Pak. j. life soc. Sci. (2024), 22(1): 3964-3977 E-ISSN: 2221-7630;P-ISSN: 1727-4915

Pakistan Journal of Life and Social Sciences
www.pjlss.edu.pk

https://doi.org/10.57239/PJLSS-2024-22.1.00291

RESEARCH ARTICLE

The Impact of the Board of Directors on the Cybersecurity Risks in the Iraqi Banking Sector

Mousa Nayyef Omairah Al-Yasari[1*], Moufida Ben Saada[2]

[1]Research Unit Accounting, Finance and Economic Modeling (MOCFINE), Higher Institute of Accounting and Business Administration, Manouba University, Tunisia
[2]Research Unit Accounting, Finance and Economic Modeling (MOCFINE), Higher Institute of Computing Science and Management, Kairouan University, Tunisia

ARTICLE INFO

Received: May 22, 2024

Accepted: Jul 10, 2024

Keywords

Governance

Cybersecurity risks

Board of directors

Audit committee

Internal audit

***Corresponding Author:**

muosaaltaee@gmail.com

ABSTRACT

By analyzing the effects of the board features on cybersecurity risks, the study sought to quantify the Effect of the board of directors on banks listed on the Iraq Stock Exchange. The attributes of the audit committee (size, independence, and technological knowledge) and the board (member diversity, size, and independence) Served as representations of the governance systems. The researcher employed a descriptive-analytical methodology, which is suitable for this type of study, along with the research design and approach used, the study population, and the sample of the study comprising 21 banks listed on the Iraq Stock Exchange's regular market, with a sample size of 189 individuals. The researcher concluded that banks with larger boards, independence, gender diversity, and technological expertise tend to have lower levels of cybersecurity risk. Additionally, banks with audit committees that have many members, independence, and technological expertise also experience lower cybersecurity risks. Furthermore, banks with a Chief Information Officer (CIO), a Chief Cybersecurity Officer (CCO), and an IT risk management committee that includes technology experts in their senior and executive management tend to have lower levels of cybersecurity risk. Efficient and high-quality internal auditing also contributes to reducing cybersecurity risks for these banks. The researcher recommended that banks should strengthen their boards and audit committees with expertise and qualifications in information and communication technology. It was also suggested that banks conduct training sessions on cybersecurity specifically for board members and generally for bank employees. Additionally, it was advised that banks establish cybersecurity risk committees at the executive management level or board level, if possible.

INTRODUCTION

Through the daily exchange of enormous volumes of sensitive data and transactions over the Internet, the banking industry plays a critical role in controlling the world economy. The banking industry uses digital technology for Internet and mobile banking to increase productivity, customer service, and transaction security (Johari, 2023). The sector is dealing with serious cybersecurity risks brought on by increased connectivity and reliance on digital platforms, which make it difficult to protect sensitive customer data, secure transactions, and halt fraudulent activities. To effectively combat these threats as cybercriminals become more skilled, institutions must employ cutting-edge

technologies. The sector constantly battles a variety of threats, such as ransomware, spyware, phishing schemes, and data breaches. (Thammareddi, et al., 2023).

The potential that information and communication technology offer pose significant hurdles for banking organizations, as highlighted by the Arab Monetary Fund. Information technology is always evolving, bringing with it new risks as well as new offerings and methods of customer communication. ICTs with malicious intent can undermine trust and security, obstruct essential financial services, and jeopardize the stability of the financial system. (Ismail, 2018: 1).

The importance of cybersecurity in the financial sector has been underscored by increased susceptibility to cyber-attacks and breaches. Beyond just information security, cybersecurity seeks to safeguard the information space. It entails protecting user property and the operational environment against outside interference. By differentiating between destructive threats like denial-of-service (DoS) attacks and non-damaging threats like system disruptions brought on by programming errors or lost internet connections, cybersecurity shields systems from dangers that arise in cyberspace. (Kala, 2023)

Cybersecurity risks have significantly altered the banking operations model due to their capacity to impair banking operations and inflict significant direct and indirect costs over several decades. Cyber risks can harm the security and integrity of critical information infrastructure, exploiting existing vulnerabilities to affect information system safety. The Financial Stability Board (FSB) defines cyber risks as a combination of the likelihood and impact of cyber incidents, which can compromise information system security or violate security policies Uddin, et al. (2020)

Managing and monitoring cybersecurity is crucial for supporting and protecting critical business information. Recognizing the threats posed by cyber risks, regulatory authorities worldwide have taken action to mitigate cyber threats' effects on the banking industry. Arab central banks have released guidelines for banks to strengthen their defenses against cyberattacks. Traditionally, information security and cybersecurity were viewed as technical matters within the bank's strategic level, with IT departments responsible for securing information capital. However, including cyber risks within operational risks is insufficient, as banking regulatory standards require banks to integrate cyber risk management strategies and policies, regularly reviewed by boards of directors. Ismail, N. (2018).

THERMOTICAL FRAMEWORK, LITERATURE REVIEW, AND ~~STUDY~~ HYPOTHESES

Banks face various risks, including traditional ones such as credit, liquidity, exchange rate, operational, and legal risks. The use of information technology has increased and altered some traditional risks associated with banking activities, leading to new forms of risks in electronic banking transactions. These include operational and strategic risks arising from poor planning and execution of a bank's electronic strategy, operational risks from the lack of integration in electronic banking systems, reputational risks from a bank's failure to meet customer needs, and legal risks from not understanding laws when dealing with customers from other countries or related to electronic contracts and signatures, among others (Hanim, 2017).

Because banks rely so significantly on the data they handle, it has been demonstrated that cyber-attacks disrupt these activities by having an impact on financial information and communication technologies. Banks in the financial sector rely on their technical infrastructure to provide most of their goods and services to clients directly. Multiple points of contact with external parties typically increase vulnerabilities that can be exploited in cyberattacks, serving as entry points to the banking system and causing disruptions in the financial system. Several factors contribute to cyber risks in financial institutions, including the increasing trend toward globalization, the early adoption and reliance on rapidly evolving technology, significant interdependencies within the financial system

and IT infrastructure, the growing sophistication of cybercriminals, and the inherent nature of financial institutions' business and services (Crisanto, et al., 2023: 3).

Moreover, the size and complexity of IT infrastructure in financial institutions make it impossible to provide complete protection and eliminate cyber risks. Therefore, cyber incidents may be highly inevitable. Cyber incidents can potentially weaken financial institutions' operational capabilities to the extent that they threaten their continuity or ability to continue operations. Herrera, et al. (2021: 174)

Because the global financial sector depends so heavily on information and communication technology for its operations and services, banks and other financial institutions are more vulnerable to unavoidable systemic cyber hazards. The entire financial system can be brought down by a single breach in a banking network, which would have direct repercussions for all banks and financial organizations. Financial institutions depend heavily on information systems to carry out their operations and plans. Basic weaknesses might give rise to a lot of cyber hazards. This can impair the business's operational and financial capabilities and possibly jeopardize its survival. Cyber threats can spread among financial organizations due to the high degree of dependency and connectivity among its components. Thus, in its most severe manifestations, cyber risk can jeopardize the stability of the financial system. (Herrera, et al., 2021: 167).

These risks can take various aspects, from the interruption of commercial operations to the theft of market data or sensitive personal information, jeopardizing data integrity, or damaging system hardware and software of the banking system in Iraq, along with its structure, has been closely tied to political, economic, and social developments, which have been reflected in its functions and activities. The banking system has gone through multiple stages since its inception in 1892, leading to the establishment of the first national governmental bank in 1935 and specialized banks by 1956. The Central Bank was tasked with monetary policy under Law No. 72 of 1956. Despite the presence of private or foreign banking institutions, Law No. 100 on the nationalization of banks was enacted in 1964, sparking widespread debate about the development and structure of the banking system. Commercial banks became state-owned to serve economic development and achieve effective supervision by the Central Bank. (Peihani, 2022: 140).

In the 1990s, the institutional structure of banks changed but retained its nature. The period since 1995 was significant in the evolution of the banking industry in Iraq, transitioning from an era of monopoly by five governmental banks to a period of banking plurality. Decision No. 142, issued under Law No. 12 of 1991, and amended Central Bank Law No. 64 of 1976, allowing the establishment of private banks under the provisions of Law No. 36 of 1981 and later under Company Law No. 21 of 1997. This law changed the competitive environment in the sector. The Central Bank was also allowed to grant licenses for private companies to engage in foreign currency trading to create a competitive environment. The number of currency trading companies increased significantly across Iraq following Decision No. 16 of 2001, which increased the capital of currency trading companies. The period from 1996 to 2003 was marked by allowing banks to fully operate. Decision No. 9 of 1996 brought a clear change in the structure of the bank, and Law No. 22 of 1997 permitted comprehensive banking activities and participation in establishing joint-stock companies. Investment Companies Regulation No. 5 of 1998 allowed the Central Bank to grant licenses for all forms of financial investment, including stocks, bonds, deposits, and loans. From 2003 to the present, there have been numerous changes in economic and financial policies and efforts to develop the financial sector through concrete measures. Despite unstable economic, social, and political conditions, the private banking sector has started to find its place and strengthen its financial capabilities (Abdelrahim, 2022).

Literature Review

The Securities and Exchange Commission (SEC) mandates that companies disclose their role in managing cybersecurity risks that have the potential to disrupt and materially affect the company. The SEC views cybersecurity risk oversight as a core duty of the board of directors. However, because there aren't enough scientific techniques to identify and evaluate the severity of these hazards, many organizations and institutions are unaware of the cybersecurity risks they face. (Mbanaso, et al., 2019: 5). Companies have started adding technology experts to their boards or forming board-level technology committees to help oversee cybersecurity and technological issues to address the risks and costs associated with security breaches and to recognize the value of having IT experts on the board. In other situations, the audit committee or a different risk committee is tasked with supervising cybersecurity and IT duties. (Higgs, et al., 2016).According to theory, agency theory emphasizes a risk management technique that might lessen agency issues (Berger, et al., 2005). However, for the board to keep an eye on risky managerial behavior and prevent any agency issues that can impair the bank's performance, board competence is crucial. (Schnatterly, et al., 2021). Assessing board competence from the standpoint of resource dependence theory might reveal its significance as a resource. This knowledge can have a significant impact on how risk management systems are established in banks, which can then have an impact on how well such institutions function. Taking into consideration the risk management knowledge of the board and how it relates to performance will provide fresh perspectives on efficient risk management that will strengthen corporate governance procedures and boost performance. (Boadi, et al., 2023). Smaili et al. (2023) sought to determine how board effectiveness affected disclosure linked to cybersecurity. After five years and using a sample of 300 company-years from the biggest listed Canadian firms, it was determined that board effectiveness has a favorable influence on the disclosure of cybersecurity concerns. Furthermore, the degree of this disclosure is positively impacted by the independence and financial expertise of the board, but not by the size of the board. The researcher will use cybersecurity disclosure as a gauge of the board's efficiency in monitoring and controlling cybersecurity risks. Vincent et al.'s (2019) goal was to find out if senior management culture, board experience, and board participation affect how mature an organization's IT risk management procedures are. The study found that while senior managers' risk-taking behavior is linked to a drop in IT risk management maturity, board engagement has a beneficial impact on this area. IT risk management maturity is influenced by board expertise, but board engagement is more crucial in understanding IT risk management maturity. The study also demonstrated that organizations with board-level risk oversight, as opposed to managerial committee monitoring, have better-developed IT risk management procedures. Furthermore, there was no discernible variation in the level of sophistication of human resource management protocols amongst firms where the entire board was accountable for risk supervision Heroux and Fortin (2022) looked at the issues of cybersecurity disclosure and the interaction between various board features. The results of content analysis of 250 S&P/TSX Composite Index businesses' annual financial reports showed that establishing a cybersecurity committee on the board is crucial for boosting cybersecurity disclosure. The degree of full cybersecurity disclosure or particular components, particularly cybersecurity risk mitigation, are correlated with the participation of female directors, board age, tenure, independence, and IT knowledge, regardless of the existence of such a committee. Radu and Smaili (2022) also examined, using a sample of S&P/TSX 60 Index businesses from 2014 to 2018, the effect of gender diversity on the board about cybersecurity disclosure. The findings demonstrated a positive relationship between gender diversity on the board and the degree of cybersecurity disclosure. It did, however, stress that to see this beneficial effect, the board had to have three or more women. In the Arab context, Masoud and Abdel Fattah (2024) sought to examine, with application to businesses listed on the Egyptian Exchange, the relationship between board composition and cybersecurity risk disclosure and the effect on stock prices. Using text analysis, the study looked at 90 observations from the annual reports of a sample of 30 companies that were listed on the Egyptian Exchange between 2020 and 2022. The

findings showed a strong positive correlation between the degree of cybersecurity risk disclosure and the size, independence, and diversity of the board. The exposure of cybersecurity risks had a notable adverse impact on stock values as well.

Study Hypotheses

The Impact of Board Size on Cybersecurity Risks:

The increasing number of cyber-attacks and security risks has attracted the attention of stakeholders, practitioners, and governance bodies, urging boards of directors to play a more active role in providing comprehensive oversight of these electronic risks (NACD, 2020). In a meeting held on March 13, 2019, the National Association of Corporate Directors' Risk Oversight Advisory Council recommended that organizations evaluate their cybersecurity strategy and assess whether they possess the necessary IT expertise and talent to fully understand IT issues and achieve their risk monitoring responsibilities (NACD, 2019).

Board size refers to the number of members that constitute the board. Proponents of agency theory suggest that large board size is not beneficial for a company because it prevents officers from effectively controlling managers due to differing opinions and the lack of cohesion and coordination that can arise in a large board. Opportunistic behavior by management is more likely to develop with many directors. Jensen and Meckling (1976) posit that it is easier for a leader to control a board of seven or eight members. Conversely, resource dependence theory states that it is beneficial for a company to increase the number of its directors to better control its resources, thereby achieving better performance. Generally, larger institutions should have larger boards because their activities are often diverse, necessitating a larger number of members. From this perspective, a larger board appears more effective (Pfeffer & Salanick, 1978).

Small boards may have significant personal relationships among members. Larger boards are less influenced by such relationships. Hence, board size is sometimes linked to board independence. Smaller boards benefit from more efficient communication and coordination, thus better monitoring. Larger boards benefit from a larger pool of information, including the knowledge and experience of the directors (Horsthuis, 2019). The 2019 Iraqi Corporate Governance Standards Guide indicated that the number of board members should not be less than seven, without specifying an upper limit.

Therefore, increasing board size helps diversify expertise and knowledge, enhancing the oversight role over executive directors. This allows for better task distribution and the division of the board into specialized committees for monitoring and following up on management activities. Additionally, the difficulty of management controlling larger boards aids in disclosing more risk-related information. Consequently, it is expected that board size negatively impacts cybersecurity risks. Based on the above, the first sub-hypothesis is formulated as follows:

H1.1: There is an impact of board size on the cybersecurity risks of banks listed on the Iraq Stock Exchange.

The Impact of Board Independence on Cybersecurity Risk:

Oversight by independent external board members is considered more effective than that provided by their internal counterparts. The importance of external board members lies in their independence from the management team and majority shareholders.

Board independence is one of the crucial elements for effective board performance in supervisory and oversight tasks, limiting executives' ability to engage in opportunistic behaviors that serve their interests without considering the shareholders' interests. This has been supported by accounting literature theories (Masoud, Abdel Fattah, 2024).

Hence independent board members lessen conflicts of interest between management and owners and strengthen the supervision function over executives. Independent directors are more likely to push businesses to act to reduce cybersecurity risks and to provide stakeholders with additional information about these risks. As a result, it is anticipated that the percentage of independent directors will have a detrimental effect on cybersecurity risks. The second sub-hypothesis is developed as follows considering the aforementioned.

H1.2: There is an impact of board independence on the cybersecurity risks of banks listed on the Iraq Stock Exchange.

The Impact of Board Members' Expertise on Cybersecurity Risks:

The board's role in managing electronic risks is expected to be strategic. The board should participate in developing a strategic cybersecurity plan and a roadmap for its implementation. However, several factors affect strategic decision-making and cybersecurity oversight, the most important of which is the need for expertise in cybersecurity and its risks (Gale et al., 2022).

While reports presented to the board by the Chief Information Security Officer or another executive will enhance cybersecurity risk oversight, it is equally important for the board to possess the appropriate expertise and skills to understand the reports and cybersecurity risks (Orla Cox & Hetal Kanji, 2022).

According to protection motivation theory, knowing and evaluating threats and how to counter them forms the foundation of the intention to manage cybersecurity risks. However, due to potential ignorance and cognitive biases, adequate assessments cannot always be made. (Chen & Yuan, 2022). Gale et al. (2022) discovered that the strongest motivator (coercive pressures) for board involvement in cybersecurity is regulation. But sometimes, directors don't know everything that comes with overseeing cybersecurity monitoring. Furthermore, the results show that directors' interactions with cybersecurity are influenced by their backgrounds and personal experiences.

Kamiya et al. (2020) discovered that the likelihood of cyberattacks is not predicted by corporate governance features at the firm level, such as CEO duality, the percentage of external directors on the board, or board size. Last but not least, businesses that prioritise risk management at the top are less vulnerable to attacks, as indicated by Board Ex data on the existence of a risk management committee on the board. This is how the third sub-hypothesis is put forth considering the analysis above.

H1.3: There is an impact of board members' expertise on the cybersecurity risks of banks listed on the Iraq Stock Exchange.

The Impact of Gender Diversity on Cybersecurity Risks

Gender diversity is a critical characteristic desired in the structure of a board of directors. By adding a diverse range of expertise, having female members on the board can improve its efficacy and supervisory role, experiences, knowledge, and ethical values. This diversity leads to high-quality discussions and consultations, thereby improving the quality of the board's decisions and providing better protection for all company stakeholders (Martinez-Jimenez et al., 2020).

The theories in accounting literature support this notion. According to resource dependency theory, having more women on the board promotes a variety of thought and experience, which strengthens the board's oversight function. (Mustafa et al., 2017). Similarly, agency theory indicates that a more diverse board increases the effectiveness of its oversight. A diverse board is more independent, which encourages companies to disclose more information to reduce agency costs and information asymmetry, thus protecting the company from risks (Idan et al., 2021).Research indicates that as compared to their male counterparts, female directors attend meetings with greater diligence and have higher attendance rates. Women also participate in monitoring activities at a higher rate than

men (Adams & Ferreira, 2009). Reducing internal conflict and increasing strategic supervision are linked to having a diverse gender representation on the board (Nielsen & Huse, 2010). Additionally, research indicates that women are less willing to take risks than men are (Beckmann & Menkhoff, 2008). According to a study, female executives are more risk averse than their male counterparts since they issue less debt and have wider earnings projections. (Huang & Kisgen, 2013).Higher percentages of female directors are associated with a greater likelihood and extent of greenhouse gas disclosure, (Eaton et al, and 2019). According to a different study, the possibility of voluntary disclosures of climate-related risks rises with the number of women on the board (Ben-Amar et al., 2017). Additionally, more public disclosures are linked to a diverse board (Upadhyay & Zeng, 2014). Furthermore, it has been demonstrated that greater gender diversity on boards lowers fraud. Capezio & Mavis Kalyan (2016) discovered a correlation between fewer fraud cases and the number of women on boards. They discovered that the probability of fraud is decreased by 0.1% for every 10% increase in the number of women on the board. According to Wahid (2023), boards with gender diversity tend to make fewer mistakes in financial reporting and participate in less fraudulent schemes. Moreover, the chance of inadequate internal controls is decreased when there are more women on the board. Internal controls over the quality of financial reporting are improved by even having one female board member (Chen et al., 2022). Observed that businesses are more inclined to reveal more cybersecurity information if there are more women on the board. It has also been established that higher levels of voluntary cybersecurity disclosures are correlated with a larger proportion of female directors on the board. It follows that the presence of female board members and gender diversity should hurt cybersecurity risks. This is because having more women on the board can improve committee performance and efficiency, which in turn raises the standard of monitoring over cybersecurity-related management choices. Diverse degrees of awareness, communication styles, and expertise are used to achieve this. In addition, women are generally more risk-averse and hold higher ethical standards. Compared to males, women also commit to attending meetings at higher rates, which results in higher-quality conversations, consultations, and a diversity of viewpoints on cybersecurity risk factors and mitigation strategies. The researcher developed the fourth sub-hypothesis in the following manner considering the points:

H1.4: There is an impact of gender diversity on the cybersecurity risks of banks listed on the Iraq Stock Exchange.

RESEARCH METHODS

Data and Sample Selection

The study population in our research consists of all 21 banks that are registered on the Iraq Stock Exchange, the regulated market, and are actively operating in Iraq. From the study population, a sample of people in managerial positions and roles relevant to the study's subject matter were chosen. (members of the board of directors, members of the audit, risk management, and governance committees, internal audit managers, information systems managers, IT managers, and information security managers). The estimated number of these individuals is 700. The sample size was 248 individuals from the population under investigation. After the completed survey was sent and distributed to the sample, 208 of the completed forms were returned, yielding an 84% response rate. Nineteen questionnaires were eliminated because their results were incomplete and not severe enough to be used for analysis.

Study Model:

After introducing the measurement of variables, the researcher presents the theoretical model built based on previous studies and the characteristics of the Iraqi context, explaining the influence of board features on cybersecurity threats. The researcher then presents the theories that will be investigated further. As illustrated in the following figure:

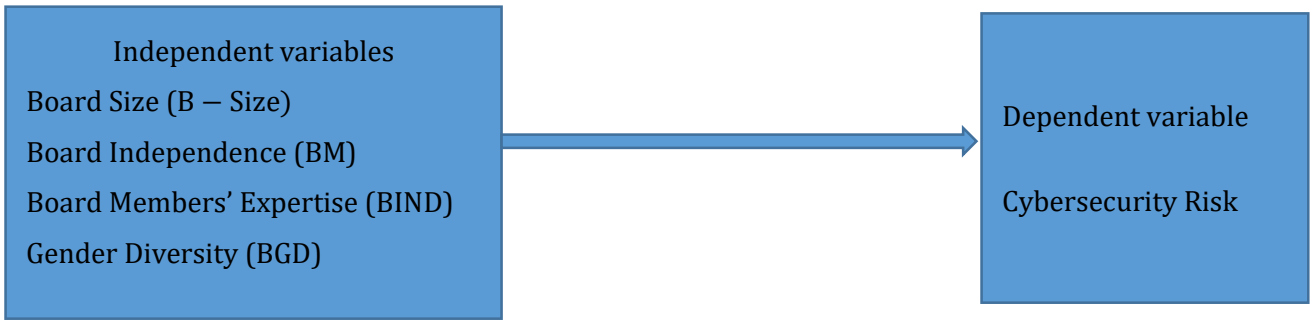

Figure 1: Study Variables

$$CSR = \beta 0 + \beta 1(Size) + \beta 2(BM) + \beta 3(BIND) + \beta 4\,(BGD) + \beta 5(BTE) + \varepsilon$$

Where:

- CSR represents Cyber Security Risks.
- Board Size (*Size*)
- Board Independence (BM)
- Board Members' Expertise (BIND)
- Gender Diversity (BGD)
- β0 (Beta-zero) denotes the intercept, representing cyber security risks not influenced by the independent variables.
- β1–β5 (Beta-one to Beta-five) are the regression coefficients for board characteristics.
- Board Technology experience (BTE) is a central variable.
- ε (Epsilon) represents the error term.

Methodology

A One-Way Analysis of Variance (ANOVA) test was used to examine differences in perspectives among sample individuals to determine whether there are significant differences in the mean responses of the research sample regarding study variables based on job roles (board member, audit committee member, risk management committee member, IT governance committee member, IT systems/technology manager, IT security/cybersecurity manager, internal audit manager, other roles).

RESULTS AND DISCUSSION

Descriptive Statistics (Independent Samples Test)

Table 1: Independent Samples Test

Variables	Category	N	Mean	Stander deviation	T value	Prob,	significance
Cybersecurity Risks	Male	146	1.29	0.17	2.893	0.024	significance
	Female	43	1.38	0.21	2.583		
Board of Directors	Male	146	1.87	0.27	0.264	0.968	Non

							significance
	Female	43	1.89	0.30	0.251		
	Female	43	2.17	0.30	1.071		

Table 1 shows that there were no statistically significant variations between the sample respondents' mean scores for the attributes of the board of directors based on gender (male vs. female) at the significance level (α = 0.05). All these variables had significance levels higher than the chosen threshold of significance (0.05). Nonetheless, based on the gender variable (male vs. female), there were statistically significant variations between the sample respondents' mean scores for the cybersecurity risks variable at the significance level (α = 0.05). This variable's significance levels were less than the chosen threshold of significance (0.05). This suggests that whereas opinions on the traits of the board of directors were not substantially different according to gender, sample respondents' opinions about cybersecurity threats were significantly different according to gender.

Testing Differences in Opinions of the Study Sample According to Job Function:

To determine whether the research sample's mean answers to the study variables vary significantly depending on their job function (board member, audit committee member, risk management committee member), IT governance committee member, head of information systems department, head of technology department, cybersecurity/IT security department head, internal audit head, others), a One-Way ANOVA test was employed to study the variations in viewpoints among the sample individuals. The related results are illustrated in Table 2:

Table 2: One-Way ANOVA test

Variables	Source of variance	Sum of squares	Degrees of freedom	Mean squares	Calculated F value	Significance level (0.05)	significance
Cybersecurity Risks	Between groups	0.189	8	0.024	0.691	0.699	Non significance
	Within groups	6.151	180	0.034			
	the total	6.340	188				
Board of Directors	Between groups	1.118	8	0.140	1.922	0.059	Non significance
	Within groups	13.088	180	0.073			
	the total	14.206	188				

Table 2 shows that the mean responses of the sample individuals to the variables of cybersecurity risks and board characteristics according to job title (board member, audit committee member) do not differ statistically significantly at the significance level of (α = 0.05)., members of the risk management committee, the IT governance committee, the heads of the information systems, technology, and cybersecurity and IT security departments, as well as the head of internal audit, were among those whose significance levels exceeded the predetermined level of significance (0.05).

Testing the study hypotheses

Table 3: Results of the stepwise multiple regression analysis using the Enter method for the impact of board characteristics on the cybersecurity risks

Independent variables	Beta	T	Sig.	R	R Square	F	Sig.
Board Size (**B − Size**)	-0.074	-4.140	0.000	0.718	0.516	48.967	0.000
Board Independence (BM)	-0.069	-4.576	0.000				
Board Members' Expertise (BIND)	-0.066	-5.342	0.000				
Gender Diversity (BGD)	-0.169	-6.731	0.000				
Constant	2.157	35.501	0.000				

The impact of the dimensions of the independent variable, board characteristics (board size, independence, gender diversity, and IT expertise), on the dependent variable, cybersecurity risks, for banks listed on the Iraq Stock Exchange is demonstrated by the regression analysis results shown in Table 3. With a value of 48.967 at a significant level of 0.000, the computer F-value indicates how relevant the model is. The independent variables that describe the characteristics of the board (as a whole) explain 51.6% of the variance in cybersecurity risks for the listed banks, according to the regression model's modified R-squared value of 0.516. This indicates that the connection between this variable and the independent variables is properly described by the regression curve. The hypothesis that board characteristics affect cybersecurity risks for banks listed on the Iraq Stock Exchange is supported by the multiple correlation coefficient R of 0.718, which shows a strong relationship or correlation between the explanatory variables and the value of the dependent variable as well as the absence of perfect correlation among the independent variables.

Model:

$$CSR = 2.157 \ - 0.074\ (Size) \ - 0.069\ (BIND) \ - 0.066(BGD) \ - 0.968\ (BTE) \ + \ \varepsilon$$

Hypothesis Testing Results

Sub-Hypothesis 1:

Board size significantly affects cybersecurity risks for banks listed on the Iraq Stock Exchange, according to the regression model. With a t-value of -4.140 and a significance level of 0.000, the regression coefficient's negative value (-0.074) denotes a significant effect at a significance level of 0.05. Thus, we agree with the notion that the size of the board affects these banks' cybersecurity risks. This suggests that a factor in lowering cybersecurity risks is the size or composition of the board. Agency theory states that larger boards have more diversified backgrounds and are less susceptible to managerial influence expertise, allowing them to carry out advisory tasks and divide workload efficiently. This is consistent with findings by Tai (2020) and Masoud (2024), who discovered a positive and significant correlation between board size and the degree of disclosure about cybersecurity risks. Tai (2020) also highlighted that board size plays a critical role in monitoring hedging decisions and leads to risk reduction. It also supports the findings of Héroux & Fortin (2022), who established a correlation between board size and the level of risk mitigation and cybersecurity disclosure. This stands in contrast to the findings of Mazumder & Hossain (2023) and Smaili et al. (2023), who discovered no meaningful connection between cybersecurity disclosure and board size.

Sub-Hypothesis 2:

Board independence significantly affects cybersecurity risks for banks listed on the Iraq Stock Exchange, according to the regression model. With a t-value of -4.576 and a significance level of 0.000, the regression coefficient's negative value (-0.069) denotes a significant effect at a significance level of 0.05. Therefore, we agree with the notion that these banks' cybersecurity risks are impacted by board independence. This implies that cybersecurity threats are decreased as board independence rises. This result is in line with the findings of Mazumder & Hossain (2023), Smaili et al. (2023), Masoud (2024), and Héroux & Fortin (2022), who have all shown that board independence and the degree of cybersecurity risk disclosure and mitigation are positively correlated. It contrasts with Hsu & Wang's (2014) findings, which indicated that boards with a higher percentage of independent directors were positively correlated with security breaches. This could be because external directors don't have enough internal knowledge of the company to effectively lower the likelihood of a breach.

Sub-Hypothesis 3:

According to the regression model, female diversity on the board significantly reduces cybersecurity risks for banks that are listed on the Iraq Stock Exchange. With a t-value of -5.342 and a significance level of 0.000, the regression coefficient's negative value (-0.066) denotes a significant effect at a significance level of 0.05. Therefore, we agree with the premise that these institutions' cybersecurity risks are impacted by the gender diversity of the board. This implies that having more women on audit committees lowers the risk associated with cybersecurity. Remeis (2023), Radu & Smaili (2022), Mazumder & Hossain (2023), Masoud (2024), and Héroux & Fortin (2022) have all found a positive correlation between board diversity and the degree of cybersecurity risk disclosure and mitigation. This finding is in line with their findings.

Sub-Hypothesis 4:

The regression model demonstrates that board member credentials and experience have a major influence on cybersecurity risks for banks listed on the Iraq Stock Exchange. With a t-value of -6.731 and a significance level of 0.000, the regression coefficient's negative value (-0.169) denotes a significant effect at a significance level of 0.05. Therefore, we agree with the premise that these institutions' cybersecurity risks are influenced by the board members' backgrounds and areas of expertise. This suggests that having people on board with training and experience in IT and related hazards helps lower the risk of cybersecurity. According to Vincent et al. (2019) and Smaili et al. (2023), board expertise in risk management and IT contributes to the maturity of IT risk management practices. Héroux & Fortin (2022) also confirmed the relationship between board expertise in IT and the level of cybersecurity disclosure and risk mitigation. These findings are consistent with the findings of the study.

CONCLUSION

By analyzing the effects of the board features on cybersecurity risks, the study sought to quantify the effect of the board of directors on banks listed on the Iraq Stock Exchange. The attributes of the audit committee (size, independence, and technological knowledge) and the board (member diversity, size, and independence) served as representations of the governance systems Together with the research design and methodology, the study population, and the sample of 21 banks listed on the regular market of the Iraq Stock Exchange, totaling 189 individuals, the researcher used a descriptive-analytical methodology that is appropriate for this kind of study.

The researcher concluded that banks with larger boards, independence, gender diversity, and technological expertise tend to have lower levels of cybersecurity risk. Additionally, banks with audit committees that have many members, independence, and technological expertise also experience lower cybersecurity risks. Furthermore, banks with a Chief Information Officer (CIO), a Chief

Cybersecurity Officer (CCO), and an IT risk management committee that includes technology experts in their senior and executive management tend to have lower levels of cybersecurity risk. Efficient and high-quality internal auditing also contributes to reducing cybersecurity risks for these banks. The researcher recommended that banks should strengthen their boards and audit committees with expertise and qualifications in information and communication technology. It was also suggested that banks conduct training sessions on cybersecurity specifically for board members and generally for bank employees. Additionally, it was advised that banks establish cybersecurity risk committees at the executive management level or board level, if possible.

REFERENCE

Berger, A. N., Clarke, G. R., Cull, R., Klapper, L., & Udell, G. F. (2005). Corporate governance and bank performance: A joint analysis of the static, selection, and dynamic effects of domestic, foreign, and state ownership. Journal of Banking & Finance, 29(8–9), 2179–2221.

Idan, H. Z., Rapani, N. H. A., Khalid, A. A., & Al-Waeli, A. J. (2021). "The Effect of Corporate Governance Attributes on Corporate Social Responsibility Disclosure in Iraqi Companies: A Literature Review", Journal of Contemporary Issues in Business and Government, 27(2), 2778-2816

Johari, Z. A., Ghazali, A. W., Isa, Y. M., Shafie, N. A., & Sanusi, S. (2023). Digital Disruption and Cybersecurity Threats: Redefining the Role Of Internal Auditing. European Proceedings of Social and Behavioural Sciences.EpSBS www.europeanproceedings.com.

Thammareddi, L., Agarwal, S., Bhanushali, A., Patel, K., & Venkata, S. (2023). Analysis Of cybersecurity threats in modern banking and machine learning techniques for fraud detection.

Crisanto J. C., Pelegrini J. U., and Prenio J. (2023). Banks' cyber security – a second generation of regulatory approaches. Financial Stability Institute FSI Insights on Policy Implementation No 50.

Jin, J., Li, N., Liu, S., & Nainar, S. K. (2023). Cyber-attacks, discretionary loan loss provisions, and banks' earnings management. Finance Research Letters, 54, 103705.

Kala, E. (2023) The Impact of Cyber Security on Business: How to Protect Your Business. Open Journal of Safety Science and Technology, 13, 51-65. Doi: 10.4236/ojsst.2023.132003.

Smaili, N., Radu, C., & Khalili, A. (2023). Board effectiveness and cybersecurity disclosure. Journal of Management and Governance, 27(4), 1049-1071.

Orla Cox and Hetal Kanji. (2022). Building Effective Cybersecurity Governance. https://corpgov.law.harvard.edu/2022/11/10/building-effective-cybersecurity-governance/.

Héroux, S., & Fortin, A. (2022). Board of directors' attributes and aspects of cybersecurity disclosure. Journal of Management and Governance, 1-46.

Peihani, M. (2022). Regulation of Cyber Risk in the Banking System: A Canadian Case Study. Journal of Financial Regulation, 8(2), 139-161.

Radu, C., & Smaili, N. (2022). Board gender diversity and corporate response to cyber risk: evidence from cybersecurity-related disclosure. Journal of Business Ethics, 177(2), 351-374.

Schnatterly, K., Calvano, F., Berns, J. P., & Deng, C. (2021). The effects of board expertise-risk misalignment and subsequent strategic board reconfiguration on firm performance. Strategic Management Journal, 42(11), 2162–2191.

Uddin, M. H., Ali, M. H., & Hassan, M. K. (2020). Cybersecurity hazards and financial system vulnerability: a synthesis of the literature. Risk Management, 22(4), 239-309.

Uddin, M. H., Ali, M. H., & Hassan, M. K. (2020). Cybersecurity hazards and financial system vulnerability: a synthesis of the literature. Risk Management, 22(4), 239-309.

Eaton, T. V., Grenier, J. H., & Layman, D. (2019). Accounting and cybersecurity risk management. Current Issues in Auditing, 13(2), C1-C9.

Horsthuis, L. W. J. (2019). Internal corporate governance mechanisms and corporate performance: Evidence from Dutch listed firms (Master's thesis, University of Twente).

Islam, M. S., Farah, N., & Stafford, T. F, (2018), Factors associated with security/cybersecurity audit by internal audit function: An international study, Managerial Auditing Journal,33(4), pp 377-409.

Ismail, N. (2018). The financial impact of data breaches is just the beginning. Retrieved from www.information-age.com: https://www.information-age.com/data-breaches-financial-impact-123470254/.

Mustafa, A. S., Che-Ahmad, A., and Chandren, S. (2017). "Board diversity and audit quality: Evidence from Turkey". Journal of Advanced Research in Business and Management Studies, 6 (1), 50-60.

Higgs, J. L., Pinsker R. E., Smith T. J., and Young G. R. (2016). The relationship between board-level technology committees and reported security breaches. Journal of Information Systems30 (3): 79– 98. https://doi.org/10.2308/isys-51402

Huang, J., & Kisgen, D. J. (2013). Gender and corporate finance: Are male executives overconfident relative to female executives? Journal of Financial Economics, 108(3), 822-839.

Adams, R. B., & Ferreira, D. (2009). Women in the boardroom and their impact on governance and performance. Journal of Financial Economics, 94(2), 291-309.

Pfeffer, J. and G. R. Salancik (1978) The External Control of Organizations: A Resource Dependence Perspective. New York: Harper and Row.

Center for Audit Quality (CAQ). 2016. A Model for Cybersecurity and Auditing. In Clinton, L. & Perera, D. (Eds), Social Contract 3.0: Implementing a Market-Based Model for Cybersecurity. Published by the Internet Security Alliance.

Vincent, N. E., Higgs J. L., and PinskerR. E. 2019. Board and management-level factors affecting the maturity of IT risk management practices. Journal of Information Systems33 (3): 117– 135. https://doi.org/10.2308/isys-52229

Abdelrahim, A., & Al-Malkawi, H. A. N. (2022). The influential factors of internal audit effectiveness: a conceptual model. International Journal of Financial Studies, 10(3), 71.

Ben-Amar, W., Chang, M., & McIlkenny, P. (2017). Board gender diversity and corporate response to sustainability initiatives: Evidence from the carbon disclosure project. Journal of Business Ethics, 142(2), 369-383.

Boadi, L. A., Isshaq, Z., & Adu-Asare Idun, A. (2023). Board expertise and the relationship between bank risk governance and performance. Cogent Business & Management, 10(3), 2283233.

Chen, H., & Yuan, Y. (2022). The impact of ignorance and bias on information security protection motivation: a case of e-waste handling. Internet Research, (ahead-of-print).

Gale, M., Bongiovanni, I., & Slapnicar, S. (2022). Governing cybersecurity from the boardroom: challenges, drivers, and ways ahead. Computers & Security, 121, 102840.

Hanim, M, A. Feby, A, M. Eko, W, T. Chitra, U, P. (2017). Risks Assessment of Information Technology Process Based on COBIT0 Framework: A Case Study of ITS Service Desk. Procedia Computer Science, 124.569-576.

Herrera Luque, F. J., Munera López, J., & Williams, P. (2021). Cyber risk as a threat to financial stability. Revista de Estabilidad Financiera/Banco de España, 40 (primavera 2021), p. 181-205.

Johari, Z. A., Ghazali, A. W., Isa, Y. M., Shafie, N. A., & Sanusi, S. (2023). Digital Disruption And Cybersecurity Threats: Redefining The Role Of Internal Auditing. European Proceedings of Social and Behavioural Sciences.EpSBS www.europeanproceedings.com.

Kamiya, S., Kang, J. K., Kim, J., Milidonis, A., & Stulz, R. M. (2020). Risk management, firm reputation, and the impact of successful cyberattacks on target firms. Journal of Financial Economics.

Martinez-Jimenez, R., Hernández-Ortiz,M,J., Fernández, C., & Ana , I. (2020). "Gender diversity influence on board effectiveness and business performance". Corporate Governance: The International Journal of Business in Society, 20(2):307-323.

Masoud, Sanaa Maher Mohammadi, Abdel Fattah, Heba Bashir Al-Toukhi. (2024). Analysis of the relationship between the characteristics of the board of directors and disclosure of cybersecurity risks and its impact on stock prices: an applied study on companies listed on the Egyptian Stock Exchange. Alexandria Journal of Accounting Research, 8(1), 1-62.

Mbanaso, U. M., Abrahams, L., & Apene, O. Z. (2019). Conceptual design of a cybersecurity resilience maturity measurement (CRMM) framework. The African Journal of Information and Communication, 23.

National Association of Corporate Directors (NACD). 2019. 2019–2020 NACD Public Company Governance Survey. The Current State of the American Boardroom. Arlington, VA: NACD. Available.

Nielsen, S., & Huse, M. (2010). The contribution of women on boards of directors: Going beyond the surface. Corporate Governance: An International Review, 18(2), 136-148.

Upadhyay, A., & Zeng, H. (2014). Gender and ethnic diversity on boards and corporate information environment. Journal of Business Research, 67(11), 2456-2463.

Wali, K., van Paridon, K., & Darwish, B. K. (2023). Strengthening banking sector governance: challenges and solutions. Future Business Journal, 9(1), 95.