International Journal of Studies in Business Management, Economics and Strategies
Volume 3, Issue 11, November - 2024
ISSN (E): 2949-883X
Scholarsdigest.org

DETERMINANTS OF CYBER RISK DISCLOSURE: REVIEW ARTICLE

Samir Emad Shaaban 1,
Ahmed Fadhil Saleh 2,
Mohamed Ahmed Dheyab 3
1 College of Administration and Economics, Tikrit University
Email: samir.emad@tu.edu.iq
2 University of Anbar (Email: ahmedf.saleh@uoanbar.edu.iq
3 College of Administration and Economics, Tikrit University
Email: m.ahmed.d@tu.edu.iq

Abstract
Disclosure of cyber risks is predominantly important, as the importance of cyber risk disclosure decisions has increased due to the large number of attacks and breaches that have affected companies' data and information. This analysis aimed to contribute to the scientific discussion to clarify the challenges facing companies in disclosing cyber risks due to rapid developments in information technology by reviewing many studies that dealt with cyber risk disclosure and the factors that affect it. Earlier studies and articles from various local, Arab, or foreign magazines were reviewed to reach the basic determinants and factors that affect this disclosure. The study reached a group of results, which were that relying on modern information technology in decision-making due to interconnected systems that contain a large set of data and information is one of the challenges that companies may face because they are more exposed to potential or actual cyber risks and the extent of the possibility of confronting and addressing these risks, in addition to another set of challenges facing companies when disclosing cyber risks, represented by previous cyber incidents, cyber security breaches, and corporate governance (board of directors size and independence, gender diversity, institutional ownership, and Foreign ownership) and the size and growth of the company, the type of activity, and the technology committee.

Keywords: Cyber risk, Cyber Security, cyber risk disclosure, determinants of cyber risk disclosure.

Introduction

The success of companies depends mainly on the skills of the different departments in these companies. Among these departments, we find risk administration, as its performance depends on identifying and drawing up plans to respond to expected risks and examining potential threats to the company or its available resources, whether material or human, to reduce them to the lowest possible level. Risk supervision emerged in the late last century as an approach to reducing organizational costs. Recently, companies have begun to show clear interest in interior auditing for its strong role in activating risk management. Protection from cyber risks is defending systems, programs, and networks from digital attacks that usually

aim to access sensitive information. In contrast, insurance companies seek to meet the requirements and requirements of the market for cyber insurance to reduce the risks of those attacks and threats (Al-Karawi & Al-Issawi, 2024).

The rapid development and growth of digital technology in global markets has led to a continuous and escalating increase in cyber threats and attacks on companies and stakeholders, including investors, lenders, and others. These threats have recently increased due to the digitization of transactions as a result of the coronavirus pandemic (COVID-19) and the ability of information network hackers to achieve high income from a cybersecurity incident through many programs, in addition to the use of encrypted assets, the growth of digital payments, and the increased reliance of companies on technology and information service providers, including cloud computing technology. In light of the increase in these risks through cyber-attacks, qualified accounting bodies have provided several frameworks and guidelines to regulate the process of disclosing these risks, including (the SEC), (AICPA), (ICEW), and others (Yaqoub, Wahab, & Al-Fartousi, 2022).

Cyber breaches can start significant losses for companies regarding financial and legal aspects that affect their reputation. Disclosure of cyber risks that public companies may face and the mechanism for organizing and confronting them has become increasingly important for investors, consumers, customers, and all stakeholders to help them make sound decisions toward companies (Remeis, 2023). Companies can also reduce uncertainty about cyber risks and assess information asymmetry with all stakeholders by disclosing cyber risks and developing a mechanism for confronting them promptly. The study (Arcuri, Brogi, & Gandolfi, 2018) presented that cyber risks represented by information security breaches can have a negative economic impact on companies due to decreased sales revenues, increased costs, decreased current and future profits, and deterioration of the company's reputation, which directly affects its market value. The economic consequences can also be mild in the long term because companies can protect their main information assets by identification the real impact of cyber risks and attacks on stock market returns and determining investment levels in information security activities.

The study (Amir, Levi, & Livne, 2018) and (SEC, Commission Statement and Guidance on Public Company Cybersecurity Disclosures, Conform to Federal Register version, 2018) also showed that the heavy reliance of companies on web technologies to arrange their financial management work increases their exposure to cyber risks and attacks, which are one of the main risks that must be controlled, as the objectives of these attacks are multiple, and maybe to steal or destroy financial assets or stealing intellectual property and other important information related to companies or their customers and business partners. The study (Forum, 2017) also showed that cyber risks are among the top five threats that the global economy may face and among the top ten threats facing companies and their future, as parties that deal with the company, such as investors, customers, and suppliers, lose confidence not only in the company that is exposed to cyber incidents and breaches but in the entire industry to which the company belongs. The increase in the requirements and needs of stakeholders for information associated to the risks facing companies led to the interest of professional accounting bodies in these requirements through the expansion of accounting disclosure, as technological development in the field of communications and the Internet has made websites

channels of great importance for companies in accounting disclosure of information quickly and at lower costs and reaching a wider range of users and stakeholders, this has led to the creation of an opportunity for companies to expand the scope of accounting disclosure and diversify the methods of presenting information through the use of audio and video files and other technologies that contribute to improving the quality of accounting disclosure of financial and non-financial information and risks and opportunities facing companies in order to attract more investors and lenders (Al-Sawy, 2022). In 2022, the SEC (SEC, The Securities and Exchange Commission today proposed proposals to its rules to enhance and standardize disclosures regarding cybersecurity risk management, strategy, governance, and incident reporting by public companies, 2022) issued amendments to strengthen and standardize cybersecurity administration and cyber incident disclosure requirements in corporate periodic reports to better inform investors and stakeholders about a company's risk management, strategy, and governance related to cyber matters and to provide timely cyber risk information to help them make sound decisions. Under the suggested rules, companies are required to disclose a material cybersecurity incident within four days, disclose cybersecurity policies and procedures to define cyber risk management and management's role in assessing and analyzing cyber risks, disclose in corporate reports any cybersecurity expertise to the board of directors, and provide their cybersecurity and risk disclosure in expanded business reporting language for easy access.

The study (Ramírez, Ariza, & Miranda, 2022) emphasized the requirement of disclosing cyber risks in terms of their nature and how to manage them. It is considered one of the ways through which investors and stakeholders can be interconnected. These cyber risks, whether confirmed or potential and the market reactions related to them must be reflected in the extent to which additional disclosures are provided to the company in the annual reports. Thus, cyber risks can fundamentally impact business processes and the integrity of financial reports.

Theoretical Outline

First: What are cybersecurity threats?

Security is the cornerstone of building any society and the basic component for developing any activity, whether in the field of education, business, or politics, as security is one of the most important services represented by the basic pillar that adds value to government activities on the Internet as a result of the development that occurred in the information society, educational technologies and cyberspace for companies and individuals (Al-Khadri, Salami, & Kalibi, 2020). With the emergence of the period cybersecurity, it became clear that security and cyberspace interact with each other, as cybersecurity is viewed as a set of technical and administrative tools used to protect computer networks from misuse and unauthorized access while recovering any electronic data that may be lost, in addition to protecting the company's assets and available resources from organizational, human, financial, technical and informational threats that enable it to implement its plans and goals (Sassawi, 2020) and (Mashtoub & Lakhwidar, 2018).

While the most important purposes of cybersecurity are as follows: (Al-Karawi & Al-Issawi, 2024)

1. Ensuring complete confidentiality that only approved persons can receive, change, or manage information.
2. Ensuring integrity that only authorized persons and processes can change the system.
3. Providing the system and the information organized by the system and its operators to ensure that only authorized entities can access the information or resources stored or used in the company's infrastructure.

As for the concept of cybersecurity risks, it is a group of organizational, technical, and administrative means used to prevent unauthorized use, misuse, and return of electronic information and communications systems and offer protection to ensure the continuity of information systems and enhance the confidentiality and privacy of data (Yaqoub, Wahab, & Al-Fartousi, 2022). The National Institute of Standards and Technology (NIST) also defined it as keeping information by preventing attacks by detecting and responding to them. In contrast, the International Organization for Standardization (ISO) defined it as the space that represents preserving confidentiality, integrity, and providing information in cyberspace. The Egyptian Cybersecurity Authority also described cybersecurity risks as the risks that companies may face, including the company's message, vision, brand, reputation, or image, due to the possibility of unauthorized access, misuse, or destruction of information, as it is considered one of the most important risks that companies may face (Egyptian Cybersecurity Authority, 2017-2021). The Saudi Cybersecurity Guide also expressed it as the environment resulting from the interaction of individuals with software and services available through the Internet via devices, technologies, and networks connected to it that do not have a physical presence (National Cybersecurity Authority, 2018). The Iraqi National Cybersecurity Strategy described it as the possibility of a threat and fragility within the country's cyberspace that harms the security of information systems and basic information infrastructure structures through cyber threats and vulnerabilities in cloud spaces (Iraqi Cybersecurity Strategy, 2020). On the other hand, cyber risks may be characterized by several cyber-attacks that contain three types, which are as follows: (Shahimi & Mahzan, 2018)

1. Cyber risks related to confidentiality ascend when private information within the company is disclosed to a third party, as in the case of a data breach.
2. Cyber risks related to integrity arise when it comes to misusing schemes, as is the case with fraud.
3. Cyber risks related to performance continuity are represented by interruption or cessation of activities and businesses.

Second: Disclosure of cyber risks Risk disclosure includes disclosing all categories of risks, both financial and non-financial, with a description of all available resources and any other relationships that may affect the company's value (ICAEW, 2011). Disclosure of cyber risks is one of the investigation areas that have received wide attention recently. A study by (Abu Samak, 2023) indicated that companies work to release cyber risks through the management report in a descriptive manner to give a positive signal to stakeholders that the company has contributed to managing cyber risks and that it has disclosed its efforts in this regard through qualitative disclosure in one of the company's reports, which leads to giving a positive and bright image of the company that it was proactive in maintaining information security and reducing cases of cyber-attacks on it.

The study (Yaqoub, Wahab, & Al-Fartousi, 2022) also presented that disclosing cyber risks in annual reports gives a positive signal about the company in the eyes of investors and stakeholders about the efforts made in the field of cyber security and the extent of protection from cyber-attacks, which contributes to reducing the phenomenon of information asymmetry between management and stakeholders to help investors evaluate the company's ability to maintain information security and reduce the likelihood of breaches and negative events in the future, which helps improve the quality of decisions made by investors towards the company and the possibility of enhancing confidence in the activities and businesses it carries out, and thus reflecting these decisions on improving the company's financial performance. The study (Yangeted, 2020) also confirmed that disclosing cyber risks contributes to positively affecting the decisions of investors and stakeholders and enhancing their confidence in the company, which is reflected in the quality of the decisions taken in light of industries that suffer from fierce cyber-attacks, which leads to increased attractiveness of investors and stakeholders towards the company.

The study (Saleh , Al-Ajami, & Al-Samadoni, 2020) indicated that releasing cyber risks has harmful effects on the company's reputation, directly affecting its goals, strategy, and information infrastructure and the destruction of the company's private information. It is one of the risks the company has faced or is expected to face, and its availability in its reports improves disclosure and transparency in its annual reports. Cyber risks include data access, information accessible to all employees and customers, and safety, privacy, accessibility, and infrastructure. Disclosure of cyber risks provides beneficial information to investors and stakeholders to help them evaluate the performance of other non-hacked companies in the same industry and activities. Abu Samak's study (Abu Samak, 2023) showed three possibilities for the feedback of investors and stakeholders: The first possibility is that investors may view the cyber hack as a private matter. In this case, investors will adjust their view of the hacked company, but they will not make any adjustments to the market value of participating companies. The second possibility is that investors may view the peer violation as positive information for competing companies, which is known as the effects of opposition, as competitors in the same industry and activities can obtain a market share from the hacked company, which leads to a positive reaction in the market for companies. The third possibility is that investors may consider the peer instruction as negative information about competing companies. This prompts investors to adjust the market value of these companies that have not been hacked.

Third: Insurance strategies for cyber risk disclosure

Cyber risk insurance strategies are as follows: (Ismail, 2021).

1. Costs associated with hiring lawyers and reporting clients whose personal information has been compromised are covered by data breach expenses.
2. Liability for privacy and system security, including defense of settlements against third parties and class actions.
3. Regulatory claims, costs of civil fines, penalties, and settlements are reimbursed, in addition to the cost of defending against government investigations.

4. Network outage, which is paid for by added costs and loss of revenue due to the network shutdown.

From the above, researchers believe that companies' response to disclosing cyber risks is the main pillar in maintaining the trust, authority, and objectivity of the information contained in companies' annual reports, especially the reports attached to the financial reports and related to disclosing information related to cyber risks that the company may face or that have already been faced, in addition to the increasing interest of accounting and regulatory bodies and authorities in encouraging companies to disclose this type of information periodically and annually. Reviewing the analysis literature and stating the most important determinants facing the disclosure of cyber risks despite the nature of the disclosure of cyber risks, there are many emerging threats and determinants that will face this type of disclosure to take into consideration, and that the disclosure of cyber risks is becoming increasingly important due to the large number of breaches and attacks that obtain information and data specific to companies, which raises real concerns about cyber security programs, and cyber risks are one of the most important and largest risks that companies that use information technology systems in operational activities can face, and therefore these determinants have emerged. The researchers purpose in this paragraph to present and analyze a set of literature that dealt with cyber risks and their impact on companies at different stages through the following:

Few studies have addressed the considerations that drive firms to higher levels of cyber risk disclosure. Jiang et al. (Jiang, Legoria, Reichelt, & Walton, 2022) examined whether firms alter their cyber risk disclosure after a cyber breach. The study found that market reactions influence firms' cyber risk disclosure behavior after a violation. Calderon & Gao (Calderon & Gao, 2022) reported that firms change their disclosure conduct after receiving an SEC comment letter on their cyber risk disclosure. Wang et al. (Wang, Yen, & Yoon, 2022) documented that firms that received observation letters changed their disclosure behavior as required by the SEC.

The study (Tosun, 2021) showed that the financial markets react to unanticipated security attacks and breaches for companies in the short, medium and long term, as it showed that the market reaction in terms of trading volume, liquidity and selling pressure expects negative changes in stock prices, which turn out to be large and negative changes only on the day following the public disclosure of security breaches and affect companies' policies in the long term, meaning that security breaches are unexpected negative shocks to companies' reputation. The study (Lending, Minnick, & Schorno , 2018) approved that the financial impact of a security breach is clear in the long term, as the study addressed measuring changes in stock returns after a data breach, as banks exposed to attacks and security breaches face significant declines in deposits, while non-banking companies face significant declines in sales in the long term. Chen et al. (Chen , Henry, & Jiang, 2023) also showed that companies' use of disclosure of cyber risks and their causative causes after data breaches, especially severe breaches, is a natural experiment and an external shock to assess the severity of cyber risks that have occurred to their companies. This was inspected on a sample of companies, and the results were that companies that suffer from data breaches and are exposed to cyber risks increase the amount of disclosure of the factors and causes of these

risks compared to companies that do not suffer from data breaches. In addition, there is no significant reaction in the markets if subsequent annual reports of hacked companies include increasing disclosure of the factors and causes of exposure to cyber risks that occurred. While Gao et al. (Gao, Calderon, & Tang, 2020) discovered a long-term increasing trend in the content and linguistic characteristics of public companies' cyber risk disclosures, which provides insight into the factors that may drive these trends, the study found that the most frequently disclosed cyber risks were service interruption (operational) risks and data breach (breach) risks. The SEC's 2011-2018 assistance positively affected on the length of cyber risk disclosure. Other factors that led to this style were the type of industry, the overall cyber risk in the general environment, the size of the company, and previous cyber breach incidents. Wang et al., 2022 (Wang, Yen, & Yoon, 2022), studied the market's reaction to SEC letters and comments connected to cyber risk disclosure. The results showed that the market reacts negatively to the responses presented by public companies to the SEC after receiving comment letters about their cyber risk disclosure. The study also showed several measures of the feature of cyber risk disclosure, including word count, readability, comprehension, and litigation language.

On the other hand, the work (Cheong, Yoon , Cho, & No , 2021) showed how to combine of content analysis and factor analysis to classify cyber risk disclosures into different risk factor categories. The study found that companies have various disclosure patterns depending on whether they have experienced cyber risk incidents or internal control weaknesses. The study (Jackson, Vanteeva , & Fearon , 2019) also specified that long documents in cyber risk disclosures are used as a tool to hide bad news that management is trying to hide from investors and stakeholders in long documents, because when the document size becomes larger, it becomes more difficult to read and understand this document, which may lead to a deviation after the earnings announcement.

The study (Sari, Adam, Fuadah, & Yusnaini, 2024) also showed the aspects that affect cybersecurity disclosure, as the results showed that the factors that affect this type of disclosure were cybersecurity breaches, exposure to previous cyber incidents, and corporate governance represented by the size and independence of the board, gender diversity, institutional ownership, and foreign ownership, in addition to the size and growth of the company, financial leverage, capital expenditures, intangible assets, type of activity, and technology committee. The study (Radu & Smaili, 2022) checked that the risk of the Internet has become one of the biggest threats companies may face in recent years. Accordingly, the boards of directors of companies must be constantly arranged to confront this risk, and have a high potential to take appropriate measures to confront actual or potential cyber risks, as the study aimed to demonstrate the impact of gender diversity on the board of directors on the disclosure of cyber risks, as the results showed a positive impact between gender diversity of the board of directors on this disclosure. The study (Higgs, Pinsker, Smith, & Young, 2016) also authorized that companies whose board of directors includes a technology committee as part of their IT governance can detect and address cybersecurity breaches. In addition, companies that have technology committees are more disclosing of cyber risks associated to companies that do not have such a committee, in addition to the company's lower likelihood of being exposed to this type of risk due to the presence of an IT committee

to indicate the company's ability to detect and address cyber risks. The study (Chen , Henry, & Jiang, 2023) also showed that the size and growth of the company do not have a substantial positive effect on the disclosure of cyber risks, and that the disclosure of small companies is easier to read and understand compared to large companies. However, it varied from the study (Higgs, Pinsker, Smith, & Young, 2016) as it found that the size of companies has a significant positive association with the disclosure of cyber risks, meaning that the larger the company size, the greater the level of disclosure. The study (Yaqoub & Ismail, 2023) aimed to measure the disclosure of non-financial threats of cybersecurity and environment in companies listed on the Iraq Stock Exchange through a proposed indicator for disclosing such a type of disclosure. The study determined that there needs to be stronger disclosure of non-financial risks in both cybersecurity and environmental aspects. This weakness is due to the absence of obligatory instructions for disclosing non-financial risks. The study recommended that the management of the Iraq Stock Exchange should prepare a guide that includes the mechanisms that normalize the disclosure of non-financial risks of cybersecurity and the environment.

The study (Mousa, Shaheen, Shehata, & Al-Bahary, 2023) also expected to shed light on the mechanisms of electronic disclosure of cyber risks, extract an accounting framework for the mechanisms of disclosure of cyber risks and governance of their management, and study and analyze the essential effects of this disclosure on the relevant annual financial reports. The study concluded that companies must assume more disclosure and transparency in financial reports in order to inform investors and stakeholders of all potential and actual essential cyber risks that may affect their activities, businesses, and financial results, in addition to disclosing the mechanism through which cyber risks can be confronted and how to manage them in order to mitigate their severity and impact. While the study (Al-Karawi & Al-Issawi, 2024) aimed to explain the management of cybersecurity risks in companies and to know the ability of internal auditing through cyber risk management to reduce insurance costs by reducing the strength of these risks on companies, the study concluded the necessity of creating continuous training programs for employees at all levels, with a focus on familiarizing them with roles, responsibilities, and rewards for adhering to regulations and guidelines that aim to update information security protection programs and administrative systems.

Conclusions

The rapid technological growth in the information system has directly and significantly affected the accounting field, as companies need to invest in digital initiatives and modern technology to survive, grow, and compete in the modern business environment. The results showed that relying on current information technology in decision-making due to interconnected systems that contain large amounts of data and information is one of the challenges facing companies because they are more exposed to cyber risks, which requires taking strong decisions and measures to confront these risks, in addition to other determinants and factors confronting companies when disclosing cyber risks, represented by corporate governance (the board of directors and its independence, gender diversity, institutional ownership and foreign ownership), previous cyber breaches, the size and growth of the company and the technology committee.

References

1. Abu Samak, A. M. (2023). Measuring the Impact of Cybersecurity Risk Disclosure on the Response of Stock Prices to Earnings Announcement: Applied Evidence from Listed Egyptian Banks. Scientific Journal of Accounting Studies.
2. Al-Karawi, Z. M., & Al-Issawi, K. J. (2024). The role of internal auditing based on cybersecurity risk management and its reflection in reducing insurance costs,. Al-Ghari Journal of Economic and Administrative Sciences.
3. Al-Khadri, J. S., Salami, H. G., & Kalibi, N. N. (2020). Cybersecurity and Artificial Intelligence in Saudi Universities: A Comparative Study. Journal of University Performance Development.
4. Al-Sawy, E. A. (2022). The Impact of Disclosure via the Internet and Social Media on the Cost of Capital in Light of Information Asymmetry with Application to Companies Listed on the Egyptian Stock Exchange. Alexandria Journal of Accounting Research.
5. Amir, E., Levi, S., & Livne, T. (2018). Do firms underreport information on cyber-attacks? Evidence from capital markets. Vol. 23.
6. Arcuri, M. C., Brogi, M., & Gandolfi, G. (2018). Effect of Cyber-Attacks on Stock Returns. Corporate Ownership & Control.
7. Calderon, T., & Gao, L. (2022). Comparing the cybersecurity risk disclosures of U.S. and foreign firms,. Journal of Emerging Technologies in Accounting.
8. Chen , J., Henry, E., & Jiang, X. (2023). Is cybersecurity risk factor disclosure informative? Evidence from disclosures following a data breach. Journal of Business Ethics.
9. Cheong, A., Yoon , K., Cho, S., & No , W. (2021). Classifying the contents of cyber security risk disclosure through textual analysis and factor analysis. Journal of information Systems.
10. Egyptian Cybersecurity Authority. (2017-2021). Supreme Council for Cybersecurity, Cabinet.
11. Forum, W. E. (2017). The Global Risks Report, 12th Edition is published by the within the framework of The Global Competitiveness and Risks Team.
12. Gao, L., Calderon, T., & Tang, F. (2020). Public companies' cybersecurity risk disclosures. International Journal of Accounting Information Systems.
13. Higgs, J., Pinsker, R., Smith, T., & Young, G. (2016). The Relationship Between Board-Level Technology Committees and Reported Security Breaches. Journal of Information Systems.
14. ICAEW. (2011). Reporting Business Risks: Meeting Expectations, Information for Better Markets Initiative.
15. Iraqi Cybersecurity Strategy. (2020). Cybersecurity Strategy in Iraq Reading the Global Cybersecurity Index, 2020, Al Bayan Center for Studies and Planning, Iraq.
16. Ismail, M. S. (2021). Electronic Insurance against Cyber Risks: Legal Problems and Proposed Solutions: A Study in Qatari and Comparative Law. International Journal of Law.

17. Jackson, S., Vanteeva , N., & Fearon , C. (2019). An investigation of the impact of data breach severity on the readability of mandatory data breach notification letters: Evidence from U.S firms. Journal of the Association for Information Science and Technology.
18. Jiang, W., Legoria, J., Reichelt, K., & Walton, S. (2022). Firm use of cybersecurity risk disclosures. Journal of Information Systems.
19. Lending, C., Minnick, K., & Schorno , P. J. (2018). Corporate governance, social responsibility, and data breaches. Financial Review.
20. Mashtoub , R., & Lakhwidar, N. (2018). The Role of Cybersecurity in Treating Commercial Terrorism. Ru'ya Journal for Cognitive and Civilizational Studies.
21. Mousa , A. A., Shaheen , A. A., Shehata, , M. A., & Al-Bahary , M. A. (2023). Measuring the impact of electronic disclosure of cyber risks on the value of the establishment: an applied study. Scientific Journal of Financial and Administrative Studies and Research.
22. National Cybersecurity Authority. (2018). National Cybersecurity Authority, 2018, Saudi Arabia.
23. Radu, C., & Smaili, N. (2022). Board Gender Diversity and Corporate Response to Cyber Risk. Evidence from Cybersecurity Related Disclosure.
24. Ramírez, M., Ariza, L. R., & Miranda, M. E. (2022). The Disclosures of Information on Cybersecurity in Listed Companies in Latin America. Proposal for a Cybersecurity Disclosure Index. Sustainability.
25. Remeis, K. (2023). Board Gender Diversity and Cybersecurity Disclosure Characteristics. Retrieved from https://scholars.unh.edu/cgi/viewcontent.cgi?article=1764&context=honors.
26. Saleh , I. R., Al-Ajami, H. A., & Al-Samadoni, H. F. (2020). The Impact of Board of Directors Characteristics on the Level of Voluntary Disclosure of Non-Financial Risks: An Applied Study,. Journal of Contemporary Business Studies.
27. Sari, L., Adam, M., Fuadah, L., & Yusnaini. (2024). Determinant Factors of Cyber Security Disclosure: A Systematic Literature Review. A Systematic Literature Review in 8th Sriwijaya Economics, Accounting, and Business Conference.
28. Sassawi, K. (2020). Cyber wars and global security: challenges and confrontation. Master's thesis, Ziane Achour University.
29. SEC. (2018). Commission Statement and Guidance on Public Company Cybersecurity Disclosures, Conform to Federal Register version. Securities and Exchange Commission 17 CFR Parts 229 and 249.
30. SEC. (2022). The Securities and Exchange Commission today proposed proposals to its rules to enhance and standardize disclosures regarding cybersecurity risk management, strategy, governance, and incident reporting by public companies. https://www.sec.gov/news/press-release/2022-39. Retrieved from https://www.sec.gov/news/press-release/2022-39.
31. Shahimi, S., & Mahzan, N. (2018). Building a Research Model and Hypotheses Development for Internal Audit Consulting: Insights from Literature and Findings of Exploratory Interviews. International Journal of Management Excellence.
32. Tosun, O. K. (2021). Cyber-attacks and stock market activity. International Review of Financial Analysis.

33. Wang, T., Yen, J.-C., & Yoon, K. (2022). Responses to SEC comment letters on cybersecurity disclosures: An exploratory study. International Journal of Accounting Information Systems.
34. Yangeted. (2020).
35. Yaqoub, I. I., & Ismail, R. A. (2023). Measuring the level of disclosure of non-financial cyber and environmental risks according to the proposed index in the Iraq Stock Exchange. Iraqi Journal of Economic Sciences, Special Issue of the Proceedings of the Sixth International Scientific Conference.
36. Yaqoub, I. I., Wahab, A. M., & Al-Fartousi, A. (2022). A proposed indicator for accounting disclosure of cyber risks in the Iraq Stock Exchange according to international requirements: An experimental study. Journal of Financial, Accounting and Administrative Studies,.
37. Sulaiman, Noor Adwa & Kamarudin, Nadratun Na'im and Shahimi, Suhaily, (2022), Internal Audit Effectiveness in Insurance and Takaful Companies in Malaysia: A Study of Internal Auditors and Auditees' Perceptions, Asian Journal of Business and Accounting, Vol. 15, No. 2.
38. Yang, Ling & Lau, Linda and Jan, Huiqi, (2020), investors' perceptions of the cybersecurity risk management reporting framework, international journal of accounting and information management, Vol. 28, No. 1.