 4 Create Deliver And Support training

…

11 ISO 9001:2015 Quality Management System Awareness training
12 Robot Automation and Machine Learning training
13 COBIT 2019 Foundation Training and Certification
14 Data Protection and Privacy training

…

21 ISO/IEC 27001:2013 Implementing Information Security Management System training"

(BSI, 2022, p. 255)

9. Item to D.9 in the cyber security disclosure index, in the event of a cyber incident, BSI discloses that it has a disaster (incident) recovery (reaction) plan.

"Responsibility of Chief Information Security Officer Group

1. Responsible for IT information security, including playing a role in the IT planning and development process in terms of information security.
2. Handle information security incidents (cyber security protection, response, and recovery)"

(BSI, 2022, p. 251)

10. Item to D.11 in the cyber security disclosure index, BSI reveals that it has data protection procedures in place.

"Establish and improve security perimeter, risk management, and fraud & AML in order to protect the customers and banking transaction processes. "
(BSI, 2022, p. 252)

In addition to the 5 items disclosed above, the 5 cyber security disclosure items added to BSI's 2023 annual report include:

6. Item A.7 in the cyber security disclosure index, Cyber risk is reported as a priority risk by BSI,
"IT management at the Bank is focused on ensuring the reliability and security of BSI systems, specifically system stabilization, infrastructure standardization, and future security improvements."
(BSI, 2023, p. 222)

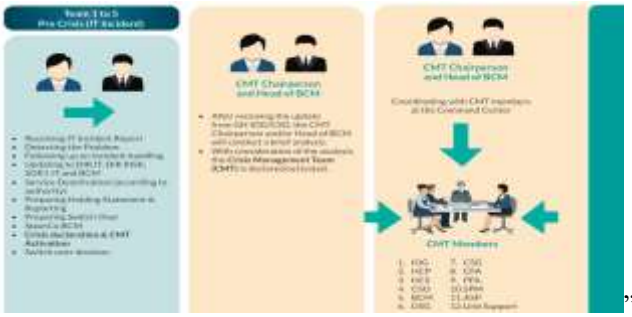
7. Item D.8 in the cyber security disclosure index, BSI reveal that the entity has controls in place to prevent unauthorized access to its data.
"The application of the basic principles of cyber security at BSI, among others:
1. Information is an asset
2. Risk compatibility
3. Compliance with regulations
4. Granting of approval
5. Adaptable and measurable
6. System safe by design
7. Layered defense
8. Segregation of duties and access restrictions …"
(BSI, 2023, p. 225)

8. Item to D.5 in the cyber security disclosure index, BSI reveal evaluating the adequacy of their cyber security disclosure controls and processes.
"BSI implements all IT policies and standard procedures in the Bank and ensures that any information owned by IT user work units is well protected against any disruptions that could result in losses due to the leakage of critical data or information. The Bank ensures adequate security oversight in any IT system development or modification and ensures the Bank's cyber resilience and security independently of the IT operational management function."
(BSI, 2023, p. 225)

9. Item to D.14 in the cyber security disclosure index, BSI reveal that the organization has the human resources to develop, set up, and test its cyber security systems.
"The Bank ensures adequate security oversight in any IT system development or modification and ensures the Bank's cyber resilience and security independently of the IT operational management function."
(BSI, 2023, p. 225)

"Furthermore, BSI has established a Chief Security Officer Office Group (CSO) work unit that manages cyber security and includes the following capabilities:
1. Security Project & QA
2. Application Identity Management
3. Network Access & Data Protection
4. IT Security Services
5. IT Security Operations
6. Security Operation Center"
(BSI, 2023, p. 226)

10. Item to F.1 in the cyber security disclosure index, BSI have a communication strategy in place in case of an attack or breach.
"Reporting System to the Board of Directors
With regard to reporting to the Board of Directors on IT dynamics, the Bank has procedures in place, as outlined below.



”

(BSI, 2023, p. 226)