Journal of Management and Governance (2023) 27:1049–1071
https://doi.org/10.1007/s10997-022-09637-6

Board effectiveness and cybersecurity disclosure

Nadia Smaili[1] · **Camélia Radu**[1] · **Amir Khalili**[1]

Accepted: 9 May 2022 / Published online: 22 June 2022

Abstract

This study explores the impact of board effectiveness on cybersecurity-related disclosure. Based on a sample of 300 firm-years consisting of the largest Canadian listed companies over a period of five years, we find evidence that board effectiveness positively affects a firm's decision to disclose cybersecurity information, and board independence and financial expertise have a positive impact on the amount of this disclosure. Independent members of the board, acting as a governance and oversight mechanism, significantly increase the disclosure of cybersecurity risks in the company's financial statements. The board has a fiduciary role to monitor management and board members' financial expertise contributes to risk assessment and management. Cybersecurity, as an emerging governance topic, demands multiple areas of expertise in technical, ethical, and financial areas. Board members should be continually trained to be aware of the evolution and diversification of business risks and should have appropriate skills and competencies to manage them. Our findings shed light on the positive impact of board members' financial expertise on the volume of cybersecurity disclosure. However, board size appears to have no impact on this amount, possibly because few board members have cybersecurity expertise.

Keywords Board effectiveness · Corporate governance · Cybersecurity disclosure · Cybersecurity

✉ Camélia Radu
radu.camelia@uqam.ca

Nadia Smaili
smaili.nadia@uqam.ca

[1] ESG UQAM (School of Management), Université du Québec à Montréal, Montréal,

1 Introduction

Cybersecurity has gained traction as a research topic in view of new business technologies, the rise of remote work, expansion of online sales and recent cyber scandals. Cyber attacks have become one of the greatest threats to organizations (Foglietta et al., 2018). Key U.S. senators have asked public companies to step up their cybersecurity measures, noting that "as our society increasingly relies on technology, businesses across all sectors of the economy must prioritize cybersecurity. A single cyberattack can cripple even the most sophisticated firms, and the public has a right to know whether companies are focused on preventing cybersecurity threats."[1]

In a report containing its priorities for 2020, the Office of Compliance Inspections and Examinations (OCIE) of the U.S. Securities and Exchange Commission indicates that the OCIE would continue to prioritize information security in each of its five examination programs. These programs focus mainly on proper configuration of network storage devices, information security governance generally and retail trading information security (SEC, 2020). The report emphasizes that culture, tone at the top and board oversight practices are key factors in protecting against cyber attacks. Board members appear to agree with the urgency of the problem: a survey of directors of U.S. public companies by the National Association of Corporate Directors (NACD[2]) in 2016–2017 indicates that 58% of respondents considered cybersecurity to be a significant risk that should be monitored. This denotes additional responsibilities for boards of directors, which have become more concerned than ever about the type of cybersecurity information to disclose and when and how to disclose it.

Overall, cybersecurity has become a top priority for boards (Li et al., 2018) and their most pressing governance issue (World Economic Forum, 2019). For their part, stakeholders interested in firms' cyber-risk management have lobbied for a corporate disclosure strategy that includes cyber risk information (Radu & Smaili, 2021). An effective board is a board that reaches its objectives (Van den Berghe & Baelden, 2005) and board effectiveness is determined by board's attributes and composition, such as board independence (Garcia-Meca & Sanchez-Ballesta, 2010), board size and split of chairman and CEO roles (Lorca et al., 2011).

Given these diverse stakeholder and regulatory pressures on the board of directors to enhance cybersecurity disclosure, an important question arises: Is an effective board of directors associated with cybersecurity disclosure? In this study, we empirically examine whether the board of directors is linked with the decision about producing a cybersecurity disclosure and the attendant choices regarding the scope it should have. John & Senbet (1998) suggest that a board's effectiveness in monitoring management is determined by its composition, independence and size. Accordingly, we examine these three traditional board characteristics to probe the role of the board of directors in management's disclosure decisions and the volume of their disclosure.

[1] U.S. Senator Doug Jones, in a press release, available at https://www.warner.senate.gov/public/index.cfm/2019/3/key-u-s-senators-lead-bipartisan-push-for-stronger-cybersecurity-by-public-companies. Accessed 2021/02/11.

[2] 2016–2017 NACD Public Company Governance Survey, available at:https://www.nacdonline.org/insights/publications.cfm?ItemNumber=37812. Accessed on 2021/02/11.

We assume there is a positive link between the board of directors and cybersecurity disclosure for different reasons. First, the board of directors, the central corporate governance mechanism, is responsible for risk management (Tricker, 2019). As cyber risk is one of the greatest risks facing businesses (World Economic Forum, 2019), the boardroom expects to have discussions about cybersecurity and ask management key questions. Stakeholders may judge the board of directors' quality by how it manages cyber risk and the amount of cybersecurity information disclosed. Second, the board of directors has a duty to consider the legal and financial ramifications of a cyberattack in its assessment of the firm's risks. Cyber attacks are a major corporate expense, as shown by the $1.7 billion price tag for the Equifax cyber breach in 2017 (Audit Analytics, 2020). Thus, the board should consider the business impacts of cyberattacks, litigation and regulatory exposure when discussing cybersecurity risks. Enhancing cybersecurity disclosure signals the board's capacity to anticipate cyber attacks and to protect stakeholders' interests. Third, according to stakeholder theory, an effective board of directors might reduce the asymmetry of information between management and stakeholders. Regarding cybersecurity issues, we therefore expect the board of directors to act as a corporate governance mechanism that reduces information asymmetry regarding cybersecurity. Finally, according to signalling theory and stakeholder theory, the board might enhance cybersecurity disclosure to reassure stakeholders that it is acting in their interests.

Based on stakeholder and signalling theories and the disclosure literature, we expect that board effectiveness will be associated with the firm's decision to disclose cybersecurity-related information. We also hypothesize that several one-dimensional measures of board effectiveness will have a positive effect on cybersecurity disclosure volume, these measures being board independence, board size and board financial expertise. Using a regression model, we test our hypothesis on a sample of 300 firm-year observations. Results show that firms with greater board effectiveness are more transparent and decide to disclose cybersecurity-related information. More independent board members and boards with more members with financial expertise also report an increased volume of cybersecurity disclosure, whereas board size does not seem to have any influence.

Overall, our study makes a threefold contribution to the literature. First, our findings provide insight on the role of corporate governance in risk disclosure. The limited prior research on disclosure of business risks focused narrowly on firm characteristics such as firm size, financial performance and industrial sector as determinants of this disclosure (Amran et al., 2009; Lopes & Rodrigues, 2007; Oliveira et al., 2011). However, the board's impact remains largely unexamined. Our study therefore complements the literature on risk disclosure by shedding light on the impact of board effectiveness on cybersecurity disclosure. Second, we also contribute to the recent cybersecurity literature. Although previous studies examined cybersecurity from various research perspectives such as technical approaches (Assante & Tobey, 2011; Jang-Jaccard & Nepal, 2014; Torres et al., 2019) and ethical approaches (Radu & Smaili, 2021), research on the role of cybersecurity in private and public companies is still relatively scarce. Third, among the future research avenues proposed, there is an expectation that voluntary disclosure would be examined from different perspectives and in different contexts (Bravo, 2018; Li et al., 2018). Prior research

on corporate governance has focused on the role, power and effectiveness of the board of directors and the impact of having a powerful and effective board Davis, 1996; Ingley & Van der Walt, 2001; Krause et al., 2013; Lorsch & MacIver, 1989; Nicholson & Kiel 2004; Schmidt & Brauer, 2006), but there is little research on cybersecurity governance on the board level. In addition, although corporate governance literature has extensively analyzed associations between corporate governance mechanisms and voluntary disclosure of financial, environmental and sustainable risks, the board's role in cybersecurity disclosure has been neglected (Rothrock et al., 2018). This is surprising, as boards have the resources and expertise to enhance this disclosure. To the best of our knowledge, this is the first study that empirically investigates the relation between the board's effectiveness and characteristics and cybersecurity disclosure.

Our findings add to the debate about why corporate governance matters. They also contribute to the corporate governance literature by providing evidence that board power could lead to extended disclosure of cyber risks.

Our results have practical implications for different stakeholders. Regulators can benefit from our findings and make recommendations on board composition. Additional disclosure requirements, guides and regulations could help firms improve their cyber risk assessment, management and disclosure. As independent board members and directors with financial expertise have a positive effect on disclosure of cybersecurity information, investors should ask for more independent boards with diversified expertise, including financial expertise. Cybersecurity is an emerging field that requires multi-faceted expertise; firm managers and board members should therefore have appropriate training and diversified skills.

The remainder of this paper is organized as follows. The next section presents the literature review and is followed by the hypothesis development in Sect. 3 and the research methodology in Sect. 4. Section 5 presents our results, and the last section contains our discussion and conclusion.

2 Board of directors' cybersecurity oversight role

2.1 Definition of cybersecurity and cybersecurity disclosure

Although cybersecurity is a term extensively used by practitioners and researchers, there is still no consensus in the literature on a general definition. Cybersecurity is a multidimensional concept, and definitions have emerged from different research perspectives. The most widely used technical definition of cybersecurity is "the safeguarding of computer networks and the information they contain from penetration and from malicious damage or disruption" (Lewis, 2006, p. 1). Craigen et al., (2014) identified technical solutions, events, strategies, processes and methods, human engagement and referent object of security as the dominant themes of cybersecurity. They developed the following multidisciplinary definition of cybersecurity: "the organization and collection of resources, processes, and structures used to protect cyberspace and cyber-enabled systems from occurrences that misalign perceived (de jure) from actual (de facto) property rights" (Craigen et al., 2014, p. 17). Using input

from stakeholders from across the country, Public Safety Canada defines cybersecurity as "the protection of digital information, as well as the integrity of the infrastructure housing and transmitting digital information. More specifically, cyber security includes the body of technologies, processes, practices and response and mitigation measures designed to protect networks, computers, programs and data from attack, damage or unauthorized access so as to ensure confidentiality, integrity and availability" (Public Safety Canada, 2018, p. 33).

Cybersecurity is a dynamic and expanding field (Newhouse et al., 2017; Radu & Smaili, 2021) recently proposed a cyber-business ethical approach based on a multi-stakeholder perspective. Concerned with the ethical principle of privacy, shareholders, along with consumers, managers, employees, and even society as a whole, are interested in firms' cybersecurity management, including its technical, financial and ethical risk perspectives. Other practitioner perspectives highlight the shortage of qualified labour as a major problem for companies (Moriarty, 2020).

Firms use cybersecurity disclosure to inform various stakeholders about their approaches to cybersecurity. Since 2011, U.S. firms have been subject to disclosure obligations requiring discussions and analysis of cybersecurity risks and cyber-attack incidents (Grant & Grant, 2014). The SEC disclosure guidance treats cyber risks like any significant business risk requiring disclosure. In Canada, various regulations on cybersecurity disclosure have been issued to guide firms on disclosure of cybersecurity risks and incidents (CSA, 2013, 2016, 2017a, b).

Risk-related disclosure is a mainly descriptive activity prescribed by regulation, and it begs improvement (Campbell et al., 2014; Hernández-Madrigal et al., 2012). For example, Li et al., (2018) recently found evidence of a positive association between cybersecurity risk disclosure and upcoming cybersecurity incidents prior to SEC guidance on cybersecurity risk disclosure, an indication of the relevance of this form of disclosure. Although, no association was found after the issue of this guidance in 2011, suggesting that firms with no material cybersecurity risks start to disclose boilerplate cybersecurity risk-related information after the SEC stressed the importance of this disclosure. We suggest later in this paper that an effective board of directors could be an effective corporate governance mechanism to help improve disclosure practices.

2.2 The board's oversight role

The board of directors and its committees, such as the audit committee and the risk management committee, are crucial corporate governance players in corporate risk management (Fama & Jensen, 1983; Jensen & Meckling, 1976; Kamiya et al., 2020). One of the board's most important roles is to protect organizations against significant risks (Xie et al., 2019). As cyber breaches become more frequent, the board is expected to effectively oversee the organization's response to cyber risks. The board is ultimately responsible for identifying, responding to, reducing and communicating the main organizational risks. In particular, the board of directors and its audit committee must first understand the organization's cyber risk context and business environment to better identify cyber risk (Lankton et al., 2020). Second, the board has the responsibility to ensure that management implements preventive and detec-

tive controls. It must also communicate informative data and material information to investors, most notably material information regarding cyber attacks (CSA, 2017a; SEC, 2018). Li et al., (2018) note that cybersecurity risk disclosure has attracted a great deal of attention in recent years, especially after the adoption of cybersecurity disclosure guides and regulations. Consequently, disclosure of cybersecurity information has become one of the board's top priorities (Li et al., 2018).

Cybersecurity strategy planning is an important board task, particularly communicating material risks to stakeholders. Kure et al., (2018) suggest that the board is a crucial player in implementing effective cybersecurity risk management. Kamiya et al., (2020) provide evidence on the board's role in reducing the impacts of cyber attacks on the firm's stakeholders. Shareholder wealth loss due to a cyber attack involving personal information is lower when the board pays more attention to cyber-risk management before the attack (Kamiya et al., 2020).

However, there is a dilemma regarding the firm's decision to disclose cybersecurity information. Firms under stakeholder pressure have incentives to disclose more information to respond to growing demand from these parties (mainly investors). At the same time, disclosing cybersecurity information has its drawbacks. Risk disclosure can negatively affect a business's market value by triggering an increase in the cost of capital and making confidential information available to competitors (Kothari et al., 2009). If a company is at high cybersecurity risk, alerting investors through a disclosure can put it in a difficult situation. As a result, firms are less likely to disclose information on cyber risks (Li et al., 2018). In addition, risk disclosure could provide key information to cyber criminals about the firm's vulnerabilities. As disclosing information on cyber attacks precipitates a sizeable negative stock market reaction, managers withhold negative information on the more severe attacks (Amir et al., 2018). In sum, the board of directors experiences all sorts of pressure regarding the decision to disclose or withhold cybersecurity-related information.

3 Hypothesis development

3.1 Board effectiveness

The board of directors monitors management on behalf of shareholders (Jensen & Meckling, 1976; John & Senbet, 1998). However, the firm is a complex nexus of contracts (Jensen & Meckling, 1976; Winter & Williamson, 1991) between shareholders and other stakeholders (Freeman, 2010; Mintzberg, 1983). According to stakeholder theory, the board's role extends beyond controlling and motivating top management to maximize shareholders' wealth; rather, it should balance, respond to and fulfill conflicting stakeholder demands (Hung, 1998; Pigé, 2002). Many of these stakeholders exert pressure to obtain more information about firms' cyber risks and cybersecurity. As the board is essential to risk management activities (Ingley & Van Der Walt, 2008) and it oversees and monitors risks (Raber, 2003), including cyber risk, as part of its fiduciary role, the stakeholder theory view of the board considers that the board balances and responds to the diverging interests of stakeholders. This could explain the decisions that the board makes regarding cybersecurity disclosure decisions.

An effective board is a board that reaches its objectives (Van den Berghe & Baelden, 2005). Hence, an effective board is aware of these demands and therefore discloses cyber-related information. The determinants of board effectiveness are board independence, size and composition (John & Senbet, 1998), complemented by other board's attributes, such as: audit committee independence, split of chairman and and CEO roles, level of director ownership and director's expertise (Lorca et al., 2011).

Stakeholders build their perception of board effectiveness by reading the firm's corporate disclosure. There is a trade-off between disclosing cyber-risk information, which is valuable for investors, and withholding this information, since hackers and cyber criminals could use it against the firm (Li et al., 2018; Wang et al., 2013). Based on signalling theory (Akerlof, 1978), disclosing good news is an opportunity for the board and management to signal that the firm is in a good position and is adept at managing risk (Allini et al., 2016; Verrecchia, 1983) has analyzed managers' decisions to disclose or withhold information and found that there are proprietary costs related to disclosure that could be a motivation for withholding information (Verrecchia, 1983). Nondisclosed information could be unreleased bad news, or it could be good news that is not sufficiently positive to offset proprietary costs. It could also be the motivation for withholding nonproprietary information, as long as it interrelates with other proprietary information (Dye, 1985). Consequently, Amir et al., (2018) find evidence of managers withholding information about severe cyber-attacks to avoid triggering a decrease in equity value on the market.

Boards that are more effective are committed to risk management and disclosure of risk-related information in their response to shareholders demands (Ben-Amar & McIlkenny, 2015). Empirical evidence indicates that board effectiveness is related to the decision to produce disclosures but not to the amount of the disclosure (Ben-Amar & McIlkenny, 2015; Rankin et al., 2011).

In conclusion, based on stakeholder and signalling theories and prior literature, we predict an association between board effectiveness and the decision to disclose cybersecurity-related information. Our first hypothesis is as follows.

> **H_1**: Board effectiveness is associated with the decision to disclose cybersecurity information.

This prediction holds in in a context similar to that of Canadian risk management reporting disclosure. We follow with a more detailed analysis of some dimensions of board effectiveness, namely board independence, board size and board expertise, and their influence on the amount of cybersecurity disclosure.

3.2 Board independence

The literature has extensively explored the effect of independent directors on the firms' outcomes and disclosure. Independent (outside) and inside directors have different functions. Independent directors monitor top management and shape strategic directions, while inside directors provide internal information to independent directors (Coles et al., 2008; Jensen, 1993; Lipton & Lorsch, 1992). Stakeholder theory

suggests that the presence of independent directors should increase disclosure, as independent directors better represent the firm's external environment and diverse stakeholders demands (Hung, 1998). Boards with a higher proportion of independent directors more effectively exercise the board's fiduciary role of monitoring top managers and ensure they act on behalf of shareholders and other stakeholders (Rosenstein & Wyatt, 1990). This improves the quality of organizational reporting.

Empirical research on the impact of board independence on disclosure shows mixed results. Some research supports the positive association between board independence and disclosure (Khan et al., 2013; Liao et al., 2015), and more particularly, risk disclosure (Abraham & Cox, 2007; Elshandidy et al., 2013; Oliveira et al., 2011; Allini et al., 2016) find no significant relationship between risk disclosure and the presence of independent directors, while Eng & Mak (2003), drawing on a sample from Singapore, show a negative impact of independent directors on disclosure. They interpret this effect as being related to the specific character of the Singapore Stock Exchange, which allows blockholders to elect independent directors to represent them, possibly resulting in blockholders receiving information directly as a substitute for disclosure.

As evidence is lacking on the impact of board characteristics on risk disclosure (Allini et al., 2016; Bravo, 2018; Li et al., 2018; Ntim & Soobaroyen, 2013), we explore this relationship, but with cybersecurity risk-related disclosure. Based on the predictions of stakeholder theory and prior research, we assume that board independence has a positive effect on cybersecurity disclosure. Accordingly, we propose this second hypothesis.

H_2: Board independence is positively associated with cybersecurity-related disclosure.

3.3 Board size

Prior studies on corporate governance consider board size to be a fundamental characteristic affecting board effectiveness (Donnelly & Mulcahy, 2008; Luo, 2005). A larger board is more efficient in monitoring and advising management (De Andres & Vallelado, 2008). It brings together a diversity of expertise and experience leading to increased disclosure and transparency (Gandía, 2008; Hidalgo et al., 2011; Samaha et al., 2015). However, it also produces more discussion and arguments, with potential erosion of board cohesiveness and effectiveness (Coles et al., 2008; Lipton & Lorsch, 1992).

Empirical research finds mixed results on the association between board size and disclosure. Some research suggests a positive relation (Abeysekera, 2010; Allegrini & Greco, 2013; Husted & de Sousa-Filho, 2019; Samaha et al., 2015), although Prado-Lorenzo & Garcia-Sanchez (2010) and Giannarakis (2014) find no relation between board size and disclosure. Recent studies on risk disclosure in particular provide evidence of a positive association between board size and risk disclosure (Allegrini & Greco, 2013; Elshandidy et al., 2013; Elshandidy & Neri, 2015; Ntim & Soobaroyen, 2013).

In conclusion, larger boards, with their diversified experience and expertise, increase firm transparency and are more likely to disclose cybersecurity risk-related information. We therefore state the following hypothesis:

H_3: Board size is positively associated with cybersecurity disclosure.

3.4 Board financial expertise

The Canadian Securities Administrators (CSA) prescribes disclosure obligations regarding cybersecurity risks. However, the accounting profession in Canada has stated that "significant judgement must be exercised in determining whether cybersecurity risks and incidents are material and require disclosure" (Canada, 2017, p. 2). The CSA has examined corporate disclosure regarding the person, group or committee responsible for cybersecurity strategy and found that the audit committee is most often responsible for overseeing cybersecurity risks (CSA, 2017a). Canadian regulation requires that every audit committee member be financially literate (Ontario Securities Commission, 2015). As financial expertise seems important for overseeing risks (including cybersecurity risks) and making disclosure decisions in that regard, we investigate the impact of board financial expertise on cybersecurity disclosure.

Prior studies show that directors with financial and accounting expertise monitor management more effectively (Erickson, Park, Reising, & Shin, 2005). Directors' financial and accounting expertise improves risk assessment and management (Elzahar & Hussainey, 2012). Boards with directors who have accounting and financial expertise are more effective in reducing information asymmetry by disclosing this information to shareholders and stakeholders (Elzahar & Hussainey, 2012; Minton et al., 2014) suggest that directors with financial expertise can prevent the risk of a crisis. Cyber risk can threaten business continuity and must be continually overseen by the board (Moore et al., 2015). Besides, other specific expertise may be needed to identify, monitoring and overseeing cybersecurity risks, such as technical (IT), legal or ethical expertise. Although this expertise is a must for a cybersecurity effective management, the study of the role and the impact of this expertise on disclosure goes beyond the scope of this research.

The most recent Spencer Stuart Board Governance Trends reporting on the boards of the 100 largest Canadian companies noted a sharp increase in nonexecutive directors with financial backgrounds, including experience and/or credentials (Spencer-Stuart, 2021). The percentage of nonexecutive directors with financial expertise increased from 36% to 2016 to 46% in 2020, whereas technology expertise on boards hovered between 2016 (6%) and 2020 (7%). As cybersecurity strategy implies more than technical expertise, boards seem to prefer financial expertise or a multidisciplinary board, which improves its risk assessment and oversight capabilities, regarding strategic, technical and ethical aspects.

Based on these arguments, we expect that the presence of directors with financial and accounting expertise is positively associated with cybersecurity disclosure. Hence, we formulate our hypothesis:

H_4: Board financial expertise is positively associated with cybersecurity disclosure.

4 Methodology

4.1 Sample and data collection

Our sample consists of the 60 largest companies listed on the Toronto Stock Exchange, forming the S&P/TSX 60 Index and representing vanguard companies in leading industries.[3] Our longitudinal study ranges from 2014 to 2018 and resulted in a final sample of 300 firm-year observations. We focus on the largest Canadian companies required to disclose risk-related information in their annual report. Given that Canadian Auditing Standards (CAS) introduced cybersecurity disclosure guides and regulation in 2013, this guidance would be reflected in corporate disclosures starting in 2014. The year 2018 was the last available year for data collection.

The sample's distribution by industry is presented in Table 1. The most prominent sectors are energy, constituting 18.33% of the sample, followed by financial services, at 16.67%, and materials, at 13.33%. The information technology and communication services sectors respectively account for 8.33% and 6.67% of the sample, while the least represented sector is healthcare, at 3.33%. The proportion of cross-listed companies in the sample is 73.33%, while 26.67% of the companies are listed exclusively on the Toronto Stock Exchange. Although the study is Canadian-based, results from our research could be generalizable, in jurisdictions where cybersecurity risk disclosure and reporting are regulated and guided similarly to Canada, to large companies, since most of the companies are cross-listed.

Consistent with Radu & Smaili (2021), we followed several steps to collect data on cybersecurity disclosure. The data were manually collected, beginning with the

Table 1 Sample Distribution by Sector

Sectors	Number of companies-year	Percentage
Communication services	20	6.67
Consumer cyclical	25	8.33
Consumer staples	30	10.00
Energy	55	18.33
Financial services	50	16.67
Healthcare	10	3.33
Industrials	30	10.00
Information technology	25	8.33
Materials	40	13.33
Utilities	15	5.00
TOTAL	**242**	**100.00**

[3] TMX Money about S&P/TSX 60 Index: https://money.tmx.com/en/quote/%5ETX60.

firms' annual reports, accessed through the System for Electronic Document Analysis and Retrieval[4] (Sedar). Using the keywords cyber, cybersecurity, security, cyber attack, attack, information security, information technology and IT, we selected the cybersecurity disclosure contained in the annual report. One of the researchers confirmed the automatically selected disclosure. Using our quantitative methodology, we measured the presence and volume of disclosure.

Data on board effectiveness were collected from the University of Toronto Board Shareholder Confidence Index (BSCI),[5] a database used in prior governance research (Ben-Amar & McIlkenny, 2015; Conheady et al., 2015). Other governance data were collected from complementary information in management or proxy circulars in Sedar, and financial data were collected from Compustat.

4.2 Research design

To test our hypotheses, we use two sets of regression models. The following binary LOGIT model, with cybersecurity disclosure decision as a dependent variable, is used to test $\mathbf{H_1}$.

$$Cyber\_Discl\_Decision_{i,t} = \beta_0 + \beta_1 Effectiveness_{i,t} + \beta_2 Firm\_Size_{i,t} + \beta_3 \mathrm{Pr}ofitability_{i,t} + \beta_4 Leverage_{i,t} + \beta_5 MTB_{i,t} + \beta_6 Industry_{i,t} + \varepsilon_{i,t} \quad (1)$$

Where, for year *t* and firm *i*: Cyber_Discl_Decision is a binary variable coded 1 if the firm discloses cyber-related information and 0 otherwise; Effectiveness is board effectiveness as measured by the BSCI; control variables are Firm_Size as measured by the natural logarithm of total assets; Profitability is measured by ROA (return on assets); Leverage, by total liability divided by book value of equity; MTB is the market-to-book ratio; and Industry is a binary variable to control for the effect of industry membership, taking the value 1 for cyber-sensitive industries (commercial banks, insurance, IT, communications and electronic shopping) and 0 otherwise.

Our model for testing hypotheses $\mathbf{H_2}$, $\mathbf{H_3}$ and $\mathbf{H_4}$ is as follows.

$$Cyber\_Discl\_Vol_{i,t} = \beta_0 + \beta_1 Independence_{i,t} + \beta_2 Board\_Size_{i,t} + \beta_3 Expertise_{i,t} + \beta_4 Firm\_Size_{i,t} + \beta_5 Profitability_{i,t} + \beta_6 Leverage_{i,t} + \beta_7 MTB_{i,t} + \beta_8 Industry_{i,t} + \varepsilon_{i,t} \quad (2)$$

Where, for year *t* and firm *i*, the dependent variable, Cyber_Discl_Vol, is the volume of cybersecurity disclosure, the independent variables are Independence (proportion of independent directors on the board), Board_Size (number of directors on the board) and Expertise (proportion of directors with financial expertise on the board). Consistent with previous literature, we control for Firm_Size, measured by the natural logarithm of total assets, Profitability, measured by ROA, Leverage, measured by total liability divided by book value of equity, MTB and Industry, a binary variable to

[4] Sedar: https://www.sedar.com/.

[5] University of Toronto, https://www.rotman.utoronto.ca/FacultyAndResearch/ResearchCentres/JohnstonCentre/BoardRatings.

control for the effect of industry membership, taking the value 1 for cyber-sensitive industries (commercial banks, insurance, IT, communication and electronic shopping) and 0 otherwise.

Our sample includes panel data collected from 300 firm-year observations for the 2014–2018 period. A pooled OLS model could induce bias in estimators (De Andres & Vallelado, 2008). As *Industry* is a time-invariant variable, we used the Hausman test to determine the most appropriate model for our test (fixed or random effects). The results of the Hausman test ($\chi^2 = 22.56$, $p = 0.002$) indicated that fixed effects was the best approach.

4.3 Variables

4.3.1 Dependent variables

Two measures are used for cybersecurity disclosure. Consistent with prior research (Ben-Amar & McIlkenny, 2015), a binary variable measuring the firm's decision to disclose information on cybersecurity is used in Eq. (1) and is labelled Cyber_Discl_Decision. It takes the value 1 if the firm discloses cybersecurity information and 0 otherwise. Our second dependent variable is the volume of cybersecurity disclosure, Cyber_Discl_Vol, used with Eq. (2). Similar to Campbell (2004), we measure disclosure volume as the number of words the firm uses to disclose cybersecurity information in its annual report.

4.3.2 Independent variables

Board effectiveness is a multidimensional concept. Some researchers measure board effectiveness using individual dimensions such as board independence, board size, board activity, audit committee independence, director ownership, board expertise or CEO duality (Elzahar & Hussainey, 2012; Lipton & Lorsch, 1992; Lorca et al., 2011). Others use a composite measure (Ben-Amar & McIlkenny, 2015; Switzer & Cao, 2011), as we do for this study. Board effectiveness (Effectiveness) is measured using the Board Shareholder Confidence Index. The index evaluates board effectiveness based on determinants of the board's ability to fulfill its duties from a shareholder perspective (Fullbrook & Spizzirri, 2018), in line with the theoretical background of our hypothesis. Used by prior research (Ben-Amar & McIlkenny, 2015; Conheady et al., 2015), the index evaluates governance variable groups in three categories: directors' individual potential, the board's group potential, and board decision outputs. The maximum score for an effective board is 150, and there are score deductions for non meeting the effectiveness criteria.

The first category, directors' individual potential, assesses the effectiveness of individual directors and consists of several criteria: independence from management, as directors must represent the interests of stakeholders rather than managers; director interlocks and executive interlocks, given perceived risks that board members may make decisions in other companies' interests if directors sit together on other boards or have interlocks with executives at other companies; excessive board membership, as a director must dedicate time to perform effectively; director attendance, since

directors must have sufficient time to dedicate to the board; and director share ownership, which motivates directors to make decisions in the interest of shareholders.

The second category, the board's group potential, which assesses the board's collective effectiveness, consists of the CEO/chair split, since the board must act independently from management; board committee independence (audit, compensation and nominating committee), to ensure no conflict of interest mars the oversight role of the activities of executive compensation, financial audit and board nomination; share structure, which should provide balanced voting rights to allow the board to represent the interests of all shareholders; a management-free meeting policy, which is important while the board hires the CEO or evaluates CEO performance; director assessments, as the board skill matrix is useful for assessing the board's collective skillset; continuing education and orientation, an important activity for developing individual skills; board retirement policies, to have a board renewed regularly; and a board gender diversity policy, to encourage better representation of women on boards.

The board decision output is the third category, including decisions with a dilution effect, i.e., pay-for-performance policies, pay risk management policies, change of control provisions, CEO share ownership, director election and executive succession planning.

Board independence (Independence) represents the ratio of non-executive board members divided by the total number of board members (Lu & Wang, 2018). Board size (Board_Size) is the total number of directors on the board (Hussain et al., 2018).

Table 2 Summary of Variables Used in the Model

List of Variables	Measurement of Variables
Dependent and independent variables	
Cybersecurity disclosure decision (Cyber_Discl_Decision)	Dummy variable equal to 1 for disclosed cybersecurity information and 0 otherwise
Cybersecurity disclosure volume (Cyber_Discl_Vol)	Number of words in the cybersecurity disclosure
Board effectiveness (Effectiveness)	Total board effectiveness score from BSCI
Board independence (Independence)	Number of non-executive board members divided by board size
Board size (Board_Size)	Total number of directors on the board
Board financial expertise (Expertise)	Number of directors with financial expertise divided by board size
Control variables	
Firm size (Firm_Size)	Natural logarithm of total assets
Profitability (Profitability)	Ratio of opening income to total assets (ROA)
Leverage (Leverage)	Ratio of total debt divided by total assets
Market to Book (MTB)	Market capitalization to shareholders' equity
Industry membership (Industry)	Industry SIC (Standard Industrial Classification) code

Board financial expertise (Expertise) is the number of board members with finance and accounting skills and expertise, divided by the total number of board members (Minton et al., 2014).

4.3.3 Control variables

We control for variables used in prior research as determinants of disclosure: firm size (Hussain et al., 2018), profitability (Liao et al., 2015), leverage (Michelon & Parbonetti, 2012), MTB (Ben-Amar et al., 2021) and industry membership (Elzahar & Hussainey, 2012). Firm size (Firm_Size) is the natural logarithm of the firm's total assets. As firm size indicates the number of firm stakeholders, bigger firms should respond to increased stakeholder pressure to disclose relevant information. It follows that volume of risk disclosure is positively associated with firm size (Zadeh & Eskandari, 2012), and a positive coefficient is predicted for firm size. Profitability (Profitability) is calculated as the ratio of opening income to total assets (ROA), and a positive coefficient is expected. The variable Leverage is the ratio of total debt divided by total assets. Higher leverage levels imply higher agency costs, and disclosure could reduce agency costs and information asymmetry (Lopes & Rodrigues, 2007). Hence, a positive coefficient is expected for leverage. Disclosure is associated with the firm's use of capital and with the market valuation of shareholders' wealth (Brammer et al., 2006). We expect a positive coefficient for MTB. Industry membership (Industry) is related to political costs (Watts & Zimmerman, 1990), but no prediction for the coefficient sign could be made.

Definitions of variables are summarized in Table 2.

Table 3 Descriptive Statistics

Variables	Mean	Median	Standard Deviation	Minimum	Maximum
Cyber_Discl_Decision	0.717	1.0	0.451	0	1
Cyber_Discl_Vol	310.18	229.50	325.294	0	1759
Effectiveness	124.49	126.00	19.241	69	150
Independence	0.763	0.833	0.206	0	1
Board_Size	11.38	11.00	2.737	5	17
Expertise	0.476	0.429	0.270	0	1
Firm_Size	10.487	10.217	2.397	3.145	16.351
Profitability	0.0209	0.025	0.201	-3.144	0.892
Leverage	0.647	0.626	0.263	-0.941	0.999
MTB	7.729	3.510	11.080	0.008	76.364
Notes: N=300					

5 Results

5.1 Descriptive statistics and correlations

Descriptive statistics are presented in Table 3. On average, 71.7% of our sample disclosed cybersecurity information. The percentage of disclosing firms increased steadily, from 56.7% to 2014, the first year of our analysis, to 85.0% in 2018, the last year of the study. This significant increase ($p<0.01$) suggests increased awareness of cybersecurity over time.

On average, the volume of cybersecurity disclosure is 310.18 words. We note high dispersion of this volume in the sample, with a standard deviation of 325.29. The volume varies from 0 to 1759 words. On average, it also increases over time, from 161.2 words in 2014 to 461.6 in 2018, a significant increase of 186.4% ($p<0.0005$).

Board effectiveness averages 124.5 out of 150, with no statistically significant differences over time. The average board effectiveness score is 83%, representing an equivalent score of 3 out of 6 based on the conversion used by Ben-Amar & McIlkenny (2015). It is comparable to the average board effectiveness of 2.52 for their Canadian sample for the 2008–2011 period.

The average percentage of independent board members is 76.3%, and there are no statistically significant differences over time. Average board size is 11 directors, and there is also no significant variation over time. On average, 47.6% of the directors have financial expertise, with no significant variation over the research period. The sample consists of the 60 largest Canadian firms in 2018, with a mean firm size of 10.49.

Table 4 presents Pearson's bivariate correlation coefficients for the variables in our regression model (2). We note a significant positive correlation between volume of cybersecurity disclosure and board size, as predicted by our third hypothesis. We continue with the multivariate analysis in the next section.

5.2 Multivariate analysis

Table 5 summarizes our test results for our first hypothesis. A LOGIT regression of cybersecurity disclosure decision on board effectiveness was carried out in Eq. (1).

Table 4 Correlation Matrix

	1	2	3	4	5	6	7	8
1. Cyber_Discl_Vol	1							
2. Independence	-0.108	1						
3. Board_Size	0.194**	0.001	1					
4. Expertise	0.038	0.165**	-0.036	1				
5. Firm_Size	0.113	-0.158**	0.029	0.121*	1			
6. Profitability	0.088	0.013	0.125*	-0.079	-0.014	1		
7. Leverage	0.144*	-0.150**	0.402**	-0.011	0.162**	0.329**	1	
8. MTB	-0.180**	-0.024	-0.213**	-0.194**	-0.088	0.087	-0.184**	1

** Denotes statistical significance at the 0.01 level (2-tailed) and * at the 0.05 level (2-tailed)

Table 5 Regression of Cybersecurity Disclosure Decision on Board Effectiveness

	Model (1)	Model (2)
Control variables		
Firm_Size	-0.0002	0.0133
	(0.037)	(0.040)
Profitability	-0.0760	-0.0668
	(0.402)	(0.415)
Lev	0.906***	0.643*
	(0.332)	(0.349)
MTB	-0.0294***	-0.0237***
	(0.008)	(0.009)
Ind	0.414*	0.520**
	(0.226)	(0.254)
Independent variable		
Effectiveness		0.0203***
		(0.005)
Constant	0.170	-2.339***
	(0.433)	(0.747)
Observations	300	300
Number of Companies	60	60
LR χ^2	33.92***	53.20***
Pseudo R-squared	0.095	0.149

Dependent variable: Cyber_Discl_Decision

All variables are defined in Table 1

Standard errors in parentheses. *** p<0.01, ** p<0.05, * p<0.1

We first regress Cyber_Discl_Decision on control variables in model (1), as in the first column of Table 5, and in model (2), using board effectiveness as a predictive variable. Table 5 shows overall model significance ($p<0.0005$) and a Pseudo R^2 of 14.9%.

Results in column (2) of Table 5 confirm our first hypothesis regarding an association between the decision to disclose cybersecurity information and board effectiveness. The coefficient on board effectiveness is positive (0.02) and strongly significant (p-value of 0.005), suggesting that more effective boards are more transparent and disclose cybersecurity-related information.

Concerning control variables, Table 5 shows a positive and significant coefficient on leverage. The decision to disclose cybersecurity information implies reducing agency costs. Information asymmetry and higher leverage are associated with more transparency. A negative and significant coefficient for market-to-book ratio is also reported in Table 5. A positive and significant coefficient on industry membership is consistent with prior literature on the influence of industry membership on the decision to disclose relevant information.

We continue with testing hypotheses $\mathbf{H_2}$ to $\mathbf{H_4}$. As we use longitudinal data, a Hausman test to decide between the fixed effects or random effects model was performed. Results of the Hausman test, (χ^2 (7)=20.64, Prob>χ^2=0.0054), show that a fixed effects model is more appropriate for our sample. Therefore, a regression with a fixed effects model for panel data was used, based on Eq. (2). The fixed effects model controls for firm, year and industry. Results of the regression of cybersecurity disclosure volume on control variables are reported in column (1) of Table 6. Regression results including independent one-dimensional measures of board effectiveness, i.e., board

Table 6 Regression of Cybersecurity Disclosure Volume on Governance Variables

	Model (1)	Model (2)
Control variables		
Firm_Size	57.910***	55.105***
	(14.012)	(13.993)
Profitability	180.752*	172.330*
	(95.214)	(95.526)
Lev	152.338	179.346
	(167.256)	(167.045)
MTB	-3.479**	-3.649**
	(1.704)	(1.691)
Independent variables		
Independence		241.500*
		(134.80)
Board_Size		10.254
		(12.022)
Expertise		304.283*
		(166.194)
Constant	-372.558*	-804.979***
	(189.364)	(279.033)
Fixed effects	Firm, year & industry	Firm, year & industry
Observations	300	300
Number of Companies	60	60
F	9.59***	6.67***
R-squared	0.140	0.167

Dependent variable: Cyber_Disclosure. All variables are defined in Table 1

Standard errors in parentheses. *** $p<0.01$, ** $p<0.05$, * $p<0.1$

independence, board size and board financial expertise, are presented in column (2) of Table 6. Overall, the model is statistically significant ($F=6.67$, $p<0.0005$), and the predictors explain 16.7% of the variation in the volume of cybersecurity disclosure.

Regarding board independence, a positive and significant ($p<0.1$) coefficient is reported in column (2) of Table 6. This finding suggests that more independent directors will disclose more cybersecurity information. As the coefficient for Board_size is not statistically significant, our hypothesis $\mathbf{H_3}$ regarding a positive association between board size and cybersecurity disclosure could not be confirmed. Board size seems to have no impact on the volume of disclosure.

A positive and significant coefficient on Expertise (304.3, $p<0.1$) provides support for our hypothesis $\mathbf{H_4}$, whereby board members' financial expertise has a positive impact on the volume of cybersecurity disclosure. Boards with more financial expertise are more transparent and increase the volume of cybersecurity-related information disclosed.

Consistent with prior research, we found that firm size has a positive and significant impact on cybersecurity disclosure. Bigger firms with more stakeholders face increased pressure to disclose relevant information.

As we expected, firm profitability has a positive impact on cybersecurity disclosure. Prosperous firms can afford higher costs related to disclosing relevant information to stakeholders. Similar to results reported in Table 5, the market-to-book ratio is negatively associated with disclosure.

6 Discussion and conclusion

Cybersecurity has become a critical issue for businesses, and more effort should be devoted to this concern. This research aimed to determine the influence of board effectiveness on disclosure of cybersecurity information. According to stakeholder theory, the board balances stakeholders' demands and plays an important role in risk management. More effective boards better identify, discuss and manage risk. We consider that more effective boards are more likely to be transparent by providing disclosure on risk management, and particularly on cybersecurity. More specifically, we predicted that cybersecurity disclosure volume would be strongly and significantly influenced by one-dimensional measures of board effectiveness in the form of board independence, board size and board financial expertise.

Based on a sample of 300 firm-year observations for the 2014–2018 period and using a regression model, we empirically tested our hypothesis. The first hypothesis, predicting an association between board effectiveness and the decision to disclose information about cybersecurity, was confirmed. A more effective board is more transparent about cybersecurity. As Canadian regulation on cybersecurity emerged in 2013 to provide guidance regarding cyber risk management and disclosure, we note a continuous increase of cybersecurity disclosure over time. Firms grew increasingly aware of cyber risks and cybersecurity, and these issues became major disclosure topics in 2018, with an average number of 461.58 words devoted to cybersecurity, compared to 161.20 in 2014.

We expected board independence, board size and board financial expertise to have a positive impact on cybersecurity disclosure volume. Our hypothesis on the positive association between board independence, board financial expertise and disclosure is confirmed, but board size has no impact on the amount of cybersecurity information disclosed.

Independent members of the board, who act as a governance and oversight mechanism, significantly increase the disclosure of cybersecurity risks in the company's financial statements. In addition, the board has a fiduciary role to monitor management. Financial expertise on the board contributes to risk assessment and management, but multifaceted expertise in technical, ethical and financial areas is required to monitor the emerging concern of cybersecurity. Board members should be continually trained to be aware of the evolution and diversification of business risks and to have appropriate skills and competencies to manage them. Our findings shed light on the positive impact of board members' financial expertise on the volume of cybersecurity disclosure. We expected reasonably that the larger the board, the more likely is to include cybersecurity-specific expertise on the board, but we provide evidence of no such relationship between the board size and the cybersecurity disclosure. The lack of impact of board size on this disclosure may be due to the lack of cybersecurity-specific expertise among most of the directors.

Overall, board effectiveness as a composite measure, and some of its one-dimensional measures, board independence and financial expertise, have a positive effect on cybersecurity disclosure. These findings have practical implications for investors, management, board members and regulators. Given the positive impact of director independence and financial expertise on the disclosure of cybersecurity information,

investors should ask for more independent boards with diversified expertise, including financial expertise. This will reduce the firm's cyber risk by enhancing disclosure transparency and volume. As cybersecurity is an emerging topic that demands multifaceted expertise, managers and the board should have an appropriate training plan while seeking to attract skilled directors. Our results can also be useful for regulators, as disclosure requirements, guides and regulations encourage disclosure of cybersecurity information. More standards and regulations could help firms improve their cyber risk assessment, management and disclosure.

This research is not without limitations. As our sample consists of large Canadian firms, results may be relevant only for this type of entity and in jurisdictions where cybersecurity risk disclosure and reporting are regulated and guided such as in Canada and in U.S. Further research could investigate the impact of board effectiveness on small and medium enterprises. The last years have witnessed major changes in the use of business technologies and increases in remote work and online sales, making cybersecurity crucial for companies. Our study covers a period ending in 2018. It would be interesting to analyze recent developments and changes in the impact of board effectiveness on cybersecurity disclosure in the last three years. We examined some one-dimensional measures of board effectiveness, i.e., board independence, size and financial expertise. Other measures could provide extensive information about the influence of board effectiveness on cybersecurity and cybersecurity disclosure and could be the subject of future research. We tested the influence of financial expertise on cybersecurity disclosure; however, cyber-risk assessment and management demand the contribution of multiple disciplines. Other important board skills and expertise, such as technical (IT), legal or ethical expertise, could have an impact on cybersecurity and are worth investigating. In addition, other board functions than audit committee or audit and risk committee would deal with cybersecurity risk disclosure. It would be interesting to further investigate what specific expertise is associated with this form of disclosure besides financial or accounting expertise. We focused on the annual report for cybersecurity disclosure. Firms can use other reports to disclose cybersecurity information and associated risks. A review of disclosures contained in various reports would provide additional insight into these different disclosure sources.

Funding Acknowledgement We would like to gratefully acknowledge the financial support of the CPA Canada – CAAA.

Declarations Not applicable.

References

Abeysekera, I. (2010). The influence of board size on intellectual capital disclosure by Kenyan listed firms. Journal of intellectual capital

Abraham, S., & Cox, P. (2007). Analysing the determinants of narrative risk information in UK FTSE 100 annual reports. *The British Accounting Review, 39*(3), 227–248

Akerlof, G. A. (1978). The market for "lemons": Quality uncertainty and the market mechanism. *Uncertainty in economics* (pp. 235–251). Elsevier

Allegrini, M., & Greco, G. (2013). Corporate boards, audit committees and voluntary disclosure: Evidence from Italian listed companies. *Journal of Management & Governance*, *17*(1), 187–216

Allini, A., Manes Rossi, F., & Hussainey, K. (2016). The board's role in risk disclosure: an exploratory study of Italian listed state-owned enterprises. *Public Money & Management*, *36*(2), 113–120

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

Amran, A., Bin, A. M. R., & Hassan, B. C. (2009). H. M. Risk reporting.Managerial Auditing Journal

Assante, M. J., & Tobey, D. H. (2011). Enhancing the cybersecurity workforce. *IT professional*, *13*(1), 12–15

Audit Analytics (2020). *Trends in Cybersecurity Breach Disclosures*

Ben-Amar, W., Francoeur, C., Marsat, S., & Wahid, S. (2021). A. How do firms achieve corporate social performance? An integrated perspective. *Corporate Social Responsibility and Environmental Management*

Ben-Amar, W., & McIlkenny, P. (2015). Board effectiveness and the voluntary disclosure of climate change information. *Business Strategy and the Environment*, *24*(8), 704–719

Brammer, S., Brooks, C., & Pavelin, S. (2006). Corporate social performance and stock returns: UK evidence from disaggregate measures. *Financial management*, *35*(3), 97–116

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

Campbell, D. (2004). A longitudinal and cross-sectional analysis of environmental disclosure in UK companies—a research note. *The British Accounting Review*, *36*(1), 107–117

Campbell, J. L., Chen, H., Dhaliwal, D. S., Lu, H., & Steele, L. B. (2014). The information content of mandatory risk factor disclosures in corporate filings. *Review of Accounting Studies*, *19*(1), 396–455

Coles, J. L., Daniel, N. D., & Naveen, L. (2008). Boards: Does one size fit all? *Journal of financial economics*, *87*(2), 329–356

Conheady, B., McIlkenny, P., Opong, K. K., & Pignatel, I. (2015). Board effectiveness and firm performance of Canadian listed firms. *The British Accounting Review*, *47*(3), 290–303

Canada, C. P. A., C. P. A (2017). *Reporting Alert: Corporate reporting*. Cybersecurity Risks and Incidents - Reassessing Your Disclosure Practices

Craigen, D., Diakun-Thibault, N., & Purse, R. (2014). Defining cybersecurity.Technology Innovation Management Review, *4*(10)

CSA, C. S. A. (2013). CSA Staff Notice 11–326 Cyber Security. https://www.osc.gov.on.ca/en/SecuritiesLaw_csa_20130926_11-326_cyber-security.htm

CSA, C. S. A. (2016). CSA Staff Notice 11–332 Cyber Security. https://www.osc.gov.on.ca/en/SecuritiesLaw_csa_sn_20160927_11-332-cyber-security.htm

CSA, C. S. A. (2017a). CSA Multilateral Staff Notice 51–347 Disclosure of Cyber Security Risks and Incidents. https://www.osc.gov.on.ca/en/SecuritiesLaw_csa_20170119_51-347_disclosure-cyber-security.htm

CSA, C. S. A. (2017b). CSA Staff Notice 33–321 Cyber Security and Social Media https://www.osc.gov.on.ca/en/SecuritiesLaw_csa_20171019_33-321_cyber-security-and-social-media.htm

Davis, G. F. (1996). The significance of board interlocks for corporate governance. *Corporate Governance: An International Review*, *4*(3), 154–159

De Andres, P., & Vallelado, E. (2008). Corporate governance in banking: The role of the board of directors. *Journal of banking & finance*, *32*(12), 2570–2580

Donnelly, R., & Mulcahy, M. (2008). Board structure, ownership, and voluntary disclosure in Ireland. *Corporate Governance: An International Review*, *16*(5), 416–429

Dye, R. A. (1985). Disclosure of nonproprietary information.Journal of accounting research,123–145

Elshandidy, T., Fraser, I., & Hussainey, K. (2013). Aggregated, voluntary, and mandatory risk disclosure incentives: Evidence from UK FTSE all-share companies. *International Review of Financial Analysis*, *30*, 320–333

Elshandidy, T., & Neri, L. (2015). Corporate governance, risk disclosure practices, and market liquidity: Comparative evidence from the UK and I taly. *Corporate Governance: An International Review*, *23*(4), 331–356

Elzahar, H., & Hussainey, K. (2012). Determinants of narrative risk disclosures in UK interim reports.The Journal of Risk Finance

Eng, L. L., & Mak, Y. T. (2003). Corporate governance and voluntary disclosure. *Journal of accounting and public policy*, *22*(4), 325–345

Fama, E. F., & Jensen, M. C. (1983). Separation of ownership and control. *The journal of law and Economics*, *26*(2), 301–325

Foglietta, C., Masucci, D., Palazzo, C., Santini, R., Panzieri, S., Rosa, L. … Lev, L. (2018). From detecting cyber-attacks to mitigating risk within a hybrid environment. *IEEE Systems Journal*, *13*(1), 424–435

Freeman, R. E. (2010). *Strategic management: A stakeholder approach*. Cambridge University Press

Fullbrook, M., & Spizzirri, A. (2018). *2018 Board Shareholder Confidence Index*. https://www.rotman.utoronto.ca/FacultyAndResearch/ResearchCentres/JohnstonCentre/JohnstonCentre/2019/12/13/The-2019-Board-Sharehold-Confidence-Index-is-now-out

Gandía, J. L. (2008). Determinants of internet-based corporate governance disclosure by Spanish listed companies.Online Information Review

Garcia-Meca, E., & Sanchez-Ballesta, J. P. (2010). The association of board independence and ownership concentration with voluntary disclosure: A meta-analysis. *European Accounting Review*, *19*(3), 603–627

Giannarakis, G. (2014). Corporate governance and financial characteristic effects on the extent of corporate social responsibility disclosure.Social Responsibility Journal

Grant, G. H., & Grant, C. T. (2014). SEC cybersecurity disclosure guidance is quickly becoming a requirement. *The CPA Journal*, *84*(5), 69

Hernández-Madrigal, M., Blanco-Dopico, M. I., & Aibar-Guzmán, B. (2012). The influence of mandatory requirements on risk disclosure practices in Spain. *International Journal of Disclosure and Governance*, *9*(1), 78–99

Hidalgo, R. L., García-Meca, E., & Martínez, I. (2011). Corporate governance and intellectual capital disclosure. *Journal of business ethics*, *100*(3), 483–495

Hung, H. (1998). A typology of the theories of the roles of governing boards. *Corporate Governance: An International Review*, *6*(2), 101–111

Hussain, N., Rigoni, U., & Orij, R. P. (2018). Corporate governance and sustainability performance: Analysis of triple bottom line performance. *Journal of business ethics*, *149*(2), 411–432

Husted, B. W., & de Sousa-Filho, J. M. (2019). Board structure and environmental, social, and governance disclosure in Latin America. *Journal of Business Research*, *102*, 220–227

Ingley, C., & Van Der Walt, N. (2008). Risk management and board effectiveness. *International Studies of Management & Organization*, *38*(3), 43–70

Ingley, C. B., & Van der Walt, N. T. (2001). The strategic board: The changing role of directors in developing and maintaining corporate capability. *Corporate Governance: An International Review*, *9*(3), 174–185

Jang-Jaccard, J., & Nepal, S. (2014). A survey of emerging threats in cybersecurity. *Journal of Computer and System Sciences*, *80*(5), 973–993

Jensen, M. C. (1993). The modern industrial revolution, exit, and the failure of internal control systems. *the Journal of Finance*, *48*(3), 831–880

Jensen, M. C., & Meckling, W. H. (1976). Theory of the firm: Managerial behavior, agency costs and ownership structure. *Journal of financial economics*, *3*(4), 305–360

John, K., & Senbet, L. W. (1998). Corporate governance and board effectiveness. *Journal of banking & finance*, *22*(4), 371–403

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

Khan, A., Muttakin, M. B., & Siddiqui, J. (2013). Corporate governance and corporate social responsibility disclosures: Evidence from an emerging economy. *Journal of business ethics*, *114*(2), 207–223

Kothari, S. P., Li, X., & Short, J. E. (2009). The effect of disclosures by management, analysts, and business press on cost of capital, return volatility, and analyst forecasts: A study using content analysis. *The Accounting Review*, *84*(5), 1639–1670

Krause, R., Semadeni, M., & Cannella, A. A. Jr. (2013). External COO/presidents as expert directors: A new look at the service role of boards. *Strategic Management Journal*, *34*(13), 1628–1641

Kure, H. I., Islam, S., & Razzaque, M. A. (2018). An integrated cyber security risk management approach for a cyber-physical system. *Applied Sciences*, *8*(6), 898

Lankton, N., Price, J. B., & Karim, M. (2020). Cybersecurity Breaches and Information Technology Governance Roles in Audit Committee Charters.Journal of Information Systems,0000–0000

Lewis, J. A. (2006). Cybersecurity and critical infrastructure protection. *Center for Strategic and International Studies*

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

Liao, L., Luo, L., & Tang, Q. (2015). Gender diversity, board independence, environmental committee and greenhouse gas disclosure. *The British Accounting Review*, *47*(4), 409–424

Lipton, M., & Lorsch, J. W. (1992). A modest proposal for improved corporate governance.The business lawyer,59–77

Lopes, P. T., & Rodrigues, L. L. (2007). Accounting for financial instruments: An analysis of the determinants of disclosure in the Portuguese stock exchange. *The International Journal of Accounting*, *42*(1), 25–56

Lorca, C., Sánchez-Ballesta, J. P., & García-Meca, E. (2011). Board effectiveness and cost of debt. *Journal of business ethics*, *100*(4), 613–631

Lorsch, J. W., & MacIver. (1989). *Pawns or Potentates: The Reality of America's Corporate Boards*. Harvard Business School Press

Lu, J., & Wang, W. (2018). Managerial conservatism, board independence and corporate innovation. *Journal of Corporate Finance*, *48*, 1–16

Luo, Y. (2005). How does globalization affect corporate governance and accountability? A perspective from MNEs. *Journal of International Management*, *11*(1), 19–41

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

Minton, B. A., Taillard, J. P., & Williamson, R. (2014). Financial expertise of the board, risk taking, and performance: Evidence from bank holding companies.Journal of Financial and Quantitative Analysis,351–380

Mintzberg, H. (1983). The case for corporate social responsibility.Journal of Business Strategy

Moore, T., Dynes, S., & Chang, F. R. (2015). Identifying how firms manage cybersecurity investment. *Southern Methodist University 32*. https://cpb-us-w2.wpmucdn.com/blog.smu.edu/dist/e/97/files/2015/10/SMU-IBM.pdf

Moriarty, K. M. (2020). *Transforming Information Security: Optimizing Five Concurrent Trends to Reduce Resource Drain*. Emerald Group Publishing

Newhouse, W., Keith, S., Scribner, B., & Witte, G. (2017). National initiative for cybersecurity education (NICE) cybersecurity workforce framework. *NIST special publication, 800*(2017), 181

Nicholson, G. J., & Kiel, G. C. (2004). A framework for diagnosing board effectiveness. *Corporate Governance: An International Review*, *12*(4), 442–460

Ntim, C. G., & Soobaroyen, T. (2013). Corporate governance and performance in socially responsible corporations: New empirical insights from a Neo-Institutional framework. *Corporate Governance: An International Review*, *21*(5), 468–494

Oliveira, J., Rodrigues, L. L., & Craig, R. (2011). Risk-related disclosures by non-finance companies. Managerial Auditing Journal

Ontario, S., & Commission, O. (2015). *National instrument* (pp. 52–110). Audit Committees

Pigé, B. (2002). Stakeholder theory and corporate governance: the nature of the board information. *Management: Journal of contemporary management issues*, *7*(1), 1–17

Prado-Lorenzo, J. M., & Garcia-Sanchez, I. M. (2010). The role of the board of directors in disseminating relevant information on greenhouse gases. *Journal of business ethics*, *97*(3), 391–424

Public Safety Canada (2018). National Cyber Security Strategy. Canada's Vision for Security and Prosperity in the Digital Age. 35

Raber, R. (2003). The role of good corporate governance in overseeing risk. *Corporate Governance Advisor*, *11*(2), 11–16

Radu, C., & Smaili, N. (2021). Board Gender Diversity and Corporate Response to Cyber Risk: Evidence from Cybersecurity Related Disclosure.Journal of business ethics,1–24

Rankin, M., Windsor, C., & Wahyuni, D. (2011). *An investigation of voluntary corporate greenhouse gas emissions reporting in a market governance system*. Accounting, Auditing & Accountability Journal

Rosenstein, S., & Wyatt, J. G. (1990). Outside directors, board independence, and shareholder wealth. *Journal of financial economics*, *26*(2), 175–191

Rothrock, R. A., Kaplan, J., & Van Der Oord, F. (2018). The board's role in managing cybersecurity risks. *MIT Sloan Management Review*, *59*(2), 12–15

Samaha, K., Khlif, H., & Hussainey, K. (2015). The impact of board and audit committee characteristics on voluntary disclosure: A meta-analysis. *Journal of International Accounting Auditing and Taxation*, *24*, 13–28

Schmidt, S. L., & Brauer, M. (2006). Strategic governance: How to assess board effectiveness in guiding strategy execution. *Corporate Governance: An International Review*, *14*(1), 13–22

Section (2018). Release Nos. 33-10459; 34-82746. Commission Statement and Guidance on Public Company Cybersecurity Disclosures. https://www.sec.gov/rules/interp/2018/33-10459.pdf
Section 2020 Examination Priorities https://www.sec.gov/about/offices/ocie/national-examination-program-priorities-2020.pdf
SpencerStuart (2021). 2020 Canada: Spencer Stuart Board Index. https://www.spencerstuart.com/research-and-insight/board-indexes
Switzer, L. N., & Cao, Y. (2011). Shareholder interests vs board of director members' interests and company performance.Review of Accounting and Finance
Torres, J. M., Comesaña, C. I., & Garcia-Nieto, P. J. (2019). Machine learning techniques applied to cybersecurity. *International Journal of Machine Learning and Cybernetics*, *10*(10), 2823–2836
Tricker, R. I. (2019). *Corporate governance: Principles, policies, and practices*. USA: Oxford University Press
Van den Berghe, L., & Baelden, T. (2005). The complex relation between director independence and board effectiveness.Corporate Governance: The international journal of business in society
Verrecchia, R. E. (1983). Discretionary disclosure. *Journal of accounting and economics*, *5*, 179–194
Wang, T., Kannan, K. N., & Ulmer, J. R. (2013). The association between the disclosure and the realization of information security risk factors. *Information Systems Research*, *24*(2), 201–218
Watts, R. L., & Zimmerman, J. L. (1990). Positive accounting theory: a ten year perspective.Accounting review,131–156
Winter, S. G., & Williamson, O. E. (1991). *The nature of the firm: origins, evolution, and development*. Oxford University Press
World Economic Forum (2019). *Regional Risks for Doing Business 2019. Insight report*.https://www.weforum.org/press/2019/10/cyberattacks-and-fiscalcrises-top-list-of-business-risks-in-2019/
Xie, J., Nozawa, W., Yagi, M., Fujii, H., & Managi, S. (2019). Do environmental, social, and governance activities improve corporate financial performance? *Business Strategy and the Environment*, *28*(2), 286–300
Zadeh, F. O., & Eskandari, A. (2012). Firm size as company's characteristic and level of risk disclosure: Review on theories and literatures.International Journal of Business and Social Science, *3*(17)

Nadia Smaili Nadia Smaili is a Full Professor of Accounting at the Ecole des sciences de gestion (ESG), University of Quebec at Montreal (UQAM). Professor Smaili's research focuses on financial statements fraud, whistleblowing and corporate governance. She has developed several courses and postgraduate programs related to prevention and detection of fraud.

Camélia Radu Camélia Radu is Associate Professor of Accounting at the Ecole des sciences de gestion (ESG), University of Quebec at Montreal (UQAM). She holds a PhD in Business Administration from HEC in Montreal, Canada. She teaches undergraduate advances financial accounting and graduate research methodology and corporate disclosure courses. Her research focuses on environmental and social disclosure, governance and cybersecurity.

Amir Khalili Amir Khalili holds a master degree from Ecole des sciences de gestion (ESG), University of Quebec at Montreal (UQAM). His research interests focus on cybersecurity and governance.