Journal of Management and Governance (2024) 28:359–404
https://doi.org/10.1007/s10997-022-09660-7

Board of directors' attributes and aspects of cybersecurity disclosure

Sylvie Héroux[1] · **Anne Fortin**[1]

Accepted: 12 October 2022 / Published online: 18 November 2022

Abstract

As cybersecurity is a critical risk issue for organizations, cybersecurity disclosure is important for financial regulators, financial analysts, shareholders, and other stakeholders. Organizations face challenges when deciding whether, what, and when cybersecurity-related information should be disclosed. Prior studies have contributed few insights regarding the potential determinants of cybersecurity disclosure. Furthermore, their findings are based on a general or narrow measurement of this disclosure. This study draws on upper echelons and signaling theories to examine the association between various board of directors' characteristics and extent of overall cybersecurity disclosure and its individual aspects. Extent of cybersecurity disclosure is measured based on a content analysis of annual financial regulatory filings of the 250 companies listed on the S&P/TSX Composite Index, using a scoring grid of 40 items grouped into seven categories representing different aspects of cybersecurity disclosure. This expanded disclosure measurement provides original insights for firms and their stakeholders. The main findings indicate that the presence of a committee responsible for cybersecurity on the board of directors is key to increasing cybersecurity disclosure. With or without such a committee, board IT expertise, board tenure, board independence, women directors, and board age are associated with the extent of total cybersecurity disclosure or some of its specific aspects, particularly cybersecurity risk mitigation. These findings contribute to the cybersecurity literature by examining which board of directors' characteristics influence the extent of specific aspects of cybersecurity disclosure. They also complement results from upper echelons-based studies on corporate reporting determinants and prior IT governance studies.

Keywords Board of directors' attributes · Cybersecurity disclosure · Upper echelons theory · Signaling theory · Cybersecurity governance · IT governance

✉ Sylvie Héroux
heroux.sylvie@uqam.ca

Extended author information available on the last page of the article

1 Introduction

Cybersecurity has become a crucial issue for organizations around the world. In the United States, for example, "cyberattacks rank as the fastest growing crime … causing catastrophic business disruption.… Cybersecurity is high stakes from Wall Street to the C-Suite, with the threat to enterprises expected to increase in frequency and force" (ISACA/Downs, 2020). Facebook (CSIS, 2021), Twitter, and Zoom (ISACA/Downs, 2020), among others, grappled with the negative consequences of significant cyber incidents/attacks in 2020 and were prompted to disclose information on these incidents to reassure their stakeholders.

Cybersecurity disclosure is important to the process of informing investors and other stakeholders about cyber risks and cyber incidents/attacks (Bakker & Streff, 2016). This practice combines strategic motives with adherence to financial regulators' cybersecurity disclosure guidelines (e.g., CSA, 2016, 2017a, 2017b; SEC, 2011, 2018). Some motives include providing additional disclosure to explain the company's actions after a cyberattack. This disclosure aims to reassure shareholders about the impact on company operations, and other stakeholders, such as clients and suppliers, about the protection of sensitive/personal data. Organizations may send a positive signal to financial markets by describing the mechanisms that were put in place to mitigate cybersecurity risks. However, "cybersecurity risk disclosure is a double-edged sword since it could reduce information asymmetry but also increase the probability of future cybersecurity incidents" (Walton et al., 2021, p. 162). As a result, organizations face many challenges in making cybersecurity disclosure decisions (e.g., finding a balance between over- and under-reporting, as in Ferraro, 2014, or choosing when to disclose cybersecurity-related information, as in Newman, 2018).

Prior studies have described the significant positive and negative consequences of disclosing cybersecurity-related information. For instance, disclosing any information security-related items in SEC annual filings is positively associated with firms' market value (Gordon et al., 2010). However, the nature of information security risk factors (e.g., risk management activities or external threats disclosed in firms' public annual report) is associated with future breaches announced in the media (Wang et al., 2013), while cybersecurity risk disclosure (in terms of presence and length/number of words) is positively associated with subsequent cybersecurity incidents (Li et al., 2018). Further, disclosing the existence of trade secrets is associated with a greater probability of facing subsequent cybersecurity breaches than not making such disclosures (Ettredge et al., 2018). In addition to these results, it should be noted that the market has a small negative reaction to disclosed cyberattacks but a much stronger adverse reaction when information withheld in that matter is discovered later (Amir et al., 2018).

Cybersecurity research can help enhance the communication of cybersecurity-related information to stakeholders (Walton et al., 2021). Results from the literature on the determinants of cybersecurity disclosure suggest that financial regulators influence disclosure practices. Indeed, information security disclosure has gained momentum following the Sarbanes–Oxley Act (SOX) (Gordon et al.,

2006). Further, firms disclose more cybersecurity-related information if an industry leader, close rival, or numerous industry peers have received a letter from the SEC commenting on their cybersecurity risk disclosure (Brown et al., 2018). Prior literature also suggests that some board of directors' attributes can impact cybersecurity disclosure. In this regard, based on stakeholder and resource dependence theories, Radu and Smaili (2021) examined the impact of board diversity on cybersecurity disclosure and found that the percentage of women on boards is positively associated with the presence and number of paragraphs/words in the annual report related to cybersecurity disclosure. In addition, based on stakeholder theory, Smaili et al. (2022) noted that board independence and financial expertise are positively associated with the amount of cybersecurity disclosure. Drawing on signaling theory, Higgs et al. (2016) found that firms with a technology committee on their board of directors are more likely to report breaches than firms without such a committee. However, there is still a dearth of research on the determinants of cybersecurity disclosure (Haapamäki & Sihvonen, 2019; Walton et al., 2021).[1] More studies are needed to identify the potential factors that would facilitate the disclosure of cybersecurity risk, improve disclosure practices, and generalize conclusions (Walton et al., 2021).

With this literature gap in mind, our first motivation was to examine if, in addition to factors such as board member gender, board independence, board financial expertise, and a board IT committee, other board of directors' characteristics could be instrumental in cybersecurity disclosure. The upper echelons framework (Hambrick & Mason, 1984) provides a relevant theoretical background for answering this research question since, through their educational background and career paths, the members of the board of directors may have developed knowledge and experience that could be useful to the board when it monitors compliance with financial regulators' cybersecurity disclosure guidelines or advises management in that matter. In that spirit, we drew on demographic characteristics identified in upper echelons literature (education and work experience, tenure, gender, and age, in Liu & Ji, 2022; Plöckinger et al., 2016) to select five variables. More specifically, consistent with upper echelons theory, we argue that board *IT* knowledge and experience (board IT expertise), *firm-specific* knowledge and experience (board tenure), *variety* of knowledge and experience (board independence), gender (women directors on the board), and directors' age (board age) could be potential determinants of cybersecurity disclosure. Further, if the board has a committee responsible for cybersecurity, this could signal that the board is prepared to be involved in cybersecurity matters, including disclosure. Thus, drawing upon signaling theory, we added a sixth variable and hypothesize that having a committee responsible for cybersecurity on the board of directors is another board-level characteristic that could be associated with cybersecurity disclosure.

[1] Haapamäki and Sihvonen (2019) identified only a small number of studies on disclosure of cybersecurity activities in their review of 39 cybersecurity-related accounting and auditing studies published between 2000 and 2018. Walton et al. (2021) found only two studies on the determinants of cybersecurity disclosure in their extensive analysis of 68 cybersecurity papers published from 2001 to 2019 in accounting, information systems, and computer science research.

Another aspect to consider is that, to our knowledge, studies on the determinants of cybersecurity disclosure limit their measurement of disclosure to one specific aspect (e.g., risk factor disclosure, as in Brown et al., 2018, or reported breaches, as in Higgs et al., 2016), or they use a general measurement (e.g., presence and number of paragraphs/words related to cybersecurity disclosure in the annual report, as in Radu & Smaili, 2021; Smaili et al., 2022). As suggested by Brown et al. (2018, p. 651) in regard to the disclosure of risk factors, "better ways of quantifying qualitative disclosure and [capturing] different aspects of qualitative disclosure" would improve the measurement of this content. Considering this methodological limit to prior studies, our second motivation was to use a refined measurement of cybersecurity disclosure based on its content.

In light of the gaps/limitations described above, the aim of this study is to examine whether various board of directors' characteristics are associated not only with the overall extent of cybersecurity disclosure but also with the extent of the different aspects disclosed. To test our six hypotheses, we analyzed the content of cybersecurity disclosures in the most recent annual regulatory filings of the 250 companies listed on the S&P/TSX Composite Index that were publicly available at the start of data collection in May 2018. We measure cybersecurity disclosure using a scoring grid of 40 items grouped into seven categories representing different aspects of cybersecurity disclosure. Regression analyses were performed on the total disclosure score, as well as on scores by disclosure categories.

The main findings suggest that board IT expertise, board tenure, board independence, and women on the board are associated with the extent of specific aspects of cybersecurity disclosure. Further, the presence of a committee responsible for cybersecurity on the board of directors is key to increasing cybersecurity disclosure. Additional analyses of firms with and without such a committee show that different board attributes stand out in each situation and significantly affect total cybersecurity disclosure and most of its aspects.

These findings contribute to the cybersecurity literature by identifying various board of directors' characteristics that could be associated with the different aspects disclosed. They also add to the results of upper echelons theory-based studies on the determinants of corporate reporting because cybersecurity disclosure is one form of this reporting. Finally, the findings complement results from prior IT governance/cybersecurity-related studies on the impact of board of directors' committees, board IT expertise, and gender diversity on boards.

Results from this study have practical implications. Management, financial analysts, and financial regulators can use the descriptive data to obtain an overview of the cybersecurity-related information that companies do or do not disclose. Managers could also use these data as a relevant benchmark tool to identify areas of improvement in their companies' cybersecurity disclosure. The findings provide financial investors with further motivation to incorporate data such as information on risk mitigation measures into their investment analysis process. Financial regulators could use the descriptive data to guide them as they monitor cybersecurity disclosure practices and update guidelines in that matter. In addition, the regression results may provide managers with a basis for adjusting their companies' board composition, since some board of directors' attributes are associated with greater transparency

regarding some aspects of cybersecurity disclosure. Results also show that having a committee responsible for cybersecurity on the board of directors can help management increase cybersecurity disclosure. Financial regulators could make this committee a requirement of listed companies, or ask them to have at least one board member with IT expertise so they can increase their cybersecurity disclosure. Lastly, the findings also provide information about the board of directors' involvement in cybersecurity disclosure issues, a consideration that financial analysts could add to their investment analysis.

The remainder of this paper is organized as follows. In Sect. 2, as background to the study, we present directors' legal duties vs. their expected role respecting cybersecurity, which we follow with the theoretical framework and the development of our hypotheses. The research method is detailed in Sect. 3. Results are presented in Sect. 4 and discussed in Sect. 5. In Sect. 6, the conclusion outlines the paper's theoretical contributions, practical implications, limitations, and research avenues.

2 Background, theoretical framework, and hypotheses development

2.1 Directors' legal duties vs. expected role respecting cybersecurity

The duties of directors are prescribed by legislation governing corporations. For example, the *Canada Business Corporation Act* (1985) and the U.S. *Model Business Corporation Act* (2017)[2] stipulate that all directors should act in the best interests of the corporation in discharging their decision-making and oversight duties, with the care that a prudent person would consider appropriate in similar circumstances. In light of corporate laws, directors serve primarily the corporation and its shareholders (shareholders' primacy) in performing these duties, but could nonetheless consider the interests of other stakeholders while still acting within the corporation's best interests.

In IT/cybersecurity-related contexts, researchers have pointed out that a gap exists between the board of directors' duties under the law and expectations regarding their cybersecurity duties (which may exceed the capacity of the board's IT governance structure or IT abilities). A case study by Georg (2017) presents

[2] This is illustrated by the following excerpts: "When acting with a view of the best interests of the corporation … the directors and officers of the corporation may consider, but are not limited to, the following factors: the interests of shareholders, employees, retirees and pensioners, creditors, consumers, and governments; the environment; and the long-term interest of the corporation" (Canada Business Corporation Act, 1985, p. 122(1.1)). Further, "In determining what the director reasonably believes to be in the best interests of the corporation, [a director may consider] (1) the long-term as well as the short-term interests of the corporation, (2) the interests of the shareholders, long-term as well as short-term, including the possibility that those interests may be best served by the continued independence of the corporation, (3) the interests of the corporation's employees, customers, creditors and suppliers, and (4) community and societal considerations, including those of any community in which any office or other facility of the corporation is located. A director may also consider, in the discretion of such director, any other factors the director reasonably considers appropriate in determining what the director reasonably believes to be in the best interests of the corporation" (Connecticut Business Corporation Act, 1997, 45 CS 101, Sect. 33–756, g). In the United States, business corporation laws are a state matter.

non-executive boards "as representatives of company stakeholders" (p. 793) but finds a gap between their information security governance and the legal requirements they must comply with in relation to this issue. Some boards of directors are not informed about the risks and potential damage to the company that may be caused by leaks of confidential data or the need for activities to mitigate this risk (part of their oversight function). Other IT/cybersecurity governance studies reveal an insufficient number of technology committees on boards (Price & Lankton, 2018), lack of board IT expertise (Ashraf et al., 2020; Valentine & Stewart, 2013), difficulty recruiting board members with both risk management and IT competence (Czarnecki, 2015), and low board involvement in IT (Price & Lankton, 2018). However, considering the importance of cybersecurity-related decisions in organizations' and boards of directors' cybersecurity oversight responsibilities (Bonime-Blanc, 2017), some governance experts continue to argue that assessment of cybersecurity risk requires a bump in board IT expertise (Czarnecki, 2015). In other words, IT expertise on the board of directors would enhance the effectiveness of organizations' cybersecurity governance (Bonime-Blanc, 2017). This would mean changes in the audit committee's role (Deloitte, 2015) or establishing a technology committee on boards of directors as a further IT governance structure (Turel et al., 2019). Hence, to discharge their oversight duties with respect to cybersecurity decisions, the board of directors (as a group) can benefit from having a technology committee (Higgs et al., 2016) and IT expertise on the board itself (Vincent et al., 2019) or on its audit committee (Ashraf et al., 2020).

Indeed, considering the magnitude of the potential consequences identified in prior studies, organizations face many challenges in making cybersecurity disclosure decisions. They must find a balance between over- and under-reporting (Ferraro, 2014), especially in the case of severe cyberattacks (Amir et al., 2018; Mitra & Ransbotham, 2015) or security breaches (Higgs et al., 2016). They must choose when to disclose cybersecurity-related information (e.g., Newman, 2018). They may assess the benefits of an independent examination of the disclosures (assurance services) (Frank et al., 2019) and, if they opt for these services, they must select an assurance service provider. To meet stakeholders' information needs in terms of different aspects of cybersecurity disclosure, organizations must anticipate stakeholders' perceptions of the quality of the cybersecurity disclosure in terms of materiality (Ferraro, 2014; Young, 2013), timeliness and reliability (Ashraf et al., 2020), or measurability, completeness, relevance, and objectivity (AICPA, 2017). Boards of directors can advise or guide management facing these challenges. Results from a NYSE survey of 200 directors from public companies indicate that cybersecurity is a board-level concern and that directors perceive cybersecurity from a financial point of view (Rashid, 2015). According to the 2018 SEC guidance,[3] "companies should disclose how the board is involved with cybersecurity" (Lankton et al., 2020, p. 2). For instance, the board of directors can be involved in management's decisions about disclosing data breaches (Higgs et al., 2016). The board can ask questions about IT risk management and discuss IT risk

[3] Since the SEC's (2011) disclosure guidelines needed to be enhanced (Ferraro, 2014; Young, 2013), the SEC issued interpretive guidance on public company cybersecurity disclosures (SEC, 2018).

issues (Vincent et al., 2019). "IT risks are the risks information technology poses to financial reporting when IT results in poor internal controls, accounting information, or cybersecurity" (Ashraf et al., 2020, p. 24). Cyberattacks and unauthorized data disclosure are examples of IT risk issues (Turel et al., 2019). Cybersecurity "exceeds the boundaries of IT and cyber risk needs to be managed with as much discipline as financial risk" (Deloitte, 2015, p. 6).

2.2 Theoretical framework

Governance researchers present board governance as both a fiduciary and an advisory body, respectively in its work of monitoring management's compliance with regulation and advising management on strategic decision making (Ben-Amar et al., 2013; Labelle et al., 2010).

Upper echelons theory (Hambrick & Mason, 1984) models the impact of top management characteristics on organizational strategic choices.[4] For instance, it has been used to examine executives' influence on corporate financial reporting (Patelli & Pedrini, 2015; Plöckinger et al., 2016). Researchers have brought the board of directors into the upper echelon model since it is an important governing and decision-making body (Hafsi & Turgut, 2013) and it sits on the highest level of the organization (Vairavan & Zhang, 2020) alongside the top management team. Under upper echelons theory, knowledge and experience gained through education, function, and other types of career backgrounds as well as "more straightforward/obvious/surface-level" personal characteristics such as gender and age, influence upper echelons' decisions because these traits are considered "valid proxies of their cognitive frames" (Vairavan & Zhang, 2020, p. 1226). Board diversity in terms of education, tenure, gender and age (Kagzi & Guha, 2018), or independence (Hafsi & Turgut, 2013) can influence organizational outcomes by bringing various perspectives and types of knowledge and experience to interactions with management.

Drawing on the underlying assumptions of upper echelons theory, we developed six hypotheses under the expectation that board education/career-related characteristics and other personal traits could be associated with reporting decisions such as cybersecurity disclosure. The associations under study take into consideration the influence of the following items on this type of disclosure: *IT* knowledge and experience (board IT expertise), *firm-specific* knowledge and experience (board tenure), *variety* of knowledge and experience (board independence), gender (women directors on the board), and directors' age (board age).

In addition, under the signaling theory lens, having a "strong board" (i.e., a board perceived as a quality resource) positively signals to stakeholders that the board can effectively monitor and advise management and protect stakeholders'

[4] Strategic choices are "complex and of major significance to the organization…. The term "strategic choice" … is intended to be a fairly comprehensive term to include choices made formally and informally, indecision as well as decision" (Hambrick & Mason, 1984, pp. 194–195). With this in mind, considering the importance of the potential consequences related to cybersecurity and the many challenges organizations face in making cybersecurity disclosure decisions, cybersecurity disclosure qualifies as a strategic decision.

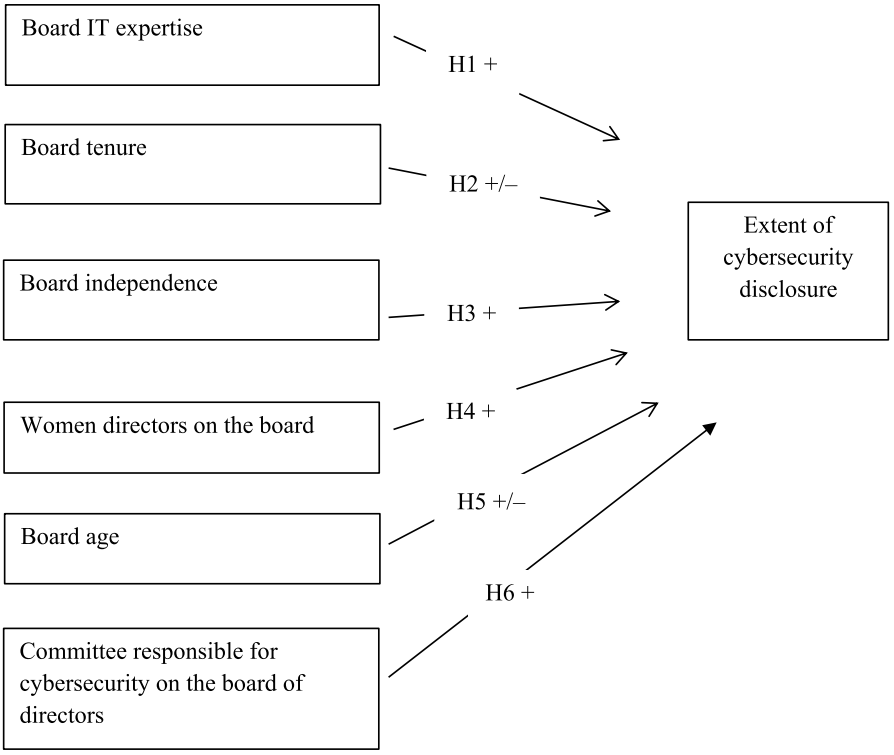

Fig. 1 The theoretical model

interests (Bear et al., 2010). Further, IT expertise on the board could itself signal that the board has the capability to exercise IT risk oversight (Higgs et al., 2016). If the board has an IT committee, it "should include at least one IT expert with profound knowledge of the business needs" (Caluwe & De Haes, 2019, p. 6191). It follows that a committee responsible for cybersecurity on the board of directors would also send stakeholders a positive signal that the board is prepared to address cybersecurity issues, including disclosure. Board members on this committee would be considered valuable resources who can advise management with respect to the extent of the firm's cybersecurity disclosure, including information such as actual cybersecurity incidents and their impacts, cybersecurity risk mitigation, and responsibility for cybersecurity strategy.

The six hypotheses under study are illustrated in Fig. 1 and are developed in the next paragraphs.

2.3 Board IT expertise

Board IT expertise in terms of education, experience, and training enables the board to better advise and oversee management in terms of IT risk management (Vincent et al., 2019). Board members with IT knowledge or experience are more aware of IT's role and more involved in IT-related oversight and strategic decision making (Jewer & McKay, 2012; Yayla & Hu, 2014). In that spirit, firms that have experienced data breaches and other IT-related operational failures have increased their board's IT expertise/competency (Benaroch & Chernobai, 2017).

In discussions about cybersecurity, audit committee members with IT expertise carry more weight than other members (Ashraf et al., 2020). Their cybersecurity knowledge and experience enable them to ask management pointed questions with respect to actual or potential cybersecurity concerns and better understand the scope and importance of data breaches (Ashraf et al., 2020). As a result, the audit committee can "better oversee management and … advise on cybersecurity risks related to financial reporting" (Ashraf et al., 2020, p. 27).

Overall, members' IT expertise helps boards be more effective in IT-related financial reporting decisions by enhancing their understanding of the impact of IT risks on financial reporting, the scope and importance of data breaches, and stakeholders' cybersecurity information needs. This "specialized" IT-related knowledge and experience is an asset when it comes to deciding what information to disclose and using the proper terms when doing so. We therefore expect that greater IT expertise on boards will lead management to disclose more cybersecurity-related information.

H1 Board IT expertise is positively associated with extent of cybersecurity disclosure.

2.4 Board tenure

Board tenure refers to directors' firm-specific knowledge and experience (Hafsi & Turgut, 2013). As board members' tenure increases over time, board members become more familiar with the firm (Barroso et al., 2011) and its strategic issues (Kesner, 1988). However, longer board tenure can have negative impacts (Baran & Forst, 2015). Longer-tenured board members are more likely to become friends with management, at the expense of shareholder interests (Vafeas, 2003). They are less effective in monitoring (Baran & Forst, 2015) and supervising management (Barroso et al., 2011). They "may be shy to introduce controversy in the decision-making process" (Hafsi & Turgut, 2013, p. 474) and may resist strategic change (Golden & Zajac, 2001). Prior studies suggest that "extended tenure of board members … can result in trenching behind existing practices and procedures, with directors distancing themselves from new ideas" (Barroso et al., 2011, p. 356).

In the context of our study, it is reasonable to characterize cybersecurity issues such as disclosure as a new challenge for boards of directors and management. Regulators have only recently provided cybersecurity disclosure guidelines (e.g., CSA, 2016, 2017a, 2017b; SEC, 2018), and practices in that matter are still evolving.

The cybersecurity oversight function would benefit from boards of directors being in a position to deal with turbulent situations such as data breaches. In light of the assumptions of upper echelons theory, some people may assume that longer-tenured boards would be reluctant to increase the extent of the organization's disclosure of cybersecurity matters and their members might not be willing to bring new ideas to management with respect to this disclosure due to a desire to hold onto existing financial reporting practices. However, others can argue that longer-tenured board members have greater knowledge and experience regarding the firm's specific cyber risks. This can incline them to encourage the disclosure of additional cybersecurity-related information such as the organization's actions to face the new challenges.

The above discussion leads to the following hypothesis:

H2 Board tenure is associated with extent of cybersecurity disclosure.

2.5 Board independence

According to Westpal and Fredrickson (2001), "board members tend to use their personal experience as a reference point or a benchmark when monitoring decisions and behaviors of top management" (Yoo & Kim, 2012, p. 147). Organizations with independent boards can benefit from a variety of learning experiences and knowledge gained by board members in other industries or businesses, as they have a large proportion of external members or non-executive directors (Yoo & Kim, 2012). In terms of IT governance activities, Jewer and McKay (2012) found that having more insiders on the board of directors was associated with less board-level IT governance, regardless of the defensive or offensive role of IT in the organization (Nolan & McFarlan, 2005). If an organization implements an IT oversight or similar committee at the board level, "independent directors are considered to be appropriate members" for increasing board engagement in IT governance (Caluwe & De Haes, 2019, p. 6191). Further, more independent boards are associated with disclosure of material information on sustainability activities (Bing & Amran, 2017) and level of corporate social reporting (Barako & Brown, 2008).

In light of the above and in the context of our study, more independent boards may bring different perspectives that allow them to consider the information needs of multiple stakeholders and be more active in monitoring and advising management with respect to cybersecurity disclosures. Boards with more outsiders (hence, fewer insiders) could be more involved in IT governance, including cybersecurity governance. Just as in the field of sustainability reporting, the materiality concept is relevant in determining the extent of cybersecurity-related information to disclose (Ferraro, 2014; Young, 2013). Thus, similar to Bing and Amran's (2017) proposition, more independent boards may influence cybersecurity disclosure by helping management define what different stakeholders consider to be material information, such as in the case of cyberattacks.

Overall, more independent boards could lead organizations to disclose more cybersecurity-related information to take into consideration all stakeholder information needs. This leads to H3:

H3 Board independence is positively associated with extent of cybersecurity disclosure.

2.6 Women directors on the board

Women are more risk and inequality averse and more sensitive to the context than their men counterparts are (Croson & Gneezy, 2009). These risk and social preferences have implications for women's behavior and decision-making process. For instance, women directors raise a wider variety of issues and assess a broader range of outcomes (Bear et al., 2010; Nielsen & Huse, 2010). Given their deeper involvement in corporate social responsibility activities (Williams, 2003), women directors tend to have a greater sense of responsibility toward stakeholders (Baalouch et al., 2019). Their higher sensitivity can affect a corporation's transparency (Larkin et al., 2013). For instance, women directors could bring about "better disclosure of material information in sustainability reporting" (Bing & Amran, 2017, p. 104). They could lead to a higher level of corporate social responsibility information (Barako & Brown, 2008). Nursimloo et al. (2020) mention a number of prior studies showing that board gender diversity is associated with increased disclosure on that topic. Further, Bravo (2018) showed that board gender diversity is positively associated with voluntary risk disclosure in annual reports, suggesting that the presence of women is significant for this disclosure.

In the same spirit, we argue that cybersecurity disclosure has a corporate social responsibility dimension, since cyberattacks or cyber incidents can affect a variety of stakeholder interests. For instance, sensitive personal information pertaining to clients or employees can be used for fraudulent purposes when an organization suffers a data breach. Payments to suppliers and lenders can be delayed, interrupted, or even cancelled when funds are misappropriated by hackers. With their heightened awareness of stakeholders' interests, women directors could expose the board and managers to other perspectives when the time comes to decide the extent of cybersecurity-related disclosure. The perspective of women is also expected to help with oversight of managerial decisions regarding cybersecurity matters. For instance, women directors' greater aversion to risk could lead to more discussions with the board and management about cybersecurity risk factors, cybersecurity risk mitigation tools, and increased disclosure of this information. In that spirit, Radu and Smaili (2021) found that gender diversity is positively associated with the presence and number of paragraphs/words in the annual report related to cybersecurity disclosure.

Overall, having women directors on their board could lead organizations to disclose more cybersecurity-related information. With this in mind, we expect the following:

H4 Having women directors on the board is positively associated with extent of cybersecurity disclosure.

2.7 Board age

Under upper echelons theory, tenure, gender, and age are different constructs. Younger executives are expected to be more open to new ideas, less risk averse, and less inclined to keep the status quo (Hambrick & Mason, 1984). "In summary, empirical studies on the effects of managerial age are generally consistent in that they find that younger [executives] are more likely to undertake risky activities" (Liu & Ji, 2022, p. 5). For instance, the age of executives has been found to be negatively associated with voluntary corporate financial disclosure (Bamber et al., 2010) and the extent of information technology adoption (Chuang et al., 2009).

One the one hand, "studies on gender are similar to studies on age in that they focus on the differences in risk attitudes" (Liu & Ji, 2022, pp. 6–7). In that spirit, Bravo (2018, p. 110) suggests that "[t]he demand for information on risks has become especially significant for stakeholders in recent years, and precisely, it is younger directors who are expected to be more sensitive to stakeholders". With this in mind, similar to women who are sensitive to stakeholders' information needs, younger directors could be more inclined than older ones to argue for more cybersecurity disclosure. On the other hand, board age could also be a proxy for experience (Kagzi & Guha, 2018), as suggested by Johnson et al. (2013). As a result, "[t]here are conflicting arguments regarding the behavior of executives at different ages" (Liu & Ji, 2022, p. 5). In short, younger executives might be willing to take risks but might also be concerned about doing so, which may lead them to follow older executives' behavior given the latter's more extensive experience.

In the context of this study, since cybersecurity is a critical risk issue for organizations, disclosing more cybersecurity-related information is important for financial regulators, financial analysts, shareholders, and other stakeholders. In light of the above, to better inform stakeholders, younger directors may be willing and prepared to disclose more cybersecurity-related information as they may be quite attuned to the cyber world and its challenges. However, some could argue that younger directors could prefer to rely on longer-tenured board members' firm-specific experience. As presented in the development of H2, arguments can be made with respect to these board members favoring either more or less cybersecurity disclosure. This is reflected in H5:

H5 Director age is associated with extent of cybersecurity disclosure.

2.8 Committee responsible for cybersecurity on the board of directors

Cyber-risk oversight has traditionally been assigned to the audit committee (NACD, 2017). A review of the 2016 proxies of S&P 100 companies revealed that 27% of these companies disclosed the audit committee's responsibilities regarding cybersecurity risk oversight (Hitchcock et al., 2017). As this responsibility is in addition to responsibilities related to financial reporting and disclosure in a broad sense, members of the audit committee could ask management questions about how cybersecurity risks are disclosed (Deloitte, 2015). However, the committee's involvement with respect to cybersecurity differs significantly by industry and business (Deloitte, 2015). Further, this oversight role "is not widespread, even among the largest firms" as only 104 out of a sample of 189 companies (55%) from among the 300 firms on the 2018 Fortune 500 "include ITG roles in the audit committee charter" (Lankton et al., 2020, p. 22).

Some firms have a risk committee separate from the audit committee. Specifically, firms "for which technology forms the backbone of their business often have a dedicated cyber risk committee that focuses exclusively on cybersecurity" (Deloitte, 2015, p. 6). Companies may also form a board-level technology committee to signal to stakeholders that the upper echelon considers IT to be a strategic tool (Turel et al., 2019) or that oversight of breach risks is a board priority (Higgs et al., 2016). These firms are more committed to cybersecurity and more inclined to react after a cybersecurity breach (Lankton et al., 2020). Indeed, "firms' responses to the SEC's act of 'encouraging' disclosure [about cybersecurity risks and cyber incidents] can be considered a form of regulatory compliance. Therefore, establishing a separate technology committee could improve governance by increasing the likelihood of disclosure (i.e., reporting breaches), and helping to signal credibility in other ways such as preventing and identifying breaches" (Higgs et al., 2016, p. 80).

Overall, prior studies show that boards of directors are involved in cybersecurity oversight to various degrees. The board as a whole or a specific board-level committee (e.g., the audit committee, or a specific risk or technology committee) may advise managers and monitor their cybersecurity decisions, including cybersecurity disclosures. It is reasonable to assume that having a board of directors committee specifically responsible for cybersecurity matters will lead a firm to disclose more cybersecurity-related information to keep stakeholders well-informed. This discussion leads to H6:

H6 The presence of a committee responsible for cybersecurity on the board of directors is positively associated with extent of cybersecurity disclosure.

3 Methods

3.1 Research design

In prior research, cybersecurity disclosure has been measured by either its presence (binary variable) or the number of paragraphs or words related to cybersecurity

disclosure (e.g., Li et al., 2018; Radu & Smaili, 2021). This means that the actual content of the disclosures has received little attention and the construct "cybersecurity disclosure" has yet to be refined. We thus propose testing the associations between the extent of cybersecurity disclosure measured on the basis of its content and the independent variables of our six hypotheses, which we developed using a multi-theoretical lens. In terms of Edmondson and McManus' (2007, p. 1158) archetypes of methodological fit in field research, this study is at the intermediate theory stage as it "presents provisional explanations of phenomena … introducing a new construct [or measure, p. 1160] and proposing relationships between it and established constructs". Such studies can include "initial tests of hypotheses enabled by prior theory" (Edmondson & McManus, 2007, p. 1165), which the current research also does. Both qualitative and quantitative data can be collected to answer the research question, and standard statistical analyses can be used to analyze the quantitative data. In this study, a qualitative analysis of financial regulators' guidelines was conducted to obtain cybersecurity disclosure items and categories and was followed by a content analysis of companies' financial regulatory filings to generate quantitative data for hypothesis testing. To test the association between the extent of cybersecurity disclosure and the various board of directors' characteristics presented in the six hypotheses, we use multiple regressions examining "the relationship between a single dependent variable and a set of independent variables" (Hair et al., 1998, p. 159).

The multiple regressions used are Tobit regressions. These regressions are appropriate when the range of the dependent variable is constrained, such as when several observations are at zero (Amemiya, 1984). This feature destroys the linearity assumption and makes use of the least squares method inappropriate (Amemiya, 1984). As each dependent variable in this study takes the value of 0 in a number of instances (18 for total disclosure score up to 199 for actual cybersecurity incidents, not tabulated), we use Tobit regressions left-censored at 0. To control for the presence of any heteroscedasticity, we use heteroscedasticity-robust standard errors.

The determination of whether hypotheses are supported is based on the significance of the regression coefficients on the independent variables. Regressions are performed for each dependent variable expressing the extent of cybersecurity disclosure (see Sect. 3.4).

3.2 Context and sample data

The study uses Canada as its context and examines the association between various board of directors' characteristics and extent of cybersecurity disclosure. The sample consists of the 250 largest companies that were operating on the Canadian financial market on May 3, 2018, retrieved from the S&P/TSX Composite Index of the Toronto Stock Exchange (TSX). This index covers approximately 95% of the Canadian equities market.[5]

[5] https://money.tmx.com/en/quote/^TSX.

Table 1 Sample companies' industrial sector membership

Industrial sector	Frequency	Percentage
Financial services	26	10.4
Energy	48	19.2
Industrials	22	8.8
Basic materials	55	22.0
Communication services and technology	19	7.6
Consumer cyclical and defensive and health care	41	16.4
Utilities	13	5.2
Real estate	26	10.4
Total	250	100.0

Toward the end of 2016, the Canadian Security Administrators (CSA) issued a staff notice on cybersecurity indicating that "many issuers either did not have any disclosure or only had non-entity specific, boilerplate disclosure" (CSA, 2016, p. 3). In early 2017, it thus issued *CSA Multilateral Staff Notice 51-347* (2017b) to provide guidance on cybersecurity disclosure. Based on the CSA's review of the cybersecurity disclosure of its registrants on the S&P/TSX Composite Index in 2016, the staff notice indicated that disclosure was low for some categories of information (e.g., responsibility for cybersecurity strategy and actual cybersecurity incidents). Cybersecurity disclosure was therefore still a fledgling practice in Canada at the start of this study, which covers the financial regulatory filings for financial periods mainly ending in 2017 or early 2018.

The large number of companies in the S&P/TSX Composite Index enables the use of statistical analyses. In addition, by considering the entire index, we avoided selection bias. Data on the firms' industrial sector membership were collected from the company description presented on the TSX Website (see Table 1).

3.3 Variables and their measurement

Table 2 presents the regression variables, the abbreviations used in the models, and measurements. Measurement of the dependent variable is further explained in the following sub-section. Figure 2 presents the steps from data collection to analysis that are further detailed in Sects. 3.3 and 3.4.

3.3.1 Dependent variable—cybersecurity disclosure

We developed an initial scoring grid comprised of 38 items, or codes. We selected the items of interest from two financial regulators' guidelines, CSA *Multilateral Staff Notice 51-347* (2017b) and the SEC's *Commission Statement and Guidance on Public Company Cybersecurity Disclosures* (2018). Both documents contain the same requirements and constituted up-to-date guidance on the topic at the start of coding in May 2018. Hence, sample firms were expected to follow these guidelines,

Table 2 Regression variables and their measurement

Variables	Abbreviations	Measurement
Dependent variables		
Total disclosure score	TDISC	Total of the 40 items detailed in Table 3, grouped into seven categories. Items measured on the basis of a content analysis of the most recent AIF, annual MD&A, and proxy circular at the start of data collection in May 2018
Category scores		
Cybersecurity risk	CYBERRISK	5 items (see Table 3)
Potential impacts	POTIMP	13 items (see Table 3)
Responsibility for cybersecurity strategy	RESPSTRAT	2 items (see Table 3)
Risk mitigation	RISKMIT	13 items (see Table 3)
Potential cybersecurity incidents	POTINC	2 items (see Table 3)
Actual cybersecurity incidents	ACTINC	3 items (see Table 3)
Other cybersecurity items	OTHERDISC	2 items (see Table 3)
Independent variables		
Board IT expertise	B_ITEXP	Percentage of board members with IT expertise. A board member was considered to have IT expertise if the firm's proxy statement indicated this fact or if the member held an IT-related diploma (educational background) or the member had an IT-related function (functional background). The member's online biography as posted on the company's website or elsewhere was useful in that regard
Board tenure	B_TEN	Mean of each board member years on the board as per the proxy statement
Board independence	B_INDEP	Percentage of independent directors identified as such in the proxy statement
Women directors on the board	B_WOM	Percentage of women directors on the board as per the proxy statement
Board age	B_AGE	Mean of directors' age as per the proxy statement or the Bloomberg database
Committee responsible for cybersecurity on the board of directors	B_CYBERCOM	The variable takes the value of 1 when any of the AIF, annual MD&A, and proxy circular specifically identifies a board committee as being responsible for cybersecurity, 0 otherwise
Control variables		
Firm size	FIRMSIZE	Natural log of total assets
Profitability	ROA	Net income to total assets as per the firm's most recent financial statements at the start of data collection in May 2018

Table 2 (continued)

Variables	Abbreviations	Measurement
Leverage	LEV	Total debt to total assets as per the firm's most recent financial statements at the start of data collection in May 2018
Market-to-book	MTB	Market value of all outstanding shares to the book value of equity at the company's year-end as per the Bloomberg database
Industry	INDUSTRY	For each of the eight industries mentioned in Table 1, the variable takes the value of 1 when the company belongs to the industry, 0 otherwise. Real estate is the industry omitted from the regressions. Data were collected based on the company description presented on the TSX Website

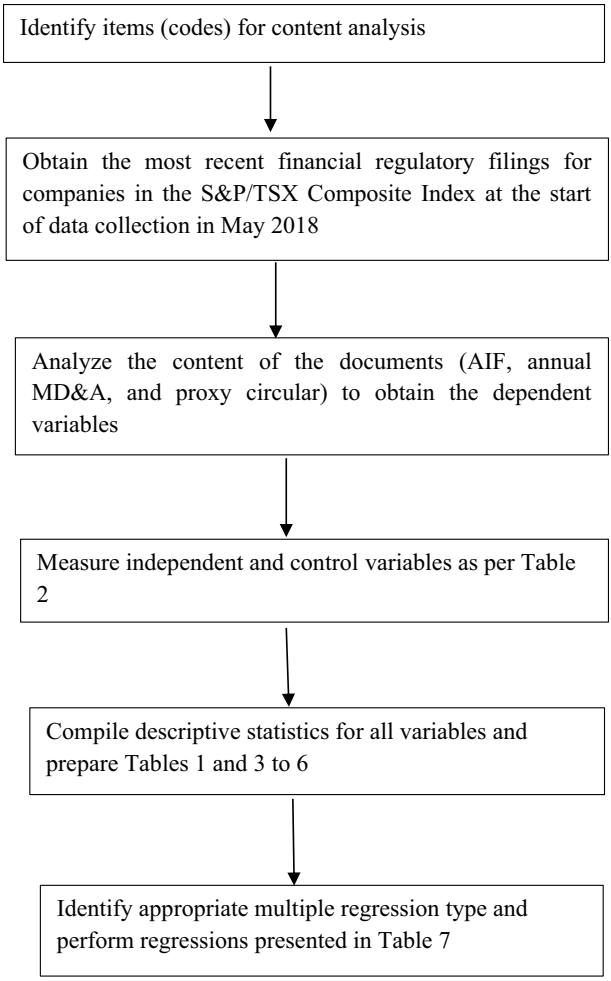

Fig. 2 Steps from data collection to analysis

as they represented best disclosure practices at the time. We thus compare actual practice to these best disclosure practices.

The two documents mentioned above indicate various items or types of items that companies are encouraged to disclose. In addition, CSA *Multilateral Staff Notice 51*-347 (2017b) groups the various items mentioned into categories: disclosure of cybersecurity risk, potential impacts of a cybersecurity incident, governance (i.e., responsibility for cybersecurity strategy), cybersecurity risk mitigation, and cybersecurity incident disclosure.[6] We used these categories but divided the cybersecurity incident disclosure category in two, i.e., potential and actual incidents. In three categories (cybersecurity risk, potential impacts of a cybersecurity incident,

[6] Items similar to those in CSA (2017b) are covered in SEC (2018) but are organized differently.

and cybersecurity risk mitigation), we had an item for "other" category-related information that companies might disclose in addition to the items identified in the two regulatory documents. We also created a category for other cybersecurity items disclosed that did not fit in the above six categories. The scoring grid thus has seven categories. We analyze the extent of total cybersecurity disclosure and of each of the categories representing different aspects of cybersecurity-related information.

To assess the extent of cybersecurity disclosure, we analyzed the content of the firms' most recent Annual Information Form (AIF), annual Management's Discussion and Analysis (MD&A), and proxy circular (i.e., management information circular) that were publicly available at the start of data collection in May 2018.[7] These documents were obtained from the Canadian repository of filings for listed firms (www.sedar.com).

A research assistant with an undergraduate degree and a graduate diploma in accounting performed the coding under the authors' close supervision and guidance. She helped develop the scoring grid and was abreast of all the types of items mentioned in the two regulatory documents that served as a basis for the identification of the items. At the start of the coding, one of the authors coded some companies and discussed the few discrepancies uncovered with the research assistant to ensure a common understanding of the items' content for the remainder of the content analysis. During the coding, frequent discussions between the authors and the research assistant ensured that any uncertainties regarding the items' interpretation in relation to the text being coded were clarified; in addition, one author performed spot checks. To locate the information on cybersecurity in the three documents mentioned above, the assistant used key words such as cyber, breach, attack, threat, surveillance, theft, hacking, electronic, technology, and network. She then read the texts to uncover any mention of the items (or codes) listed on the grid and any new items related to cybersecurity. The authors approved the emerging items found by the research assistant and classified them as "other" items at first. Hence, these items were counted in the total disclosure score of each company. It subsequently seemed appropriate to present statistics for frequently encountered "other" items. The authors found that more than 5% of the sample companies mentioned two items, financial fraud/theft of funds and board IT expertise. The frequency of these items is presented separately in Table 3 and analyzed in the results section. Hence, the final scoring grid has 40 items, including, in three categories, an "other" item that contains miscellaneous information mentioned only by a small number of companies.

Using excerpts from firms' documents, the "Appendix" provides examples of the coding of some items in the different categories of the scoring grid. Each item was

[7] "An AIF provides material information about a company … [and] its operations, prospects, risks and other factors that impact its business". "Financial statements must be accompanied by the MD&A …, a narrative explanation, through the eyes of management, of how a company performed during the period covered by the financial statements, and of the company's financial condition and future prospects". "A proxy is a method by which a shareholder appoints a person or company to act on the shareholders' behalf at a shareholder meeting…. When a company solicits proxies, it must also prepare an information circular … [which] includes information on how to exercise a proxy and provides details of the matters to be voted on at the shareholder meeting". https://www.osc.ca/en/industry/companies/continuous-disclosure.

Table 3 Frequency of scoring grid items in cybersecurity disclosures

Categories and items		Number of companies disclosing item[a]
Cybersecurity risk		
1	General description	209
2	Description specific to the company	98
3	Third-party exposure	86
4	Social media risk	4
5	Other	4
Potential impacts of a cybersecurity incident		
6	Disruption of activity/operational delays (lost revenues)	208
7	Reputational harm	181
8	Compromising of confidential data	178
9	Litigation, fines, and liability	133
10	Corruption or destruction of data	128
11	Unauthorized access to sensitive information	102
12	Remediation costs	77
13	Decreased competitive advantage	66
14	Regulatory investigations	58
15	Financial fraud/theft of funds	26
16	Effectiveness of internal control over financial reporting	18
17	Higher insurance premiums	5
18	Other	16
Responsibility for cybersecurity strategy		
19	Party responsible for cybersecurity strategy mentioned	114
20	Responsibilities mentioned	90
Cybersecurity risk mitigation		
21	Controls over unauthorized access	184
22	Insufficient mitigation	145

Table 3 (continued)

Categories and items		Number of companies disclosing item[a]
23	Disaster/incident recovery/response plan	73
24	Education (board)	63
25	Data protection	50
26	Insurance	43
27	Education (all staff)	43
28	Board IT expertise	32
29	Reliance on third-party experts	28
30	Testing of recovery plan	12
31	Adjustments from previous attacks	3
32	Disclosure controls and procedures related to cybersecurity	3
33	Other	18
Potential cybersecurity incidents		
34	Nature of the incidents	136
35	Source	88
Actual cybersecurity incidents		
36	Experienced cyberattacks or no loss resulting from cyberattacks or indicates did not have such attacks	51
37	Impact	41
38	Details on incidents	9
Other cybersecurity items disclosed		
39	Legislation	52
40	Issuer's expertise	15

[a]The numbers in this column indicate the number of companies disclosing the item in one or more of three documents, i.e., the AIF, annual MD&A, and/or proxy circular. Each item/piece of information is counted only once per company. Within each disclosure category, the items are presented in descending order by number of companies that disclosed the item, except for the other item in the category

measured as a binary variable whereby a value of 1 represents the existence of this disclosure element. For the three "other" items, each different piece of information pertaining to a company was coded 1. We computed total and category disclosure scores for each company by counting each item/piece of information only once even if it appeared in more than one document from among the AIF, annual MD&A, or proxy circular.

3.3.2 Independent and control variables

The independent variables in the regression model are selected based on the six hypotheses tested, namely, board IT expertise (B_ITEXP), board tenure (B_TEN), board independence (B_INDEP), women directors on the board (B_WOM), board members' age (B_AGE), and a committee responsible for cybersecurity on the board of directors (B_CYBERCOM).

Control variables include firm size (FIRMSIZE), profitability (ROA), leverage (LEV), and market-to-book (MTB). Larger firms tend to disclose more on information security activities than smaller firms do (Gordon et al., 2006). Amir et al. (2018) argue, but fail to demonstrate, that profitability influences the disclosure of negative information such as cyberattacks. In Radu and Smaili (2021), firm size and return on assets are positively related to level of cybersecurity disclosure. Higher-leveraged firms and firms with growth opportunities provide more disclosure to reduce information asymmetry (Ben-Amar et al., 2017; Bravo, 2018). Industrial sector (INDUSTRY) is also controlled for, as Gordon et al. (2006) showed that industry membership has an impact on the extent of disclosure of information security activities.

Measurement of the independent and control variables is presented in Table 2.

3.4 Regression models

To test the hypotheses, the following regression model is used for total disclosure score and each of the seven category scores.

$$\begin{aligned} \text{CYBERSECDISC} = {} & \beta_0 + \beta_1 \text{B\_ITEXP} + \beta_2 \text{B\_TEN} + \beta_3 \text{B\_INDEP} + \beta_4 \text{B\_WOM} \\ & + \beta_5 \text{B\_AGE} + \beta_6 \text{B\_CYBERCOM} + \beta_7 \text{FIRMSIZE} \\ & + \beta_8 \text{ROA} + \beta_9 \text{LEV} + \beta_{10} \text{MTB} + \text{INDUSTRY} + \varepsilon, \end{aligned}$$

where CYBERSECDISC is the generic dependent variable name for extent of cybersecurity disclosure. It is broken down into eight dependent variables, i.e., one for total disclosure score (TDISC) and one for each of the seven disclosure categories representing different aspects of cybersecurity-related information, as follows: cybersecurity risk (CYBERRISK); potential impacts (POTIMP); responsibility for cybersecurity strategy (RESPSTRAT); risk mitigation (RISKMIT); potential cybersecurity incidents (POTINC); actual cybersecurity incidents (ACTINC); and other cybersecurity items disclosed (OTHERDISC).

4 Results

4.1 Descriptive statistics

4.1.1 Cybersecurity disclosure

Table 3 presents the number of companies that disclose the 40 scoring grid items in one or more of the AIF, annual MD&A, and proxy circular. Each item is counted only once per company. Within each disclosure category, the items are presented in descending order by number of companies that disclosed the item, except for the "other" item.

The following observations on different aspects of cybersecurity disclosure can be inferred from Table 3. The vast majority of companies (209, 83.6%) present only a general description of cybersecurity risk in the risk factor section of their documents. The five potential impacts of a cybersecurity incident mentioned by more than half of the companies are: disruption of activity/operational delays; reputational harm; compromising of confidential data; litigation, fines, and liability; and corruption or destruction of data. Surprisingly, less than half of the companies (114, 45.6%) indicate the party responsible for cybersecurity strategy. In terms of cybersecurity risk mitigation, control of unauthorized access is the most frequently mentioned item (184, 73.6%). The majority of companies indicate that their cybersecurity mechanisms might not be sufficient to prevent cybersecurity incidents (145, 58%). More than half of the companies mention potential cybersecurity incidents (136, 54.4%) but few refer to actual cybersecurity incidents (51, 20.4%), not even to indicate that they do not experience attacks (only six companies do so, not tabulated). In terms of other cybersecurity items disclosed, 52 companies (20.8%) refer to legislation that they are obligated to follow.

Table 4 presents the mean total disclosure score and cybersecurity information category scores by industrial sector. The mean total disclosure score is rather low (mean = 11.58 vs. a possible maximum score of 40) while the maximum score is 28 (not tabulated). In terms of disclosure categories, the mean of POTINC (0.90) represents 45% of the number of items (2) while the mean of ACTINC (0.40) has the lowest proportion, 13.3%, of its items (3). RISKMIT's mean (2.80) also represents a low percentage, 21.5%, of the 13 items in the category. The extent of cybersecurity disclosure differs by industrial sector for TDISC and varies among all categories except for POTIMP (not tabulated).

4.1.2 Independent and control variables

Descriptive statistics for independent and control variables are presented in Table 5, while Table 6 shows a correlation matrix. On average, 14% of board members have IT expertise (B_ITEXP), board members have been on the board for seven and a half years (B_TEN), 77% of board members are independent

(B_INDEP), women directors represent 20% of board members (B_WOM), the mean board member age is 61.88 years (B_AGE), and 36% of the companies have a committee responsible for cybersecurity on the board of directors (B_CYBERCOM). The average firm size as measured by the natural logarithm of total assets is 8.63. Average return on assets, leverage, and market-to-book are respectively 5.63%, 51.62%, and 3.26. All independent and control variables except for B_TEN, B_AGE, ROA, and MTB are correlated with TDISC (highest correlation = 0.335 with B_CYBERCOM). B_ITEXP, B_INDEP, B_WOM, and B_CYBERCOM are correlated among themselves, with 0.236 (between B_ITEXP and B_WOM) being the highest such correlation. B_AGE is highly correlated with B_TEN (0.413) and less with B_INDEP (0.140). Variables are generally correlated with firm size and LEV, but not with ROA and MTB. The highest correlation (0.567) is between FIRMSIZE and LEV. The modest size of the correlations among variables suggests that multicollinearity is not a problem in this study. In fact, the highest variance inflation factor is 2.74.

4.2 Regression results

4.2.1 Main results

Table 7 presents the results of the Tobit regressions used to test the hypotheses regarding the association between board-level characteristics and extent of overall and individual aspects of cybersecurity disclosure.

Results show that Board IT expertise (B_ITEXP) (H1) is positively associated with RISKMIT and ACTINC. Contrary to expectations, it is negatively associated with POTIMP. Hence, the hypothesis is supported for two aspects of cybersecurity disclosure.

Board tenure (B_TEN) (H2) is negatively associated with disclosure about cybersecurity incidents, i.e., POTINC and ACTINC. The hypothesis is supported for two aspects of cybersecurity disclosure.

Board independence (B_INDEP) (H3) is positively associated with RESPSTRAT and RISKMIT. The hypothesis is thus supported for two aspects of cybersecurity disclosure.

Women directors on the board (B_WOM) (H4) is positively associated only with RISKMIT. The hypothesis is thus supported for one aspect of cybersecurity disclosure.

Board age (B_AGE) (H5) is not associated with any dependent variable. The hypothesis is thus not supported.

Total disclosure (TDISC) and almost all categories of cybersecurity disclosure except for POTINC are associated positively with a committee responsible for cybersecurity on the board of directors (B_CYBERCOM) (H6). The hypothesis is supported for total disclosure and for all aspects of cybersecurity disclosure except one.

Overall, the predicted relationships between the independent variables and extent of cybersecurity disclosure were all significant ($p \leq 0.10$ or better) for total disclosure score or the score of one or more disclosure category, except for board age. We

Table 4 Total disclosure score and category scores

	N	TDISC (40 items)	CYBERRISK (5 items)	POTIMP (13 items)	RESPSTRAT (2 items)	RISKMIT (13 items)	POTINC (2 items)	ACTINC (3 items)	OTHER-DISC (2 items)
Mean	250	11.58	1.60	4.79	0.82	2.80	0.90	0.40	0.27
Standard deviation		6.25	1.00	2.76	0.93	2.00	0.82	0.85	0.52

TDISC total disclosure score, *CYBERRISK* cybersecurity risk score, *POTIMP* potential impacts of a cybersecurity incident score, *RESPSTRAT* responsibility for cybersecurity strategy score, *RISKMIT* cybersecurity risk mitigation score, *POTINC* potential cybersecurity incidents score, *ACTINC* actual cybersecurity incidents score, *OTHERDISC* other cybersecurity items disclosed score

Table 5 Descriptive statistics for independent and control variables

Variables	Description	Mean	Median	Std dev.	Min	Max
Panel A: independent variables						
B_ITEXP	Percentage of board members with IT expertise	14%	7%	19%	0	78%
B_TEN (years)	Mean number of years that directors have been on the board	7.50	7.11	3.56	1.75	22.00
B_INDEP	Percentage of independent directors on the board	77%	80%	14%	8%	100%
B_WOM	Percentage of women directors	20%	20%	12%	0	50%
B_AGE (years)	Mean of directors' age	61.88	62.11	3.59	48.00	70.58
B_CYBERCOM	An indicator variable equal to 1 if a board committee is responsible for cybersecurity, 0 otherwise	0.36	0	0.48	0	1
Panel B: control variables						
FIRMSIZE	Natural log of total assets	8.63	8.38	1.71	4.18	14.06
ROA	Return on assets	5.63%	3.68%	27.14%	−38.70%	422.20%
LEV	Leverage	51.62%	52.35%	22.83%	1.01%	118.84%
MTB	Market-to-book	3.26	1.81	11.59	0.32	180.18

Table 6 Pearson correlations

Variables	TDISC	B_ITEXP	B_TEN	B_INDEP	B_WOM	B_AGE	B_CYBERCOM	FIRMSIZE	ROA	LEV
TDISC[a]	1									
B_ITEXP	0.194***	1								
B_TEN	−0.059	−0.055	1							
B_INDEP	0.133**	0.132**	−0.072	1						
B_WOM	0.189***	0.236***	−0.027	0.154**	1					
B_AGE	0.040	−0.002	0.413***	0.140**	0.088	1				
B_CYBERCOM	0.335***	0.141**	0.020	0.153**	0.157**	0.128**	1			
FIRMSIZE	0.226***	0.122*	0.032	0.097	0.385***	0.241***	0.278***	1		
ROA	0.006	0.006	0.004	−0.041	−0.020	−0.075	−0.061	−0.190***	1	
LEV	0.264***	0.131**	0.049	0.076	0.326***	0.167***	0.197***	0.567***	−0.046	1
MTB	0.051	0.056	0.012	−0.025	−0.068	−0.084	−0.070	−0.106*	0.049	0.173***

[a]For readability, correlations are provided only for the total disclosure score

*, **, and *** Denote $p \leq 0.10$, $p \leq 0.05$, and $p \leq 0.01$ (two-tailed tests). N = 250. Variables are defined in Table 2

can conclude that all hypotheses but one are supported depending on the specific aspect of cybersecurity disclosure considered.

In terms of the control variables, large firms (FIRMSIZE) tend to disclose more in some categories, i.e., RESPSTRAT and OTHERDISC. Profitability (ROA) is associated with total disclosure (TDISC) and all disclosure categories except RISKMIT. Leverage (LEV) and market-to-book (MTB) are positively associated only with some of the disclosure categories, namely, LEV with TDISC and CYBERRISK, and MTB with RISKMIT, POTINC, and OTHERDISC.

4.2.2 Additional analyses

The results from the main analyses indicate that a committee responsible for cybersecurity on the board of directors is important for total cybersecurity disclosure and almost all of its aspects. These results lead to the investigation of whether board and company characteristics and board attributes associated with cybersecurity disclosure differ between companies that have such a committee and those that do not.

Table 8 shows that companies with a committee responsible for cybersecurity on the board of directors have a greater percentage of board members with IT expertise, independent directors, women directors, and older board members. These companies are also larger and more leveraged.

Table 9 presents board attributes significantly associated ($p \leq 0.10$ or less) with the cybersecurity disclosure of companies with a committee responsible for cybersecurity on the board of directors (Panel A) and of those without this committee (Panel B).[8] Results presented in Panel A show that when companies have this board committee, board IT expertise influences positively the disclosure of actual cybersecurity incidents (ACTINC). Board tenure has a negative association with total disclosure (TDISC) as well as some aspects of disclosure (CYBERRISK, RESPSTRAT, RISKMIT, and POTINC). Board independence is negatively associated with total disclosure (TDISC) and disclosure about cybersecurity incidents (POTINC and ACTINC). Women directors seem to positively influence disclosure about cyber risks (CYBERRISK) and other disclosures (OTHERDISC) but negatively influence disclosure of actual incidents (ACTINC). Board age is negatively associated with disclosure of responsibility for cybersecurity strategy (RESPSTRAT) and other disclosures (OTHERDISC). In summary, while a committee responsible for cybersecurity on the board of directors positively affects total cybersecurity disclosure and most of its aspects, another board attribute stands out, i.e., board tenure, which conversely shows a negative association with total cybersecurity disclosure and some of its aspects. In addition, board independence influences negatively three aspects.

When companies have no committee responsible for cybersecurity on the board of directors (Table 9, Panel B), board IT expertise affects positively the disclosure of cybersecurity risk mitigation measures (RISKMIT). Board tenure has a negative association with disclosure about actual cyber-incidents (ACTINC). Board independence is positively associated with total disclosure (TDISC) and five aspects of disclosure (POTIMP, RISKMIT, POTINC, ACTINC, OTHERDISC). Women

[8] For readability, Table 9 does not present the full regression results for each dependent variable.

Table 7 Tobit regression results for total disclosure score and category scores

Variables	TDISC	CYBERRISK	POTIMP	RESPSTRAT	RISKMIT	POTINC	ACTINC	OTHERDISC
B_ITEXP	−0.007 (−0.00)	0.131 (0.32)	−2.119** (−1.87)	−0.102 (−0.29)	1.508** (2.07)	−0.238 (−0.58)	2.234** (2.02)	0.222 (0.35)
B_TEN	−0.137 (−1.10)	−0.011 (−0.44)	0.002 (0.03)	0.011 (0.59)	−0.056 (−1.53)	−0.065*** (−2.68)	−0.128* (−1.95)	−0.048 (−1.39)
B_INDEP	3.315 (0.88)	−0.555 (−0.89)	1.892 (1.04)	0.754** (1.80)	2.195** (2.30)	−0.193 (−0.31)	−0.921 (−0.48)	0.895 (1.18)
B_WOM	3.808 (0.93)	0.458 (0.64)	0.345 (0.17)	0.778 (1.12)	3.342*** (2.57)	−0.500 (−0.62)	−2.249 (−0.93)	0.518 (0.47)
B_AGE	0.006 (0.05)	−0.001 (−0.03)	−0.026 (−0.39)	0.023 (1.21)	0.052 (1.25)	−0.011 (−0.44)	−0.009 (−0.13)	−0.044 (−1.24)
B_CYBERCOM	3.642*** (4.69)	0.334** (2.24)	0.560* (1.38)	2.241*** (18.59)	0.928*** (3.60)	−0.039 (−0.22)	1.152*** (2.35)	0.371* (1.47)
FIRMSIZE	0.250 (0.81)	−0.060 (−0.95)	0.155 (0.95)	0.105** (2.15)	−0.040 (−0.40)	0.058 (0.86)	0.038 (0.20)	0.242** (2.27)
ROA	1.433*** (3.03)	0.433*** (4.86)	0.444* (1.61)	−3.152** (−1.89)	0.259 (1.26)	0.365*** (3.15)	−5.381* (−1.47)	1.510*** (4.68)
LEV	3.717* (1.47)	0.862** (1.84)	1.616 (1.28)	−0.078 (−0.22)	0.956 (1.07)	0.388 (0.73)	1.588 (1.19)	0.234 (0.34)
MTB	0.017 (0.94)	0.004 (1.15)	0.003 (0.33)	−0.002 (−0.24)	0.010** (1.76)	0.007*** (2.48)	−0.003 (−0.20)	−0.104** (−2.31)
Intercept	1.053 (0.14)	1.477 (1.08)	2.498 (0.63)	−3.563*** (−3.22)	−3.717 (−1.45)	0.511 (0.33)	−3.238 (−0.72)	−4.380* (−1.87)
Industry	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
N observations	250	250	250	250	250	250	250	250
N left-censored at 0	18	40	36	135	33	98	199	192
F-statistic	5.92	5.85	1.97	35.93	7.95	3.93	4.86	7.80
p-value	<0.001	<0.001	0.014	<0.001	<0.001	<0.001	<0.001	<0.001

*, **, and *** Denote $p \leq 0.10$, $p \leq 0.05$, and $p \leq 0.01$ (all tests are one-tailed, except for the intercept, B_TEN and B_AGE). *t*-statistics (in parentheses) are calculated based on heteroscedasticity-robust standard errors. Variables are defined in Table 2

Table 8 Descriptive statistics for independent and control variables for companies with and without a committee responsible for cybersecurity on the board of directors

Variables	Companies with B_CYBERCOM (Std dev.) N = 89	Companies without B_CYBERCOM (Std dev.) N = 161	F	p[a]
B_ITEXP	17.94% (21.14%)	12.20% (18.23%)	5.049	**0.026**
B_TEN (years)	7.60 (3.79)	7.45 (3.44)	0.100	0.752
B_INDEP	80.15% (14.19%)	75.63% (13.94%)	5.951	**0.015**
B_WOM	22.47% (10.89%)	18.66% (11.83%)	6.286	**0.013**
B_AGE (years)	62.50 (3.12)	61.54 (3.79)	4.110	**0.044**
FIRMSIZE	9.27 (1.87)	8.27 (1.51)	20.733	**0.000**
ROA	3.42% (4.93%)	6.85% (33.59%)	0.916	0.339
LEV	57.67% (22.15%)	48.28% (22.58%)	10.039	**0.002**
MTB	2.17 (1.71)	3.86 (14.37)	1.219	0.271

[a]Significant differences are in bold (two-tailed tests)

directors foster increased disclosure about cybersecurity risk mitigation measures (RISKMIT), and board age is not associated with cybersecurity disclosure. In summary, when there is no committee responsible for cybersecurity on the board of directors, board independence is the characteristic that stands out since it positively affects total cybersecurity disclosure and most of its aspects. Further, disclosure about risk mitigation measures is positively associated with board IT expertise, board independence, and women directors.

It should be noted that when two groups of companies are differentiated (i.e., as having or not having a committee responsible for cybersecurity on the board of directors), we obtain the same results in some instances as we did in the main analysis, but for only one of the groups. For example, the three positive associations with RISKMIT are significant in the main analysis and for the companies without a committee. In such situations, the companies in the group showing significant relationships drive the main results, although the same associations are present in the other group without being significant. In other cases, the two groups show associations of opposite signs, which cancel out in the main analysis, rendering the relationship non-significant (e.g., board independence in the total disclosure regressions). In addition, several new relationships appear when the two groups are considered separately (e.g., board tenure in the case of companies with a committee and board independence in the case of companies without a committee).

4.2.3 Robustness analyses

Endogeneity can occur for several reasons, including omitted variables and reverse causation. We ran Tobit regressions with additional variables to control for a possible endogeneity problem due to omitted variables. We used "board size" (number of

Table 9 Results of hypothesis tests—significant relationships for companies with and without a committee responsible for cybersecurity on the board of directors

Hypothesis	Variables	Predicted relationship	TDISC	CYBER RISK	POTIMP	RESPSTRAT	RISKMIT	POTINC	ACTINC	OTHER DISC
Panel A: companies with a committee responsible for cybersecurity on the board of directors										
H1	Board IT expertise	+							+	
H2	Board tenure	+/−	−	−		−	−	−		
H3	Board independence	+	−					−	−	
H4	Women directors on the board	+		+					−	+
H5	Board age	+/−				−				−
Panel B: companies without a committee responsible for cybersecurity on the board of directors										
H1	Board IT expertise	+					+			
H2	Board tenure	+/−							−	
H3	Board independence	+	+		+		+	+	+	+
H4	Women directors on the board	+					+			
H5	Board age	+/−								

Significant relationships at $p \leq 0.10$ or less

board members), as larger boards have more members who can advise management (Songini et al., 2021), including on cybersecurity disclosure. We also used "percentage of executives on the board", as management is usually responsible for preparing cybersecurity information and thus influences its extent. According to Michelon and Parbonetti (2012, p. 487), "CEO duality reduces overall accountability, thus making companies less transparent". Hence, this control variable was added to the regressions. Results for our independent variables in Table 7 hold for all regressions (not tabulated). However, in addition, B_TEN has a negative effect on RISKMIT. The three additional control variables were not significant in any regression, except for a marginally positive influence of "percentage of executives on the board" on RESPSTRAT and POTINC, and CEO duality on ACTINC.

Cybersecurity disclosure has become a topic of particular interest for the Canadian Securities Administrators only quite recently (CSA, 2016), and best cybersecurity reporting practices were not established at the time of data collection. As shown in this study, the level of cybersecurity disclosure is low in annual financial regulatory filings published in 2018 (mean = 11.58 on 40 items, Table 4). Considering this evidence and the fact that cybersecurity disclosure constitutes only a small part of total firm disclosure, we believe that firms will not decide on their board structure or composition based on the extent of their cybersecurity disclosure. In other words, cybersecurity disclosure would not entail changes to board structure or composition. Hence, endogeneity originating from reverse causation should not be an issue in this study.

4.2.4 Sensitivity analysis

In their study on Canadian companies on the S&P/TSX60 Index, Radu and Smaili (2021) showed that there must be three or more women directors on the board before gender diversity can have a positive impact on cybersecurity disclosure (measured by number of words and paragraphs). To account for the effect of this number of women directors, we replaced B_WOM by B_WOM3+ in our regression with additional control variables. B_WOM3+ equals 1 when there are three or more women on the board (n = 79), 0 otherwise (n = 171). In addition to RISKMIT ($\beta = 0.913$, $t = 2.43$, $p = 0.008$), the presence of at least three women on the board positively influences TDISC ($\beta = 1.926$, $t = 1.69$, $p = 0.046$), CYBERRISK ($\beta = 0.385$, $t = 1.96$, $p = 0.026$), and POTIMP ($\beta = 0.740$, $t = 1.29$, $p = 0.099$) (not tabulated). Results for other independent variables are similar to those presented in Table 7, but with the addition of a negative effect of B_TEN on RISKMIT.

5 Discussion

The aim of this study was to examine the association between various board of directors' characteristics and an expanded measurement of cybersecurity disclosure that takes into account the extent of overall disclosure as well as individual disclosure aspects. Based on upper echelons theory, we argued that board IT expertise (*IT* knowledge and experience), board tenure (*firm-specific* knowledge and experience),

board independence (*variety* of knowledge and experience), women directors on the board (gender), and board age (age) could be potential determinants of cybersecurity disclosure. Drawing upon signaling theory, we expected that having a committee responsible for cybersecurity on the board of directors could be another board-level characteristic that could be associated with cybersecurity disclosure. The latter was measured using a content analysis of the annual filings of S&P/TSX Composite Index companies, using a 40-item scoring grid representing seven aspects/categories of disclosure. The main results are discussed first. They indicate that the presence of a committee responsible for cybersecurity on boards of directors is key to increasing cybersecurity disclosure. Further, board IT expertise, board tenure, board independence, and women directors are associated with the extent of specific aspects of cybersecurity disclosure. Further discussion based on the results of hypothesis tests for companies with and without such a committee provides additional interesting insights.

Under H1, we expected that board IT expertise could positively influence the extent of cybersecurity-related disclosure. These expectations were met by our finding that boards with a greater proportion of IT experts are related to greater disclosure of cybersecurity risk mitigation and actual cybersecurity incidents; however, they are also associated with less disclosure about the potential impacts of cybersecurity incidents. Since IT expertise helps boards to oversee IT risk (Higgs et al., 2016; Jewer & McKay, 2012; Vincent et al., 2019; Yayla & Hu, 2014), boards with IT expertise may push management to put in place (and disclose) mechanisms to mitigate cybersecurity risks. Further, as they can ask management relevant questions about actual incidents (Ashraf et al., 2020), they might be well-positioned to advise management in terms of disclosing more on these incidents. As for the potential impacts of cybersecurity incidents, boards with IT expertise cognizant of the cybersecurity risk mitigation mechanisms implemented by the organization may be less worried about these impacts, leading them to deemphasize their disclosure. In other words, board IT knowledge and experience are associated with providing more information on actual cybersecurity-related events/actions (actual incidents and risk mitigation) and less information on their anticipated consequences (potential impacts).

Plöckinger et al. (2016, p. 65) highlight that "[s]tudies of executive tenure and financial reporting choices mostly arrive at conclusions in line with upper echelons predictions", i.e., a negative association between tenure and reporting. In the same spirit, similar to Baran and Forst (2015), our findings related to H2 illustrate the negative influence of longer-tenured boards, since they were found to have an adverse effect on two specific disclosure categories, potential and actual cyber-incidents. This may be because long-tenured board members might be resistant to change (Golden & Zajac, 2001) and less effective in overseeing management (Barroso et al., 2011). Our findings suggest that boards with greater firm-specific knowledge and experience are concerned about cybersecurity incidents and may favor less disclosure on that matter, whether the incidents have happened (actual incidents) or could happen (potential incidents). These boards are also less eager to provide information on cybersecurity risk mitigation, as revealed in our robustness and sensitivity

analyses. Fear of the consequences of divulging trade secrets (Ettredge et al., 2018) may underlie this attitude.

As we expected under H3, our findings indicate that board independence can positively affect extent of cybersecurity disclosure. As independent board members are informed by the variety of knowledge and experience that they have gained in other businesses or industries (Yoo & Kim, 2012), more independent boards may focus on disclosure about cybersecurity risk mitigation and responsibility for cybersecurity strategy. Similar to Bing and Amran (2017), this finding suggests that independent boards consider this information to be material to stakeholders. Since less independent boards are associated with lower IT governance at the board of directors' level (Jewer & Mckay, 2012), we find that such boards are less interested in disclosing cybersecurity risk mitigation mechanisms and responsibility for cybersecurity strategy. This finding complements Georg's (2017) study examining non-executive boards' tasks respecting information security. Overall, results from this study suggest that boards with a variety of knowledge and experience gained in different organizations seem to focus on the individual aspects of cybersecurity disclosure that are expected to be addressed by every firm (responsibility for cybersecurity strategy and cybersecurity risk mitigation), encouraging management to disclose more information on these aspects.

As discussed in the development of H4, women board members influence the extent of cybersecurity risk mitigation disclosure. This is in line with the fact that they are more risk averse than their men counterparts (Croson & Gneezy, 2009). Since women board members have a greater sense of social responsibility toward stakeholders (Williams, 2003) and a propensity to advocate for firm transparency (Larkin et al., 2013), boards with a greater proportion of women may lead management to disclose more about the mechanisms put in place to mitigate cybersecurity risk. In fact, as shown by our sensitivity analysis of the presence of women board members, having at least three women on the board (as in Radu & Smaili, 2021) also influences favorably the extent of total cybersecurity disclosure and disclosure about cybersecurity risk and potential impacts.

Contrary to our expectation in H5, board age is not significantly associated with cybersecurity disclosure. This is in line with studies on corporate financial reporting "[that] did not reveal any observable age effect" (Plöckinger et al., 2016, p. 65), e.g., Ran et al. (2015). In light of Liu and Ji (2022), this finding could also reflect the fact that there are conflicting arguments concerning the effect of board age, discussed previously in our theoretical framework.

As expected under H6, establishing a committee responsible for cybersecurity on the board of directors appears to be an effective IT governance structure (Turel et al., 2019), as it is associated with an increase in the extent of all but one aspects of cybersecurity disclosure. This finding is in line with Higgs et al. (2016), who suggest a positive association between a technology committee and reported breaches. Although most of the boards of larger firms have yet to adopt cybersecurity oversight as part of their role (Lankton et al., 2020), we nonetheless observe that this committee is a key driver of cybersecurity disclosure. Its presence signals that the board is concerned about cybersecurity issues, as Rachid (2015) mentioned, and intends to take cybersecurity risks and disclosures seriously. Such a committee may help management and boards better

understand and address stakeholders' various information needs. The committee might also lead the organization to expand some categories of its cybersecurity disclosure.

To complement the initial findings, we deepened our analysis by looking at board characteristics associated with cybersecurity disclosure by firms with or without a board committee responsible for cybersecurity. These additional findings suggest that firms with this committee, which positively affects total cybersecurity disclosure and most of its aspects, display another significant board attribute, i.e., board tenure, which is negatively associated with total cybersecurity disclosure and four out of seven of its aspects. This suggests that greater firm-specific knowledge and experience (board tenure) seems to "slow down" this committee when the time comes to decide to increase the extent of their cybersecurity disclosure. This is in line with upper echelons theory's underlying assumption that longer-tenured individuals are more committed to the status quo. In addition, board independence, which represents board members' variety of knowledge and experience, dampens the committee's role in enhancing total cybersecurity disclosure.

At firms without a board committee responsible for cybersecurity, board independence is the characteristic that emerges and positively affects total cybersecurity disclosure and five out of seven of its aspects. This result is in line with Smaili et al.'s (2022) positive impact of board independence on the amount of cybersecurity information. This suggests that the variety of knowledge and experience of more independent boards seems to "substitute for" a committee responsible for cybersecurity with respect to the role of enhancing cybersecurity disclosure, as these attributes seem to contribute to increasing such disclosure. Further, disclosure about risk mitigation measures is also positively associated not only with board independence, but also with board IT expertise and women directors. These results for risk measures disclosure are similar to those obtained in the main analysis.

6 Conclusion

Overall, our findings provide a fair illustration of upper echelons theory by highlighting that board education/career-related characteristics and other personal traits are associated with reporting decisions such as cybersecurity disclosure. More specifically, they suggest that the influence of *IT* knowledge and experience (board IT expertise), *firm-specific* knowledge and experience (board tenure), *variety* of knowledge and experience (board independence), gender (women directors on the board), and directors' age (board age) is apparent in different aspects of cybersecurity disclosure. In light of signaling theory, an organization signals the quality of its board of directors by disclosing in its annual filings that it has a committee responsible for cybersecurity on the board. In other words, this indicates that the board is a strong and valuable resource that can monitor and advise management on cybersecurity disclosure and lead to greater transparency with stakeholders. This is shown by the significant and positive associations between this key driver and almost all aspects of cybersecurity disclosure.

6.1 Contributions

Our first motivation was to contribute to fill the literature gap on the determinants of cybersecurity disclosure (Haapamäki & Sihvonen, 2019; Walton et al., 2021). With this in mind, based on upper echelons and signaling theories, this study brings many new insights to this limited literature.

First, prior research has examined the influence of a few board of directors-related characteristics (Higgs et al., 2016; Radu & Smaili, 2021; Smaili et al., 2022) on an individual aspect of cybersecurity disclosure or on a general measurement of this disclosure. In this study, we examined the potential influence of six characteristics on the extent of total and several individual aspects of cybersecurity disclosure. Our consideration of five characteristics selected from the literature on upper echelons theory allowed us to identify the attributes that are associated with certain aspects of disclosure. This approach reflects reality in practice, as board members have different individual characteristics that can impact their ability to monitor and advise management on strategic decision making. Our results thus provide original insights regarding the specific aspects of cybersecurity disclosure that attract the board of directors' attention and affect its willingness/preparedness to influence this content. Indeed, the findings that some aspects of cybersecurity disclosure are related to different board characteristics suggest that a mix of board characteristics could help the board focus on a diversity (and a greater number) of aspects of cybersecurity disclosure.

Second, our findings add to the results of upper echelons theory-based studies on the determinants of corporate reporting because they pertain specifically to cybersecurity disclosure. Findings show that board of directors' attributes such as expertise (educational/functional background), tenure, independence, and gender matter in varying degrees, depending on the specific aspects of the cybersecurity disclosure. It should be noted that prior studies that examined the influence of women directors (Radu & Smaili, 2021) and board independence Smaili et al. (2022) on cybersecurity disclosure used different theoretical frameworks, i.e., stakeholder and resource dependence theories and stakeholder theory, respectively. Further, as pointed out by Liu and Ji (2022, p. 7) in their review of upper echelons theory, the "effects of gender on disclosure have not been fully studied".

Third, our main findings related to a committee responsible for cybersecurity (our sixth board attribute) complement results from prior IT governance/cybersecurity related studies on board-level committees (Lankton et al., 2020; Turel et al., 2019), board IT expertise (Ashraf et al., 2020; Jewer & McKay, 2012; Vincent et al., 2019), gender diversity on boards (Radu & Smaili, 2021), and board effectiveness (Smaili et al., 2022) by providing information on board of directors' attributes associated with a strategic outcome, namely cybersecurity reporting. More specifically, a committee responsible for cybersecurity on the board of directors is a key IT governance structure for increasing cybersecurity disclosure. Additional analyses indicate that in companies without such a governance structure, board independence is the main determinant of cybersecurity disclosure.

Lastly, measurement of cybersecurity disclosure in prior research refers to the presence and number of words related to this disclosure (Li et al., 2018; Radu & Smaili, 2021; Smaili et al., 2022) or specific aspects of disclosure (such as

information security risk factors, Wang et al., 2013, or breaches reported, Higgs et al., 2016). In contrast, and in line with our second motivation, we measure the content of cybersecurity disclosure and quantify *more than one* aspect of disclosure with a 40-item scoring grid instead of focusing *only* on the presence/absence of cybersecurity-related information or the number of paragraphs/words. In addition, similar to Radu and Smaili (2021), Smaili et al. (2022) and Wang et al. (2013), we analyze the annual report. However, we also collect information from two other annual documents, the annual information form and the proxy statement. In line with the second motivation of the study, based on this refined measurement of cybersecurity disclosure, results from this study contribute to the cybersecurity literature as they reveal important aspects of cybersecurity disclosure, in addition to *actual cyber incidents/breaches* and general disclosure about *cyber risk*, which have been the main focus in prior cybersecurity disclosure studies. For instance, we find that information on *cybersecurity risk mitigation* (e.g., controls, education, data protection, and insurance) can be enhanced by board IT expertise, board independence, and women directors on the board. Further, more independent boards call for more information on *responsibility for cybersecurity strategy*. Findings also indicate that having a committee responsible for cybersecurity on the board of directors leads to more cybersecurity disclosure at large.

In summary, this study contributes to filling the literature gap on the determinants of cybersecurity disclosure, based on a theoretical framework that differs from those used in prior studies, and on a refined measurement of cybersecurity disclosure. It also contributes to the IT governance literature as it highlights the impact of a having a committee responsible for cybersecurity on the board of directors, an IT governance structure.

6.2 Practical implications

Based on a qualitative analysis of financial regulators' guidelines conducted to obtain cybersecurity disclosure items and categories, followed by a content analysis of 250 companies' financial regulatory filings, this study generates descriptive data and quantitative data for hypothesis testing that provide original insights for firms and their stakeholders.

More specifically, descriptive data on the number of companies that disclosed each item, as well as category and total disclosure mean scores, provide board of directors and management (the highest levels of company decision makers), financial analysts, and financial regulators an overview of which cybersecurity-related information companies disclose or fail to disclose. These descriptive data could be used as a relevant benchmark tool by boards of directors in their oversight function and by managers in charge of reporting seeking to identify areas of improvement in their company's cybersecurity disclosure. Financial analysts could be interested in knowing who is responsible for cybersecurity strategy in companies or which risk mitigation measures are taken, and could integrate this information in their investment analysis process. Financial regulators could also use these descriptive

data as a starting point for discussions with companies as part of their efforts to enhance cybersecurity disclosure guidelines. This process could lead regulators to adjust the guidelines they provide to organizations in that respect.

In addition, the results pertaining to board of directors' characteristics associated with cybersecurity disclosure are helpful for managers who are open to collaborating with boards to improve transparency toward stakeholders. Indeed, in the turbulent cybersecurity world, firms could benefit from adjusting their board composition if they aim to provide more information to their stakeholders on the cybersecurity challenges they face. Thus, the study's results may provide firms with a basis for adjusting their actual board composition or developing new criteria for recruiting board members, since some board of directors' attributes are associated with greater transparency regarding some aspects of cybersecurity disclosure while others are not. For instance, having more board members with IT expertise, more independent board members, and more women on boards helps increase disclosure on the actions that companies take to mitigate cybersecurity risk.

Further, board of directors with a committee responsible for cybersecurity could help managers to enhance cybersecurity disclosure by focusing on that issue, raising relevant questions, and having open discussions with management on the challenges and potential impacts surrounding different aspects of cybersecurity disclosure before agreeing on disclosing more information. Findings respecting board of directors' characteristics associated with cybersecurity disclosure could also help financial analysts enhance their knowledge about the board's involvement in helping managers address cybersecurity disclosure issues. This could signal that the upper echelons are taking cybersecurity-related matters seriously, which could influence the analysts' investment analysis process. Further, these findings provide financial market participants with interesting insights in view of their need for additional cybersecurity-related information. In that spirit, financial regulators might explore the relevance and feasibility of asking listed companies to have a committee responsible for cybersecurity on their boards of directors or to have at least one board member with IT expertise to increase cybersecurity disclosure. For instance, in case of a cyberattack, increasing cybersecurity disclosure might reassure individual shareholders about the value of their investment and clients and suppliers about the protection of their sensitive data/personal data.

6.3 Limitations and research avenues

As with any research, there are limitations. However, they could open up some research avenues. First, this study concentrated its investigation on board of directors' characteristics. Since boards of directors and management are both important governing and decision-making bodies, it would be relevant to draw on upper echelons theory assumptions to explain the joint effects of their characteristics on the extent of cybersecurity disclosure.

Second, given that cybersecurity disclosure depends on companies' actual cybersecurity risk management activities, this study reported only what companies choose to disclose among risks they face and the measures they take. Third, the

measurement of some independent variables, such as boards of directors with a committee responsible for cybersecurity and board members' IT expertise, was based on publicly disclosed information in the company filings or the internet. The value for these variables may understate the actual situation. To overcome these limits, interviews or surveys could be used to determine actual cybersecurity risk management activities and actual board structure and IT expertise, and to investigate practical issues in that respect.

Fourth, the current investigation looked at disclosure by companies in a single country. The study could be expanded to other areas of the world to allow for comparisons between countries, taking into consideration directors' duties under the law.

Lastly, the data cover a fiscal period for each company. A sample covering several such time periods would make it possible to examine the evolution of cybersecurity disclosure practices and contextualize the results.

Appendix

Examples of scoring per category

Category	Selected items	Excerpts from coded documents	Reference
Cybersecurity risk	Description specific to the company	Our business often requires that our clients' applications and information, which may include their proprietary information and personal information they manage, be processed and stored on our networks and systems, and in data centers that we manage. We also process and store proprietary information relating to our business, and personal information relating to our members…. The Company faces risk inherent in protecting the security of such personal data	CGI, MD&A, November 8, 2017, p. 56

Category	Selected items	Excerpts from coded documents	Reference
Potential impacts of a cybersecurity incident	Reputational harm	Any system failure, cyberattack or a breach of systems could result in … reputational harm affecting customer and investor confidence…. Furthermore, media or other reports of perceived security vulnerabilities of our systems, even if no breach has been attempted or had occurred, could adversely impact our brand and reputation and materially impact our business and financial results	Bombardier, MD&A, February 15, 2018, p. 115
	Financial fraud/theft of funds	If the Corporation becomes a victim to a cyber phishing attack it could result in a loss or theft of the Corporation's financial resources	Advantage Oil & Gas, AIF, March 5, 2018, p. 55
Responsibility for cybersecurity	Responsibilities mentioned	Through its enterprise and operational risk management frameworks, the Company makes all managers accountable by asking them to confirm their sector's compliance with procedures, describe the processes in place for ensuring this compliance, and confirm that policies and procedures are up to date. The risks that could arise are also assessed and quantified, as well as the measures taken to manage the most material risks	Industrial Alliance, MD&A, February 15, 2018, p. 38

Category	Selected items	Excerpts from coded documents	Reference
Cybersecurity risk mitigation	Insufficient mitigation	Element Fleet cannot ensure that its current security measures will effectively counter security risks, prevent future slowdowns or disruptions, protect against cyber-attacks or address the security and privacy concerns of existing and potential users	Element Fleet Management, AIF, March 28, 2018, p. 38
	Reliance on third-party experts	Keyera also relies on many third party service providers with respect to its information technology security and storage of information and data	Keyera, AIF, February 15, 2018, p. 70
Potential cybersecurity incidents	Nature of the incidents	Damage or failure from a number of sources, including, but not limited to, hacking, computer viruses, security breaches, natural disasters, power loss, vandalism, theft and defects in design. We may also be targets of cyber surveillance or a cyber attack from cyber criminals, industrial competitors or government actors	Eldorado Gold Corporation, AIF, March 29, 2018, pp. 128–129
Actual cybersecurity incidents	Details on incidents	In 2017, our consumers were targeted by criminals through our PC Plus loyalty program. The intention of the targeted attack was to monetize the loyalty points the consumers had earned in stores and points earned using their President's Choice Financial MasterCard	Loblaws, AIF, February 22, 2018, p. 12

Category	Selected items	Excerpts from coded documents	Reference
Other cybersecurity items disclosed	Legislation	Among the various regulations, NERC has established a set of currently enforced standards and continues to issue new and revised standards to ensure that utilities and other users, owners and operators of the bulk electricity system in North America implement and sustain preventive, detective and corrective measures to mitigate cyber and physical security risks to critical infrastructure	Hydro One, AIF, March 29, 2018, p. 32

Acknowledgements The authors are grateful for the financial support of the accounting department at ESG UQAM, the Corporate Reporting Chair, ESG UQAM, the Autorité des marchés financiers (AMF—Québec), and the research assistance of Geneviève Girard and Souha Khaldi. They also thank the three anonymous reviewers for their insightful comments and suggestions.

Funding This study was funded by the accounting department at ESG-UQAM, the Corporate Reporting Chair, ESG-UQAM, and the Autorité des marchés financiers (AMF—Québec).

Data availability Data are available from public sources.

Code availability Not applicable.

Declarations

Conflict of interest The authors have no relevant financial or non-financial interests to disclose.

References

Amemiya, T. (1984). Tobit models: A survey. *Journal of Econometrics, 24*, 3–61.

American Institute of Certified Public Accountants (AICPA). (2017). *Reporting on an entity's cybersecurity risk management program and controls: Attestation guide*. American Institute of Certified Public Accountants.

Amir, E., Levi, S., & Livne, T. (2018). Do firms underreport information on cyberattacks? Evidence from capital markets. *Review of Accounting Studies, 23*(3), 1177–1206.

Ashraf, M., Michas, P. N., & Russomanno, D. (2020). The impact of audit committee information technology expertise on the reliability and timeliness of financial reporting. *The Accounting Review, 95*(5), 23–56.

Baalouch, F., Ayadi, S. D., & Hussainey, K. (2019). A study of the determinants of environmental disclosure quality: Evidence from French listed companies. *Journal of Management & Governance, 23*(4), 939–971.

Bakker, T. G., & Streff, K. (2016). Accuracy of self-disclosed cybersecurity risks of large U.S. banks. *Journal of Applied Business and Economics, 18*(3), 39–51.

Bamber, L. S., Jiang, J., & Wang, I. Y. (2010). What's my style? The influence of top managers on voluntary corporate financial disclosure. *The Accounting Review, 85*(4), 1131–1162.

Barako, D. G., & Brown, A. M. (2008). Corporate social reporting and board representation: Evidence from the Kenyan banking sector. *Journal of Management & Governance, 12*(4), 309–324.

Baran, L., & Forst, A. (2015). Disproportionate insider control and board of director. *Journal of Corporate Finance, 35*, 62–80.

Barroso, C., Villegas, M. M., & Pérez-Calero, L. (2011). Board influence on a firm's internationalization. *Corporate Governance: An International Review, 19*(4), 351–367.

Bear, S., Rahman, N., & Post, C. (2010). The impact of diversity and gender composition on corporate social responsibility. *Journal of Business Ethics, 97*(2), 207–221.

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.

Ben-Amar, W., Francoeur, C., Hafsi, T., & Labelle, R. (2013). What makes better boards? A closer look at diversity and ownership. *British Journal of Management, 24*(1), 85–101.

Benaroch, M., & Chernobai, A. (2017). Operational IT failures, IT value destruction, and board-level IT governance changes. *MIS Quarterly, 41*(3), 729–762.

Bing, N. S., & Amran, A. (2017). The role of board diversity on materiality disclosure in sustainability disclosure. *Global Business and Management Research: An International Journal, 9*(4), 96–109.

Bonime-Blanc, A. (2017). *A strategic cyber roadmap for the board*. Retrieved August 26, 2020, from https://corpgov.law.harvard.edu/2017/01/12/a-strategic-cyber-roadmap-for-the-board/

Bravo, F. (2018). Does board diversity matter in the disclosure process? An analysis of the association between diversity and the disclosure of information on risks. *International Journal of Disclosure and Governance, 15*(2), 104–114.

Brown, S. V., Tian, X., & Tucker, J. W. (2018). The spillover effect of SEC comment letters on qualitative corporate disclosure: Evidence from the risk factor disclosure. *Contemporary Accounting Research, 35*(2), 622–656.

Caluwe, L., & De Haes, S. (2019). Board engagement in IT governance: Opening up the black box of IT oversight committees at board level. In *Proceedings of the 52nd Hawaii International Conference on System Sciences* (pp. 6189–6197). Retrieved August 26, 2020, from https://scholarspace.manoa.hawaii.edu/handle/10125/60053

Canada Business Corporations Act. (1985). *R.S., 1985, c. C-44, s. 1; 1994, c. 24, s. 1(F)*. Retrieved October 26, 2021, from https://laws-lois.justice.gc.ca/eng/acts/c-44/page-1.html

Canadian Securities Administrators (CSA). (2016). *CSA staff notice 11-332: Cyber security*. Montreal, Canada. Retrieved September 24, 2021, from https://www.bcsc.bc.ca/-/media/PWS/Resources/Securities_Law/Policies/Policy1/11332-CSA-Staff-Notice-September-27-2016.pdf

Canadian Securities Administrators (CSA). (2017a). *Multilateral staff notice 51-347: Disclosure of cyber security risks and incidents*. Canadian Securities Administrators.

Canadian Securities Administrators (CSA). (2017b). *CSA staff notice 33-321: Cyber security and social media*. Canadian Securities Administrators.

Center for Strategic and International Studies (CSIS) – Washington, D. C. (2021). *Significant cyberincidents*. Retrieved January 20, 2021, from https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents

Chuang, T.-T., Nakatani, K., & Zhou, D. (2009). An exploratory study of the extent of information technology adoption in SMEs: An application of upper echelon theory. *Journal of Enterprise Information Management, 22*(1/2), 183–196.

Connecticut Business Corporation Act, 1997, 45 CS 101, sect. 33–756, g. Retrieved October 26, 2021, from https://www.cga.ct.gov/current/pub/chap_601.htm#sec_33-756

Croson, R., & Gneezy, U. (2009). Gender differences in preferences. *Journal of Economic Literature, 47*(2), 448–474.

Czarnecki, G. M. (2015). Cyber threats necessitate a new governance model. *NCAD Directorship* (September/October), 8–9.

Deloitte. (2015). *The board's-eye view of cyber crisis management*. Retrieved August 26, 2020, from https://www2.deloitte.com/global/en/pages/risk/articles/boards-view-cyber-crisis-management.html

Edmondson, A. C., & McManus, S. E. (2007). Methodological fit in management field research. *Academy of Management Review*, *32*(4), 1155–1179.

Ettredge, M. L., Guo, F., & Li, Y. (2018). Trade secrets and cybersecurity breaches. *Journal of Accounting and Public Policy, 37*(6), 564–585.

Ferraro, M. F. (2014). "Groundbreaking" or broken? An analysis of SEC cybersecurity disclosure guidance, its effectiveness and implications. *Albany Law Review, 77*(2), 297–346.

Frank, M. L., Grenier, J. H., & Pysoha, J. S. (2019). How disclosing a prior cyberattack influences the efficacy of cybersecurity risk management and independent assurance. *Journal of Information Systems, 33*(3), 183–200.

Georg, L. (2017). Information security governance: Pending legal responsibilities of non-executive boards. *Journal of Management & Governance, 21*(4), 793–814.

Golden, B. R., & Zajac, E. J. (2001). When will boards influence strategy? Inclination × power = strategic change. *Strategic Management Journal, 22*(12), 1087–1111.

Gordon, L. A., Loeb, M. P., Lucyshyn, W., & Sohail, T. (2006). The impact of the Sarbanes-Oxley Act on the corporate disclosures of information security activities. *Journal of Accounting and Public Policy, 25*, 503–530.

Gordon, L. A., Loeb, M. P., & Sohail, T. (2010). Market value of voluntary disclosures concerning information security. *MIS Quarterly, 34*(3), 567–594.

Haapamäki, E., & Sihvonen, J. (2019). Cybersecurity in accounting research. *Managerial Auditing Journal, 34*(7), 808–834.

Hafsi, T., & Turgut, G. (2013). Boardroom diversity and its effect on social performance: Conceptualization and empirical evidence. *Journal of Business Ethics, 112*(3), 463–479.

Hair, J. F., Jr., Anderson, R. E., Tatham, R. L., & Black, W. C. (1998). *Multivariate data analysis* (5th ed.). Prentice Hall.

Hambrick, D. C., & Mason, P. A. (1984). Upper echelons: The organization as a reflection of its top managers. *Academy of Management Review, 9*(2), 193–206.

Higgs, J., Pinsker, R. E., Smith, T. J., & Young, G. R. (2016). The relationship between board-level technology committees and reported security breaches. *Journal of Information Systems, 30*(3), 79–98.

Hitchcock, C., Lamm, B., & Parsons, K. (2017). *On the board's agenda: US trends in audit committee reporting*. Deloitte Development LLC. Retrieved August 26, 2020, from https://www2.deloitte.com/content/dam/Deloitte/us/Documents/center-for-board-effectiveness/us-cbe-january-2017-on-the-boards-agenda.pdf

Information Systems and Control Association (ISACA)/Downs, F. (2020). *Top cyberattacks of 2020 and how to build cyberresiliency*. Retrieved January 20, 2021, from https://www.isaca.org/resources/news-and-trends/industry-news/2020/top-cyberattacks-of-2020-and-how-to-build-cyberresiliency

Jewer, J., & McKay, K. N. (2012). Antecedents and consequences of board IT governance: Institutional and strategic choice perspectives. *Journal of the Association for Information Systems, 13*(7), 581–617.

Johnson, S. G., Schnatterly, K., & Hill, A. D. (2013). Board composition beyond independence: Social capital, human capital, and demographics. *Journal of Management*, *39*(1), 232–262.

Kagzi, M., & Guha, M. (2018). Board demographic diversity: A review of literature. *Journal of Strategy and Management, 11*(1), 33–51.

Kesner, I. F. (1988). Directors' characteristics and committee membership: An investigation of type, occupation, tenure, and gender. *Academy of Management Journal, 31*(1), 66–84.

Labelle, R., Gargouri, M., & Francoeur, C. (2010). Ethics, diversity management and financial reporting quality. *Journal of Business Ethics, 93*, 335–353.

Lankton, N., Price, J., & Karim, M. (2020). Cybersecurity breaches and information technology governance roles in audit committee charters. *Journal of Information Systems*. https://doi.org/10.2308/isys-18-071

Larkin, M. B., Bernardi, R. A., & Bosco, S. M. (2013). Does female representation on boards of directors associate with increased transparency and ethical behavior? *Accounting and the Public Interest, 13*(1), 132–150.

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.

Liu, M., & Ji, D. (2022). An overview of the literature on upper echelons. *Accounting Perspectives*. https://doi.org/10.1111/1911-3838.12288

Michelon, G., & Parbonetti, A. (2012). The effect of corporate governance on sustainability disclosure. *Journal of Management & Governance, 16*(3), 477–509.

Mitra, S., & Ransbotham, S. (2015). Information disclosure and the diffusion of information security attacks. *Information Systems Research, 26*(3), 565–584.

National Association of Corporate Directors (NACD). (2017). *Cyber-risk oversight—Director's handbook series*. National Association of Corporate Directors.

Newman, C. A. (2018). When to report a cyberattack? For companies, that's still a dilemma. *The New York Times*, March 5. Retrieved August 26, 2020, from https://www.nytimes.com/2018/03/05/business/dealbook/sec-cybersecurity-guidance.html

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.

Nolan, R., & McFarlan, F. W. (2005). Information technology and the board of directors. *Harvard Business Review, 83*(10), 96–106.

Nursimloo, S., Ramdhony, D., & Mooneeapen, O. (2020). Influence of board characteristics on TBL reporting. *Corporate Governance, 20*(5), 765–780.

Patelli, L., & Pedrini, M. (2015). Is tone at the top associated with financial reporting aggressiveness? *Journal of Business Ethics, 126*, 3–19.

Plöckinger, M., Aschauer, E., Hiebl, M. R. W., & Rohatschek, R. (2016). The influence of individual executives on corporate financial reporting: A review and outlook from the perspective of upper echelon theory. *Journal of Accounting Literature, 37*, 55–75.

Price, J. B., & Lankton, N. (2018). A framework and guidelines for assessing and developing board-level information technology committee charters. *Journal of Information Systems, 32*(1), 109–129.

Radu, C., & Smaili, N. (2021). Board gender diversity and corporate response to cyber risk: Evidence from cybersecurity related disclosure. *Journal of Business Ethics, 177*, 351–374.

Ran, G., Fang, Q., Luo, S., & Chan, K. C. (2015). Supervisory board characteristics and accounting information quality: Evidence from China. *International Review of Economics & Finance, 37*, 18–32.

Rashid, F. Y. (2015). NYSE survey examines cybersecurity in the boardroom. *Security Week*, May 28. Retrieved August 26, 2020, from https://www.securityweek.com/nyse-survey-examines-cybersecurity-boardroom

Securities and Exchange Commission (SEC). (2018). *17 CFR parts 229 and 249 [Release nos. 33-10459; 34-82746] commission statement and guidance on public company cybersecurity disclosures*. Securities and Exchange Commission.

Securities and Exchange Commission (SEC), Division of Corporation Finance. (2011). *CF disclosure guidance: Topic no. 2, cybersecurity*.

Smaili, N., Radu, C., & Khalili, A. (2022). Board effectiveness and cybersecurity disclosure. *Journal of Management and Governance*. https://doi.org/10.1007/s10997-022-09637-6

Songini, L., Pistoni, A., Tettamanzi, P., Fratini, F., & Minutiello, V. (2021). Integrated reporting quality and BoD characteristics: An empirical analysis. *Journal of Management and Governance, 26*, 579–620.

Turel, O., Liu, P., & Bart, C. (2019). Board-level IT governance. *IT Professional, 21*(2), 58–65.

Vafeas, N. (2003). Length of board tenure and outside director independence. *Journal of Business Finance & Accounting, 30*(7–8), 1043–1064.

Vairavan, A., & Zhang, G. P. (2020). Does a diverse board matter? A mediation analysis of board racial diversity and firm performance. *Corporate Governance, 20*(7), 1223–1241.

Valentine, E. L. H., & Stewart, G. (2013). The emerging role of the board of directors in enterprise business technology governance. *International Journal of Disclosure and Governance, 10*(4), 346–362.

Vincent, N. E., Higgs, J. L., & Pinsker, R. E. (2019). Board and management-level factors affecting the maturity of IT risk management practices. *Journal of Information Systems, 33*(6), 117–135.

Walton, S., Wheeler, P. R., Zhang, Y., & Zhao, X. (2021). An integrative review and analysis of cybersecurity research: Current state and future directions. *Contemporary Accounting Research, 35*(1), 155–186.

Wang, Y., Kannan, K., & Ulmer, J. (2013). The association between the disclosure and the realization of information security risk factors. *Information Systems Research, 24*(2), 201–218.

Westpal, J. D., & Fredrickson, J. W. (2001). Who directs strategic change? Director experience, the selection of new CEOs, and change in corporate strategy. *Strategic Management Journal, 22*(12), 1113–1137.

Williams, R. J. (2003). Women on corporate boards of directors and their influence on corporate philanthropy. *Journal of Business Ethics, 42*(1), 1–10.
Yayla, A. A., & Hu, Q. (2014). The effect of board of directors' IT awareness on CIO compensation and firm performance. *Decision Sciences, 45*(3), 401–435.
Yoo, J. W., & Kim, K. (2012). Board competence and the top management team's external ties for performance. *Journal of Management & Organization, 18*(2), 142–158.
Young, S. (2013). Contemplating corporate disclosure obligations arising from cybersecurity breaches. *Journal of Corporate Law, 38*, 659–678.

Sylvie Héroux, Ph. D., M. Sc., CPA auditor, is a full professor in the area of audit/assurance and business ethics in the École des sciences de la gestion, Université du Québec à Montréal, Canada. Her research interests pertain to the corporate governance, the IT governance, and cybersecurity. Her research has been published in journals such as *Managerial Auditing Journal, Accounting Perspectives, Journal of Applied Accounting Research, Australian Accounting Review, Journal of Management and Governance, Corporate Governance: The International Journal of Business in Society; Information Systems Management; Journal of Information Systems; Journal of Information Systems and Technology Management; and Information and Computer Security*.

Anne Fortin, PhD, is a full professor of accounting in the École des sciences de la gestion, Université du Québec à Montréal, Canada. Her main research areas are users' role in standard setting, accounting information and user decision making, IT governance, cybersecurity, CSR, and accounting education. She has published in several journals including *Accounting, Organizations and Society, Contemporary Accounting Research, Journal of Business Ethics, Accounting and Business Research, Journal of Information Systems, Information Systems Management, Information and Computer Security, Accounting Perspectives, Sustainability Accounting, Management and Policy Journal, Journal of Accounting, Ethics & Public Policy, Australian Accounting Review, Accounting Education*.

Authors and Affiliations

Sylvie Héroux[1] · **Anne Fortin**[1]

Anne Fortin
fortin.anne@uqam.ca

[1] Accounting Department, Université du Québec à Montréal, École des sciences de la gestion (ESG UQAM), Montreal, QC, Canada