Future Business Journal

RESEARCH

Open Access

The impact of cybersecurity disclosure on banks' performance: the moderating role of corporate governance in the MENA region

Dalia Hussein Elsayed[1], Tariq H. Ismail[2,3*] and Eman Adel Ahmed[1]

Abstract

This study aims to: (1) examine the impact of cybersecurity disclosure on banks' performance and (2) explore whether the existence of a chief risk officer (CRO), an information technology (IT) committee, and a board of directors (BOD)' size moderates the association between cybersecurity disclosure and bank performance. The study used manual textual analysis to measure cybersecurity disclosure in a sample of listed banks in the MENA region countries based on data from 2019 to 2021. The data were collected from annual reports and financial statements of banks available at Orbis Bank Focus database. The study employed a random effect regression model to test the hypotheses and discuss the results. The findings show that banks in the MENA region are increasingly interested in disclosing cybersecurity information, where cybersecurity disclosure over the sample years is increasing from 17% in 2019 to 19.6% in 2021. In addition, the results show that cybersecurity disclosure has a positive and significant influence on bank performance. Furthermore, the findings indicate that the presence of a CRO moderates the relationship between cybersecurity disclosure and bank performance. These findings show that depending largely on a bank's CRO to handle complex and dynamic risks can have serious consequences for decision making processes connected to managing cybersecurity risk and disclosure. This paper creates a new research paradigm by focusing on the disclosure of cybersecurity information in the MENA banking sector, where exploring the moderating role of the CRO, IT committee, and board size in enhancing the cybersecurity disclosure-bank performance relationship is lacking. The findings provide practical implications for various stakeholders, where it reveals the current practices of cybersecurity disclosure of banks in the MENA region with the objective of minimizing information asymmetry, maintaining public trust, and identifying potential risks of financial distress. In addition, the results direct the attention of banks and regulators toward the role of CRO in risk governance, particularly in managing cyber risks within the banking industry.

Keywords Cyberattacks, Cybersecurity disclosure, Chief risk officer, Information technology committee, Bank performance, MENA region

JEL Classification G30, L20, M14, N20

Introduction

Various disruptions have had a substantial impact on the financial performance and profitability of financial institutions around the world. Pandemic outbreaks, battles, and cyberattacks are some of the disruptions that have happened. Previous research has revealed the impact of the COVID-19 pandemic on global financial institutions, particularly those in Europe, resulting in significant operational disruptions [5, 34]. As a result, financial markets

*Correspondence:
Tariq H. Ismail
t.hassaneen@foc.cu.edu.eg
[1] Department of Accounting, Faculty of Management Sciences, October University for Modern Sciences and Arts (MSA), 6th of October City, Egypt
[2] Department of Accounting, Faculty of Commerce, Cairo University, Cairo, Egypt
[3] International Academy for Engineering and Media Science, 6th of October City, Egypt

were put under pressure, resulting in a decline in their financial performance.

The usage of digital technologies and artificial intelligence, the development of hybrid work environments, and the use of cryptographic assets have all contributed to the increased anxiety and a higher level of risk of cyberattacks for various organizations [58]. Cyberattacks are intentional actions that seek to alter, disrupt, or destroy computer systems and networks. In addition, it can result in data breaches, where private and confidential information is released to unauthorized parties. Consequently, this leads to negative consequences for organizations, including financial losses resulting from fraudulent transactions and reputation damage [80]. Aside from financial losses, it can result in other expenses such as litigation, attorney's fees, and cybersecurity improvements [63]. Furthermore, preserving clients' trust in the business and repairing reputational damage takes time and money. Thus, cybersecurity has become a significant concern for every company and bank in the world.

As the frequency of cyberattacks and cybersecurity data breaches is increasing due to major technological developments, there is an increasing call from a variety of stakeholders for a more transparent disclosure from organizations regarding the cyber risk they face, the way they identify and measure it, and the strategies and actions they take to manage such a risk. Accordingly, nowadays, financial regulators and accounting standard setters have directed their attention toward cyber risk and cybersecurity disclosure as part of business risk disclosures. Recently, regulatory entities in the USA and Canada have issued several guidelines highlighting the importance of cybersecurity disclosure [21–23, 75, 76]. With the continuous increase in cyberattack risks, the SEC released guidelines in [77] requesting registered firms to provide standardized and enhanced disclosures about cyber incidents, cybersecurity, cyber risk management, strategy, governance, and incidents.

Although previous research has demonstrated that cybersecurity is an important concern for regulatory agencies, accounting standard setters, corporate governance actors, and practitioners, more research into cybersecurity disclosures and their repercussions is required. This is especially true given the ongoing discussion over the repercussions of its revelation. Most prior studies on the consequences of cybersecurity and cyber risk disclosures found that these disclosures can reduce uncertainty and information asymmetry, allowing investors to make more informed decisions, which improves firm performance and valuation [16, 35]. However, it has been argued that disclosing too much cybersecurity information and confidential information related to security threats, together with firms' risk management activities, may reduce the information asymmetry and increase the possibility of cyberattacks [16, 83, 84] that can negatively affect the firm's value and performance [12]. Accordingly, the first objective of this study is to explore how cybersecurity disclosures can affect banks' performance in the countries of the MENA region. This study focuses on the banking sector, as it is vulnerable to a higher risk of cyberattacks than other sectors. This is due to the growing digitalization of banking operations and the use of financial technology, including internet banking, mobile banking, digital currency, etc., which is a crucial technology in banks and makes them more susceptible to cyberattacks.

The increase in cyberattacks and security risks has led regulatory bodies to call on and expect the board of directors (BODs) to become more engaged in the management of the organizations' cyber risks and their disclosures [39, 52]. In addition, the increased concern with cybersecurity risk has led many firms and banks to extend and delegate such tasks to the board-level IT committee and the other committees to manage such risks. Further, the emphasis in corporate governance (CG) best practices and governance legislation, particularly within the banking sector, has been on the risk management responsibility of the board, specifically in relation to cyber risk mitigation [72, 81]. This motivated many prior studies to investigate how CG mechanisms such as boards of directors, IT committees, audit committees, and risk committees can influence cybersecurity disclosure. However, most of this prior research is conducted in developed markets, such as the US and Canada (e.g., [41, 42]), and very few studies are carried out in developing countries, such as Bangladesh (e.g., [62]), with a scarcity of studies in the MENA region countries, where cybersecurity issues and their related disclosures are still in their early stages. In addition, addressing how the CRO can affect cybersecurity disclosures is lacking. This pinpoints another gap to be addressed in this study to explore how the BODs' size, the presence of the IT committee, and the presence of the CRO can influence the cybersecurity disclosure-bank performance relationship in the MENA region.

The MENA region's banking industry is quickly expanding, and many of the region's countries are enjoying economic growth and development. In 2022, the Gulf Cooperation Council (GCC) economies reported a 7.5% increase in GDP, the highest year in more than a decade. The prevalence of the oil and gas industry and the rapid growth of digitization have made this region more vulnerable to cyberattacks [61, 87]. Accordingly, regulatory authorities are continuously directing and forcing banks to improve their risk management procedures and cybersecurity to preserve the stability of the financial system.

GCC banks made increased investments in systems and infrastructure to manage cyber risk more effectively. In addition, central banks in this region are actively combating cyber addiction by establishing standards and governance. For example, CBB banks in the Kingdom of Saudi Arabia and Qatar have changed the reporting requirements for cybersecurity incidents based on the "operational risk management module". To defend the local financial system from cyberattacks, the central bank of the United Arab Emirates has constructed a networking and cybersecurity operations center. In combination with the COVID-19 pandemic, the MENA region had a notable increase in cybercrime, which has been termed a "cyber pandemic" [50, 70]. In the meantime, there was a 250% increase in cyberattacks in 2020 as a result of suspicious activity by hackers and others [18, 50]. Accordingly, the growing importance of financial institutions in the MENA region motivates this study to explore cybersecurity issues and their related disclosures in the MENA region.

The legislative framework for risk disclosure in the MENA region has changed dramatically during the last decade. Countries such as the United Arab Emirates (UAE), Saudi Arabia, Egypt, and Morocco have developed frameworks that adhere with international regulations, such as the Basel III framework, to improve the transparency of risk-related information disclosed by banks [45]. In accordance with Basel III regulations, the Central Bank of Bahrain requires banks to give substantial information about their risk management instruments to cover any losses, as well as sufficient information for stakeholders to assess the bank's risk profile (Central Bank of Bahrain [24]). Due to its importance in reducing information asymmetry and adhering to international norms, risk disclosure has therefore gained importance in the MENA region [11, 59]. Many banks in the MENA region still lag in providing detailed risk disclosures, particularly regarding non-financial risks like cyber risk [8, 26, 60].

This study makes several contributions to the literature. *First*, it builds on previous studies examining cybersecurity disclosures, which mostly focus on firms rather than banks (e.g., [12, 16, 35, 83]). Exploring such issues in the banking sector is crucial due to the fact that the risk of cyberincidents in the financial sector, including banks, is higher than in other sectors. *Second*, it explores cybersecurity disclosure in banks in the context of MENA region countries, which is still a voluntary disclosure and is in its early stages. It is important to offer more general insights into the different types of disclosures in different environments. *Third*, this study extends prior studies that either examined the cybersecurity disclosure-performance relationship (e.g., [12, 16, 35, 84]) or the determinants of cybersecurity disclosure [41, 42, 53, 62] by examining how the engagement of the BODs, the presence of the IT committee, or the presence of the CRO can moderate the cybersecurity disclosure-bank performance relationship, which has yet to be examined in prior studies.

The remainder of this paper is as follows: Section "Literature review and hypotheses development" provides a discussion of previous studies on cybersecurity disclosure and bank performance with the development of the hypotheses. Section "Research method" presents the research method, which includes the sample selection and collection of data, variables' measurements, and empirical models. Section "Results and discussion" presents the discussion of the results. Section "Conclusions, limitations, and recommendations for future research" presents the conclusions, limitations, and recommendations for future research.

Literature review and hypotheses development

Cybersecurity disclosure and bank performance

Organizations utilize cybersecurity disclosure to notify various stakeholders about their cyber risk mitigation measures and related challenges [16]. Disclosing such information enables various stakeholders to evaluate the organization's cyber risk management methods [79] as well as the actions taken by management and the board to mitigate such risk. Furthermore, organizations with higher cybersecurity disclosure may be seen as having greater cybersecurity knowledge and are considered to be more proactive in managing cyber risks by implementing appropriate cybersecurity policies and activities. Accordingly, this can minimize the costs of cyberattack incidents [16] and the consequences of negative market reactions [12, 20, 37, 64].

Based on the agency theory, the board of directors plays a crucial role in monitoring management decisions and actions to reduce the conflict of interest between agents and principals. As cyberattacks have increased during recent times, the board role has extended to oversee cyber risk management [6]. Thus, more cybersecurity disclosure reflects the enhanced monitoring role of the board in managing cyber risk and increased level of protection that is reflected in the performance. In addition, the relationship between cybersecurity disclosure and bank performance can be viewed in another way in the context of agency theory, where corporate disclosure can act as a monitoring tool, which is crucial in providing information about the firm's governance and performance [40, 49]. Firms and banks that provide more disclosure about cyber risk and cybersecurity information, together with different actions that management takes to mitigate such risks, allow investors to obtain private information that is costly and difficult to obtain. The voluntary information related to different risks, especially

cyber risk and related cybersecurity information, reduces the uncertainty associated with bank performance [1, 13], decreases information asymmetry, and lowers the cost of capital [17, 40]. As a result, investors can make more informed judgments and attract more investors to the bank, which can improve the bank's performance and valuation [16, 35, 51].

Alternatively, the relationship between cybersecurity disclosure and performance can be interpreted from the perspective of signaling theory. According to this theory, voluntary disclosure by firms, including financial institutions, about their cybersecurity measures and actions provides signals to the market about how organizations manage their cyber risks and how they engage in mitigating and detecting their security breaches [35]. These information or signals allow investors to assess the risk management and reduce the uncertainty regarding the organization's future cash flow, encouraging investors to make informed investment decisions in these banks or firms, which consequently affect their performance [51] and valuation [16, 35]. In addition, more up-to-date information regarding cybersecurity procedures in which banks disclose can signal more security against cyber risks and crimes and less probability for the steal of confidential information. This helps to convey trust to stakeholders and thus enhances the bank's performance.

From the perspective of clients or banks' customers, providing such cybersecurity disclosure provides trust to the bank clients about the safety of their money in the bank through sharing the efforts made by the management to secure their money and wealth, which positively affects the bank's performance [62, 81].

Based on the stakeholders' theory, stakeholders usually engage in continuous pressure on organizations for provision of different types of disclosures, including cybersecurity information, which is a new aspect of information during recent times [7, 71]. Banks and firms' disclosure of cybersecurity information and the adopted cyber risk management methods help to satisfy the stakeholders' information needs and make organizations avoid further pressures. Consequently, this helps in enhancing the banks or firms' reputation, and in enhancing the stakeholders' confidence [7] that improves performance.

Several previous research suggested that cybersecurity disclosure has an important role in improving organizational performance, lending support to the agency and signaling theory. For example, Gordon et al. [35] used publicly traded firms with annual reports filed with the US SEC (1641 disclosing firm-years and 19,266 non-disclosing firm-years) for the period from 2000 to 2004. They found that enterprises' voluntary disclosure of information security has a positive relationship with the market value of US firms. Furthermore, Berkman et al. [16] used 9677 firm-year observations of US companies in the period 2012–2016 and discovered a link between cybersecurity knowledge, as measured by the tone of cybersecurity disclosures, and market value for US enterprises. Wang et al. [83] proposed that the type of the firms' declared security risk indicators can assist forecast breach announcements. Using a sample of US publicly traded firms between 1997 and 2008, they found that the market reactions after security breach announcements varied based on the nature of the disclosure,

On the other hand, it has been argued that disclosing too much and specific confidential information about cybersecurity and the management measures and actions toward cyber risk may increase the possibility of cyberattacks [16, 84]. According to this point of view, the market may consider the firm's or banks' revelation of this detailed information about their information technology environment and management cybersecurity actions as proprietary information, which may make the market respond negatively [12]. As a result, this can negatively affect the firm's or bank's value and make them more vulnerable to cyberattacks, which can negatively affect their performance [84].

Considering the above-mentioned theoretical arguments and the cybersecurity disclosure literature, this paper follows the first point of view related to the agency and the signaling theory, assuming that more cybersecurity disclosure would increase the banks information transparency and reduce the uncertainty regarding cyber risk and its management inside the bank, which consequently affects positively the bank performance and its market value. Thus, we argue that cybersecurity disclosure may have a positive impact on the bank's performance. Accordingly, the first hypothesis is developed as follows:

H_1 Cybersecurity disclosure is positively associated with the banks' performance in the *MENA* region.

The moderating role of board size in the association between cybersecurity disclosure and bank performance

The BODs is a core component of CG mechanisms. Among the most important roles of the BODs, it is the provision of resources for the organization and the monitoring of management on behalf of the shareholders [43]. The BODS plays an important role in risk management, risk governance, and risk disclosure [52, 69]. However, the recent increase in cyberattacks and security risks made regulatory bodies call for the BODs to have a more active role in the monitoring and management of these cyber risks and their disclosure. The Securities Exchange Commission considers risk oversight an important role

of the BODs and requires firms to disclose the board's role in the oversight of risks and their impact on the business organization's strategy.

Based on the agency theory, effective BODs will monitor management effectively and attempt to reduce information asymmetry between them and the shareholders through the provision of different types of voluntary disclosure, including cyber risk and cybersecurity disclosures. Accordingly, the larger the board size, the more monitoring over management actions, the more management of potential risks is expected, and consequently, the more corporate disclosure [27, 73]. Similarly, based on the resource-based theory, a larger number of board members lead to a wide variety of experiences, education, knowledge, and opinions, which consequently improves the monitoring role of the board and enhances its risk management ability, affecting its performance positively with better levels of disclosure [27, 73, 74].

Several empirical research provides support for these theoretical approaches. For example, Elzahaby and Hussainey [27] used a sample of 72 UK firms and revealed that having a larger number of board members can improve decision making quality and disclosure levels due to the diversity of knowledge and skills. Adam et al. [2] shown that a larger board size leads to a wider range of knowledge and various perspectives, which improves the firm's disclosure policy. Hsu and Wang [44] used a sample of S&P 1500 firms from 1997 to 2009 and discovered that a greater board size correlates with a lower risk of security breaches. Beasley et al. [15] surveyed chief audit executives in Global audit information network in 2004. They noted that most financial institutions with varied boards would establish a comprehensive cybercrime strategy and stringent risk management procedures. Elshandidy and Neri [25] used a sample of 1890 firm-year observations and revealed that board size improves voluntary risk disclosure procedures in UK enterprises. As a result, a broader BOD with diversified experience is projected to increase banks' willingness to disclose cybersecurity information.

However, on the other side, it has been argued that larger board sizes with diverse attributes and dispersed points of view would lead to poor coordination, communication, and monitoring problems (known as the free-riding problem; [49]). This can negatively affect the monitoring, risk management duties, and corporate disclosure decisions. Supporting this point of view, Mazumder and Hossain [62] examined the association between board attributes (board size, independence, and gender diversity) and cybersecurity disclosure using 30 listed commercial banks in Bangladesh (with 210 bank-year observations). They showed that board size has no effect on cybersecurity disclosures in banks in Bangladesh. However, they found that board independence and gender diversity are associated with higher levels of cybersecurity disclosure. Lending et al. [53] used 271 data breaches in US over the period from 2004 to 2012 and found that firms with a large board size with less financial experience and who have experienced a breach tend to reduce the size of the board in a governance change after the breach. Al-Sartawi [10] used a sample of 94 listed firms in year 2018 in the MENA region and shoed that having more diverse board with IT knowledge and experience lad to better decisions when facing cyber threats.

Based on the above-mentioned theoretical claims and results of previous studies, it is concluded that the size of the BODs can affect either positively or negatively the cybersecurity disclosure and bank performance relationship. Accordingly, the second hypothesis is developed as follows:

H_{2a} The board of directors' size moderates the association between cybersecurity disclosure and banks' performance in the *MENA* region.

The moderating role of the information technology committee in the association between cybersecurity disclosure and bank performance

It has been argued that the BODs are not enough to address cybersecurity risks alone because not all of the board members have the suitable IT expertise to address and manage such types of risks and prevent cyber breaches [19, 30, 66]. Accordingly, many firms and banks have changed their ways of addressing cyber risks. This is done by appointing technology experts on the board or by delegating such tasks to separate committees, such as the board-level IT committee, audit committee, or risk committee. This is to help the board members oversee and manage cyber risk and complex technology issues [42]. According to the agency theory, effective board members lead to better monitoring of management with better corporate disclosure [27, 73]. Thus, it can be expected that having a separate board-level IT committee will lead to effective management over potential cyber risks and better monitoring of management with more corporate disclosure.

From the signaling theory perspective, management has private information about firm's information technology and the adopted cybersecurity disclosure. Thus, this provides a condition for sending signals to the market through the formation of board-level IT committee. Firms with board-level IT committees send a message to stakeholders that the oversight of cyber risk and cybersecurity is a priority at the board level [42].

According to a study by EY [31] on 76 Fortune 100 companies between 2018 and 2020, 87% of the firms surveyed allocated the monitoring of cybersecurity to an IT committee. This matches the resource-based theory, indicating that the existence of an IT committee with additional and diverse IT experience and technical knowledge would enhance the monitoring of cyber risks with their complex issues and related cybersecurity disclosures. For instance, Higgs et al. [42] used a sample of 634 reported breaches in US from 2005 to 2014. They showed that firms with board-level IT committees are more likely to disclose breaches than firms without IT committees. In addition, they found that firms with more mature IT committees are less likely to report a breach, indicating that a well-established and mature IT committee helps to prevent security breaches. Héroux and Fortin [41] examined the association between board attributes and cybersecurity disclosure level in 250 companies that were operating on the Canadian financial markets in year 2018. They concluded that the existence of a committee responsible for cybersecurity on the board level is essential for increasing their cybersecurity disclosures. In addition, their results show that other board of directors' attributes (board IT expertise, tenure, independence, female directors, and age) is associated with cyber security disclosure.

Based on the above discussion, it is expected that the board-level IT committee can positively affect the cybersecurity disclosure and bank performance relationship. Accordingly, the third hypothesis is developed as follows:

H_{2b} The existence of the IT Committee moderates the association between cybersecurity disclosures and banks' performance in the *MENA* region.

The moderating role of the chief risk officer in the association between cybersecurity disclosures and bank performance

Among the ways that firms and banks adopt to address risks, including cyber risk and its related cybersecurity disclosures, it is the appointment of a CRO, who adopts the responsibility of oversight of risk management issues and ensures an effective risk governance structure [28, 55]. Thus, CRO can enhance the BOD monitoring role over management actions helping in reducing the agency problem, according to the agency theory.

According to the signaling theory, firms tend to provide shareholders information about different aspects including risks and their management and help to improve stakeholders' decision making and firm valuation [16, 35]. The appointment of CRO serves as a sign that the firm is committed to risk management, including cyber risks. Firms and banks with a CRO at the board level with experience regarding different types of risks and a high level of technical experience can improve the risk management process [28] and reduce the likelihood of cybercrimes, leading to better performance. In addition, CROs have the necessary communication skills to report on enterprise risk management strategies and communicate such information to external stakeholders regarding the firm's risk profile, which consequently enhances corporate risk disclosure [55, 82]. Erin et al. [28] used 55 bank-year observations from 2012 to 2016 in Nigeria and showed that financial institutions need to hire CROs to be responsible for risk management within the institution, which is essential for an effective risk governance framework. Liebenberg and Hoyt [55] used US firms that have announced appointment of CRO between 1997 and 2001 (final sample of 26 firms) and found that highly leveraged firms are more likely to have a CRO. They interpreted such results as matching the assumption that firms appoint CROs to signal to lenders their commitment to enterprise risk management and provide more disclosure regarding the firm's risk profile. Viljoen et al. [82] examined 29 non-financial firms listed in top 40 indexed in the JSE securities exchange in South Africa in 2011. They provided evidence about firms that employed CROs and those with more frequent meetings of risk committee, which were found to have enhanced levels of risk disclosure.

However, on the other hand, it has been argued that the presence of a CRO is not enough to mitigate the risks faced by banks and firms, where all risk management capabilities should be available across all levels of management in the enterprise. Erin et al. [29] used 250 firm-year observations in the Nigerian financial sector for years 2013–2017. They found that the presence of a CRO does not necessarily reduce the impact of the risk on the enterprise, indicating that the existence of a CRO alone cannot sufficiently prevent the risks faced by enterprises today.

Based on the above discussion, it is expected that the existence of a CRO in the bank can affect the cybersecurity disclosure and bank performance relationship. Hence, the fourth hypothesis is developed as follows:

H_{2c} The existence of a CRO moderates the association between cybersecurity disclosure and banks' performance in the *MENA* region.

Research method

Sample and data collection

Although cyberattacks are a major threat to all types of enterprises, the frequency of the cyberattacks in the

banking sector is so frequent that it can be considered one of the most prominent risks faced by the banking industry. This can be due to the growing digitization of banking operations. Accordingly, this study uses a sample of listed banks in countries within the MENA region for the years 2019–2021. The selection of the time frame is due to the fact that in the early years, there was an absence of an internationally recognized approach for disclosing cyber risk in financial institutions, along with a lack of incentive for businesses to disclose such risks because of confidentiality matters, which resulted in limited information being disclosed. However, nowadays, with recent technological developments, the prioritization of cybersecurity risk governance regulations has emerged as a prominent concern within enterprises' governance goals. Thus, disclosure of cyber risk and cybersecurity information is a relatively recent development on the global scale [62, 78] and is in its early stages in the banking sector of MENA region countries.

Moreover, the study designates the timeframe (2019–2021) based on multiple factors. *First*, inadequate governance frameworks concerning cybersecurity may have exacerbated vulnerabilities during the COVID-19 pandemic, indicating a lack of norms governing cybersecurity disclosures prior to the pandemic. *Second*, the International Cybersecurity Strategy (2018–2021) was formulated in 2018 and implemented in 2019 with the strategic aim of mitigating cyber risks and fostering confidence in the communications and information infrastructure, applications, and services across various critical sectors, thereby ensuring a secure and dependable digital environment for Middle Eastern countries in all its domains. *Third*, following the COVID-19 pandemic, the Financial Stability Board (32) proposed measures to improve the regularity of cyber incident reporting. Upon implementation, these guidelines should assist countries in establishing an efficient incident reporting system that collects necessary information regarding cyber occurrences.

The sample includes 86 listed banks from 12 countries in the MENA region, yielding 256 bank-year observations from 2019 to 2021. Table 1 presents the sample composition by country. This study uses the annual reports and financial statements of banks available at Orbis Bank Focus database.

Table 1 The study' sample

Country	No. of banks	Percentage
Bahrain	6	6.9
Egypt	21	24.4
Iraq	4	4.7
Jordan	11	12.9
Kuwait	7	8.1
Lebanon	7	8.1
Morrocco	4	4.7
Oman	8	9.3
Qatar	6	7
Saudi Arabia	6	6.9
Tunis	2	2.3
United Arab Emirates	4	4.7
Final sample of banks	86	100

The study' variables

This section presents the variables used in this study, including the independent variable (cybersecurity disclosure), the dependent variable (return on assets; ROA), moderating variables (board size, presence of IT committee, and presence of a CRO), and control variables (capital adequacy ratio and bank size) as follows:

Independent variable: cybersecurity disclosure

To measure cybersecurity disclosure, this study adopts manual textual analysis using a list of 21 keywords that are developed based on prior studies (e.g. [36, 54, 62]). The list of keywords is provided in Table 2; where the textual analysis is done through counting the presence of cyber-related keywords in the banks' annual reports. Manual textual analysis enables considering the context of the sentence. To check the reliability of manual textual analysis, we rely on another researcher to manually count the cyber-related keywords in the sample banks' annual reports; where the same list of words was used and differences were reconciled.

Dependent variable

The dependent variable is bank performance, which is evaluated by return on assets (ROA). The ROA is determined by dividing net profit after taxes by total assets. ROA is an accounting-based indicator that reflects bank operating performance [14, 56]. In banking, ROA is utilized more commonly than return on equity (ROE).

Moderating variables

The increased frequency of cyberattacks and associated security threats has prompted authorities to place a greater emphasis on CG standards and the inclusion of particular disclosures. These disclosures concern the involvement of board members in risk monitoring, as well as the potential involvement of board committees [39, 52].

CG best practices and laws, notably in the banking industry, have focused on the board's risk management obligations, particularly in regard to cyber risk mitigation [72, 81]. As a result, three CG mechanisms are examined

Table 2 Cybersecurity list of keywords

"cyberattacks", "cybersecurity", "cybercrime", "cyber-risk", "swift-attacks/swift", "cyber-insurance", "internet_hacking", "online_crimes", cyber_dangers, "security-threat," "virus," "online-security," "online-threat," "security breach," "security-incident," "computer-virus," "system-security," "information-technology-security," "technology-risk," "technology-threat," "information-technology-risk".

to determine their moderation role in the cybersecurity disclosure-bank performance relationship: board size, as measured by the total number of board of directors' members; the presence of an IT committee, as measured by a dummy variable, and the presence of a CRO, as represented by a dummy variable.

Corporate governance requirements are influenced by board size, as larger boards of directors are more likely to develop a complete risk management system and follow the risk governance process [3, 9, 47]. Most financial institutions with diverse boards would develop a thorough cybercrime strategy and strict risk governance [29]. The presence of (CRO) in board rooms is essential, as they play a crucial role in effectively communicating risk management objectives and strategies to investors, and they have a main supervisory function to construct an effective risk governance framework [28, 55]. Since not every member of the board has the IT expertise to handle cybersecurity threats and stop breaches, financial institutions' boards of directors must set up efficient IT governance procedures to reduce cyber risks. This can be done by creating an independent IT committee [19, 72].

Control variables

Based on previous studies, this study uses controls bank-specific factors like bank size and capital requirements. Bank's size is measured by the natural logarithm of the bank's total assets. The impact of bank size on financial performance is a topic of academic debate, since it has been suggested that there is a positive relationship between bank size and performance. A capital requirement is measured by the capital adequacy ratio. According to Mandagie [57], banks have the potential to enhance their profitability by expanding their activities, provided that they have sufficient capital. The existence of insufficient assets has the potential to result in a rise in non-performing loans, thereby depleting the capital reserves of banks and affecting the banks' performance. The descriptions of the variables and related measures are shown in Table 3.

Empirical models

This study investigates the association between banks cybersecurity disclosure, bank performance, and the composition of governance tools as a moderator using panel data analysis. By starting to check the stationarity using Levin–Lin–Chu test, all the variables were found stationary at 90% confidence level. There was no need for differences or lags. For panel regression, the Hausman specification test was used to select the appropriate model; the fixed effect model (FEM) or the random effect model (REM). Hence, the results of the Hausman test

Table 3 Variables description

Variables	Description	Measurement	Prior studies
Independent variable			
CYSD_Score	Cybersecurity disclosure	Scores for cybersecurity disclosure based on content analysis of banks annual reports	Li et al. [54], Gordon et al. [36] , Mazumder and Hossain [62]
Dependent variable			
ROA	Bank performance	Net income after tax divided by total assets	Nahar et a.l [67], Harkati et al. [38] Mazumder and Hossain [62], Gatzert and Schubert [33]
Moderating variables			
BOD_Size	Board size	Total number of directors in the board	Mollah et al. [65], Jallali and Zoghlami [48], Nahar and Jahan [68], Mazumder and Hossain [62]
ITC	IT committee existence	Dummy variable which assigned a value of "1" IT committee if exists in BOD; and the value of "0" otherwise	Mollah et al., [65], Jallali and Zoghlami [48]
CRO_Presence	CRO presence	Dummy variable which assigned a value of "1" if CRO exists in BOD; and value the "0" otherwise	Mollah et al. [65], Jallali and Zoghlami [48]
Control variables			
Bank_Size	Bank size	Natural logarithm of bank total asset	Jallali and Zoghlami [48], [33], Nahar and Jahan [68]
CAR	Capital adequacy ratio	$\frac{(\text{Tier 1 Capital} + \text{Tier 2 Capital})}{\text{Risk weighted average assets}}$	Jallali and Zoghlami [48]

Table 4 Descriptive statistics of cybersecurity disclosure for the sample years

Year	Obs	Min	Max	Mean	SD
2019	86	0	0.78	0.170	0.181
2020	86	0	0.89	0.164	0.184
2021	86	0	0.89	0.196	0.203
2019–2021	258	0	0.89	0.177	0.189

Table 5 Descriptive statistics of other variables

	Minimum	Maximum	Mean	SD
CYSD_Score	0	0.89	0.177	0.189
ITC	0	1	0.440	0.498
BOD_Size	6	28	10.255	2.805
CRO_Presence	0	1	0.560	0.497
ROA	−0.181	0.312	0.028	0.041
Bank_Size	18.134	31.7187	24.115	2.6752
CAR	0.050	0.529	0.219	0.331
Observations	258			

indicate that the p value for Eqs. 1 and 2 is greater than 5% indicating that REM is the most suitable model [86].

To test H_1, banks' performance *ROA* is regressed on cybersecurity disclosure *CYSD_Score*, while controlling for bank's capital adequacy ratio *CAR*, bank size *Bank_Size*, Board Size *BOD_Size*, presence of CRO *CRO_presence,* and IT Committee presence *ITC*. Hence, the regression model is as follows:

$$\begin{aligned} ROA_{i,t} = \alpha &+ \beta_1 CYSD\_Score_{i,t} \\ &+ \beta_2 BOD\_Size_{i,t} \\ &+ \beta_3 CRO\_presence_{i,t} \\ &+ \beta_4 ITC + \beta_5 Bank\_Size_{i,t} \\ &+ \beta_6 CAR_{i,t} + \varepsilon t \end{aligned} \quad (1)$$

To test H_{2a}, H_{2b}, and H_{2c}, banks' performance *ROA* is regressed on cybersecurity disclosure *CYSD_Score*, while board size *BOD_Size*, presence of CRO *CRO_presence,* and IT Committee presence *ITC* are the moderating variables. The moderating effects are the matrix of interaction terms of cybersecurity disclosure and three CG mechanisms, i.e., *CYSD_Score*BOD_Size, CYSD_Score*CRO_presence, and CYSD_Score*ITC*. The control variables in model (2) are *CAR* and *Bank_Size*, which are bank's capital adequacy ratio and banks' size. Hence, the regression model is as follows:

$$\begin{aligned} ROA_{i,t} = \alpha &+ \beta_1 CYSD\_Score_{i,t} + \beta_2 BOD\_Size_{i,t} + \beta_3 CRO\_presence_{i,t} + \beta_4 ITC_{i,t} \\ &+ \beta_5 CYSD\_Score_{i,t} * BODSIZE_{i,t} + \beta_6 CYSD\_Score_{i,t} * CRO\_presence_{i,t} \\ &+ \beta_7 CYSD\_Scorei, t * ITC_{i,t} + \beta_8 Bank\_Size_{i,t} + \beta_9 CAR_{i,t} + \varepsilon t \end{aligned} \quad (2)$$

Results and discussion

Descriptive statistics

Table 4 presents the cybersecurity disclosure over the sample period (2019–2021) among listed banks in the MENA region. The mean of cybersecurity disclosure *CYSD_Score* is 17.7% with a maximum value of 89% and minimum of 0. However, cybersecurity disclosure for each of the years separately is increasing from 17% in 2019 to 19.6% in 2021, showing an increasing trend of cybersecurity disclosure over the years in the MENA region. This result is consistent with that reported in Mazumder and Hossain [62] related to the Bangladesh context, Berkman et al. [16] and Gatzert and Schubert [33] in the US context. This suggests a growing adoption of cyber technology in the globe in general and the MENA region, with a particular emphasis on the banking industry. This indicates an increased awareness among listed banks in the MENA region to provide more attention to this risk, which, in turn, is reflected in the increasing levels of cybersecurity disclosure.

With regard to IT committee, the results in Table 5 indicate that 44% of the sample banks in the MENA region have IT board-level committee. According to the International Risk Governance Council [46], IT committees are crucial risk governance tools for mitigating cybercrimes and increasing cyber risk disclosure. The BODs_size represents the number of directors on the board of the banks with a minimum of six members and a maximum of 28 members in the sample banks. The mean of CRO presence indicates that on average almost 56% of the banks in the sample have a separate CRO responsible for banks risk management strategy rather than a risk committee manager who is responsible for managing daily risk operations.

The ROA has an average of 2.8%, with a minimum value of -18.1% and a maximum value of 31.2%. It is unsurprising that a significant portion of the sample of banks in the Mena region experienced lowered profitability and occasional losses during the observed period, given the consequences of the COVID-19 pandemic. Furthermore, the mean of the bank size (as measured by natural logarithm of bank total assets) is 24.1. The bank's capital requirement *CAR* exhibits an average of 21.9% with minimum and maximum values of 5.01% and 52.9%, respectively,

Table 6 Pearson's correlation matrix

Variable	ROA	CYSD_Score	BOD-Size	ITC	CRO-Presence	Bank_Size	CAR
ROA	1						
CYSD_Score	0.183**	1					
BOD_Size	0.115*	0.029	1				
ITC	0.148**	0.030	0.055	1			
CRO-Presence	0.224**	0.056	0.011	0.108	1		
Bank_ Size	−0.312**	−0.062	−0.102	−0.097	−0.233	1	
CAR	−0.075	−0.027	0.105	−0.047	−0.077	0.017	1

**$p < 0.01$, *$p < 0.05$

Table 7 Random effect regression results

Variables	Coefficients	
	Model (1)	Model (2)
Dependent variable: ROA		
CYSD_Score	0.458* (0.268)	0.828* (0.460)
BOD_ Size	−0.025 (0.017)	−0.025 (0.017)
ITC	−0.024 (0.101)	−0.024 (0.101)
CRO_presence	0.196** (0.102)	0.264* (0.138)
*CYSD_Score *CRO_presence*		1.083** (0.561)
Bank _size	0.025 (0.018)	0.025 (0.019)
CAR	0.351** (0.146)	0.351** (0.147)
Cons	−0.138 (0.520)	−0.128 (0.543)
Year	Yes	Yes
Adjusted R^2	0.643	0.697
Prob > *F*	0.000	0.000
Observations	258	258

Standard errors are in parentheses, ***$p < 0.01$, **$p < 0.05$, and *$p < 0.10$.

indicating a significant degree of variation in capital adequacy ratio across sample banks.

Pearson's correlation

Table 6 shows Pearson's correlation matrix among the variables of the study. The correlation between cybersecurity disclosure *CYSD_Score* and bank performance *ROA* is positive and significant. In addition, the CG tools of board size *BOD_Size*, CRO existence *CRO_presence*, and IT Committee *ITC* are positively and significantly correlated with bank performance *ROA*. The correlation coefficients among the independent variable, the independent variable, and control variables are all below 0.7, indicating the absence of multicollinearity between variables.

Regression analysis

The impact of cybersecurity disclosure on bank performance

Regression results of model (1) and (2) are summarized in Table 7, Column (1) shows the regression results of model (1) examining the impact of cybersecurity disclosure *CYSD_Score* on bank performance *ROA* in the MENA region. The empirical model is well fitted, with an adjusted R^2 of 64.3%. The results show that the coefficient between *CYSD_Score* and *ROA* is positive and significant ($p < 0.10$). This suggests that banks with higher levels of cybersecurity disclosure will consequently have better performance. Hence, the first hypothesis is accepted. Such result supports the theoretical argument of the agency theory. More disclosure about cyber risk and cybersecurity information allows investors to access valuable information, mitigates uncertainties about bank performance, and reduces information asymmetry between managers and investors. Consequently, this reduces capital costs and attracts more investors, affecting the banks' performance and its valuation positively.

Furthermore, the results support the signaling theory suggesting that more cybersecurity disclosures provide signals to the market about how the management engages in mitigating and detection of cyber risks. Accordingly, this reduces the uncertainty regarding the banks' future cash flows, allowing investors to make sound decisions and attract more investors, which positively affects the banks' performance. The results are consistent with those of prior studies indicating that cybersecurity disclosure play an essential role in enhancing firms' value (e.g., [16, 35]) and help in predicting the security breach announcements (e.g., [83]).

Regression results show a significant positive association (at the 5% significance level) between the existence of CRO and bank performance *ROA*. The findings suggest that banks with CROs will be able to improve the risk management process and ensure effective risk governance [28, 55] which can reduce the likelihood of cybercrimes leading to a better performance. However, the coefficients of *BOD_Size* and presence of IT committee *ITC* with banks performance *ROA* are insignificant indicating that the number of BODs and IT committee has no impact on the banks' performance in the MENA region.

The *CAR* is positively and significantly associated with bank performance *ROA* (at the 5% significance level). This result is consistent with those of Wu et al. [85] and Ajayi et al. [4], who indicated that higher CAR indicates banks' ability to withstand financial downturns and unexpected losses. The asset portfolio also significantly impacts a financial institution's performance. Allocating resources to poor and high-risk assets hinders economic advancement, while diversifying investments over high-quality assets enhances overall performance. However, there is a positive but insignificant association between bank size and bank performance.

The moderating role of board size, IT committee, and CRO presence in the association between cybersecurity disclosure and bank performance

Column (2) of Table 7 shows the regression results of model (2) examining the moderating role of board size, IT committee, and CRO existence on the relationship between cybersecurity disclosures and bank performance in the MENA region. The adjusted R^2 of model (2), which includes a moderator variable, exhibited an increase from 64.3 to 69.7%. The observed improvement in performance implies that complying with risk governance tools, such as the CRO existence has a beneficial effect on bank performance and effectively addresses the potential risks linked to new threats.

The coefficients of *BOD_Size, ITC,* with *ROA* are negative and insignificant indicating that the number of members of BODs and IT committee has no impact on the bank's performance in the MENA region. Accordingly, the interaction terms of cybersecurity disclosure *(CYSD_Score*) with *BOD_Size* and presence of IT committee are not run in the regression model (2), as they cannot be considered as moderators for the cybersecurity disclosure-bank performance relationship. These results are inconsistent with the resource-based theory and the agency theory and some previous studies (e.g., [2, 25, 27, 52, 73]). This indicates that larger BODs with effective monitoring over management actions and with a wide variety of experiences do not appear to enhance the risk management ability of the board as well as the levels of disclosure, including cybersecurity disclosure and banks' performance. However, the results are in line with those of Mazumder and Hossain [62] which provide evidence that board size has no effect on cybersecurity disclosures in banks of Bangladesh. In addition, the results are inconsistent with prior studies showing that the existence of an IT committee is essential for increasing cybersecurity disclosure (e.g., [41, 42]). Accordingly, H_{2a} and H_{2b} are not supported.

The results show a significant positive association between both *CRO-presence* and the interaction term of CRO presence and cybersecurity disclosure *CYSD_Score*CRO_presence* with the banks' performance *ROA*, which means that H_{2C} is accepted. This result demonstrates that the presence of CROs plays a crucial role in risk governance, particularly in managing cybersecurity risks within the banking industry in the MENA region. The findings suggest that banks that have CROs serving at the board level, with expertise in many risks, are able to enhance the risk management process, which is consistent with the results of Erin et al. [28]. In addition, the results support the claims that CROs have the necessary communication skills to report on the institution's risk management strategies providing such information to external stakeholders and consequently enhancing the levels of corporate risk disclosure, which is consistent with Liebenberg and Hoyt [55] and Viljoen et al. [82].

Table 8 Fixed effect regression results

Variables	Coefficients	
	Model (1)	Model (2)
Dependent variable: Tobins_Q		
CYSD_Score	0.836* (0.455)	1.275* (0.669)
BOD_ Size	−0.091** (0.036)	−0.089** (0.037)
ITC	0.134(0.131)	0.145 (0.132)
CRO_presence	0.327** (0.156)	0.443** (0.203)
*CYSD_Score*CRO_presence*		1.397* (0.789)
Bank _Size	−0.085 (0.060)	0.082 (0.060)
CAR	0.082 (0.175)	0.087 (0.175)
Cons	3.479** (1.513)	3.433** (1.515)
Year	Yes	Yes
Adjusted R^2	0.461	0.489
Prob > *F*	0.000	0.000
Observations	258	258

Standard errors are in parentheses, ***$p < 0.01$, **$p < 0.05$, and *$p < 0.10$.

Robustness test

The robustness test is needed to ensure the reliability of the results of the regression models based on the variables selected. Hence, the robustness test is made by using Tobin's Q as an alternative measure of the dependent variable, banks' performance, instead of the ROA. The Hausman test resulted in the fixed effect model being the optimal model since it has a *p* value less than 0.05. The results of the regression mode1 (1) are reported in Table 8 and are the same as the main analysis of the random effect model in Table 7, where cybersecurity disclosure and the presence of CRO have a significant positive impact on ROA.

Conclusions, limitations, and recommendations for future research

Several studies have shown that cybersecurity disclosure can help banks reduce risk [16, 79] and improve performance [1, 13, 62, 81]. However, research regarding the banking sector in the MENA region is scarce. As a result, this study addresses a gap in the literature by investigating the influence of cybersecurity disclosure on bank performance in the countries in the MENA region. Furthermore, it seeks to investigate the moderating influence of several governance tools (BOD size, IT committee presence, and CRO existence, and) in the relationship between cybersecurity disclosure and bank performance. The findings indicate that the banks in the MENA region are becoming increasingly interested in disclosing cybersecurity information and that cybersecurity disclosure has a favorable and significant influence on bank performance. Furthermore, the findings show that having a CRO as a moderator improves the association between cybersecurity disclosure and bank performance, but it does not account for the influence of other moderating variables (BOD size and IT committee presence). The presence of a CRO plays a key role in identifying, assessing, and communicating cybersecurity risks in bank disclosures. Integrating cybersecurity procedures with risk management methods enhances transparency, builds stakeholder trust, and minimizes financial losses from cyberattacks.

The banking sector is currently receiving significant attention from various stakeholders, such as the public, regulators, media, and international agencies, due to its susceptibility to various risks. Therefore, we recommend that financial institutions adopt a more integrated, forward-looking, effective, and practical strategy for addressing the problem of cybercrimes and assaults. Additionally, implementing better board supervision, cultivating a robust risk culture, enhancing risk responsibility, and promoting enhanced risk transparency can significantly mitigate the risk posed by cybercrime. Hence, this paper contributes toward the advancement of cybersecurity within the industry by highlighting the significance of the monitoring functions of the board and CRO. The implications of the study's findings may have practical significance for banks and policymakers in their efforts to effectively manage cyber risks and enhance bank performance. This study pinpoints the current practices of cybersecurity disclosure among the banking regulators in the MENA region, with the objective of minimizing information asymmetry, maintaining public trust, and identifying potential risks of financial distress through regulatory guidance. Banks and policymakers should consider integrating cybersecurity or technological expertise into their boards to enhance their understanding of cyber risks and to strengthen disclosure practices. Such diversity in board members enables the board to evaluate potential threats and formulate appropriate policies to mitigate them. It is advisable for policymakers in the MENA region to prioritize the improvement of information disclosure regarding cyber risk, cybersecurity information, and governance strategies within the banking sector. We propose that stakeholders engage in voluntary information exchange about cyber events among market participants. Regulatory entities have the ability to create taxonomies for risks and occurrences, as well as impose reporting requirements, to assess the current or possible consequences for the continued supply of critical services. Finally, it is advised that an information and communication technology (ICT) strategy and risk framework be developed, which should include incident response strategies and a clearly defined hierarchy for making crucial business decisions.

However, as is the case in studies related to disclosure, this study has some limitations that provide avenues for additional research. *First*, the study is limited to only three governance tools; future research may add other governance tools like risk committee characteristics, demographic characteristics of CRO, and risk management tools. Future research could explore additional factors, such as the ownership structure of banks and the cost of capital, which may impact cybersecurity disclosure practices and their associated financial outcomes. *Second*, future research should evaluate the impact of cybersecurity disclosure on bank performance from a market perspective. *Third*, the scope of this research was limited to banks operating in the MENA region. Although this study lays the groundwork for future empirical research in this area, it is recommended that a study be conducted on the comparative analysis of countries in the MENA region in relation to other continents around the world, with a particular focus on cybersecurity disclosure and governance tools. *Fourth,* to measure cybersecurity disclosure, we use a manual textual analysis to count the presence of cyber-related keywords in banks' annual reports. We focused on specific key words related to the occurrence of cyberattacks and their related terminology. However, future research could incorporate additional terms such as "governance risk" and "strategy risk" that are pertinent within the broader framework of risk management and governance practices. Also future research could expand on this by utilizing automated content analysis to examine the frequency of cybersecurity disclosures based on keyword counts. Additionally, focusing on the quality of annual reports, a more meaning-focused approach by conducting discourse analysis of cybersecurity disclosure narratives exploring the relevance of cybersecurity disclosure language to stakeholder

decisions could also be used by future research. *Fifth*, limited sample period (2019–2021) for cybersecurity disclosures in the MENA region banking sector. We selected this period based on the availability of reliable data, the notable increase in cyberattacks, and the implementation of regulatory measures during these years. We recognize that an extended timeframe could offer a more thorough understanding of the dynamic environment of cybersecurity disclosures, particularly in light of continuous technological improvements and heightened regulatory scrutiny in this field. Further research is needed to expand the dataset beyond 2021 to include more contemporary patterns and developments in cybersecurity disclosure. Such an approach would provide profound insights into how enterprises' disclosures evolve in response to emerging cyber threats and changing regulatory requirements, especially after the COVID-19 pandemic. *Finally,* this study relies on the content analysis of annual reports; however, we recommend combining quantitative content analysis with qualitative methods like interviews to gain a more comprehensive understanding of banks' cybersecurity disclosures. This approach could involve conducting interviews with board members, Chief Risk Officers (CROs), cybersecurity officers, and compliance officers to gain insights into the decision making processes behind these disclosures.

Abbreviations

CRO	Chief risk officer
IT	Information technology
BOD	Board of directors
ROA	Return on assets
ROE	Return on equity
FEM	The fixed effect model
REM	The random effect model
CYSD	Cybersecurity disclosure
CAR	Capital adequacy ratio

Acknowledgements
We thank the editor and the anonymous reviewers for their constructive comments.

Author contributions
TI developed the original draft, helped in methodology, edited and reviewed the draft, and made constructive changes to the draft. DE prepared the original draft as well as reviewing the literature. EA collected the data, analyzed the results, and concludes the draft. All authors have read and approved the manuscript.

Funding
The authors received no specific funding.

Availability of data and materials
Secondary sources of data as annual reports and financial statements of banks in the MENA region are collected from Orbis Bank Focus database https://bib.kuleuven.be/english/ebib/collection/data/databases/orbis_bank_focus.

Declarations

Ethics approval and consent to participate
Not applicable.

Consent for publication
Not applicable.

Competing interests
The authors declare that they have no conflict of interest.

Received: 16 July 2024 Accepted: 29 October 2024
Published online: 14 November 2024

References

1. Acharya VV, Ryan SG (2016) Banks' financial reporting and financial system stability. J Account Res 54(2):277–340
2. Adam R, Almeida H, Ferreira D (2005) Powerful CEOs and their impact on corporate governance. Rev Financ Stud 18(4):1403–1432
3. Aebi V, Gabriele S, Markus S (2012) Risk management, corporate governance, and bank performance in the financial crisis. J Bank Finance 36(12):3213–3226
4. Ajayi SO, Ajayi HF, Enimola DJ, Orugun FI (2019) Effect of capital adequacy ratio (CAR) on profitability of deposit money banks (DMB's): a study of DMB's with International operating license in Nigeria. Res J Finance Account 10(10):84–91
5. Akinbowale OE, Klingelhöfer HE, Zerihun MF, Mashigo P (2024) Development of a policy and regulatory framework for mitigating cyberfraud in the South African banking industry. Heliyon 10(1):1–17
6. Al Balushi, M. (2017). Regulating Cybersecurity in Corporate America. Specific Reference to Corporate Espionage. Specific Reference to Corporate Espionage.(September 14, 2017).
7. 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, 1-19.
8. Al-Hadi A, Al-Abri A (2022) Firm-level trade credit responses to COVID-19-induced monetary and fiscal policies. Res Int Bus Finance 60(7):1–11
9. Al-Hadi A, Hasan MM, Habib A (2016) Risk committee, firm life cycle, and market risk disclosures. J Corp Gov Int Rev 24(2):145–170
10. Al-Sartawi AMM (2020) Information technology governance and cybersecurity at the board level. Int J Crit Infrastruct 16(2):150–161
11. Alsheikh A, Hassan M, Mohd-Saleh N, Abdullah M, Alsheikh W (2021) Firm's size, mandatory adoption of IFRS and corporate risk disclosure among listed non-financial firms in Saudi Arabia. J Account Finance 17(2):1–28
12. Amir E, Levi S, Livne T (2018) Do firms underreport information on cyber-attacks? Evidence from capital markets. Rev Account Stud 23:177–1206
13. Baumann U, Nier E (2004) "Disclosure, volatility, and transparency: an empirical investigation into the value of bank disclosure. Econ Policy Rev 10(4):31–45
14. Battaglia F, Gallo A (2015) Risk governance and Asian bank performance: an empirical investigation over the financial crisis. Emerg Mark Rev 25:53–68
15. Beasley MS, Clune R, Hermanson DR (2005) Enterprise risk management: an empirical analysis of factors associated with the extent of implementation. J Account Public Policy 24(6):521–531
16. Berkman H, Jona J, Lee G, Soderstrom N (2018) Cybersecurity awareness and market valuations. J Account Public Policy 37(6):508–526
17. Botosan CA (1997) Disclosure level and the cost of equity capital. Account Rev 72(3):3323–3349
18. Bouhamdan RF, Mostapha N, Hegazy W (2023) Corporate governance and anti-corruption disclosure: evidence from MENA region. Eur J Sci Innov Technol 3(2):122–136
19. Calderon TG, Gao L (2022) Changes in corporate cybersecurity risk disclosures after SEC comment letters. J Account Public Policy 41(5):106993
20. Campbell K, Gordon LA, Loeb MP, Zhou L (2003) The economic cost of publicly announced information security breaches: empirical evidence from the stock market. J Comput Secur 11(3):431–448
21. Canadian Securities Administrators (CSA) (2016) CSA staff notice 11-332: cyber security, Montreal, Canada. https://www.bcsc.bc.ca/-/media/PWS/Resources/Securities_Law/Policies/Policy1/11332-CSA-Staff-Notice-September-27-2016.pdf

22. Canadian Securities Administrators (CSA) (2017) Multilateral staff notice 51-347: disclosure of cybersecurity risks and incidents, Montreal, Canada. https://www.osc.ca/sites/default/files/pdfs/irps/20170119_51-347_disclosure-cyber-security.pdf
23. Canadian Securities Administrators (CSA) (2013) CSA Staff Notice 11-326: cybersecurity, Montreal, Canada. https://www.bcsc.bc.ca/-/media/PWS/Resources/Securities_Law/HistPolicies/HistPolicy1/11326-CSA-Staff-Notice.pdf
24. Central Bank of Bahrain (2020) Risk Management Framework, CCB Rulebook, Bahrain. Available at: https://cbben.thomsonreuters.com/rulebook/om-1228. Accessed 15 Jun 2024.
25. Elshandidy T, Neri L (2015) Corporate governance, risk disclosure practices, and market liquidity: comparative evidence from the UK and Italy. Corp Gov Int Rev 23(4):331–356
26. Elzahaby MA (2023) Corporate narrative disclosure practices in the Middle East and North Africa (MENA) region: a systematic literature review. Int J Discl Gov 20(3):296–315
27. Elzahar H, Hussainey K (2012) Determinants of narrative risk disclosures in UK interim reports. J Risk Finance 13(2):133–147
28. Erin O, Asiriuwa O, Olojede P, Ajetunmobi O, Usman T (2018) Does risk governance impact bank performance? Evidence from the Nigerian banking sector. Acad Account Financ Stud J 22(4):1–14
29. Erin OA, Kolawole AD, Noah AO (2020) Risk governance and cybercrime: the hierarchical regression approach. Future Bus J 6:1–15
30. EY (2018) SEC guidance on cybersecurity: board considerations. https://assets.ey.com/
31. EY (2020) What companies are disclosing about cybersecurity risk and oversight in 2020. EY Center for Board Matters. https://ey.com/us/boardmatters
32. Financial Stability Board (2020) Effective Practices for Cyber Incident Response and Recovery: Final Report. Available at: https://www.fsb.org/uploads/P191020-1.pdf. Accessed 19 Jun 2024.
33. Gatzert N, Schubert M (2022) Cyber risk management in the US banking and insurance industry: a textual and empirical analysis of determinants and value. J Risk Insur 89(3):725–763
34. Groenendaal J, Helsloot I (2021) Cyber resilience during the COVID19 pandemic crisis: a case study. J Conting Crisis Manag 29(4):439–444
35. Gordon LA, Loeb MP, Sohail T (2010) Market value of voluntary disclosures concerning information security. Manag Inf Syst Q 34(3):567–594
36. Gordon LA, Loeb MP, Lucyshyn W, Zhou L (2015) Increasing cybersecurity investments in private sector firms. J Cybersecur 1(1):3–17
37. Gordon LA, Loeb MP, Zhou L (2011) The impact of information security breaches: has there been a downward shift in costs? J Comput Secur 19(1):33–56
38. Harkati R, Alhabshi SM, Kassim S (2020) Does capital adequacy ratio influence risk-taking behaviour of conventional and Islamic banks differently? Empirical evidence from dual banking system of Malaysia. J Islam Account Bus Res 11(9):1989–2015
39. Hartmann CC, Carmenate J (2021) Academic research on the role of corporate governance and IT expertise in addressing cybersecurity breaches: implications for practice, policy, and research. Curr Issues Audit 15(2):A9–A23
40. Healy PM, Palepu KG (2001) Information asymmetry, corporate disclosure, and the capital markets: a review of the empirical disclosure literature. J Account Econ 31(1–3):405–440
41. Héroux S, Fortin A (2022) Board of directors' attributes and aspects of cybersecurity disclosure. J Manag Gov 28:359–404
42. Higgs J, Pinsker RE, Smith TJ, Young GR (2016) The relationship between board-level technology committees and reported security breaches. J Inf Syst 30(3):79–98
43. Hillman AJ, Dalziel T (2003) Boards of directors and firm performance: integrating agency and resource dependence perspectives. Acad Manag Rev 28(3):383–396
44. Hsu C, Wang T (2014) Exploring the association between board structure and information security breaches. Asia Pac J Inf Syst 24(4):531–557
45. International Finance Corporation (IFC) (2021) Corporate governance in MENA: building a framework for transparency and accountability. Washington, DC: World Bank Group. https://www.ifc.org
46. International Risk Governance Council (IRGC) (2005) White paper no. 1: risk governance—towards an integrative approach. https://irgc.org/risk-governance/irgc-risk-governance-framework
47. Ismail TH, Ahmed EA (2022) Impact of risk governance on performance and capital requirements: evidence from Egyptian banks'. Corp Ownersh Control 19(2):179–193
48. Jallali S, Zoghlami F (2022) Does risk governance mediate the impact of governance and risk management on banks' performance? Evidence from a selected sample of Islamic banks. J Financ Regul Compliance 30(4):439–464
49. Jensen MC, Meckling WH (1976) Theory of the firm: managerial behavior, agency costs and ownership structure. J Financ Econ 4(4):305–360
50. Karim S, Naeem MA, Mirza N, Paule-Vianez J (2022) Quantifying the hedge and safe-haven properties of bond markets for cryptocurrency indices. J Risk Finance 23(2):191–205
51. Khlif H, Hussainey K (2016) The association between risk disclosure and firm characteristics: a meta-analysis. J Risk Res 19(2):181–211
52. Kure HI, Islam S, Razzaque MA (2018) An integrated cyber security risk management approach for a cyber-physical system. Appl Sci 8(6):1–29
53. Lending C, Minnick K, Schorno PJ (2018) Corporate governance, social responsibility, and data breaches. Financ Rev 53(2):413–455
54. Li H, No WG, Wang T (2018) SEC's cybersecurity disclosure guidance and disclosed cybersecurity risk factors. Int J Account Inf Syst 30:40–55
55. Liebenberg AP, Hoyt RE (2003) The determinants of enterprise risk management: evidence from the appointment of chief risk officers. Risk Manag Insur Rev 6(1):37–52
56. Lundqvist SA, Vilhelmsson A (2018) Enterprise risk management and default risk: evidence from the banking industry. J Risk Insur 85(1):127–157
57. Mandagie Y (2021) Analyzing the impact of CAR, NIM and NPL on ROA of banking companies: an empirical study on BEI listed companies). INQUISITIVE Int J Econ 1(2):72–87
58. Mangelsdorf ME (2017) What executives get wrong about cybersecurity. MIT Sloan Manag Rev 58(2):21–24
59. Maside-Sanfiz JM, Iglesias-Casal A, Mazahreh QAS, López-Penabad MC (2024) The impact of competition on environmental and social performance in the MENA banking sector. Corp Soc Responsib Environ Manag 31(4):2589–3684
60. Mateev M, Sahyouni A, Tariq MU (2023) Bank regulation, ownership and risk-taking behavior in the MENA region: policy implications for banks in emerging economies. Rev Manag Sci 17(1):287–338
61. Mawgoud, A.A., Taha, M.H.N., Khalifa, N.E.M., Loey, M. (2020), "Cyber Security Risks in MENA Region: Threats, Challenges and Countermeasures", Hassanien, A., Shaalan, K., Tolba, M. (Eds), *Proceedings of the International Conference on Advanced Intelligent Systems and Informatics 2019, Advances in Intelligent Systems and Computing*, Springer, Cham, 912-921.@@@
62. Mazumder MMM, Hossain DM (2023) Voluntary cybersecurity disclosure in the banking industry of Bangladesh: does board composition matter? J Account Emerg Econ 13(2):217–239
63. Meisner M (2017) Financial consequences of cyber-attacks leading to data breaches in healthcare sector. Copernic J Finance Account 6(3):63–73
64. Modi SB, Wiles MA, Mishra S (2015) Shareholder value implications of service failures in triads: the case of customer information security breaches. J Oper Manag 35:21–39
65. Mollah S, Hassan MK, Al Farooque O, Mobarek A (2017) The governance, risk-taking, and performance of Islamic banks. J Financ Serv Res 51:195–219
66. National Association of Corporate Directors (NACD) (2012) Cybersecurity and the board. In: NACD board leadership conference, Arlington, VA
67. Nahar S, Azim M, Jubb C (2016) The determinants of risk disclosure by banking institutions: evidence from Bangladesh. Asian Rev Account 24(4):426–444
68. Nahar S, Jahan MA (2021) Do risk disclosures matter for bank performance? A moderating effect of risk committee. Account Europe 18(3):378–406
69. Pagach D, Warr R (2011) The characteristics of firms that hire chief risk officers. J Risk Insur 78(1):185–211
70. Pham L, Karim S, Naeem MA, Long C (2022) A tale of two tails among carbon prices, green and non-green cryptocurrencies. Int Rev Financ Anal 82(3):102–139
71. Radu C, Smaili N (2022) Board gender diversity and corporate response to cyber risk: evidence from cybersecurity related disclosure. J Bus Ethics 177(2):351–374

72. Rahman MB, Karim T, Chowdhury IU (2021) Role of boards in cybersecurity risk profiling: the case of Bangladeshi commercial banks. Glob J Manag Bus Res 21:49–58
73. Saggar R, Singh B (2017) Corporate governance and risk reporting: Indian evidence. Manag Audit J 32(450):378–405
74. Samaha K, Khlif H, Hussainey K (2015) The impact of board and audit committee characteristics on voluntary disclosure: a meta-analysis. J Int Account Audit Tax 24:13–28
75. SEC (2011) Cf disclosure guidance: Topic no. 2. https://www.Sec.Gov/divisions/corpfin/guidance/cfguidance-topic2.Htm
76. SEC (2018) Commission statement and guidance on public company cybersecurity disclosures. https://www.Sec.Gov/rules/interp/2018/33-10459.Pdf
77. SEC (2023) Cybersecurity risk management, strategy, governance, and incident disclosure. https://www.sec.gov/rules/2022/03/cybersecurity-risk-management-strategy-governance-and-incident-disclosure#33-11216
78. Skinner CP (2019) Bank disclosures of cyber exposure. Iowa Law Rev 105(1):239–281
79. Smaili N, Radu C, Khalili A (2023) Board effectiveness and cybersecurity disclosure. J Manag Gov 27(4):1049–1071
80. Tariq N (2018) Impact of cyberattacks on financial institutions. J Internet Bank Commer 23(2):1–11
81. Uddin MH, Ali MH, Hassan MK (2020) Cybersecurity hazards and financial system vulnerability: a synthesis of literature. Risk Manag 22(4):239–309
82. Viljoen C, Bruwer BW, Enslin Z (2016) Determinants of enhanced risk disclosure of JSE top 40 companies: the board risk committee composition, frequency of meetings and the chief risk officer. South Afr Bus Rev 20(1):208–312
83. Wang Y, Kannan K, Ulmer J (2013) The association between the disclosure and the realization of information security risk factors. Inf Syst Res 24(2):201–218
84. Wang T, Yen JC, Yoon K (2022) Responses to SEC comment letters on cybersecurity disclosures: an exploratory study. Int J Account Inf Syst 46:100567
85. Wu N, Zhao J, Musah M, Ma Z, Zhang L, Zhou Y, Li K (2023) Do liquidity and capital structure predict firms' financial sustainability? A panel data analysis on quoted non-financial establishments in Ghana. Sustainability 15(3):1–22
86. Zainodin HJ, Yap SJ (2013) Overcoming multicollinearity in multiple regression using correlation coefficient. In: AIP conference proceedings, American Institute of Physics, vol 1557, pp 416–419
87. Zeng Q, Pu S, Zhang X (2020) Statistical tests for integrity attacks on cyber physical systems. Asian J Control 22(1):600–605

Publisher's Note

Dalia Hussein Elsayed is currently an Assistant lecturer of accounting at the Faculty of Management Sciences in October University for Modern Sciences and Arts (MSA), Egypt. She earned her master's degree and PhD in accounting from the Faculty of Commerce, Cairo University, Egypt and her PhD thesis was about using tone management in corporate narrative disclosures in detecting a firm's earnings management and assessing earnings quality. Besides this, academic background, she has working experience in banking and taxation services. She has written a number of research papers and published several articles in esteemed journals, such as the Journal of Applied Accounting Research. Her research interest is in the area of financial reporting, corporate narrative reporting, corporate governance, and corporate disclosure.

Tariq H. Ismail is a Professor of Accounting at the Faculty of Commerce, Cairo University, Egypt. He is currently the Dean of Business School at the International Academy of Engineering and Media Science, Egypt. He has published numerous articles in a number of high-ranked, peer-reviewed journals listed in Clarivate Analytics Emerging Markets Index, SCOPUS, the Australian Business Deans Council quality list, and has many books which had worldwide audience. He had many research grants and excellence awards for the contributions he made in his field. He is the founder and the editor of the Academy Journal of Social Sciences, as well as, the associate editor of Journal of Humanities and Applied Social Sciences. He is on the editorial board of several reputable journals. His current research focuses on disclosure quality and financial reporting, accounting in emerging economies, and corporate governance.

Eman Adel Ahmed is an Assistant lecture at the Department of Accounting, Faculty of Management Sciences, October University for Modern Sciences and Arts (MSA), Egypt. Her research interest is covers risk governance, capital requirements, disclosure strategies in the banking sector. Her research papers have published in refereed reputable journals as Journal of Applied Accounting Research, and Corporate Ownership & Control.