KnE Social Sciences
SEABC
8th Sriwijaya Economics, Accounting, and Business Conference
Volume 2024

Research Article

Determinant Factors of Cyber Security Disclosure: A Systematic Literature Review

Lia Sari[1], Mohamad Adam[2], Luk Luk Fuadah[2] and Yusnaini[2]*

[1]Sjakhyakirti University, Indonesia
[2]Sriwijaya University, Indonesia

Abstract.
Cyber security disclosures as risk factor disclosures are particularly important. The importance of cyber security disclosure decisions is intensified by a significant number of data breaches that occur throughout the year raising serious concerns about corporate cyber security programs. Costs of data breaches can be significant. On the other hand, research on cyber security disclosure is still rare. This study aims to identify the factors that influence cyber security disclosures. Articles from various international journals were reviewed. Literature review was conducted to find determinant factors that determine cyber security disclosures. The results show that the determinant factors of cyber security disclosures are cyber security breach/previous cyber incidents, peer breach, public attention, WFH, board size, board independence, board gender diversity, institutional shareholders, foreign shareholders, capital expenditure, intangible asset, firm's size, firm's growth, firm's leverage, firm's profitability, firm's loss, industry, guidance, technology committee, and executive change. Based on the literature review, the authors provide suggestions for future research. This research contributes by providing a comprehensive discussion of the determinant factors of cybersecurity disclosure from various studies. The limitation of this study is that the authors only reviewed articles published in English. Future research must include articles published in multiple languages.

Keywords: cyber, cybersecurity, disclosure, cybersecurity disclosure, determinants

Corresponding Author: Yusnaini; email: yusnaini@fe.unsri.ac.id

Published: 3 May 2024

Publishing services provided by Knowledge E

Selection and Peer-review under the responsibility of the SEABC Conference Committee.

1. Introduction

Over the last decade, digitization has occurred in all fields. This development took place very quickly. Digital technology offers convenience and practicality in our lives. In line with that, the importance of corporate awareness in managing cyber threats needs to be increased. Cyber Security has become a new dimension in risk management [1]. Cyber security can be defined as information security and protection of electronic systems, networks, devices, programs or data from theft or damage [2]. Awareness of protecting digital assets is an important concern for companies because cyber attacks can affect company performance. Cyber risk is one of the biggest risks for companies that use information technology systems in their operational activities.

Cyber Security Disclosure is a relatively new corporate disclosure agenda. Cyber security disclosures among risk factor disclosures are particularly important. The importance of cyber security disclosure decisions is intensified by a significant number of data breaches that occur throughout the year raising serious concerns about corporate cyber security programs. Costs of data breaches can be significant. On the other hand, research on cyber security disclosure is still rare.

The high number of cyber attacks raises the need for stakeholders for adequate information related to Cyber Security. Stakeholders will demand transparency from public companies regarding Cyber Security risk management. To address this growing concern, every public company must ensure strong Cyber Security governance and provide adequate disclosure on how Cyber Security is prioritized and managed.

Public companies must understand the importance of Cyber Security and make appropriate disclosures on this matter. Such disclosure will enable companies to demonstrate their accountability and involvement in these issues and build stakeholder trust. Public companies should not only implement effective Cyber risk management programs but also provide timely and useful information about these initiatives to stakeholders through Cyber Security Disclosures.

Research in this field is interesting to study because research related to Cyber Security Disclosure is still relatively rare [3]. In particular, research related to the determinant of Cyber Security Disclosure is still very limited. This article is the first article to conduct a systematic literature review on determinant Cyber Security Disclosures. This article will help increase understanding of the factors that drive an increase in the level of Cyber Security Disclosure based on a review of previous studies. The research question in this article is what factors that influence cyber security disclosure based on previous studies.

This study aims to identify the factors that influence cyber security disclosures. Articles from various international journals were reviewed. Literature review was conducted to find determinant factors that determine cyber security disclosures. Based on the literature review, the researcher provides suggestions for future research. This research contributes by providing a comprehensive discussion of the determinant factors of cyber security disclosure from various studies.

The results shows that the determinant factor of cyber security disclosures are board size, board independence, board gender diversity, institutional shareholders, foreign shareholders, cyber security breach / previous cyber incidents, peer breach, public attention, WFH, capital expenditure, intangible asset, firm's size, firm's growth, firm's

leverage, firm's profitability, firm's loss, industry guidance, technology committee, and executive change.

2. Literature Review

Attribution From a search through Google Scholar, the authors only found 1 study based on a literature review on cyber security in accounting research. [4] wrote a literature review on cyber security in accounting research. Their research reviews 39 articles that discuss cyber security in accounting research.

The authors searches articles through Google Scholar with the keywords 'cyber security disclosure' and 'cyber risk disclosure'. An online search with these keywords returns only a small number of articles. The authors then expands the search with the keywords 'cyber incident reporting' and 'information security breaches'. From this step, a number of articles related to cyber security disclosure were obtained. Furthermore, manually, the authors sort the articles related to the determinant factor of cyber security disclosure. Previous articles from 2016 to the last in 2023. These articles were published in reputable international journals. From here, 12 relevant articles regarding the determinants of cyber security disclosure are obtained as follows:

3. Research Methods

The authors takes the following steps to conduct a systematic literature review:

The authors searches the article through Google Scholar with the keywords 'cyber security disclosure', 'cyber risk disclosure', 'cyber incident reporting' and 'information security breaches'.

The authors reads manually all the articles obtained, then selects relevant articles about the determinant factor of cyber security disclosure.

After that, the authors conducted a systematic literature review of the selected articles, including the name of the journal, the country context of the research location, the industrial sector that was the object of research, the theory used, the year of observation, and the research findings.

The next step, the authors draw conclusions and suggestions for further research.

TABLE 1: Related Research Determinant Factor Cyber Security Disclosure.

	Author	Title	Journal
1.	(Wu et al., 2023)	**The Effect of Remote Workforce on Firms' Cybersecurity Risk Disclosures and Incidents**	SSRN Elsevier e-journals
2.	(Mazumder & Hossain, 2022)	**Voluntary cybersecurity disclosure in the banking industry of Bangladesh: does board composition matter?**	Journal of Accounting in Emerging Economies
3.	(Arcy & Basoglu, 2022)	**The Influences of Public and Institutional Pressure on Firms' Cybersecurity Disclosures**	Journal of the Association for Information Systems
4.	(Masoud & Alutaibi, 2022)	**The determinants of cybersecurity risk disclosure in firms' financial reporting: Empirical evidence**	Research in Economics journal
5.	(Chen et al., 2022)	**Is Cybersecurity Risk Factor Disclosure Informative? Evidence from Disclosures Following a Data Breach**	Journal of Business Ethics
6.	(Radu & Smaili, 2021)	**Board Gender Diversity and Corporate Response to Cyber Risk: Evidence from Cybersecurity Related Disclosure**	Journal of Business Ethics
7.	(J. Haislip et al., 2021)	**The Impact of Executives ' IT Expertise on Reported Data Security Breaches**	Information Systems Research
8.	(Gao et al., 2020)	**Public Companies' Cybersecurity Risk Disclosures**	International Journal of Accounting Information Systems
9.	(J. Z. Haislip et al., 2020)	**The influences of CEO IT expertise and board-level technology committees on form 8-K disclosure timeliness**	Journal of Information Systems
10.	(Swift et al., 2020)	**The Impact of Cyber Breaches on the Content of Cybersecurity Disclosures**	Journal of Forensic and Investigative Accounting
11.	(Li et al., 2018)	**SEC ' s cybersecurity disclosure guidance and disclosed cybersecurity risk factors**	International Journal of Accounting Information Systems
12.	(Higgs et al., 2016)	**The Relationship Between Board-Level Technology Committees and Reported Security Breaches**	Journal of Information Systems

4. Results and Discussion

The author reviews based on the context of the country where the research is carried out, the theory used in each study, the industrial sector studied, and the types of disclosure studied. The result is as follows:

4.1. Country Context of Research

A review based on the context of the country studied shows that most (83%) of the research was conducted in the context of the United States ([5]; [6]; [3]; [7]; [1]; [8];

Table 2: Review Based on Country, Theory, Industrial Sector, Type of Disclosure, and Year of Observation.

No.	Author, Year	Country context	Theory	Industry sector	Timely-Quarterly-Annually Disclosure	Year of Observation
1.	(Wu et al., 2023)	US		Multi sector firms	10-K filings Item 1A section	2017 - 2022
2.	(Mazumder & Hossain, 2022)	Banglades	Agency Theory & Resource-Based Theory	Bank	Annual report	2014 -2020
3.	(Arcy & Basoglu, 2022)	US	Legitimacy Theory & Institutional Theory	Multi sector companies	8-K report	2005-2018
4.	(Radu & Smaili, 2021)	Canada	Stakeholder Theory, Resource Dependence Theory, Critical Mass Theory	Company multi sector	Annual Report	2014-2018
5.	(Masoud & Alutaibi, 2022)	US		listed firms		2006 - 2016
6.	(Chen et al., 2022)	US	Stakeholder Theory	Multi sector firms	Item 1A of the 10-K filing	
7.	(J. Haislip et al., 2021)	US	Upper Echelon Theory	Multi sector firms	8-K Report	2005 - 2017
8.	(Gao et al., 2020)	US	Agency Theory	listed firms	10-K Report	2007 - 2018
9.	(Swift et al., 2020)	US		Firms multi sector	10-K report	2012 - 2015
10.	(J. Z. Haislip et al., 2020)	US	IT Expertise Literature	Multi sector firms, exclude financial services and utility industries	8-K Report	2005-2014
11.	(Li et al., 2018)	US		Multi Sector firms	10-K report	2007 - 2015
12.	(Higgs et al., 2016)	US	Signaling Theory	Multi sector firms	8-K report	2005-2014

[9]; [10]; [11]; [12], only a small part was carried out in the context of Canada [13] and Bangladesh [14] This means that almost all of the research (92%) is conducted in the context of developed countries, where information technology is so advanced and cyber security disclosure is quasi-mandatory. Only a few studies have been conducted in the context of developing countries (8% of the total), namely Bangladesh. No research has

been conducted in other developing countries, for example ASEAN, the Middle East, etc.

4.2. Applied Theory

The theories used to explain the phenomenon of cyber security disclosure are agency theory [3]; [14], Resource-Based Theory [14]; [13], Legitimacy Theory dan Institutional Theory [5], Stakeholder Theory [6]; [13], Signaling Theory [7], dan Critical Mass Theory [13].

4.3. Industrial Sector

If the analysis is carried out based on the industry sector, it can be seen that most of the research is carried out on multi sector companies (90%), only a small portion (10%) is carried out on special sectors, such as banking [14]

4.4. Industrial Sector

Most (60%) of cyber security disclosure data sources were obtained from 10K Report [6]; [3]; [1]; [14]; [13]; [9]; [10]). A small number of studies (40%) used data obtained from 8K Report ([5]; [7]).

4.5. Main Findings About Determinant Cyber Security Disclosure

4.5.1. Breach Dan Cyber Security Disclosure

Empirical evidence shows that breach or cyber incident has a significant effect on cyber security disclosures. [5] find that data breach announcements are positively associated with cyber security disclosures. [10] find that past breach, significantly correlated with cyber security disclosures. [8] find that cyber disclosure is significantly positively correlated with Breach. Firms with Breaches disclosing more cyber security risk disclosures in fiscal years t or t + 1 than are firms without breaches. [6] find that firms experiencing a data breach increase the amount of cyber security risk factor disclosures compared to matched firms with no data breach. The severity of data breaches affects the results. Cyber security risk factor disclosures increase only after severe data breaches.

[3] find that prior incidents are significantly associated with the total number of words and the use of litigious language cyber security disclosures, but not with cyber security disclosures readability. [9] find that material breaches significantly impact the number of words in cyber security disclosures, decreasing boilerplate disclosure for breach years and post-breach years from the two pre-breach years, [1] find that cyber security risk disclosures of firms with cyber security incidents are much longer than that of firms without cyber security incidents. The findings from the literature review show that the occurrence of a breach, incident, or cyber attack has a significant effect on the breadth of cyber security disclosures.

4.5.2. Data Breaches By Industry Peers And Cyber security Disclosures

From a search of the determinant cyber security disclosure literature, only 1 study examined the relationship between data breaches by industry peers and cyber security disclosures. [5] find that data breaches by industry peers are negatively associated with cyber security disclosures. The relationship between data breaches by industry peers and cyber security disclosures is stronger (more positive) when the focal firm has an external breach, as compared to when it has an internal breach.

4.5.3. WFH Dan Cyber Security Disclosure

Companies that carried out remote work prior to the pandemic tended to experience cyber security incidents and disclose cyber security risk in their annual reports [10], both before and during the pandemic period. However, this relationship has become weaker during the pandemic period.

4.5.4. Public Attention and Cyber Security Disclosure

Arcy & Basoglu [5] find that public attention after data breach announcements is positively associated with cyber security disclosures. This association stronger (more positive) for external breaches than for internal breaches.

4.5.5. Firm's Size and Cyber Security Disclosure

Assets have a positive and significant effect on cyber security disclosure, whereas employees have an insignificant positive effect on cyber security disclosure [5] [13]

found that firm's size has a significant positive effect on cyber security disclosure. Chen [6] found that firm's size has no significant positive effect on cyber security disclosure. The disclosures for small firms are easier to read than those for large firms, company size is significantly associated with readability [3]. Higgs [7] found significant positive correlations between breach reporting and firm's size. Different results were found by [14] who found an insignificant negative result.

4.5.6. Firm's Growth and Cyber Security Disclosure

Empirical evidence from previous research shows that Firm's Growth has a significant negative effect on Cyber Security Disclosure ([14]; [13]. Chen [6] found positive insignificantly influence Firm's Growth on Cyber Security Disclosure

4.5.7. Firm's Profit and Cyber Security Disclosure

Firm's profit matters positive significant to cyber security disclosure [5]; [13], other studies have found insignificant positive effects ([14] and insignificant negative [3].

4.5.8. Firm's Leverage and Cyber Security Disclosure

Research on the effect of leverage on cyber security disclosure showed similar results, negative but not significant ([5]; [6]; [14]; [13])

4.5.9. Firm's Loss and Cyber Security Disclosure

Arcy & Basoglu [5] found that loss has an insignificant positive effect on cyber security disclosure.

4.5.10. Capital Expenditure and Cyber Security Disclosure

Arcy & Basoglu [5] found that Capital expenditure has an effect negative significant to cyber security disclosure.

4.5.11. Industry and Cyber Security Disclosure

Cyber Security Disclosures on industry consumer services, software and services, and banking are easier to read than disclosures in other industries. Cyber Security Disclosures in such industries as consumer services, software and services, and banking contain a significant proportion of litigious language than those in other industries [3].

4.5.12. Board Size and Cyber Security Disclosure

Radu & Smaili [13] found an insignificant positive effect between Board size and cyber security disclosure while [14] showed findings negative insignificant association between Board size and cyber security disclosure.

4.5.13. Board Independence and Cyber Security Disclosure

Mazumder & Hossain [14] found significant positive results for Board Independence and cyber security disclosure, [13] found positive insignificant influence Board Independence on cyber security disclosure.

4.5.14. Board Diversity and Cyber Security Disclosure

In-depth research on influence Board Diversity regarding cyber security disclosure conducted by [13] . Using the percentage of women, the Blau Index, and the critical mass of three women as the measurement for board diversity, the findings show a positive and significant association between the presence of cyber security disclosure and board diversity. Similar results were also obtained by [14] who found a significant positive effect on board diversity and cyber security disclosure.

4.5.15. Institutional Shareholders and Cyber Security Disclosure

Mazumder & Hossain [14] examine the influence of Institutional Shareholders on Cyber Security Disclosure and found negative significant effect.

4.5.16. Foreign Shareholders and Cyber Security Disclosure

Mazumder & Hossain [14] examine the influence Foreign Shareholders terhadap Cyber Security Disclosure and found a negative insignificant result.

4.5.17. Islamic Banking and Cyber Security Disclosure

Mazumder & Hossain [14] examines the influence of Islamic banking on Cyber Security Disclosure and found an insignificant positive result.

4.5.18. Guidance And Cyber Security Disclosure

Li [1] found evidence that there were big changes following the SEC's cybersecurity disclosure guidelines in 2011. Gao [3] found that the 2011 SEC Guidance and 2018 SEC Guidance had a positive effect on cyber security disclosure. In addition, the annual increase in the percentage of firms providing cyber security risk disclosures is much larger following the disclosure guidelines.

4.5.19. Intangible Asset And Cyber Security Disclosure

Gao [3] found that cyber security risk disclosures easier to read when companies have a high proportion of intangible assets.

4.5.20. Technology Committee And Cyber Security Disclosure

A positive and significant relationship between breach and technology committee is shown that firms with a technology committee are more likely to have reported breaches in a given year than firms without a committee. A significant negative relationship between breach and old technology committee shows that the longer and more stable the technology committee, the less often companies experience breaches [7]. IT expertise at the TMT level (CEOs, CFOs, CIOs) plays a significant role in reducing reportable Data Security Breach occurrences [12]. Research [11] show significant associations between Form 8-K reporting timeliness and both IT-expert CEOs and technology committees.

4.5.21. Executive Change And Cyber Security Disclosure

Gao [3] found that executive change has a significant negative relationship to cyber security disclosures. Executive change reduces the formal education required to read cyber security changes.

5. Finding and Conclusion

The scarcity of research on the determinant factor of cyber security disclosure provides ample opportunity for future research to explore this topic. The results show that the determinant factor of cyber security disclosures are board size, board independence, board gender diversity, institutional shareholders, foreign shareholders, cyber security breach / previous cyber incidents, peer breach, public attention, WFH, capital expenditure, intangible asset, firm's size, firm's growth, firm's leverage, firm's

6. Implications, Limitations, and Suggestions

This research contributes by providing a comprehensive discussion of the determinant factors of cyber security disclosure from various studies. The limitation of this research is that the researcher only reviewed articles published in English. Future research may include articles published in multiple languages. Based on the literature review, the researcher provides suggestions for future research. Cyber security is one of the problems faced by all companies today, but research in this field is still very little. There are still wide open opportunities to explore the topic regarding cyber security disclosure determinant factors.

References

[1] Li H. GW, Wang T. SEC'S cybersecurity disclosure guidance and disclosed cybersecurity risk factors. *Journal of Accounting Information Systems*. 2018:1–6.

[2] Schatz D, Bashroush R, Wall J, Towards A. More representative definition of cyber security. *Jdfsl*. 2017;12:53–74.

[3] Gao L. Calderon Tg, Tang F. Public companies ' cybersecurity risk disclosures. *International Journal of Accounting Information System*. Epub Ahead Of Print 30 June 2020. Doi: Https://Doi.Org/10.1016/J.Accinf.2020.100468

[4] Haapamäki E, Sihvonen J. Cybersecurity in accounting research. *Managerial Auditing Journal*. 2019;34(7):808–834.

[5] Arcy J, Basoglu A. The influences of public and institutional pressure on firms' cybersecurity disclosures. *J Assoc Inf Syst*. 2022;23(3):779–805.

[6] Chen J, Henry E, Jiang X. Is cybersecurity risk factor disclosure informative? Evidence from disclosures following a data breach. 2022.

[7] Higgs J, Pinsker R, Smith T, et al. The relationship between board-level technology committees and reported security breaches. *Journal of Information Systems*. https://doi.org/10.2308/isys-51402

[8] Masoud N, Al-Utaibi G. The determinants of cybersecurity risk disclosure in firms' financial reporting: Empirical Evidence. *Res Econ*. 2022;76(2):131–140.

[9] Swift O, Colon R, Davis K. The impact of cyber breaches on the content of cybersecurity disclosures. *J Forensic Investig Account*. 2020;12.

[10] Wu Q, Yoon K, No G. The effect of remote workforce on firms' cybersecurity risk disclosures and incidents. *SSRN Elsevier E-Journals*. 2023;1–23. https://doi.org/10.2139/ssrn.4342761

[11] Haislip J, Lim JH, Pinsker R. The impact of executives' IT expertise on reported data security breaches. *Inf Syst Res*. 2021;32(2):318–334.

[12] Haislip JZ, Karim KE, Lin KJ, Pinsker RE. The influences of CEO IT expertise and board-level technology committees on form 8-k disclosure timeliness. *J Inf Syst*. 2020;34(2):167–185.

[13] Radu C, Smaili N. Board gender diversity and corporate response to cyber risk: Evidence from cybersecurity related disclosure. *Journal of Business Ethics*.

[14] Mazumder MMM, Hossain DM. Voluntary cybersecurity disclosure in the banking industry of Bangladesh: Does board composition matter? *Journal of Accounting in Emerging Economies*.