International Journal of Innovative Technologies in Economy

e-ISSN: 2414-1305

Scholarly Publisher
RS Global Sp. z O.O.
ISNI: 0000 0004 8495 2390

Dolna 17, Warsaw,
Poland 00-773
+48 226 0 227 03
editorial_office@rsglobal.pl

ARTICLE TITLE	A BIBLIOMETRIC ANALYSIS OF CYBER SECURITY RISK DISCLOSURE
ARTICLE INFO	Lola Melindia, Yaeni Maryani, Fitri Pebrianti, Siti Jubaedah. (2025) A Bibliometric Analysis of Cyber Security Risk Disclosure. *International Journal of Innovative Technologies in Economy*. 2(50). doi: 10.31435/ijite.2(50).2025.3386
DOI	https://doi.org/10.31435/ijite.2(50).2025.3386
RECEIVED	05 June 2025
ACCEPTED	23 June 2025
PUBLISHED	27 June 2025
LICENSE	The article is licensed under a **Creative Commons Attribution 4.0 International License.**

A BIBLIOMETRIC ANALYSIS OF CYBER SECURITY RISK DISCLOSURE

Lola Melindia
Faculty of Economics and Business, Universitas Swadaya Gunung Jati, Indonesia

Yaeni Maryani
Faculty of Economics and Business, Universitas Swadaya Gunung Jati, Indonesia

Fitri Pebrianti
Faculty of Economics and Business, Universitas Swadaya Gunung Jati, Indonesia

Siti Jubaedah
Faculty of Economics and Business, Universitas Swadaya Gunung Jati, Indonesia

ABSTRACT

Along with experiencing significant financial losses due to data breaches in the company. To attract stakeholders' attention, companies need to disclose the cyber risks they face. This study aims to explain the progress and patterns in cyber risk disclosure and the variables that are often associated with the practice. The research used a systematic literature review of 155 research articles from Scopus (2020-2024) using the keywords cybersecurity disclosure in the fields of computer science, social science, business management, accounting, economics, and finance. Data was limited to English journal articles and analysed using bibliometric analysis with the VOS viewer application. The results show that research on cyber risk disclosure in Scopus.com is still limited, but shows an increasing trend in various countries' companies. The cited articles are identified as references for future research. On accounting conceptualisations regarding the voluntary disclosure of such corporate social responsibility information related to cyber risk threats.

KEYWORDS

Bibliometric Analysis, Cybersecurity Disclosure, Systematic Literature Review, Voluntary Disclosure

CITATION

Lola Melindia, Yaeni Maryani, Fitri Pebrianti, Siti Jubaedah. (2025) A Bibliometric Analysis of Cyber Security Risk Disclosure. *International Journal of Innovative Technologies in Economy*. 2(50). doi: 10.31435/ijite.2(50).2025.3386

Introduction.

The world has changed drastically due to the rapid development of information and communication technology, which has become a major part of society (Alodat et al., 2024). The advancement of digital information technology has revolutionized the business world by providing various conveniences. Information and communication technology is a human creation that is fundamentally imperfect, making it vulnerable to risks (Vostoupal et al., 2024). One of the biggest threats to the strategic achievements of companies is cyber attacks, a significant risk that affects the global economy (Alodat et al., 2024). Significant cybersecurity risks can affect the course of business operations and the accuracy of financial statements. However, empirical studies related to trends and practices of cybersecurity risk disclosure by public companies are still minimal (Gao et al., 2020).

The types of cyberattack are constantly evolving. Attackers use various tactics, such as ransomware, distributed denial of service (DDos), and denial of service (Dos). DoS and DDoS attacks are the most common and frequent forms of attacks that can threaten devices with malicious intent. According to Cloudflare's report on cyber threats, between 2020 and 2021, DDos attacks increased by almost a third, with a 75% increase in

the last three months. Furthermore, according to the Neustar report, when comparing the first half of 2019 with the same period in 2018, the frequency of DDoS attacks increased by 200% while the volume increased by 73%. The increasing prevalence of DDoS attacks is indicated in Cisco's annual internet report for 2018–2023 (Rizal et al., 2025). Through the disruption of a country's important sites, cyberattacks become more frequent and exert global influence and international competition. According to the World Economic Forum's 2019 Global Risk Report, cyber risk is second only to climate change. According to a study, there are more than 40 million cyberattacks worldwide (Alodat et al., 2024).

In recent years, the frequency and severity of malicious cyberattacks have increased. These cyberattacks have a serious impact on the businesses of publicly traded companies and, consequently, their investors. IBM released its annual Data Breach Cost Report in July 2023, which examines the costs incurred by 553 organizations as a result of data breaches that occurred between March 2022 and March 2023. Half of Hacked Organizations Don't Want to Increase Security Spending Despite Soaring Breach Costs. According to the study, the average loss from data breaches reached $4.45 million in 2023, which is a record high and an increase of more than 15% over the previous three years (Uslaner & Brunetto, 2024).

Another case like SolarWinds was a major cyber incident in late 2020, in which hackers allegedly linked to the Russian state managed to infiltrate SolarWinds network management software, which is used by thousands of organizations, including US government agencies. This attack is known as a 'supply chain attack', where malicious code is inserted into software updates issued by SolarWinds, allowing hackers to access sensitive data without being detected. The U.S. Securities and Exchange Commission (SEC) filed a lawsuit against SolarWinds and its former Chief Information Security Officer (CISO), Timothy Brown, for securities fraud and making false claims before, during, and after the devastating cyberattack. The SEC alleges that SolarWinds did not disclose its vulnerability to cyberattacks and the impact of the attacks on its financial performance (Stempel, 2024). In response to the increasing cyber threats and attacks, the Securities and Exchange Commission (SEC) has tightened its oversight of cyber risk disclosures by public companies. The SEC is also reviewing the cybersecurity policies, processes, and control mechanisms implemented to address such risks (Gao et al., 2020).

Cyberattacks targeting companies result in reputational damage and large financial losses (Agrafiotis et al., 2018). Cyberattacks that are capable of crippling even the most advanced companies underscore the importance for stakeholders to know the level of exposure of companies to these threats and the steps that have been taken to address them (Alodat et al., 2024). Cyberattacks can result in major disruptions to a company's operational activities. As companies grow, challenges related to cybersecurity become increasingly complex. One of the main obstacles in cybersecurity is the need to manage the interaction between the digital world and the real world in the process of data exchange (Li & Liu, 2021). After an incident occurs, the company has the potential to experience various adverse impacts, including financial losses, a decline in the stock price if listed on the stock exchange, a decrease in the company's image, recovery costs, and the risk of facing lawsuits (Boggini, 2024). Losing confidential data and supply chain disruptions are some of the other risks that can be caused by cybersecurity breaches (Seid et al., 2024). At the same time, cybersecurity issues are making executives and stakeholders aware of the possible loss of clients and business opportunities, which attracts more researchers' attention and makes this topic controversial (Alodat et al., 2024). We show that the risk of loss of reputation can be understood as a result of implementing an efficient risk management strategy (Kamiya et al., 2021). Stakeholders are now demanding greater transparency from businesses in this area as a result of their growing concerns about increasing cyberattacks and threats to their interests (Gao et al., 2020; Mazumder & Hossain, 2023; Alodat et al., 2024). These cyber-related incidents result in huge economic losses and pose a serious risk to a country's vital infrastructure. To address this problem, governments in various countries have begun to evaluate and actively manage and monitor their cybersecurity capabilities and maturity levels (Jeong et al., 2019). This situation highlights the board's responsibility to increasingly focus on efforts to increase cybersecurity-related disclosures. In contrast to mandatory financial disclosure, which is intended to provide financial and non-financial information to corporate stakeholders, disclosure seeks to provide transparency to a wide range of corporate stakeholders, including investors and customrs (Leuz & Wysocki, 2016; Agrafiotis et al., 2018).

Based on the results of the researcher's search on the Scopus.com page, research related to cyber risk disclosure in 2020 to 2024 is still very limited, therefore this research is important to fill the void of cyber risk disclosure literature. In addition, this research is also important because the many cases of data breaches indicate a low awareness of the implementation of transparent cyber risk disclosure. Cyber risk disclosure can help gain legitimacy from stakeholders and support better information technology governance. These cyber-

related incidents result in huge economic losses and pose serious risks to a country's vital infrastructure. One of the biggest challenges in network security is identifying and collating important and appropriate features from vast data sets to support the intrusion detection process (Beechey et al., 2021). To address this issue, governments in various countries have started to evaluate and actively manage and monitor their cybersecurity capabilities and maturity levels (Jeong et al., 2019). This situation highlights the responsibility of boards to increasingly focus on efforts to improve cybersecurity-related disclosures. In contrast to mandatory financial disclosures, which are intended to provide financial and non-financial information to a company's stakeholders, disclosures aim to provide transparency to a company's various stakeholders, including investors (Leuz & Wysocki, 2016; Agarwal et al., 2024). Basically, cybersecurity objectives are divided into three main areas: Enabling authorised users to access information promptly, protecting sensitive data, and maintaining the integrity and credibility of information by guaranteeing its accuracy and reliability (Gordon & Loeb, 2006; Alodat et al., 2024).

To promote openness and trust in the digital environment, regular reporting and accountability are essential. The low level of voluntary disclosures related to cybersecurity risks in accounting practices drives the need for efforts to understand the underlying reasons or determinants that may motivate companies to increase such disclosures, given the importance of disclosures in supporting business strategies and influencing overall management decision-making. Several studies have examined the factors or determinants that influence cybersecurity risk disclosures, thereby providing a deeper understanding of the important reasons behind such disclosures. First, Boggini (2024) points out that based on the purposes of ESRS S4 reporting, regulatory compliance—such as Article 32 GDPR and Article 21 NIS 2—contributes to increased disclosure of cybersecurity risks. Article 32 of the GDPR and Article 21 of the NIS 2 encourage the improvement of sustainability reporting content, while Article 20 of the NIS 2 focuses on improving the quality of the cybersecurity information disclosed. This shows that regulations and reporting obligations play an important role as a determinant in driving better disclosure of cybersecurity risks. Next, the research of Vostoupal et al. (2024) shows that legal challenges, especially those related to criminal liability, are an important determinant of cybersecurity risk disclosure. Such risks can be minimized through careful vulnerability disclosure policies, authorization of specific testing activities, and setting the scope of the disclosure program. In addition, the provision of explicit consent by vendors for certain actions as well as the implementation of measures to maintain whistleblower confidentiality, such as through coordinators and digital certificates can increase the motivation for disclosure. Additional factors affecting the efficacy of cybersecurity risk disclosure include sector-specific regulations, such as those relating to the financial and healthcare sectors, and legal frameworks related to cybersecurity and data protection. Additionally, according to Alodat et al. (2024) businesses that have larger boards of directors, more independent directors, and more frequent board meetings also usually disclose more information related to cybersecurity. Effective boards of directors are typically committed to maintaining transparency, by providing voluntary disclosures that focus on issues such as cybersecurity. According to research by Alodat et al. (2024), female board members also tend to be more cautious when providing information related to cybersecurity and prefer to keep it confidential.

Cyber risk disclosure is ultimately necessary for businesses to prevent financial and non-financial losses, improve information technology governance, and gain credibility from stakeholders. Overall, recent trends show that transparent and timely disclosure of cybersecurity risks, as well as the implementation of stricter security practices, are becoming increasingly important to protect investor interests and maintain market integration, hence the need for a literature review study on cybersecurity risk disclosure. Through keyword analysis of the dimensions of cybersecurity risk disclosure, clustering of authors based on similarity of article content, collaboration of leading countries and journals in the cybersecurity risk disclosure literature, provision of high-impact articles in each content based on citation ratio, and mapping of variables associated with cybersecurity risk disclosure that have the potential to be further developed in future research, this study seeks to shed light on the trends and developments in research on cybersecurity risk disclosure as well as explain the variables that are often associated with such disclosure. Businesses, financial institutions, governments, academics, and researchers are among the groups interested in thoroughly examining the cyber risk disclosure literature, and they will benefit from the conclusions of this study. The novelty of this study is that it provides.

Research Method.

This study uses a descriptive approach with a systematic literature review method. The data of this study amounted to 155 research articles published in Scopus.com between 2020 and 2024. The data is limited to article types, journals, and English-language only. Literature search based on the keywords cyber security disclosure, in the fields of computer science, social science, business management, and accounting; economics, econometrics, and finance. Data analysis using bibliometrics with the VOS viewer application. A statistical method of evaluating literature that incorporates the use of quantitative analysis is called bibliometric analysis. The research data was processed using the VOS viewer application which included Co-occurrence analysis to identify research topics statistically by calculating paired data in collection units, Co-authorship analysis using existing documents to identify relationships between different studies, and bibliographic analysis to reveal researcher activities related to the research field.

Results and Discussion.

This study was successful in gathering preliminary data from 392 articles obtained using the keyword cyber security disclosure. The categorized articles came from Scopus-indexed journals with a publication period of 2020 to 2024. However, for 2024, the publications analyzed only cover up to early December 2024, so it does not cover all articles published during that year. The selection of Scopus-indexed journals was done because the available references include publications from various reputable publishers around the world, so it is considered appropriate as a reference. After the screening process was carried out, the number of articles that were processed further was 155, with the screening stages as presented in Table 1.

Table 1. Screening of Research Data

	Screening	The Number of paper obtained becomes
1	All paper with cyber security disclosure word search	392
2	Restricted to 2020 - 2024	224
3	Restricted 3 subject area: 1) Bussiness Management and Accounting; 2) Economics, Econometrics and Finance; 3) Sosial Sciences; 4) Computer science	196
4	Types of documents funded articles, conference paper	171
5	Required publication stage: final publication	155
6	Required source type journal, conference proceeding	58
7	Cited language: English	155
8	Data used for processing	155

Source: data processed (2024)

Research and publication trends related to cyber risk over the period 2020 to 2024 show a significant increase in attention to cyberattacks. This can be seen from the distribution and development shown in the graph in Figure 1.

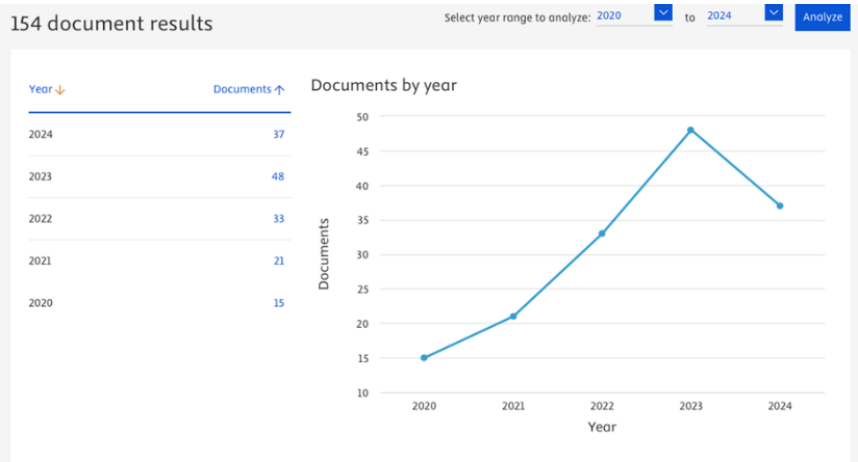

Fig. 1. *Graph of Cyber Risk Research Development from 2020 to 2024*
Source: https://www.scopus.com/

Figure 1 shows the development of the number of publications related to the topic of cyber risk from 2020 to 2024. In general, there is a significant upward trend in the number of documents during this period. In 2020, the number of publications recorded was only 15 documents. This figure reflects the low starting point of cyber risk research. However, this trend began to increase in the following years. In 2021, the number of publications increased to 21 documents, then rose significantly to 33 documents in 2022.

This increase shows the growing attention of researchers to cyber security and risk issues, along with the increasing complexity of digital threats globally. The year 2023 recorded the highest number of publications in the last five years, with 48 documents. This is an indication that cyber risk is increasingly becoming an important focus of academic and practical studies, especially due to its wide-ranging impact on the economy, business and government sectors. In 2024, there was a slight decrease in the number of publications to 37 documents. However, this decrease cannot be used as a final indicator, because the 2024 data may not reflect all publications in a full year, given the time-consuming scientific publication process and additional publications at the end of the year. Therefore, there is still a possibility that the number of documents will continue to grow.

Overall, this publication pattern shows that the topic of cyber risk is consistently growing and tends to increase. Variations in the number of publications from year to year can be influenced by a variety of factors, including the dynamics of information security policy, the increase in global cyberattacks, and shifts in research focus across different disciplines. Furthermore, Figure 2 presents an annual graph that categorizes publications based on their source.

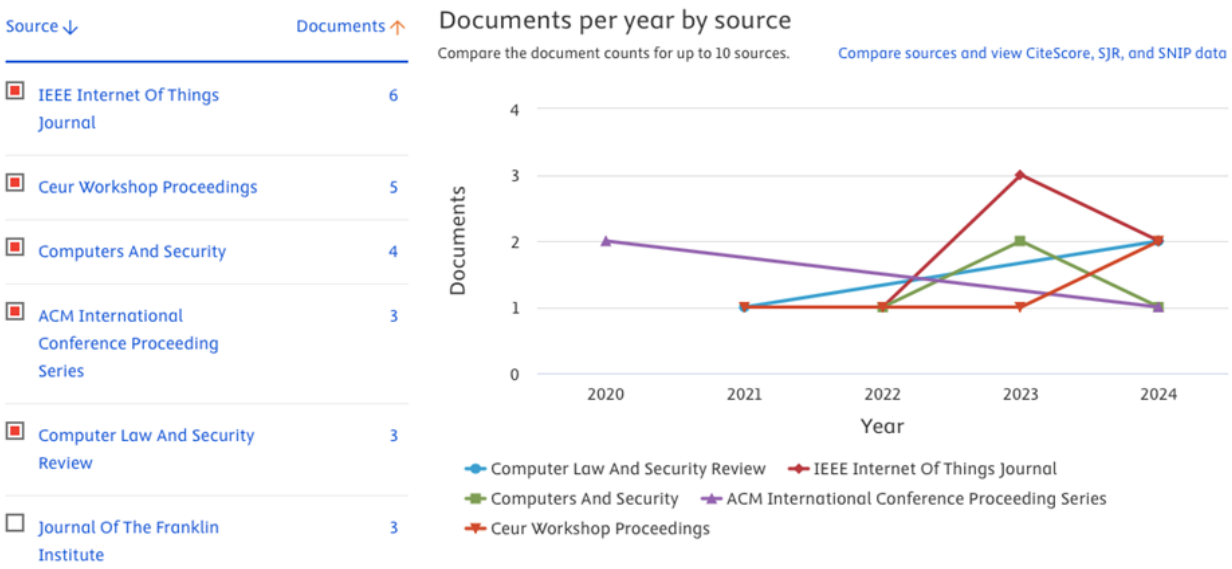

Fig. 2. *Cyber Risk Research Chart by Source 2020 to 2024*
Source: https://www.scopus.com/

Figure 2 shows the distribution of the number of publications by source or journal that published articles related to cyber risk from 2020 to 2024. Based on the graph, the IEEE Internet of Things Journal is listed as the source with the highest number of publications, with six documents. This shows that the topic of cyber risk related to the Internet of Things (IoT) is a major concern in the scientific and information technology community.

IoT is one of the fastest growing technological innovations, but it also presents major security challenges. The large number of interconnected devices creates gaps that can be exploited by cyber criminals. Therefore, the increase in the number of publications in the journal indicates a high awareness and urgency to understand and address cyber risks in IoT systems. Besides IEEE, some other sources that are also active in publications related to this topic include Ceur Workshop Proceedings (5 documents), Computers and Security (4 documents), ACM International Conference Proceeding Series (3 documents), and Computer Law and Security Review (3 documents). This variety of sources shows that cyber risk issues are not only discussed in a technical context, but also in legal policy aspects and multidisciplinary scientific conferences.

This trend indicates the importance of cross-sector collaboration to comprehensively respond to cyber threats. Going forward, the implementation of security technologies such as encryption, advanced authentication, and regular software updates will be key in maintaining the integrity and reliability of IoT-based systems. Furthermore, Figure 3 shows the distribution of documents based on the author who made the publication.

Fig. 3. *Graph of Cyber Risk Publications by Author*
Source: https://www.scopus.com/

Figure 3 shows the distribution of publications based on the names of authors involved in cyber risk-related research. From the graph, the author with the most contributions is Loutocký, P., who recorded three publications. Meanwhile, a number of other authors such as Ashraf, M., Cavusoglu, H., Dou, C., Eyeleko, A.H., Feng, T., Kasl, F., Khan, R.A., and Malinka, K. have two publications each. This distribution provides a snapshot of authors active in the field of cyber risk studies, and can be used as a reference to identify key figures or thought leaders in the field. Their consistent engagement demonstrates a deep interest and expertise in issues related to cyber threats and risk mitigation.

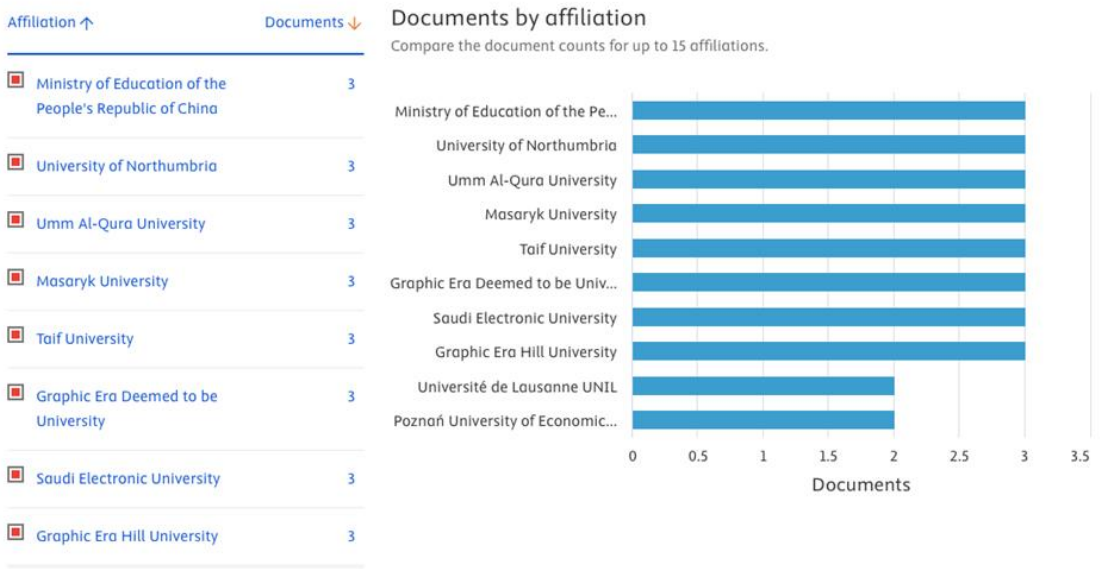

Fig. 4. *Graph of Cyber Risk Publications Author Affiliation*
Source: https://www.scopus.com/

In addition, this information is very useful for novice researchers or institutions that want to build academic cooperation, because it can be directed to authors who have proven to be productive and active. Such contribution patterns can also serve as an indicator of global research trends, particularly in the domains of information technology, cybersecurity, and digital risk management. By identifying high-contributing authors, the academic and industry communities can gain a better insight into who are the pioneers in this research. It also opens up opportunities for greater international collaboration in developing innovative solutions to evolving cyber risk challenges. Furthermore, Figure 4 will show the distribution of documents by author affiliation, providing insight into the institutions that are most active in research on this topic.

Figure 4 presents data on the institutional affiliation of authors involved in publications on cyber risk during the period 2020 to 2024. Based on the graph, it can be seen that the contribution of publications comes from various institutions with a relatively even number. Each institution listed, such as Ministry of Education of the People's Republic of China, University of Northumbria, Umm Al-Qura University, Masaryk University, Taif University, and Graphic Era Hill University, each contributed three documents related to this topic.

This balanced distribution shows that research on cyber risk is not only focused by one institution or country, but has become a global concern. Institutions from different countries with diverse educational backgrounds, geographies and research approaches actively participated in this study. This reflects that cyber risk is a transnational and multidisciplinary issue that demands international collaboration.

The active participation of institutions from China, Europe, the Middle East and South Asia also indicates a heightened awareness of digital security threats globally. In other words, the issue of cyber risk has gained an important place on the global academic research agenda. In addition, this balanced distribution may also open up opportunities for cross-institutional cooperation and enrich perspectives in the development of more comprehensive security solutions. Overall, the data in Figure 4 reinforces previous findings that cyber risk-related research is showing an inclusive growth trend, not centred on one particular institution or region, but rather widely spread globally.

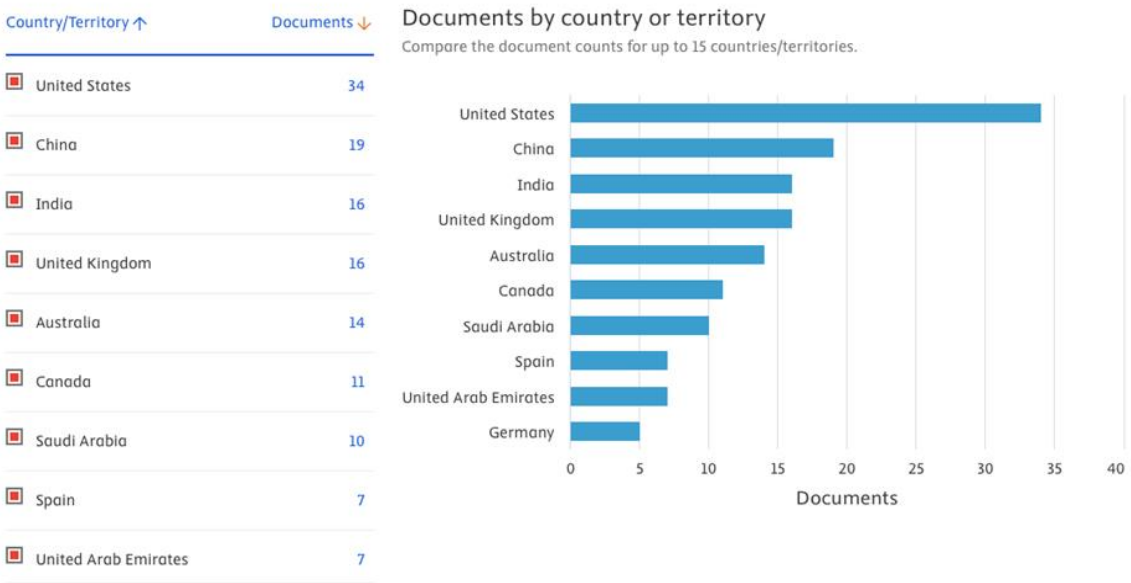

Fig. 5. *Graph of Countries with the Highest Number of Cyber Risk Disclosure Publications*
Source: https://www.scopus.com/

Figure 5 shows the distribution of the number of publications related to cyber risk disclosures by country or region in the last four years. This data provides insight into the countries that are most active in research in this field. It is seen that the United States ranks first with a total of 34 articles, making it the country with the largest contribution to research on cyber risk disclosure. This suggests that this topic is a major concern in the United States, likely due to the high level of digitalization, strict regulations related to cybersecurity, and the increasing cyber threats to companies and institutions in the country.

China came in second place with 19 articles, which shows a fairly high research interest in the country. As one of the countries with the largest digital economy in the world, China has a great interest in

understanding and managing cyber risks, both in the business and government sectors. India and the UK share the third position with 16 articles each. India, as one of the global information technology hubs, has an interest in cyber risk disclosure to protect its technology industry and business. Meanwhile, the UK, as one of the financial and technology centers in Europe, is also active in research related to cyber risk to strengthen digital security policies and regulations. Australia came in fourth place with 14 articles, indicating that the country is also active in research related to cyber risk, likely due to the increasing cyber threats in the Asia-Pacific region as well as government policies to improve national cybersecurity.

Canada is ranked fifth with 11 articles, signaling a significant research focus in this area, which can be attributed to the country's cybersecurity policies as well as the challenges faced by Canadian companies in dealing with digital threats. In addition to the top five, there are several other countries that have also contributed to cyber risk disclosure research, including Saudi Arabia, Spain, and the United Arab Emirates, which each have 7 articles. These countries have shown considerable involvement in research on this topic, which may be influenced by national regulations, industry interests, as well as the level of cyber threats faced by each country.Overall, the distribution of publications by country shows that cyber risk disclosure is a global issue that attracts the attention of different countries with different levels of digitalization and regulation. With the rise of cyber threats in various sectors, research in this area continues to grow, involving various countries trying to understand, manage, and mitigate the risks posed by the digital world. The article with the highest number of citations in this study can be seen in Table 1, which can be used as the main reference in understanding the development of studies related to cyber risk disclosure. In addition, Figure 6 will display a table grouping the most cited documents by type, providing more information on the most influential types of research in this field.

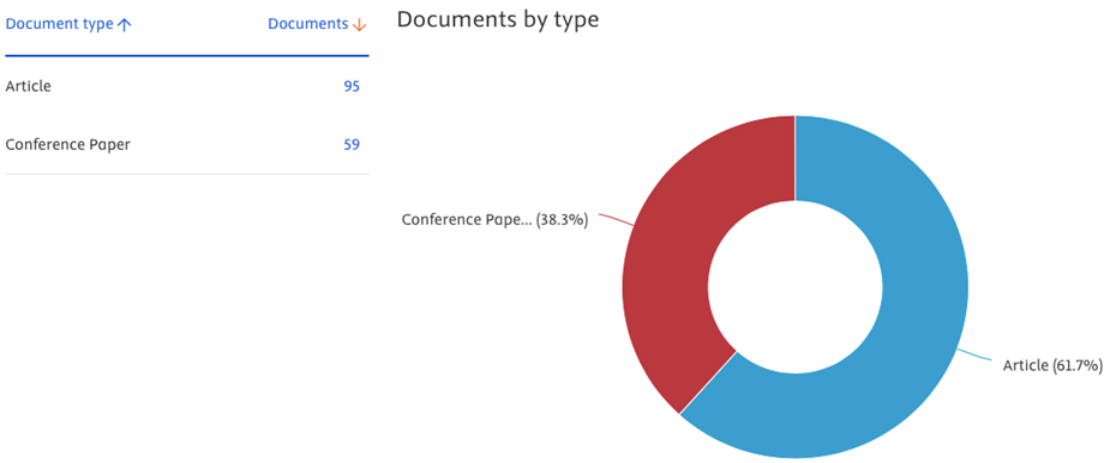

Fig. 6. *Number of documents by type*
Source: https://www.scopus.com/

Figure 6 shows the distribution of publications related to cyber risk by document type, which is divided into journal articles and conference papers. The majority of publications are in the form of journal articles, with 95 articles (61.7%), indicating that research in this field is more widely published through scientific journals that have gone through a peer review process. Meanwhile, conference papers amounted to 59 documents (38.3%), showing that preliminary and exploratory research was also widely presented in academic forums before being published further. This difference reflects the scientific community's preference for disseminating their findings. Furthermore, Figure 7 will show cyber risk documents based on subject areas.

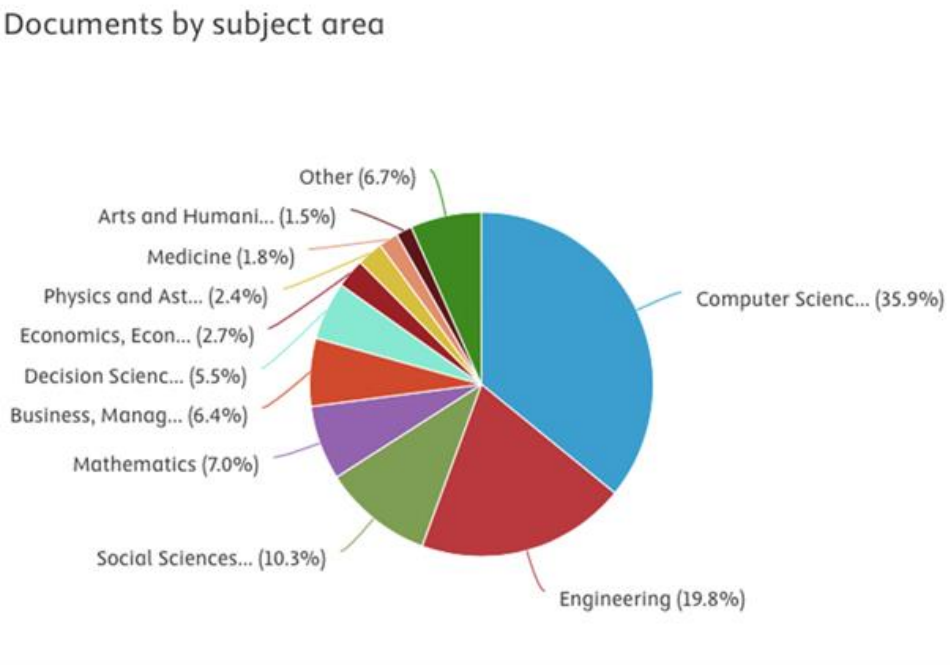

Fig. 7. *Number of documents by Subject Area*
Source: https://www.scopus.com/

The figure above shows the distribution of documents based on subject areas that discuss the theory of cyber risk attacks. From the data presented, it can be seen that the field of Computer Science is the most dominant field in discussing this topic, which is 35.9% of the total documents analyzed. This shows that the issue of cyber risk attacks is very relevant in the world of information technology and computing, where various aspects of system, network and data security are the main focus of research.

In the second position, Engineering contributed 19.8%. This shows that technical and engineering approaches in dealing with cyber risks also receive great attention, especially in terms of developing reliable hardware and security systems. Social Sciences took third place with a contribution of 10.3%, reflecting the importance of social, policy and human behavior approaches in understanding and managing cyber risks. Meanwhile, Mathematics contributed 7.0%, which is commonly used in algorithm development, cryptography, and risk modeling.

Furthermore, Business and Management contributed 6.4%, signaling that cyber risk is also a concern in the corporate sector, especially in terms of risk management, consumer data protection, and operational sustainability. Decision Science contributed 5.5%, highlighting the role of data-driven decision-making in tackling cyber threats. Smaller contributions came from Economics (2.7%), Physics and Astronomy (2.4%), Medicine (1.8%), and Arts and Humanities (1.5%). This shows that while the scope of cyber risk attack topics extends to various disciplines, the main focus is still on technical and applied sciences. The "Other" category accounts for 6.7%, which may include fields such as law, education, or other interdisciplinary fields not specifically mentioned but still relevant to cyber risk issues. Overall, this distribution suggests that the topic of cyber risk is mostly discussed in the context of technology and engineering, although approaches from social science, economics and other fields are also important to provide a more comprehensive perspective. Table 2 mentioned in the narrative also indicates the list of articles with the highest number of citations, which can be used as a key reference in further studies on cyber risk attacks.

Table 2. Articles based on Highest Citation

No	Author	Title	Year	Journal	Citation
1	Patrick Cichy, Oliver Salge	Privacy Concerns and Data Sharing in the Internet of Things: Mixed Methods Evidence from Connected Cars	2021	MIS Quarterly	75
2	Theoretical framework and hypothesis development	Cyber-attacks and stock market activity	2021	International Review of Financial Analysis	51
3	Lei Gao, Thomas G. Calderon, Fengchun Tang	Public companies cybersecurity risk disclosure	2020	International Journal of Accounting Information Systems	45
4	Shilpi Jain, Soni Agrawal	Percelved vulnerability of cyberbullying on sosial networking sites: effects of security measures addivtion and self-Disclosure	2020	Indian Growth and Development Review	30
5	Roberto Doriguzzi-Corin	FLAD: Adaptive Federate Learning for DDoS attack detection	2024	Computers & Security	23
6	Rishikesh Sahay , D.A. Sepulveda Estay, Weizhi Meng, Christian D. Jensen, Michael Bruhn Barfod	A comparative risk analysis on Cybership system with STPA-Sec, Stride and Coras	2023	Computers & Security	16
7	Zaina Abuabed, Ahmad Alsadeh, and Adel Taweel.	STRIDE threat model-based framework for assessing the vulnerabilities of modern vehicles	2023	Computers & Security	13
8	Mattia Caldarulo, Eric W. Welch, Mary K. Feeney	Determinants of cyber-incident among small and medium US cities	2022	Government Information Quarterly	13
9	Huw Dylan, Thomas J Maguire	Secret Intelligence and Public Diplomacy in the Ukraine War	2022	Survival Global Politics and Strategy	12
10	E.V.A. Eijkelenboom, B.F.H. Nieuwesteeg	An analysis of cybersecurity in Dutch annual reports of listed companies	2021	Computer Law & Security Review	8

Source: https://www.scopus.com/

Research and publication trends related to cybersecurity disclosure show relatively low numbers. Based on Table II, Patrick Cichy and Oliver Salge are the authors with the highest number of citations, 75 citations, which examine theories related to cyber risk disclosure in the field of social science. "Privacy Concerns and Data Sharing in the Internet of Things: Mixed Methods Evidence from Connected Cars" delves into the topic of how drivers' privacy concerns and data-sharing decisions are influenced by both virtual and physical threats.

Visualizations, overlays, and network density were generated in the bibliometric analysis using Vosviewer. The results of visualization with Vosviewer of 155 articles taken from the Scopus database form a network that not only indicates the relationship between keywords but also shows the intensity of the relationship which is reflected through the distance between elements. The network visualization of keywords related to cyber security disclosure can be seen in Figure 8.

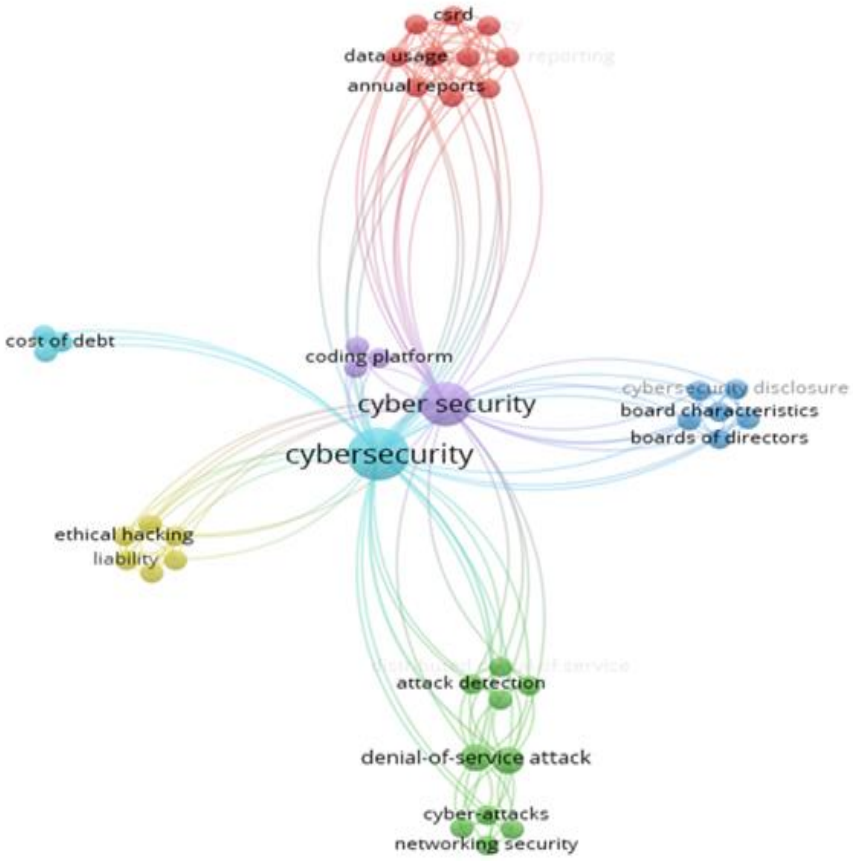

Fig. 8. *Area Keyword Network Visualisation*
Source: Vosviewer, 2024

Based on Figure 8, the visualization of keywords on the topic of cyber security disclosure shows a variety of lines and colors in the network, which represents the relationship between clusters that are interconnected with other keywords. Keywords with the same color indicate high co-occurrences. The most frequently occurring keywords in this study are shown by six large clusters with different colors, namely cybersecurity, cyber security, coding platform, board characteristics, denial-of-service attack, and annual reports. The six keyword clusters generated by Vosviewer provide interesting clues for further research, but the latest trends in cybersecurity disclosures are still under-researched, opening up opportunities for novelty in future research. In addition to the visual network, an overlay display can also be used to illustrate the data. The color of each keyword represents the year of publication of the article. Nodes with darker colors indicate older articles, while nodes with lighter colors indicate newer or more relevant articles. The overlay visualization can be seen in Figure 9.

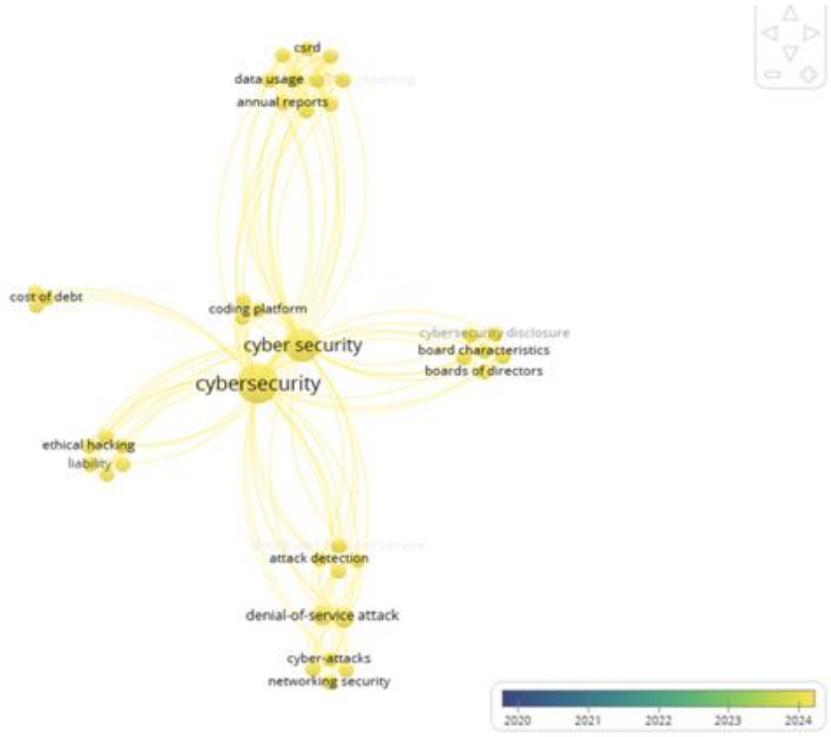

Fig. 9. *Overlay Visualisation*
Source: Vosviewer, 2024

Figure 9 shows the results of a bibliometric study that used overlay visualization to map and cluster cybersecurity disclosure research trends according to historical traces or publication years. This information can be used as a reference to identify and map the latest developments in research conducted throughout the 2020-2024 period. Node colors in the overlay representation stand for keywords that denote the publication year.

Based on the observation in Figure 9, all keywords related to cybersecurity disclosure have yellow-colored nodes. This indicates that the research topic began to be widely discussed by researchers in 2024. In the period 2020-2023, the number of studies discussing this topic is still relatively limited, so this topic can be considered as a new trend that needs to be further developed in future studies.

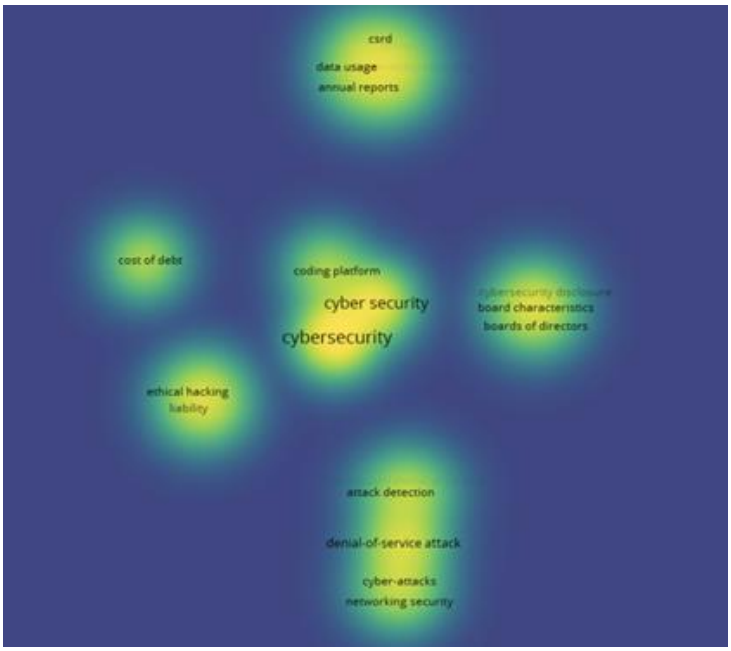

Fig. 10. *Overlay Visualisation*
Source: Vosviewer, 2024

Through density visualization, researchers can observe the frequency of use of a keyword. The indicator that shows how often the keyword is researched is marked by the color in the visualization. The brighter or more prominent the color of a keyword, the more frequently it is researched. Conversely, the dimmer or darker the color, the less frequently the keyword is the focus of research. The level of saturation in the use of keywords marked with a light color indicates that the topic has been widely researched and indexed in Scopus. Examples of frequently researched keywords include cybersecurity, ethical hacking, board characteristics, denial-of-service attacks, and annual reports. Meanwhile, dark-colored nodes indicate that the keywords or topics are rarely researched, such as cost of debt, privacy, cybersecurity disclosure, sustainability disclosure, and sustainability reporting. This indicates that research related to cybersecurity disclosure is still relatively low, so these topics or keywords provide extensive and potential research opportunities for further exploration.

Conclusions.

Based on the results of bibliometric analysis conducted from 2020 to 2024, research related to cyber risk disclosure is still relatively limited, thus opening up great opportunities for further research. Companies are advised to increase transparency in cyber risk disclosure as a strategic effort to build trust and gain legitimacy from stakeholders. Future research should examine more deeply the key factors that drive companies to be more open in their disclosure of information related to cybersecurity. In addition, regulators and policymakers need to develop clearer guidelines and standards regarding cybersecurity disclosures so that companies can comply with best practices and reduce cyber risks. Closer collaboration between businesses, governments, and academic institutions can also encourage stronger cybersecurity and disclosure practices, and contribute to better governance and risk management frameworks.

One of the limitations of this research is the source of the data. The study relied solely on articles published in Scopus from 2020 to 2024, so it could ignore other relevant studies published in other databases that are not indexed by Scopus. This study also has some methodological limitations because it uses bibliometric analysis. This method only provides an overview, not an in-depth analysis, although it is useful for finding research trends related to cyber risk. As a result, the research findings are more theoretical and do not examine their immediate impact on companies looking to increase transparency in disclosing cyber risks.

For further research, it is recommended to use a combination approach of bibliometric analysis and qualitative case studies to obtain deeper insights related to cyber risk disclosure. In addition, expanding the scope of data sources is also important by including research from various databases other than Scopus to obtain a more comprehensive perspective. Furthermore, future research should specifically explore the relationship between regulations, corporate policies, and transparency of cyber risk disclosure, so that it can make a more applicable contribution to the business world and policymakers in managing and mitigating cyber threats.

REFERENCES

1. Agarwal, N., Agarwal, S., & Chatterjee, C. (2024). Data breach notification laws and the cost of private debt. *British Accounting Review*. https://doi.org/10.1016/j.bar.2024.101518
2. Agrafiotis, I., Nurse, J. R. C., Goldsmith, M., Creese, S., & Upton, D. (2018). A taxonomy of cyber-harms: Defining the impacts of cyber-attacks and understanding how they propagate. In *Journal of Cybersecurity* (Vol. 4, Issue 1). Oxford University Press. https://doi.org/10.1093/cybsec/tyy006
3. Alodat, A. Y., Hao, Y., Nobanee, H., Ali, H., Mansour, M., & Al Amosh, H. (2024). Board characteristics and cybersecurity disclosure: evidence from the UK. *Electronic Commerce Research*. https://doi.org/10.1007/s10660-024-09867-w
4. Beechey, M., Kyriakopoulos, K. G., & Lambotharan, S. (2021). Evidential classification and feature selection for cyber-threat hunting. *Knowledge-Based Systems*, *226*. https://doi.org/10.1016/j.knosys.2021.107120
5. Boggini, C. (2024). Reporting cybersecurity to stakeholders: A review of CSRD and the EU cyber legal framework. *Computer Law and Security Review*, *53*. https://doi.org/10.1016/j.clsr.2024.105987
6. Gao, L., Calderon, T. G., & Tang, F. (2020). Public companies' cybersecurity risk disclosures. *International Journal of Accounting Information Systems*, *38*. https://doi.org/10.1016/j.accinf.2020.100468
7. Gordon, L. A., & Loeb, M. P. (2006). *Managing cybersecurity resources: A cost-benefit analysis* (Vol. 1). McGraw-Hill.
8. Jeong, J. J., Grobler, M., Chamikara, M. A. P., & Rudolph, C. (2019). *Fuzzy Logic Application to Link National Culture and Cybersecurity Maturity*. https://geerthofstede.com/research-and-vsm/dimension-data-matrix/
9. Kamiya, S., Kang, J. K., Kim, J., Milidonis, A., & Stulz, R. M. (2021). Risk management, firm reputation, and the impact of successful cyberattacks on target firms. *Journal of Financial Economics*, *139*(3), 719–749. https://doi.org/10.1016/j.jfineco.2019.05.019

10. Leuz, C., & Wysocki, P. (2016). *The Economics of Disclosure and Financial Reporting Regulation: Evidence and Suggestions for Future Research*. http://ssrn.com/abstract=2733831http://ssrn.com/abstract=2733831www.ecgi.org/wphttps://ssrn.com/abstract=2733831
11. Li, Y., & Liu, Q. (2021). A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments. *Energy Reports*, *7*, 8176–8186. https://doi.org/10.1016/j.egyr.2021.08.126
12. Mazumder, M. M. M., & Hossain, D. M. (2023). Voluntary cybersecurity disclosure in the banking industry of Bangladesh: does board composition matter? *Journal of Accounting in Emerging Economies*, *13*(2), 217–239. https://doi.org/10.1108/JAEE-07-2021-0237
13. Rizal, R., Selamat, S. R., Mas'ud, M. Z., & Widiyasono, N. (2025). Enhanced Readiness Forensic Framework for the Complexity of Internet of Things (IoT) Investigation Based on Artificial Intelligence. *Journal of Advanced Research in Applied Sciences and Engineering Technology*, *50*(1), 121–135. https://doi.org/10.37934/araset.50.1.121135
14. Seid, E., Satheesh, S., Popov, O., & Blix, F. (2024). FAIR: Cyber Security Risk Quantification In Logistics Sector. *Procedia Computer Science*, *237*, 783–792. https://doi.org/10.1016/j.procs.2024.05.166
15. Stempel, J. (2024, July 19). *SolarWinds beats most of US SEC lawsuit over Russia-linked cyberattack*. Reuters. https://www.reuters.com/legal/us-judge-dismisses-most-sec-lawsuit-against-solarwinds-concerning-cyberattack-2024-07-18/
16. Uslaner, J. D., & Brunetto, J. (2024, May 31). *The SEC's new cybersecurity disclosure rules decoded: what they mean for investors*. Reuters. https://www.reuters.com/legal/legalindustry/secs-new-cybersecurity-disclosure-rules-decoded-what-they-mean-investors-2024-05-31/
17. Vostoupal, J., Stupka, V., Kasl, F., Loutocky, P., & Malinka, K. (2024). *The Legal Aspects of Cybersecurity Vulnerability Disclosure: To the NIS 2 and beyond*. https://www.enisa.europa.eu/topics/cybersecurity-policy/nis-directive-new