Electronic Commerce Research
https://doi.org/10.1007/s10660-024-09867-w

Board characteristics and cybersecurity disclosure: evidence from the UK

Ahmad Yuosef Alodat[1] · Yunhong Hao[1] · Haitham Nobanee[2,3,4] · Hazem Ali[5] · Marwan Mansour[6] · Hamzeh Al Amosh[7]

Accepted: 13 May 2024

Abstract
The purpose of this study is to explore the influence of board of directors characteristics on the cybersecurity disclosure (CSD) of firms listed on the London Stock Exchange. The current study used an empirical approach to data collection and analysis. The independent variable is the boards of directors' characteristics; the dependent variables are the CSD. The study analysed 2250 observation of the UK. listed firms for the period of 2011–2020. The results of the current study show a significant and positive relationship between the extent of CSD and the board size, board independence and board meeting; in terms of board gender diversity yielded an insignificant and positive relationship with the extent of CSD. The findings indicate that firms with more independent and larger board, and high meeting frequency promote cybersecurity transparency and reduce related information asymmetric with stakeholders. The analyses have implications for policymakers, top management, corporate executives and practitioners. Firms are encouraged to restructure their board to enhance its effectiveness to better support and monitor CSD. This is the first study in the UK that examined the determinants of CSD. This adds value to the literature on CSD, in addition to contributing to an understanding of the relationship between board characteristics and CSD.

Keywords Corporate governance · Cybersecurity disclosure · Board characteristics · The UK

1 Introduction

Cybersecurity is a significant risk affecting the global economy. Cybersecurity issues at large publicly traded companies have enlarged the stakeholders' as well as executives' sensitivity to the risk of losing out on business opportunities and customer base. It has gained more attention among researchers as a controversial

Extended author information available on the last page of the article

Published online: 04 June 2024

topic in light of new development in business technologies, the expansion of online sales worldwide, the rise of remote work, and the recent cyber scandals [70]. Society has become highly dependent on technology,this makes it imperative for firms to enhance CSD to provide transparency and build stakeholder trust. One of the greatest threats to firms strategic achievement has become cyber-attacks [21]. A cyber-attack can cripple even the most developed firms, so stakeholders have the right to know if the firm's exposure to cyber-attacks and what actions companies have taken to address those attacks. This draws attention to the responsibility of the board has become more interested in raising CSD.

Cyber-attacks have recently escalated to exercise global influence and international competition by disrupting vital sites of countries. In the 2019 Global Risks Report the World Economic Forum issued; Cyber risks were listed second only to climate change (World Economic Forum 2019). One study showed that more than 40 million cyber-attacks globally [69]. Considering the pervasive nature and considerable costs accompanying cyber-attacks occurrence, the disclosure of the cyber-attacks faced by companies, and how these threats are dealt with become increasingly critical for stakeholders.

CSD is a relatively new and important agenda for corporate disclosure. Stakeholders are interested in the demand for information related to CSD and the need to provide that information through disclosure practices [18]. On the other hand, cyber risks are gaining a corporate nature, as cybercriminals often hack corporate cybersecurity and steal confidential data to get quick financial illegal advantages (Bourdon, 2017). Consequently, stakeholders' concerns about the escalation of cyber-attacks and the threat to their interests increased, prompting them to demand companies more transparency in this area [24],Mazumder and Hossain, 2022).

The integration of technology within corporate frameworks has underscored the critical significance of cybersecurity as an integral component of risk management. This heightened emphasis stems from the considerable attention CSD have garnered from various stakeholders [28, 44, 45].Cyber attacks targeting firms inflict enduring reputational damage and substantial financial losses [2]. Cybersecurity is increasingly recognized as a critical organizational issue that is most effectively managed through its integration into a comprehensive managerial control framework [26, 27]. This progress is attributed in part to the oversight and enforcement conducted by regulatory bodies (SEC, 2018), Partly due to the enhanced direction provided by the prominent Big 4 accounting firms and regulatory bodies within the audit industry [27]. The role of market discipline is important [11]. As a part of a managerial control system, cybersecurity has also become very much an auditing matter and managerial accounting subject to disclosure policy considerations, internal control assessment, and cost–benefit analysis [57]. Gordon and Loeb [25] delineate cybersecurity's goals into three primary realms: facilitating timely access for authorized users, safeguarding the confidentiality of sensitive data, and preserving the integrity and trustworthiness of information by ensuring its accuracy and reliability. Moreover, Consistent reporting and accountability are essential for fostering transparency and trust in the digital landscape. As the threat landscape evolves, prioritizing CSD becomes even more paramount in safeguarding sensitive information and maintaining the integrity of systems.

CSD is critical as cybersecurity risks are a major concern for firms, business leaders, and governance. In recent years, cybersecurity risks have been rated as the greatest potential risk by firms in Europe and the USA [60]. The duty of the board includes disclosure of cyber security that may affect the decision-making process of shareholders. Considering cybersecurity information is crucial in market data, because internal control weaknesses, and information technology control weaknesses in particular can carry significant negative implications for financial reporting quality (Rosati et al., 2020).

Effective disclosure of cybersecurity incidents is paramount as it serves as a reflection of companies within the European stock market, which includes the directive on network and information systems security (NIS) and general data protection regulation (GDPR), it is not limited to annual reports [61]. Through the oversight role played by the board of directors, it must be awake in managing threats and CSD. Thus, the focal responsibilities for boards of directors include disclosure of cybersecurity that may affect the decision-making process of shareholders. Considering cybersecurity information is crucial in market data, cybersecurity topic must be a top priority for corporate boardrooms (Li and Wang, 2018; [58]), as it considered to be the most pressing attributes of good governance [7], which can achieve the goals of the companies through the characteristics of the board of directors such as board size, board gender diversity, board independent [48].

The oriented discourse of cybersecurity has become an important issue that needs to strengthen its governance, given that cybersecurity risks are now a major concern for business organisations today [55]. Moreover, Previous studies are still unclear regarding corporate governance and corporate risk disclosure [60]. Previous literature was limited to investigating the effect of corporate governance mechanisms on non-financial and financial performance, such as social responsibility and sustainable development (e.g., Alodat et al., 2023c [50],). Moreover, There exists a paucity of research examining the intersection of corporate governance and CSD on a global scale. Our study aims to address this gap in the literature by offering insights into this underexplored area, thereby contributing to the body of knowledge on the subject.

The nexus between board characteristics and cybersecurity disclosure remains underexplored within the academic literature, particularly in light of the recent Cybersecurity disclosure guidance. Existing studies predominantly concentrate on interpreting the guidance rather than examining the gaps therein. For instance, Target's 2014 Financial Statement underscores the significance of cybersecurity breaches, yet the broader implications for board characteristics in such disclosures warrant further scholarly attention (Jin, J., 2015).

This study aims to investigate the effect of board characteristics and cybersecurity disclosure in the annual reports of the firms listed in the U.K. during 2011–2020. Interestingly, studies are relatively few, and some studies have been conducted (i.e., [60, 70],Mazumder and Hossain, 2022) in defferent context. As a consequence, the outcomes of these studies can not be generalised to companies in other contexts. Accordingly, further investigation is needed into different cultural, legal, and economic environments. As a result, our study aims to bridge the gap in the literature on the cybersecurity disclosure, which has important implications for different

regulators and stakeholders in the UK. Thus, the main objective is to investigate the relationship among characteristics of the board such as (board Independent, meetings, size and gender diversity) and cybersecurity disclosure in developed country.

We selected the UK for this inquiry because it offers an environment where cybersecurity disclosure regulations are voluntary [19]. This study contributes in several ways. First, we present a new guide to the growing literature on cybersecurity disclosure in an important European context in the United Kingdom. Second, our study provides evidence of the relationship between board characteristics and cybersecurity in the U.K. and which is considered the first study, and there is a dearth of research related to this nexus, and this study covers the research gap. Corporate governance and cybersecurity research in publicly traded firms is very necessary because this sector's business valuation and operational activities influence directly by the operations-related risks which will need a high monitoring function. The literature has dealt broadly with voluntary disclosure and its determinants, such as disclosure of CSR, sustainability, integrated reporting, and ESG performance. On the contrary, the literature has not provided enough evidence about the factors that influence cybersecurity disclosure. This enables further research in this field, and our investigation begins with an examination of the impact of characteristics of the board on firms CSD. As the board of directors has the experience and resources to enhance the level of cybersecurity disclosure, which avoids companies from exposing to suffering long-lasting financial as well as reputational damages. So that was our contributions.

The study proceeds as follows. Literature review, theoretical perspective and hypotheses development in Sect. 2. The research method includes data and sample selection and measures in Sect. 3. Section 4 reports the result and discussion, and the conclusion section is presented in the final section.

2 Literature review, theoretical perspective and hypotheses development

Several theories have been applied to understand many corporate governance issues, such as stakeholder theory, resource dependence theory and agency theory [7, 51]. According to Rao et al. [62], the variation in voluntary disclosure practices can be explained by corporate governance, as one of the most important board characteristics is expected to play two roles [31]. The first of these is resource dependence,for the success and survival of the firm, the board effectiveness provides resources and strategies. The second role is that of the agency issue including monitoring management to reduce agency costs.

The disclosure of the information is one of the main demands of stakeholders. Accordingly, companies must share and display information with various stakeholders without exception (Lauesen, 2013). Over time, the information contributed to creating a state of satisfaction among the various parties, as companies practised disclosing their environmental and social contributions to satisfy the various stakeholders and avoid further potential pressures [8]. Furthermore, the disclosure of information related to information security may be of special

importance, as it indicates the company's ability to preserve the information of customers, shareholders and investors, enhancing stakeholders' confidence. Accordingly, we argue that the board can play a critical role in maximising stakeholder value through cybersecurity governance and promoting transparency and disclosure in this issue.

The effects of board of directors on cybersecurity disclosure, stakeholder theory, agency theory and resource dependency theory were investigated. From the resource dependency theory perspective, directors may bring valuable skills, knowledge, and recommendations for organisational success and economic resources [7, 37]. On behalf of the shareholders the board monitors the firm (Jensen and Meckling, 1976). However, a firm is a set of contracts between stakeholders and shareholders [22]. According to stakeholder theory, the role of the board is not only to maximise shareholders' wealth, but the conflicting demands of stakeholders must be balanced [34]. Many stakeholders are pressing for more revelations about a firm's cybersecurity [55]. Information governance is receiving increasing attention from stakeholders, including cybersecurity information and related risks and issues that affect business continuity [55]. Disclosures about the organisation's ability to respond to cyber-attacks and incidents may effectively enhance its reputation and attract more customers (Rodrigues et al., 2022). On the other hand, many governance-related factors may play in support of corporate cybersecurity strategy. Rosati et al. (2020) argued that internal control weaknesses, and information technology control weaknesses in particular can carry significant negative implications for financial reporting quality. Previously, many determinants supporting the performance of sustainability and social responsibility in companies were measured, like corporate governance, characteristics of the board and ownership structure. These factors may extend to enhancing cyber security disclosure in terms of consolidating the relationship with various stakeholders and meeting their aspirations for information.

The aspirations of stakeholders are witnessing a remarkable development with the passage of time, especially with regard to their information needs, especially modern information related to electronic risk management [60]. Therefore, these demands have received a quick response from the companies operating in the market. Specifically, companies may enhance their ability to govern cybersecurity and enhance transparency in this area to enhance the level of trust with stakeholders [17]. This indicates the goodwill of firms by developing a disclosure strategy.

According to agency theory, the corporate monitoring and control tool is the board of directors. The effectiveness of the characteristics of the board of directors plays an important role in minimises the information asymmetry between investors and management by providing the necessary disclosures [67]. According to resource dependency theory, The board considers value from a firm's intangible management and resources through value-creating characteristics such as skills, leadership qualities, professional experience, awareness, and diverse views. These characteristics enable the firm to generate new ideas and modern practices [8, 31],Mazumder and Hossain, 2022).

2.1 Board size and cybersecurity disclosure

To increase the awareness of the board of directors of the potential risks of a firm, the members of the board of directors must be increased, which could propel disclosures of the risk [64]. According to agency theory, the larger board has to do with effective monitoring and control of managerial procedures. According to Saleh et al. [66], a larger boards size has diverse skills, ideas and experiences than a smaller one. This helps and positively improves the level of firm disclosures [9]. Moreover, the size of the board of directors can increase the representation of different stakeholders, thus maximising their value and fulfilling their aspirations.

Board size is expected that the larger the board, the more experiences and knowledge it entails, and this usually leads to higher monitoring and controlling efficiency that can be reflected in improved corporate disclosures by management [1]. Some studies have shown a positive impact of the size of the board on firm disclosures [15, 49]. The study by Lakhal [42] showed that the size of the board of directors negatively affects the disclosures of firms. Similarly, some research shows that the board size is insignificant [12]. Subsequently, this research proposes the following hypothesis:

H1: There is a significant positive relationship between board size and cybersecurity disclosure.

2.2 Board Independent and cybersecurity disclosure

According to agency theory, independence of the board is more objective and effective in evaluating the performance of executives. This helps the independent manager's thinking in reducing the conflict of interests among shareholders and management and gives expectations that the firm seeks to achieve the interests of a group of stakeholders [1]. Independent directors follow long-term practices to add to a higher level of disclosure of the firm [15]. Previous studies on board independence positively impact the firm's level of disclosures [20],Mazumder and Hossain, 2022).

According to the resource dependency theory, independent directors have more resources, such as experience, legitimacy and knowledge, which influence decision-making and firm behaviours [59]. They bring to the top management skill, discipline, control, supervision and advice [8]. Subsequently, this probably helps independent directors with their experience and up-to-date knowledge to disclose a higher level of new disclosure practices such as cybersecurity. Based on the arguments regarding board independent and cybersecurity disclosure:

H2: There is a significant positive relationship between board independence and cybersecurity disclosure.

2.3 Board gender diversity and cybersecurity disclosure

The role of women on the board of directors may improve cybersecurity disclosure in various ways, including general and specific knowledge, independence, stakeholder sensitivity, ethical sensitivity, risk oversight, leadership style and other characteristics. In addition, Women can take on the role of monitoring and oversight of cybersecurity [60]. More women on board help enhance disclosure on cybersecurity and corporate governance [70]. It is well documented in the literature that gender diversity represents a key proxy for an effective board composition [38, 72]. Prior research revealed the relationship of the women on the board with disclosure issues more than men [23, 47, 74]. Women have a good higher level of firm disclosure [14]. Therefore, the board is increasingly interested in cybersecurity issues [60].

According to stakeholder theory, number of female directors on the board of directors will likely build a strong stakeholder orientation, enhancing cybersecurity disclosure practices [32]. Female on the board are more diligent, independent and committed [73]. This enhances effective oversight. They can be active and involved in promoting ethical behavior and promote a culture of cybersecurity through increased disclosure of cybersecurity. Regarding the effect of board of the gender diversity on CSD, there is very scant evidence,more specifically, using evidence from Bangladesh listed banking, Mazumder and Hossain (2022) showed a significant positive relationship between gender diversity on the board and cybersecurity disclosure. The study conducted by Radu and Smaili [60] in the promoting firms in Toronto revealed that there is a positive and significant relationship between gender diversity in the board of directors and disclosure of cybersecurity. Thus, the third hypothesis drawn in this study is as follows:

H3: There is a positive and significant relationship between board gender diversity and cybersecurity disclosure.

2.4 Board meeting and cybersecurity disclosure

The frequency of board meetings shows a degree of diligence and commitment when the directors conduct their activities [7]. For a more effective and efficient board of directors, the frequency of meetings is one of the most important characteristics (Aladwey et al., 2022). Frequency of board meetings can provide opportunity for some issues, such as stakeholder demands and firm disclosures, through meetings that increase the effectiveness of the instrument board and enhance accountability and transparency [9]. Board meetings enhance and improve managers' understanding of decisions and activities through the continuous flow of information [46]. In addition, Laksmana [43] found the relationship among the board meeting frequency and the voluntary disclosure, a positive and important significant. In addition, Laksmana [43] found the relationship among board meeting frequency and the voluntary disclosure a positive and important significant.

Accordingly, the board of directors frequent are expected to result in higher cybersecurity disclosure by board members. Since more corporate disclosure and transparency are linked to better practices of the governance, firms that actively

share in their own operations will be more inclined to CSD. the fourth hypothesis drawn in this study is as follows:

H4: There is a positive significant relationship between meeting of the board and cybersecurity disclosure.

3 Research method

3.1 Data and sample selection

The study sample consists of FTSE 350 non-financial listed firms in the UK and the study period starts from 2011–2020. Manually from corporate reports and their websites, data related to cybersecurity disclosure was collected. The remaining financial data and characteristics of the board of directors are collected from Thomson Reuters Eikon. According to the global industry classification Standard (GICS) the financial sector was excluded from the sample because it is subject to different regulations and rules, making it not parallel to other sectors [3, 4, 10]. Second, firms that missing data during the study period were excluded. Finally, the sample included ten years from 2011–2020, and included 225 non-financial firms, and yielding 2250 observations.

3.2 Measures

3.2.1 The dependent variable

A measure has been used to cybersecurity disclosure consistent with previous studies such as (Mazumder and Hossain, 2022; [60]), Measures disclosure of

Table 1 Measurement of variables

Dependent variables	Acronym	Measurements
Cybersecurity disclosure	CSD	If cybersecurity information is disclosed it takes a value of 1, otherwise 0
Independent variables		
Board size	BOSI	Total number of board members
Board independence	BODIN	Percentage of independent board members
Board gender diversity	BGD	Percentage of female board members
Board meeting	BDMET	Number of meetings held by the board during a year
Control variables		
Profitability	ROA	Net income divided by total assets
Firm size	FSIZE	Natural logarithm of total assets
Leverage	LEV	As the total liabilities divided by total assets
Audit committee independence	ACI	proportion of independent directors on the audit committee

cybersecurity through a binary variable that takes a value of 1 if the firm information about cybersecurity is disclosed and 0 otherwise. The binary variant is considered appropriate for measuring cybersecurity disclosure. In addition, Mansour et al. [52] confirm that binary scoring is considered excellent in research that intended to present firm compliance scores. Table 1 presents the operational definitions of our research variables.

3.2.2 The independent variable

Four board characteristics as independent variables were included in this study, which represent the board characteristics, namely board independence, meetings, size and gender diversity [7]. First, board size is measured by the total number of directors on the firm board as used by prior studies, including Kweh et al. [41]. Following that, Ciftci et al. [16] and Hlel et al. (2019) independence of the board is measured as a ratio of non-executive of the independent directors to total directors of number. Meanwhile, gender diversity of the board is measured using a percentage of board directors female [39, 60]. Then, board meetings are measured using number of meetings held by the board during a year, which is similarly used in prior studies such as Kweh et al. [41].

3.2.3 Control variables

The current study evaluated four control variables, Along with the independent variables for this study: audit committee independence [65], profitability [47], firm size [50], and leverage [54].

3.3 Study model

Further, our study used CSD as a dependent variable. We collected the independent variables: board size (BOSI), independence of the board (BODIN), board gender diversity (BGD) and board meeting (BDMET). Finally, control variables: audit committee independence (ACI), profitability (ROA), firm size (FSIZE) and leverage (LEV).

$$\begin{aligned} \mathrm{CSD} = {} & \beta 0 + \beta 1\mathrm{BOSI}_{it} + \beta 2\mathrm{BODIN}_{it} + \beta 3\mathrm{BGD}_{it} + \beta 4\mathrm{BDMET}_{it} \\ & + \beta\, 5\mathrm{ACI}_{it} + \beta 6\mathrm{ROA}_{it} + \beta 7\mathrm{FSIZE}_{it} + \beta 8\mathrm{LEV}_{it} + \mathrm{u}_{it} \end{aligned}$$

4 Result and discussion

4.1 Descriptive analysis

Table 2 below reports the descriptive statistics for the full sample consisting of 2250 firms for the whole year observations, which include the mean, standard deviations, minimum and maximum of all variables of this study.

Table 2 Descriptive statistics

Variables	Samples	Mean	SD	Minimum	Maximum	skewness	kurtosis
CSD	2250	0.642	0.479	0	1	−.599	1.35
BDMET	2250	8.154	4.497	4	27	1.01	1.39
BOSI	2250	8.607	2.417	4	19	.206	1.24
BGD	2250	24.83	15.87	0	66.6	1.39	2.91
BODIN	2250	61.04	18.17	7.14	100	1.16	−1.02
ROA	2250	4.344	9.098	−55.33	52.94	−1.06	1.79
FSIZE	2250	8.285	1.083	2.81	12.47	. 83	3.88
LEV	2250	0.277	0.178	0	0.867	1.04	1.77
ACI	2250	77.46	29.01	0	100	−1.01	2.58

Table 2 provides the descriptive statistics for the cybersecurity disclosure variable, where the mean value of CSD is 0.642 with a maximum and minimum level of 1 and 0, respectively. Meanwhile, for the overall board characteristics BOSI, the mean value was 8.607 with a maximum and minimum level of 4 and 19, respectively. In addition, the BGD means were recorded at 24.83, with a 66.6% maximum and 0% minimum. The standard deviation was recorded at 15.87. Moreover, where the mean value of BODIN is 61.04, with a maximum and minimum level of 100 and 7.14, respectively.

4.2 Diagnostic tests

To prevent misleading study results, the diagnostic tests on the data distribution in terms of linearity, outliers, normality, autocorrelation, multicollinearity and heteroscedasticity were checked in detail [29]. Regarding normality, the skewness and kurtosis outcomes for normality and the univariate method for outliers all confirmed that no problem was present. According to Barka and Legendre (2017), the

Table 3 VIF and correlation matrix

Variables	CSD	BDMET	BOSI	BGD	BODIN	ROA	FSIZE	LEV	ACI	VIF
CSD	1									
BDMET	0.090*	1								1.03
BOSI	0.207*	0.148*	1							1.05
BGD	0.039*	0.056*	0.018	1						1.05
BODIN	0.069*	0.040*	0.075*	0.192*	1					1.05
ROA	0.011	0.045*	0.005	0.041*	0.026	1				1.01
FSIZE	0.035	−0.046*	0.020	0.061*	0.063*	0.090*	1			1.02
LEV	0.014	−0.018	0.011	0.005	−0.007	−0.002	0.001	1		1.00
ACI	0.539 *	0.068*	0.166*	−0.008	0.036	0.025	0.069*	−0.002	1	1.04

* Correlation is significant at the 0.05 level

correlation matrix confirmed that there is no multicollinearity existing relationship as there are no correlated variables above 0.80. In addition, the variance inflation factor (VIF) was used to explore multicollinearity. If the value is > 10, this indicates a high level of multicollinearity [29]. Table 3 shows that there is no multicollinearity problem.

4.3 Regression results

Table 4 shows the Breusch-Pagan (L.M.) test obtained < 0.05 (i.e., significant) while the Hausman test's resulting value < 0.05 (i.e., significant) indicates the preference for the fixed effects model. Moreover, the table presents the results of fixed effect regression for board characteristics and cybersecurity disclosure. The model was deemed fit and statistically significant, whereby this value suggested that the model was statistically valid and the R2 within the model was 21.25%. R2. Therefore, the regression equation statistically explained the variation in the model assessed. In view of the results, H1, H2 and H4 are supported, while H3 is not supported.

The results showed that there is a positive and significant relationship between board size (BOSI) and cybersecurity disclosure. This means that firms with a larger board size provide more disclosure to cybersecurity. According to agency theory supports this result the larger boards implement effective control measures to reduce risks. Consistent with previous studies related to the board size and voluntary disclosure (e.g., [7, 30, 40]). Moreover, larger boards represent a larger segment of stakeholders and thus implement policies that are consistent with stakeholder demands. Contrary to expectations, our results do not show a significant impact of board diversity on cybersecurity disclosure. It appears that female board participation does not enhance cybersecurity disclosures, nor does it advise other board members on

Table 4 Fixed effect regression results for board characteristics and cybersecurity disclosure

Variables	Coefficients	t-stat
BOSI	0.04693	5.11***
BODIN	0.00436	2.75***
BGD	0.00065	0.50
BDMET	0.00889	2.78***
ROA	−0.00266	−2.69***
FSIZE	0.00935	1.37
LEV	6.31007	6.01***
ACI	0.00683	9.87***
Constant	−0.72423	−5.55***
R^2 within	0.2125	
N	2250	
Hausman test	39.97***	
Breusch-Pagan test	2648.3***	
Heteroskedasticity	4.107***	
Autocorrelation	2509.7***	

***Significant at the 0.01 level

providing disclosures about cybersecurity risks. This may be attributed to females' reticence about cybersecurity risks information and ways to address them by companies so that this information does not reach hackers, which provides them with ways to develop their attempts to launch more cyber-attacks on the company.

Additionally, our results showed that the relationship between board independence (BODIN) and cybersecurity disclosure was positive and significant. This means that firms with a greater percentage of independent directors further enhance cybersecurity governance by providing valuable disclosures to users and various stakeholders. This result is consistent with the stakeholders' perspective that the more independent boards tend to consider the demands of stakeholders. Furthermore, independent boards promote transparency and good governance, reducing information asymmetry, providing more disclosures about cybersecurity risks, and reducing agency problems. Generally, the results are consistent with previous studies related to board independence and cybersecurity disclosure (e.g., [60],Mazumder and Hossain, 2022; [70]). However, a positive but insignificant relationship between board gender diversity and cybersecurity disclosure does not allow us to form any conclusion regarding the relationship between the size of the board of directors and cybersecurity disclosure.

The results showed the relationship between the board meeting (BDMET) and cybersecurity disclosure; the result was significance positive. This finding means that firms with board meetings frequency provide a higher level of cybersecurity disclosure. The frequency meetings of the board to its diligence to considering discussing cybersecurity disclosure issues, which reduces information asymmetry and ensures more transparency [5]. According to the stakeholder theory that the most active and frequent board meeting in the consensus will discuss the most sensitive issues of stakeholders and this agrees with the results of our study. This finding supports the agency theory that the frequency of board meetings is involved in the effective oversight of administrative procedures, which enhances cybersecurity governance [55]. This evidence is consistent with previous studies related to the frequency board meetings and disclosure of the voluntary (e.g., [40]).

This study includes four variables that function as control variables in studying cybersecurity disclosure. Audit committee independence, profitability, firm size, and leverage are variables. All control variables are subjected to multivariate tests in the model to determine whether firm characteristics affect cybersecurity disclosure. The results of these variables are as follows: the profitability was found to be negative and insignificant related to measuring cybersecurity disclosure ($t = -2.69$). Firm size was results showed that it is not significant and positive related to cybersecurity disclosure ($t = 1.37$). Leverage is positively and significantly related to cybersecurity disclosure ($t = 6.01$). Audit committee independence was found to be positively and significantly related to measuring cybersecurity disclosure ($t = -9.87$).

Table 5 Fixed effect regression results for board characteristics and cybersecurity disclosure

Variables	Small firms		Large firms	
BOSI	0.05517	3.19***	0.04299	3.95***
BODIN	0.00406	2.38***	0.00467	1.97*
BGD	−0.00020	−0.11	0.00074	0.41
BDMET	0.00872	1.90*	0.00946	2.33**
ROA	−0.00216	−2.69***	−0.01424	−1.60
FSIZE	0.01454	1.44	0.00457	0.52
LEV	6.2207	35.48***	−0.00010	−1.08
ACI	0.00835	9.16***	0.00482	5.21***
Constant	−0.85853	−4.92***	−0.55038	−2.98***
R^2	Within 0.2766		Within 0.1633	
N	1104		1146	

*Significant at the 0.10 level; **significant at the 0.05 level; ***Significant at the 0.01 level

5 Endogeneity concerns

5.1 Sensitivity tests

To check the robustness and accuracy of the main findings, the study divided firms into two groups based on firm size; large and small firms. The consistent results for the classified groups in both models imply that the main results in Table 4 are robust and accurate (Table 5).

5.2 Two-stage least squares

In our study, we utilize a two-stage least squares (2SLS) estimation approach to mitigate the challenge of endogeneity. 2SLS is recognized as a robust method for addressing endogeneity concerns. As suggested by [6, 71], when properly applied,

Table 6 Instrumental variables (2SLS) regression

	Coef	St.Err	*t*-value	*p*-value	[95% Conf	Interval]	Sig
BOSI	.055	.048	2.15	.04	−.039	.149	*
BODIN	.005	.008	2.08	.09	−.007	.024	*
BGD	.027	.003	1.03	.12	.022	.033	
BDMET	.120	.034	2.35	.02	−.078	.054	**
ROA	.057	.044	1.30	.194	−.029	.142	
FSIZE	.003	.01	−0.58	.561	−.001	0	
LEV	4.31	0.01	4.01	.122	−.066	.59	***
ACI	0.01	.002	1.02	.111	−.033	.66	
R2			0.1902				

***$p < .01$; **$p < .05$; *$p < .1$

2SLS can yield reliable outcomes. Our analysis reveals that the findings presented in Table 6 closely align with the primary results.

6 Conclusion

Cybersecurity issues have become critical to firms, sensitive to the various stakeholders and users of the information, and more attention should be devoted to cybersecurity disclosure. This study aims to investigate the influence of the board characteristics (i.e., the board size, gender diversity, independence and meeting) on cybersecurity disclosure. Based on stakeholder theory, agency theory, and resource dependency theory, the researchers posit that firms with independent directors, larger board sizes, and boards with more frequent meetings are likely to positively influence the level of cybersecurity disclosure. The most effective boards work to be transparent by providing voluntary disclosures, especially disclosures related to cybersecurity. At the same time, females on boards tend to reserve information related to cyber security and do not prefer to disclose it.

The findings of our study have important implications for many parties, such as regulators, policymakers, government agencies, investors, analysts, shareholders, data users, and other stakeholders. Our results provide important insights for regulators about the importance of board characteristics in supporting corporate cybersecurity governance, providing greater transparency and reducing information asymmetry in the marketplace. On the other hand, our findings are of interest to policymakers and government agencies that seek to continually address cybersecurity risks and attacks. Therefore, appropriate policies and guidelines must be developed to enhance corporate governance through the characteristics of the most effective boards of directors in promoting the disclosure process. Furthermore, analysts, investors, shareholders and other data users monitor companies' performance in addressing cybersecurity risks, and this is reflected through the availability of relevant information and disclosures. Thus, the present findings provide them with insight into the importance of the board's characteristics in promoting the dissemination of information related to cyber security, enhancing their understanding and assessment for making informed decisions and providing valuable market analysis. In addition, shareholders monitor the performance of companies and their vigilance to respond to cyber-attacks, and therefore their selection of the right agents will provide more of that information, which reassures them of the company's current situation by reducing information asymmetry and providing them with appropriate disclosure.

Our study provided important results and multiple implications and filled an important gap in the literature. Nevertheless, It can provide the important of the limitations to which the current study is subject opportunities for future researchers. First, the study explored the relationship between board characteristics and cybersecurity disclosure in non-financial firms listed on the U.K. So, it is interesting to see the role of the board's characteristics in disclosing cyber security in other sectors, such as banks, for example. Second, we investigated in the U.K. context; future research may study other similar contexts to provide greater

opportunities for generalisation of the findings. Moreover, future studies should be undertaken across developing countries to provide a more comprehensive understanding of cybersecurity disclosure and firm's performance worldwide. Additionally, Future research can focus on other mechanisms of corporate governance that can affect cybersecurity, as this enhances the ethical dimension of firms and compliance with reinforce each other.

Acknowledgements The authors acknowledge the support from the Program of the National Social Science Foundation of China (19AGL015).

Funding information Projects of National Social Science Foundation of China (19AGL015).

References

1. Adel, C., Hussain, M. M., Mohamed, E. K., & Basuony, M. A. (2019). Is corporate governance relevant to the quality of corporate social responsibility disclosure in large European companies? *International Journal of Accounting and Information Management, 32*(6), 301–332.
2. Agrafiotis, I., Nurse, J.R., Goldsmith, M., Creese, S. and Upton, D., (2018). A taxonomy of cyber-harms: Defining the impacts of cyber-attacks and understanding how they propagate. *Journal of Cybersecurity*, *4*(1), p.tyy006.
3. Aladwey, L., Elgharbawy, A. and Ganna, M.A., (2021). Attributes of corporate boards and assurance of corporate social responsibility reporting: evidence from the U.K. *Corporate Governance: The International Journal of Business in Society*, 22 (4), 748–780.
4. Aladwey, L., Elgharbawy, A. and Ganna, M.A., (2021). Attributes of corporate boards and assurance of corporate social responsibility reporting: evidence from the U.K. *Corporate Governance: The International Journal of Business in Society*.
5. Alodat, A. Y., Al Amosh, H., Khatib, S. F., & Mansour, M. (2023). Audit committee chair effectiveness and firm performance: The mediating role of sustainability disclosure. *Cogent Business and Management, 10*(1), 2181156.
6. Alodat, A. Y., Nobanee, H., Salleh, Z., & Hashim, H. A. (2023). The impact of longer audit committee chair tenure and board tenure on the level of sustainability disclosure: The moderating role of firm size. *Business Strategy & Development, 6*(4), 885–896.
7. Alodat, A. Y., Salleh, Z., & Hashim, H. A. (2022). Corporate governance and sustainability disclosure: Evidence from Jordan. *Corporate Governance: The International Journal of Business in Society, 23*(3), 587–606.
8. Alodat, A. Y., Salleh, Z., Hashim, H. A., & Sulong, F. (2022). Corporate governance and firm performance: Empirical evidence from Jordan. *Journal of Financial Reporting and Accounting, 20*(5), 866–896.
9. Alodat, A.Y., Salleh, Z., Hashim, H.A. and Sulong, F., (2022c). Investigating the mediating role of sustainability disclosure in the relationship between corporate governance and firm performance in Jordan. *Management of Environmental Quality: An International Journal*, (ahead-of-print).
10. Alodat, A. Y., Salleh, Z., Hashim, H. A., & Sulong, F. (2024). Sustainability disclosure and firms' performance in a voluntary environment. *Measuring Business Excellence, 28*(1), 105–121.
11. Amir, E., Levi, S., & Livne, T. (2018). Do firms underreport information on cyber-attacks? Evidence from capital markets. *Review of Accounting Studies, 23*, 1177–1206.
12. Amran, A., Lee, S. P., & Devi, S. S. (2014). The influence of governance structure and strategic corporate social responsibility toward sustainability reporting quality. *Business Strategy and the Environment, 23*(4), 217–235.
13. Ben Barka, H., & Legendre, F. (2017). Effect of the board of directors and the audit committee on firm performance: A panel data analysis. *Journal of Management & Governance, 21*(3), 737–755.
14. Burgess, Z., & Tharenou, P. (2002). Women board directors: Characteristics of the few. *Journal of business ethics, 37*(1), 39–49.
15. Cheng, E. C., & Courtenay, S. M. (2006). Board composition, regulatory regime and voluntary disclosure. *The international journal of accounting, 41*(3), 262–289.

16. Ciftci, I., Tatoglu, E., Wood, G., Demirbag, M., & Zaim, S. (2019). Corporate governance and firm performance in emerging markets: Evidence from Turkey. *International Business Review, 28*(1), 90–103.
17. Ciglic, K., & Hering, J. (2021). A multi-stakeholder foundation for peace in cyberspace. *Journal of Cyber Policy, 6*(3), 360–374.
18. Cortez, E. K., and Dekker, M. (2022). A Corporate Governance Approach to Cybersecurity Risk Disclosure. *European Journal of Risk Regulation*, 1–23.
19. Cyber Security Regulation and Incentives Review, (2016). https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/579442/Cyber_Security_Regulation_and_Incentives_Review.pdf
20. Donnelly, R., & Mulcahy, M. (2008). Board structure, ownership, and voluntary disclosure in Ireland. *Corporate Governance: An International Review, 16*(5), 416–429.
21. Foglietta, C., Masucci, D., Palazzo, C., Santini, R., Panzieri, S., Rosa, L., Cruz, T., & Lev, L. (2018). From detecting cyber-attacks to mitigating risk within a hybrid environment. *IEEE Systems Journal, 13*(1), 424–435.
22. Freeman, R.E., (2010). *Strategic management: A stakeholder approach*. Cambridge university press.
23. Galletta, S., Mazzù, S., Naciti, V., & Vermiglio, C. (2022). Gender diversity and sustainability performance in the banking industry. *Corporate Social Responsibility and Environmental Management, 29*(1), 161–174.
24. Gao, L., Calderon, T. G., & Tang, F. (2020). Public companies' cybersecurity risk disclosures. *International Journal of Accounting Information Systems, 38*, 100468.
25. Gordon, L. A., & Loeb, M. P. (2006). *Managing cybersecurity resources: A cost-benefit analysis* (Vol. 1). McGraw-Hill.
26. Gordon, L. A., Loeb, M. P., Sohail, T., Tseng, C. Y., & Zhou, L. (2008). Cybersecurity, capital allocations and management control systems. *European Accounting Review, 17*(2), 215–241.
27. Haapamäki, E., & Sihvonen, J. (2019). Cybersecurity in accounting research. *Managerial Auditing Journal, 34*(7), 808–834. https://doi.org/10.1108/MAJ-09-2018-2004
28. Haapamäki, E. and Sihvonen, J., (2022). Cybersecurity in accounting research. In *Artificial Intelligence in Accounting* (pp. 182–214). Routledge.
29. Hair, J. F., Jr., Babin, B. J., & Anderson, R. E. (2010). *A global p-erspect-ivie*. Kennesaw State University.
30. Harun, M. S., Hussainey, K., Kharuddin, K. A. M., & Al Farooque, O. (2020). CSR disclosure, corporate governance and firm value: A study on GCC Islamic banks. *International Journal of Accounting & Information Management, 28*(4), 607–638.
31. Hillman, A. J., & Dalziel, T. (2003). Boards of directors and firm performance: Integrating agency and resource dependence perspectives. *Academy of Management review, 28*(3), 383–396.
32. Hillman, A. J., Cannella, A. A., Jr., & Harris, I. C. (2002). Women and racial minorities in the boardroom: How do directors differ? *Journal of management, 28*(6), 747–763.
33. Hlel, K., Kahloul, I., & Bouzgarrou, H. (2020). IFRS adoption, corporate governance and management earnings forecasts. *Journal of Financial Reporting and Accounting, 18*(2), 325–342.
34. Hung, H. (1998). A typology of the theories of the roles of governing boards. *Corporate Governance: An International Review, 6*(2), 101–111.
35. Jensen, M.C. and Meckling, W.H., (2019). Theory of the firm: Managerial behavior, agency costs and ownership structure. In *Corporate Governance* (pp. 77–132). Gower.
36. Jin, J., (2015). Cybersecurity disclosure effectiveness on public companies.
37. Kesner, I. F., & Johnson, R. B. (1990). An investigation of the relationship between board composition and stockholder suits. *Strategic Management Journal, 11*(4), 327–336.
38. Khatib, S. F. A., Abdullah, D. F., Elamer, A., & Hazaea, S. A. (2022). The development of corporate governance literature in Malaysia: A systematic literature review and research agenda. *Corporate Governance, 22*(5), 1026–1053.
39. Kılıç, M. and Kuzey, C., (2016). The effect of board gender diversity on firm performance: evidence from Turkey. *Gender in management: An international journal*.
40. Kumar, K., Kumari, R., Nandy, M., Sarim, M. and Kumar, R., (2022). Do ownership structures and governance attributes matter for corporate sustainability reporting? An examination in the Indian context. *Management of Environmental Quality: An International Journal*, (ahead-of-print).

41. Kweh, Q. L., Ting, I. W. K., Hanh, L. T. M., & Zhang, C. (2019). Intellectual capital, governmental presence, and firm performance of publicly listed companies in Malaysia. *International Journal of Learning and Intellectual Capital, 16*(2), 193–211.
42. Lakhal, F. (2005). Voluntary earnings disclosures and corporate governance: Evidence from France. *Review of Accounting and Finance, 4*(3), 64–85.
43. Laksmana, I. (2008). Corporate board governance and voluntary disclosure of executive compensation practices. *Contemporary accounting research, 25*(4), 1147–1182.
44. Li, H., No, W. G., & Wang, T. (2018). SEC's cybersecurity disclosure guidance and disclosed cybersecurity risk factors. *International Journal of Accounting Information Systems, 30*, 40–55.
45. Li, H., No, W. G., & Wang, T. (2018). SEC's cybersecurity disclosure guidance and disclosed cybersecurity risk factors. *International Journal of Accounting Information Systems, 30*, 40–55.
46. Liao, L., Lin, T. P., & Zhang, Y. (2018). Corporate board and corporate social responsibility assurance: Evidence from China. *Journal of Business Ethics, 150*(1), 211–225.
47. Liao, L., Luo, L., & Tang, Q. (2015). Gender diversity, board independence, environmental committee and greenhouse gas disclosure. *The British accounting review, 47*(4), 409–424.
48. Lorca, C., Sánchez-Ballesta, J. P., & García-Meca, E. (2011). Board effectiveness and cost of debt. *Journal of business ethics, 100*(4), 613–631.
49. Majumder, M. T. H., Akter, A., & Li, X. (2017). Corporate governance and corporate social disclosures: A meta-analytical review. *International Journal of Accounting & Information Management, 25*(4), 434–458.
50. Mansour, M., Aishah Hashim, H., Salleh, Z., Al-ahdal, W. M., Almaqtari, F. A., & Abdulsalam Qamhan, M. (2022). Governance practices and corporate performance: Assessing the competence of principal-based guidelines. *Cogent Business & Management, 9*(1), 2105570. https://doi.org/10.1080/23311975.2022.2105570
51. Mansour, M., Al Amosh, H., Alodat, A. Y., Khatib, S. F., & Saleh, M. W. (2022). The Relationship between Corporate Governance Quality and Firm Performance: The Moderating Role of Capital Structure. *Sustainability, 14*(17), 10525. https://doi.org/10.3390/su141710525
52. Mansour, M., Hashim, H. A., & Salleh, Z. (2020). Datasets for corporate governance index of Jordanian non-financial sector firms. *Data in brief, 30*, 105603. https://doi.org/10.1016/j.dib.2020.105603
53. Mazumder, M.M.M. and Hossain, D.M. (2022). Voluntary cybersecurity disclosure in the banking industry of Bangladesh: does board composition matter? *Journal of Accounting in Emerging Economies*, Vol. ahead-of-print No. ahead-of-print. https://doi.org/10.1108/JAEE-07-2021-0237.
54. Michelon, G., & Parbonetti, A. (2012). The effect of corporate governance on sustainability disclosure. *Journal of management and governance, 16*(3), 477–509.
55. Mueller, M. (2017). Is cybersecurity eating internet governance? Causes and consequences of alternative framings. *Digital Policy, Regulation and Governance, 19*(6), 415–428. https://doi.org/10.1108/DPRG-05-2017-0025
56. Mundial, F.E., (2019). The global risks report 2019. *Ginebra: Foro Económico Mundial*.
57. Nobanee, H., Alodat, A., Bajodah, R., Al-Ali, M., & Al Darmaki, A. (2023). Bibliometric analysis of cybercrime and cybersecurity risks literature. *Journal of Financial Crime, 30*(6), 1736–1754.
58. Nobanee, H., Alodat, A.Y., Dilshad, M.N., El Sayah, A., Alas' ad, S.N., Al Shalabi, B.O., Alsadi, S.F., Al Marri, N.M. and Fiza, F.K., 2023b. Mapping cyber insurance: a taxonomical study using bibliometric visualization and systematic analysis. *Global Knowledge, Memory and Communication*.https://doi.org/10.1108/GKMC-03-2023-0082
59. Pfeffer, J. and Salancik, G.R., 2003. *The external control of organisations: A resource dependence perspective*. Stanford University Press.
60. 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.
61. Ramírez, M., Rodríguez Ariza, L., & Gómez Miranda, M. E. (2022). The disclosures of information on cybersecurity in listed companies in latin america—Proposal for a cybersecurity disclosure index. *Sustainability, 14*(3), 1390.
62. Rao, K. K., Tilt, C. A., & Lester, L. H. (2012). Corporate governance and environmental reporting: An Australian study. *Corporate Governance: The International Journal of Business in Society, 12*(2), 143–163.
63. Rosati, P., Gogolin, F., & Lynn, T. (2022). Cyber-security incidents and audit quality. *European Accounting Review, 31*(3), 701–728.
64. Saggar, R., & Singh, B. (2017). Corporate governance and risk reporting: Indian evidence. *Managerial Auditing Journal, 32*(4/5), 378–405.

65. Saha, R., & Kabra, K. C. (2021). Corporate governance and voluntary disclosure: Evidence from India. *Journal of Financial Reporting and Accounting, 20*(1), 127–160.
66. Saleh, M. W. A., Zaid, M. A. A., Shurafa, R., Maigoshi, Z. S., Mansour, M., & Zaid, A. (2021). Does board gender enhance Palestinian firm performance? The moderating role of corporate social responsibility. *Corporate Governance, 21*(4), 685–701. https://doi.org/10.1108/CG-08-2020-0325
67. Salleh, z., seno, r., alodat, a.y.m. and hashim, h.a., (2022). does the audit committee effectiveness influence the reporting practice of ghg emissions in malaysia?. *journal of sustainability science and management*, *17*(1), pp.204–220.
68. Securities and Exchange Commission (SEC) (2018). Commission statement and guidance on public company cybersecurity disclosures. Available at: www.sec.gov/rules/interp/2018/33-10459.pdf (accessed 13 November 2018).
69. Shackelford, S.J. and Bohm, Z., 2016. Securing North American critical infrastructure: A comparative case study in cybersecurity regulation. *Can.-USLJ*, *40*, p. 61.
70. Smaili, N., Radu, C. and Khalili, A., (2022). Board effectiveness and cybersecurity disclosure. *Journal of Management and Governance*, pp. 1–23.
71. Ullah, I., & Zeb, A. (2023). FinTech and firm's cash holdings: Evidence from China. *Digital Policy, Regulation and Governance, 25*(5), 522–541.
72. Velte, P., Stawinoga, M., & Lueg, R. (2020). Carbon performance and disclosure: A systematic review of governance-related determinants and financial consequences. *Journal of Cleaner Production, 254*, 120063.
73. Virtanen, A. (2012). Women on the boards of listed companies: Evidence from Finland. *Journal of Management and Governance, 16*(4), 571–593.
74. Williams, R. J. (2003). Women on corporate boards of directors and their influence on corporate philanthropy. *Journal of Business Ethics, 42*(1), 1–10.

Authors and Affiliations

Ahmad Yuosef Alodat[1] · Yunhong Hao[1] · Haitham Nobanee[2,3,4] · Hazem Ali[5] · Marwan Mansour[6] · Hamzeh Al Amosh[7]

✉ Ahmad Yuosef Alodat
ahmad.alodat90@gmail.com; ahmad.alodat@mail.zjgsu.edu.cn

Yunhong Hao
haoyh@mail.zjgsu.edu.cn

Haitham Nobanee
nobanee@gmail.com;
haitham.nobanee@oxcis.ac.uk; haitham.nobanee@liverpool.ac.uk; haitham.nobanee@adu.ac.ae

Hazem Ali
yahyahazem2025@gmail.com

Marwan Mansour
m.mansour@aau.edu.jo

Hamzeh Al Amosh
hamza_omosh@yahoo.com

[1] School of Business Administration, Zhejiang Gongshang University, Hangzhou 310018, China

[2] College of Business, Abu Dhabi University, Abu Dhabi, UAE

[3] Oxford Centre for Islamic Studies, University of Oxford, Oxford, UK

[4] Faculty of Humanities and Social Sciences, The University of Liverpool, Liverpool, UK

[5] School of Economics and Managememt, Yiwu Industrial and Commercial College, Jinhua, China

[6] Faculty of Business, Economics and Social Development, Amman Arab University, Amman, Jordan

[7] College of Accounting Sciences, University of South Africa, Pretoria, South Africa