International Journal of Disclosure and Governance
https://doi.org/10.1057/s41310-024-00226-7

ORIGINAL ARTICLE

How the three lines of defense can contribute to public firms' cybersecurity effectiveness

Sylvie Héroux[1] · Anne Fortin[1]

Received: 9 January 2023 / Accepted: 17 January 2024

Abstract

This interpretative field study examines how public firms deal with cybersecurity-related issues, emphasizing how the three lines of defense can contribute to cybersecurity effectiveness. Sixteen interviews were conducted with 18 participants, including 13 executives/senior managers in internal audit, information technology (IT), and information security (IS) in 13 different public firms. The many cybersecurity structures, processes, or relational mechanisms established by the three lines of defense in the participating organizations are identified. These governance mechanisms are used as a baseline for analyzing how teams in internal audit, IT, IS, cybersecurity, legal, finance, corporate communications, and environmental, social and governance (ESG) are engaged and collaborate in dealing with cybersecurity-related issues. This study entered into the "black box" to document how different organizational functions are involved in IT/IS governance mechanisms associated with cybersecurity. Findings can help board of directors and management reflect on the nature of cybersecurity activities that could be implemented to enhance cybersecurity effectiveness. Regulators may consider the issues raised by participants to clarify regulations about cybersecurity disclosure.

Keywords Cybersecurity · IIA's three lines model · Cybersecurity governance · IT governance · Internal audit

Introduction

> "As the digital age of information and technology has rapidly integrated into daily life, the importance of cybersecurity has become paramount for businesses… Companies must install information security systems and monitor cybersecurity controls to protect their organizations from breaches or attacks" (Coleman et al 2022, p. 3).

These excerpts from a recent research report (Coleman et al 2022) highlight the importance of cybersecurity issues by public companies. In July 2023, the SEC adopted rules that require registrants, in addition to disclosing material cybersecurity incidents, "to describe their processes, if any, for assessing, identifying, and managing material risks from cybersecurity threats, as well as the material effects or reasonably likely material effects of risks from cybersecurity threats and previous cybersecurity incidents." In view of these mandatory requirements, it is essential to understand the actions that public firms take to address cybersecurity-related issues, as this can provide insights for developing/improving cybersecurity practices and assist financial regulators in enhancing their guidelines.

Prior research has addressed cybersecurity practices. Research on managing and controlling information and information technology risks has dealt with IT investments and the implementation of IT controls (e.g., Gordon et al 2008; Lainhart 2000; Wallace et al 2011), the dimensions of information technology material weaknesses (Li et al 2012), information-security policy compliance (Stafford et al 2018), the role of internal auditing (e.g., Islam et al 2018; Slapnicar et al 2022), and cyber incidents (e.g., Amir et al 2018; Carré et al 2018). However, Haapamäki and Sihvonen (2019, p. 830) underline that research on "cybersecurity in private and public companies is still relatively scarce."

Our research objective is to investigate how public firms deal with cybersecurity-related issues. To that end,

✉ Sylvie Héroux
heroux.sylvie@uqam.ca

Anne Fortin
fortin.anne@uqam.ca

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

Published online: 23 February 2024

we document firms' cybersecurity activities (e.g., control, detection, remediation, and external disclosure). Specifically, our research question is: how can the involvement of the three lines of defense (The Institute of Internal Auditors (IIA), 2013, 2020) in IT/IS governance mechanisms associated with cybersecurity contribute to cybersecurity effectiveness? The three lines of defense model is a "risk-management oversight and strategy-setting methodology actively used by many organizations" (Allen et al 2018, p. 136). Based on the IIA's Global Technology Audit Guide (GTAG): Assessing cybersecurity risk (IIA, 2016), the roles of the first line relate to the provision of cybersecurity services/support to the organization's customers/staff "charged with safeguarding the assets of the organization" (p. 6). The second line supports cybersecurity risk management "and oversight functions" (p. 6) (governance). The third line is the provision of assurance/advice "to senior management and the board of directors" (p. 6) regarding the governance and risk management of cybersecurity activities. We use the IT/IS governance perspective that gradually emerged from interviews with 18 participants to present our findings.

By analyzing how the internal audit, IT/IS/cybersecurity, legal services, finance, corporate communications, and ESG (Environmental, Social and Governance) functions are engaged and collaborate in dealing with cybersecurity-related issues, we provide an overview of the contribution of the first, second, and third lines of defense in that matter. Findings will provide insights to boards of directors, audit committees, and executives about how governance and management models could be applied in practice to deal more effectively with cybersecurity issues. Results also highlight areas for improvement that could be useful to financial regulators. The study contributes to the literature by looking not only at the three lines of defense in cybersecurity-related structures, as Slapnicar et al (2023) did, but also at processes and relational mechanisms.

Background

The cybersecurity literature synthesis by Haapamäki and Sihvonen (2019) and the integrative review by Walton et al (2021) provide insights into the methods organizations use to face cybersecurity challenges. For instance, coordination between internal auditors and IS specialists is essential to effective IS/cybersecurity (Islam et al 2018; Steinbart et al 2012, 2013, 2018; Wallace et al 2011). Further, the number of reported internal control shortcomings, incidents of noncompliance, and security incidents is positively associated with the quality of the internal audit/IS functions relationship (Steinbart et al 2018). By collaborating closely, the internal audit and IT/IS functions gain and discuss relevant cybersecurity information. This can lead them to contribute to cybersecurity effectiveness, as they can help board members, managers, and other functions (e.g., corporate communications, legal services) gain a thorough understanding of cybersecurity-related issues and activities.

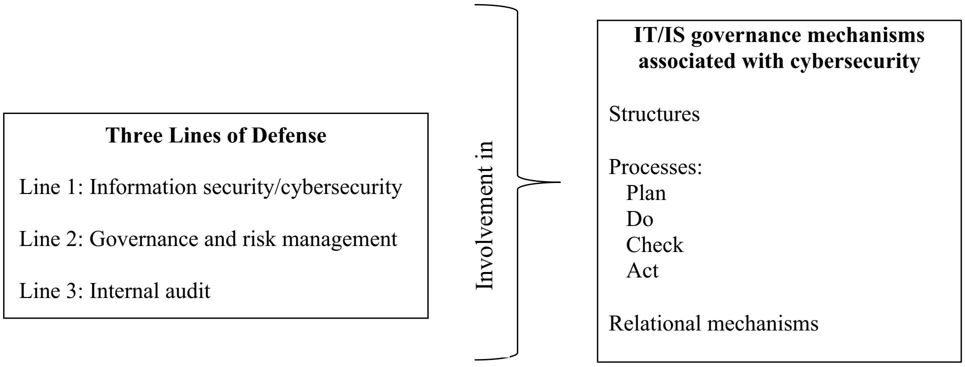
The internal audit function is uniquely positioned to look across the organization (Kahyaoglu and Caliyurt 2018). As the third line of defense (IIA, 2020), internal audit is expected to provide assurance to the board of directors, the audit committee, and management (Chambers and Odar 2015; Kahyaoglu and Caliyurt 2018). Internal audit effectiveness is influenced by many factors including audit scope limitation, risk-based auditing, interaction between internal and external audit, and cooperation with the audit committee (Turetken et al 2020). Extensive risk assessment enhances the extent of cybersecurity focus in the internal audit process (Islam et al 2018). Indeed, nowadays, continuous cybersecurity assurance should be included in the scope of internal audit (Kahyaoglu and Caliyurt 2018). Effective cybersecurity audit contributes to cybersecurity risk management (Slapnicar et al 2022). Internal auditors should apply a structured risk-based program built around a cyber assurance framework and develop an ongoing audit plan (Kahyaoglu and Caliyurt 2018). They should participate in cybersecurity controls testing (Caron 2021) and "check that employees follow safety policies and are trained on safety issues" (Lois et al 2021, p. 33) to mitigate organizations' exposure to external violations. By achieving these actions, the internal audit function gains a thorough understanding of the organization's cybersecurity challenges. This puts internal auditors in a privileged position to advise executives, the board, and its audit committee with respect to cybersecurity-related issues decision-making.

With this in mind, we investigate how public firms deal with cybersecurity-related issues. Specifically, we document how the three lines of defense represented by internal audit and other functions can contribute to cybersecurity effectiveness.

IT/IS governance perspective

As described in the next section, we adopt a qualitative research method based on interviews. We followed an interpretive and inductive approach, without using preconceived theoretical assumptions. The IT/IS governance perspective gradually emerged as the data coding and data analysis progressed, based on participants' comments on the objectives and steps for dealing with cybersecurity-related issues used by different functions in their organization, the sources or frameworks used to accomplish this work, the training of human resources, and the use or non-use of external human resources. IT/IS governance appears to be a relevant perspective for interpreting the data and presenting the results

Fig. 1 Research Framework


Three Lines of Defense
Line 1: Information security/cybersecurity
Line 2: Governance and risk management
Line 3: Internal audit
Involvement in
IT/IS governance mechanisms associated with cybersecurity
Structures
Processes:
Plan
Do
Check
Act
Relational mechanisms

since cybersecurity is "fully contained in information security" (von Solms and von Solms 2018, p. 5), and "IT governance and IS security is a tightly knit concept" (Nicho 2018, p. 10).

To facilitate understanding of the study, this section presents the IT/IS governance concepts that were used to interpret the data collected. The presentation of results rests on the three main dimensions of IT governance, namely structures, processes, and relational mechanisms (e.g., De Haes and Van Grembergen 2009; Wilkin and Chenhall 2010). Structures refer to committees (De Haes and Van Grembergen 2009) and formal positions and roles for IT-related decision-making (Bowen et al 2007). Processes focus on the implementation of IT management techniques and procedures (Bowen et al 2007), including activities such as performance measurement, regular self-assessments, independent assurance, and monitoring (De Haes and Van Grembergen 2009). Relational mechanisms involve IT leadership and other mechanisms such as partnerships and informal meetings between business and IT executives (De Haes and Van Grembergen 2009).

In addition, to deepen the analysis, we went into greater detail regarding the processes. Following Nicho (2018, p. 16), who built an IS governance model, the identified processes were broken down into the following four stages:

- Plan: select appropriate frameworks/standards using a risk-based approach;
- Do: establish, apply, and maintain frameworks/standards;
- Check (audit/oversight): monitor and measure the effectiveness of controls;
- Act: modify and update controls based on internal feedback and change in the business environment.

The analysis builds on the roles of the IIA's three lines of defense with respect to cybersecurity risk assessment (IIA, 2016) that were referenced by participants during interviews. In this study, the first line of defense deals with information security, including cybersecurity; the second line relates to governance and risk management; and the third line concerns the internal audit activity.

Figure 1 illustrates the research framework.

In summary, cybersecurity activities are performed by various functions representing the three lines of defense via structures, processes, and relational mechanisms. Together, they contribute to cybersecurity effectiveness.

Research method

The research is a field study that involved conducting interviews to collect the data. We chose a qualitative interpretive approach to achieve the research objective (Patton 2015). This brought us into the "black box," allowing us to uncover new knowledge regarding cybersecurity activities.

Pre-approval for the research was obtained from the institutional ethics committee for research on human subjects. In this paper, generic expressions are used to preserve the anonymity of participants and organizations, such as participant position titles and educational background, and committee names. For the same reason, a range is provided for organizational size. Details that are too specific are also intentionally omitted.

Sampling

We used a purposeful sampling strategy (Patton 2015). The objective of the participant search was to identify high-ranking executives/senior managers in internal audit, IT, IS, and corporate communications who possessed extensive knowledge of various cybersecurity-related aspects of their organization. The participants sought must have been working in public companies, since these organizations are required to report on cybersecurity in their public filings. Selection of participants resulted from personal contacts and Internet searches. Contacts with internal auditors were especially helpful in identifying individual stakeholders who were knowledgeable about and experienced with cybersecurity-related issues and activities and were willing to participate in the study.

Interview process

The interviews took place as follows: After presenting ourselves, we recalled the purpose of the interview, asked for confirmation of agreement to record the interview, and asked demographic questions. Then, an interview guide was used to orient the exchanges between the researchers and the participants. The semi-structured interviews involved open-ended questions that dealt with topics such as the nature of participants' work, their involvement in cybersecurity, the company IT/IS/cybersecurity governance structure, responsibility for cybersecurity strategy, the measures deployed to reduce cybersecurity-related risks, cybersecurity incident management, the steps in the preparation of external cybersecurity information by different parties in the participating organization, the sources or frameworks used to accomplish this work, human resources cybersecurity training, and whether external experts were used in the process. Examples of questions from the interview guide are: What is the nature of your work with respect to cybersecurity? Who are responsible for the cybersecurity strategy in your organization? What are the measures put in place to reduce the risks related to cybersecurity? What frameworks do you use in your work? Do you use information systems/IT experts (internal or external) to help you perform your work with respect to cybersecurity?

Sample

Between January and April 2021, a total of 16 semi-directed interviews were conducted on Zoom with 18 participants from 13 different public firms[1]. Each lasted about 60 min, for a total of 1060 min. All interviews were digitally recorded and professionally transcribed, resulting in 430 pages of verbatim text. By the end of the interviews, the researchers believed that they had reached saturation since the last interviews did not yield significant new elements.

Table 1 shows that the following sectors were represented: financial services (3), industrial products (3), communications and media (3), consumer products (2), industrial services (1), and utilities (1). The diversity of the sectors represented in the sample extends the applicability of the findings to various industries. The total assets of the organizations were in the C$1.5–10 bn up to the C$100–400 bn ranges. All the organizations had implemented the three lines of defense, and the participants knew the role of each line and referred to it in their interviews. Table 1 also indicates the generic titles of the participants, who were all senior executives or directors from the following functions: internal audit (7), IT/IS or cybersecurity (6), corporate communications (2), ESG (2), and legal services (1). Participants had between 15 and 42 years of experience. Their educational background was varied and appropriate for their function.

Data analysis process

We followed an inductive approach to code the verbatim transcripts. Figure 2 illustrates the steps taken in the data analysis process, which are described in the following paragraph.

Each researcher coded the verbatims individually and prepared a table for each interviewee. The objective of the coding was to identify the organizations' structures and the actions of internal audit, IT, IS, cybersecurity, and other functions related to cybersecurity. It emerged from our respective preliminary coding that the findings could be grouped according to the three main dimensions of IT governance, namely structures, processes, and relational mechanisms (De Haes and Van Grembergen 2009; Wilkin and Chenhall 2010). In light of Miles and Huberman (1994), our individual findings were consolidated into a first set of three tables illustrating in detail these three dimensions for each of the interviews in relation to cybersecurity. Since the objective was to be exhaustive in our coding, the tables included items that were identified by one or both of the researchers. Any item identified by only one researcher was validated by the other researcher by returning to the transcripts. We then collapsed the various structures, processes, and relational mechanisms identified for each interviewee/organization into three summary tables. Further, to facilitate the analysis of the many processes mentioned by participants, we broke them down into four stages (plan, do, check, and act) based on Nicho's (2018) definitions. Finally, the items were linked to the line(s) of defense involved, based on participants' statements regarding the activities carried out within the organization and the individuals/line(s) of defense who perform them. We reviewed the three tables several times before arriving at those analyzed in this article. These tables summarize the items common to several organizations, or those specific to some of them, in terms of the structures, processes, and relational mechanisms involved in cybersecurity.

The final tables presented in the following section constitute the basis for presentation of the results, documenting how the three lines of defense can contribute to cybersecurity effectiveness.

[1] Two of the 16 interviews were conducted with two participants at the same time (Organizations #10 and #12), bringing the total number of participants to 18.

Table 1 Organizations and participants

Organizations		Total assets	Participants			
#	Sector	(Ranges in C$)	#	Generic title	Total years of experience	Educational background[a]
1	Financial Services	100–400 bn	1	Senior Director, Internal Audit	18	Information systems management degree
			2	Senior Director, Cybersecurity	20	Human resources management degree
			3	ESG Director	24	Finance degree, CPA
2	Industrial products	1.5–10 bn	4	Director, Internal Audit	25	Accounting degree, CPA
3	Industrial products	1.5–10 bn	5	Director, Legal Services	20	Law degree
4	Communications and media	1.5–10 bn	6	CISO	28	Business administration degree
5	Financial Services	10–100 bn	7	Vice President, Internal Audit	33	Law degree
			8	Manager, Corporate Communications	26	Law degree, MBA
6	Communications and media	1.5–10 bn	9	Director, Cybersecurity	42	Electronics degree; numerous courses in cybersecurity
7	Financial Services	10–100 bn	10	Vice President, Internal Audit	30	Accounting degree, CPA
8	Utilities	10–100 bn	11	CISO	20	MBA, CISSP
9	Consumer products	1.5–10 bn	12	Vice President, Corporate Communications	40	Law degree
10	Industrial Services	1.5–10 bn	13	Vice President, Internal Audit	32	Accounting degree, CPA
			14	Chief Information Officer	26	Engineering degree
11	Industrial products	1.5–10 bn	15	Vice President, Internal Audit	15	Accounting degree, CPA, CFE, MBA
12	Consumer products	1.5–10 bn	16	Senior Director, Internal Audit	25	Accounting degree, CPA
			17	Vice President, Information Technology	40	IT degree, MBA
13	Communications and media	10–100 bn	18	ESG Director	23	Engineering degree, environment

[a] CPA, Chartered Professional Accountant; MBA, Master of Business Administration; CISSP, Certified Information Systems Security Professional; CFE, Certified Fraud Examiner

Findings and analysis

This section analyzes a variety of the cybersecurity components deployed by the participating organizations. The analysis indicates the presence of these components but not the extent of their use by the sampled organizations.

Results are summarized in Tables 2, 3, and 4. Each table highlights the involvement of the first line (information security, including cybersecurity), second line (governance and risk management), and third line of defense (the internal audit activity) in structures, processes, and relational mechanisms that can contribute to the effectiveness of cybersecurity. Using our IT/IS governance framework, the tables portray how cybersecurity activities are carried out in public companies. As shown in these tables, more than one line of defense could be involved in the same mechanism. Findings are illustrated with some excerpts from the verbatim transcripts.

The first three sections present respectively structures, processes, and relational mechanisms that can contribute to the effectiveness of cybersecurity in the organization. Those involved specifically in cybersecurity external disclosure activities are presented in "Cybersecurity external disclosure activities" section. "Issues raised by participants" section highlights some issues raised by participants.

Structures

In light of De Haes and Van Grembergen (2009) and Bowen et al. (2007), structures refer to the formal positions, committees, and roles of the three lines of defense with respect to cybersecurity.

The board of directors delegates responsibility for technology risk, including cybersecurity, to the audit committee, the risk management committee, or both board committees. The risk management committee may even establish a

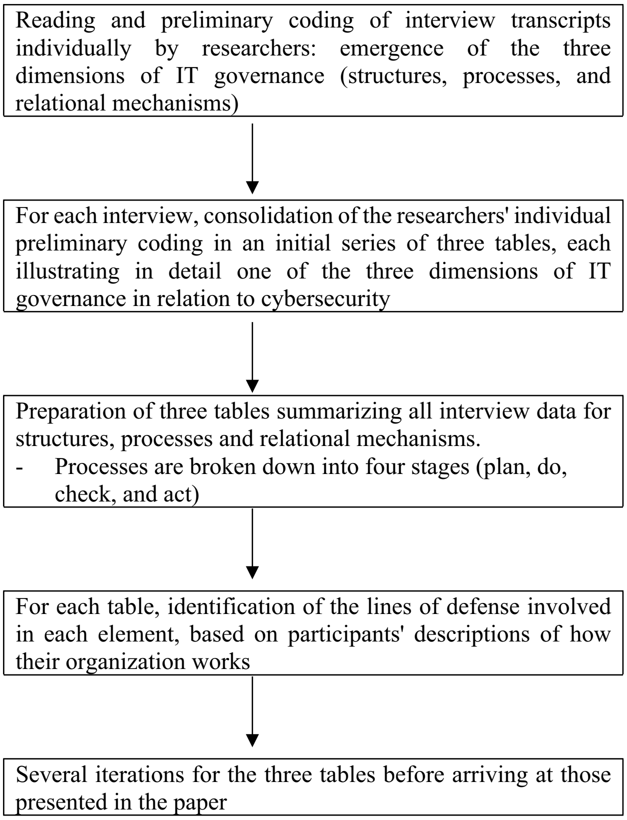

Reading and preliminary coding of interview transcripts individually by researchers: emergence of the three dimensions of IT governance (structures, processes, and relational mechanisms)
For each interview, consolidation of the researchers' individual preliminary coding in an initial series of three tables, each illustrating in detail one of the three dimensions of IT governance in relation to cybersecurity
Preparation of three tables summarizing all interview data for structures, processes and relational mechanisms.
- Processes are broken down into four stages (plan, do, check, and act)
For each table, identification of the lines of defense involved in each element, based on participants' descriptions of how their organization works
Several iterations for the three tables before arriving at those presented in the paper

Fig. 2 Data analysis process

subcommittee specifically dedicated to overseeing technology risk. The technology expertise of committee members varies from one organization to another. In some organizations, the board members have a solid technology background that enables them to ask questions of management and the internal audit function and to follow developments in cybersecurity. In other boards or board committees, this is not the case:

> You almost have to be an IT person to ask a cyber question that holds up. That means that boards are embarrassed to ask those types of questions. They don't want it to be in the minutes. So if you don't give them the ideas and the words on paper and tell them that these are the questions to ask, they don't know what to ask. (Participant 10, Vice President, Internal Audit)

This reflects Kahyaoglu and Caliyurt's (2018) suggestion concerning actively involving internal auditors by engaging in discussions with the board/audit committee and management and helping them think about the organization's cybersecurity vulnerabilities.

At the management level, responsibility for cybersecurity is assigned to an executive who may be a Chief Information Security Officer (CISO) or a Director of Cybersecurity (first line). This executive typically reports to the Vice President of IT or the Chief Information Officer/Chief Technology Officer (CIO/CTO), who may or may not be part of the organization's executive committee. Sometimes the cybersecurity officer reports to the Chief Financial Officer (CFO). The cybersecurity officer develops and implements a security and data protection strategy for the company and prepares information on the subject for public documents. In addition, this is usually the person who presents cybersecurity-related aspects to the audit committee or the risk management committee, and, less frequently, to the full board of directors.

Several committees at the executive level are involved in risk management (second line). Some have a broader scope than cybersecurity (risk management committee, IT governance committee, and IT security committee), whereas others focus on it (cybersecurity steering committee).

The internal audit function is responsible for auditing cybersecurity-related aspects (third line). Its reports can provide the cybersecurity services/support personnel (first line), senior management (second line) and the board of directors with avenues for improvement in the governance and risk management of cybersecurity activities.

In summary, a mature structure based on the three lines of defense has the following characteristics. As the third line (assurance/advise), the internal audit function reports functionally to the audit committee and administratively to the president or the CFO. This function has IT internal auditors and it ensures that the established policies and standards are aligned with best practices, and it audits/tests cybersecurity processes. As the second line (governance and risk management), the IT function reports to the CIO/CTO or the CFO. The CIO/CTO reports to the president and is a member of the executive committee, ESG reports to the CFO, and there is a risk committee at the executive level. As the first line (information security, including cybersecurity), the CISO reports to the CIO or COO and to the full board of directors or the audit committee. There are information security/cybersecurity teams in the business units.

In a less mature structure, there is no CIO or CISO, only a cybersecurity manager who reports to an IT Vice President who is not part of the executive committee. There is no risk committee at the executive level, and the internal audit team has few cybersecurity-related assignments. Furthermore, there are variations in structure between the two maturity levels. Some structures are very elaborate, with several governance committees (second line) overseeing the various activities of the first line.

Processes

Processes focus on the implementation of management techniques and procedures, including activities such as

Table 2 Three lines of defense's involvement in structures associated with cybersecurity

Structures	Roles/responsibilities	Lines of defense
At the board level		
Audit committee or risk management committee	Is responsible or co-responsible for monitoring technological risk including cyber risk Follows up with internal auditor concerning cybersecurity disclosure	Discuss with Lines 2–3
Governance committee	Monitors ESG reporting (including cybersecurity)	Discuss with Lines 2–3
At the management level		
An executive (CISO or Director), Cybersecurity	Develops and implements a corporate data security and data protection strategy Prepares cybersecurity information for public documents Presents cybersecurity issues to the audit committee or the risk management committee, or the full board of directors	Line 1
Risk management committee Composed of several people from different business units and Line 2 representatives	Collects information and determines what will be presented to the board of directors	Line 2
IT governance committee Composed of senior management representatives, including IT and internal audit	Monitors projects from an IT perspective (e.g., security plan, alignment of projects with the organization's business realities, improvements, action plan, follow-up on cyber incidents)	Line 2
Information security committee Composed of business unit managers, IT representatives, and senior management representatives	Monitors the information security plan and reviews incidents and status of third parties	Line 2
Cybersecurity steering committee Composed of senior IT and security executives and representatives of the legal and internal audit functions	Follows up on the cybersecurity aspect of IT projects and prepares communications for the audit committee	Line 2
The finance and legal functions	Are responsible for risk factors presented in public disclosure documents (MD&A)	Line 2
The communications function	Is responsible for communications in public information documents (including cybersecurity and CSR/ESG information)	Line 2
The internal audit function	Is responsible for auditing cybersecurity aspects	Line 3
Disclosure committee (disclosure in public information documents) Composed of senior executives from administrative functions and/or business units	Is responsible for writing cybersecurity information with, among others, CISO and IT representatives Follows up quarterly on cyber incidents	Lines 1–2
An ESG manager	Is responsible for ESG information, including cybersecurity Prepares ESG information for public documents Presents ESG progress and priorities to the board of directors' governance committee	Line 2

performance measurement, regular self-assessments, and monitoring (De Haes and Van Grembergen 2009; Bowen et al 2007). Further, in light of Nicho (2018), the processes are divided into four stages labeled Plan, Do, Check (audit/oversight), and Act. The three lines of defense are involved in these stages to various extents.

"Plan"

The "plan" stage refers to the selection of appropriate frameworks/standards using a risk-based approach (Nicho 2018). It includes items such as approach, frames of reference, internal policies, predefined key performance indicators, and plans and programs for cybersecurity risk management and governance.

Cybersecurity is one of the risks identified in a comprehensive risk-based management and governance approach, on which the three lines of defense base their actions. To develop internal cybersecurity standards and policies, organizations select from numerous frameworks, from those borrowed from public regulations to extant literature on IT governance, information security, third party governance, and ESG criteria (all three lines). They also

Table 3 Three lines of defense's involvement in processes associated with cybersecurity

Panel A –Plan: Select appropriate frameworks/standards using a risk-based approach		Lines of defense
Approach	Comprehensive approach based on risks, including those related to cybersecurity	Lines 1–2–3
Frames of reference	Reporting: 52-109, 51-201; reporting standards by the SASB helpdesk	Lines 1–2–3
	IT governance: COBIT, CMMI	
	Information security: NIST, ITIL, ISO 27000, PCI, ISF	
	Third party governance: CSAE 3416, analysis grid to assess criticality	
	ESG criteria: SASB, MSCI, CDP	
Internal policies	Security, including cybersecurity	Line 2
	Management of safety risks in relation to third parties	
Cybersecurity key performance indicators (KPI)	Identification of measurable targets	Lines 1–2
	Inclusion in the executive compensation system	
	Inclusion in cybersecurity disclosure	
Internally defined materiality criteria	For determining whether information/change is material/important	Lines 1–2
Financial resources/investments	Associated with different levels of cybersecurity risk tolerance	Line 2
Plans and programs	Cybersecurity action/improvement plan	Lines 1–2
	Specific cybersecurity program/protocol/contingency plan	
	Risk management program, including cybersecurity	Line 2
	Internal audit plan:	Line 3
	Mandate regarding business processes, including security	
	Specific mandate regarding security/cybersecurity	
Tools	Registers for recording:	Line 1
	Risks and categorizing them	
	Cybersecurity events/incidents	
	Cybersecurity operational dashboard	
	Cybersecurity event procedures manual	Line 2
	Risk/impact assessment grid, probability, velocity	
Panel B – Do: Establish, apply, and maintain frameworks/standards		Lines of defense
Cybersecurity activities	Centralized around the IT/information security/cybersecurity function	Line 1
	Access	
	Existing controls	
	Incidents that occurred	
	Reporting of issues	
	Follow up on testing results	
	Phishing tests	
	Breach tests	
Daily press review	Be informed of cybersecurity incidents	Line 1
Formal/informal training	Employee cybersecurity training:	Line 1
	Formal: annual and periodic, awareness campaign, e-learning, notices	
	Informal: virtual meeting, capsules	
	Informal training of business unit representatives on cybersecurity through reports/presentations	
	Formal training	
	Of the CISO on cybersecurity	Line 1
	Of the IT internal auditors	Line 3
	Informal training of board of directors by the CISO on cybersecurity questions to ask	Line 1
	Formal/informal training of the audit committee or its chair on cybersecurity by audit firms or internal auditors	Line 3
Communication to all members of the organization	Changes in cybersecurity performance indicators (KPIs)	Line 2
Cybersecurity management maturity	Assessment by the IT function	Line 2

Table 3 (continued)

Panel B – Do: Establish, apply, and maintain frameworks/standards		Lines of defense
Use of the expertise of external consultants	For assisting in the assessment of cybersecurity management maturity	Lines 2–3
	For benchmarking	
	For specific or permanent mandates regarding cybersecurity	
	For internal audit mandates regarding cybersecurity	
	For IT consulting mandates	

Panel C –Check (audit/oversight): Monitor and measure the effectiveness of controls		Lines of defense
Self-assessment of cybersecurity controls	Based on defined cybersecurity frameworks/policies/targets	Line 3
Follow up/evaluation of cybersecurity action plans	Submission to management	Lines 2–3
	Follow-up by the officials involved	
	Evaluation by internal audit	
Tests on the effectiveness of controls	On security (including cybersecurity) by internal audit	Line 3
	Test results can be used by the external auditor	
Follow-up regarding cybersecurity failures/test results	By the internal audit function with management (and the IT function)	Lines 1–2–3
Audit	Of cybersecurity performance indicators by the internal audit function	Line 3
	Of third-party governance by the internal audit function	
	Of third-party governance by the external auditor	Discuss with Line 3
Assessment of the cybersecurity control environment	By the external auditor as part of the annual financial statement audit	Discuss with Line 3
Report/presentation	On cybersecurity priorities and key performance indicators by the cybersecurity officer to the board of directors and the executive committee	Line 1
	On cybersecurity by the CISO or the Chief Technology Officer (CIO) in the presence of the head of internal audit to the audit committee	Lin es 1-2
	On cybersecurity by internal audit to the risk management committee/audit committee of the board of directors and to management	Line 3
	On third party governance by internal audit to the risk management committee	
Monitoring	Of the improvement plan and cybersecurity performance indicators by the audit committee through the CISO, the CIO or the internal audit function	Lines 1–2–3
	By benchmarking from external governance agencies' reports	Line 2
	Of existing cybersecurity measures by	Line 2
	Regulatory agency	
	External governance agencies	

Panel D –Act: Modify and update controls based on internal feedback and change in the business environment		Lines of defense
Changes/adjustments	To controls following the internal cybersecurity incident management process	Lines 2–3
Monitoring	Of cybersecurity maturity with the audit committee in connection with investments	Lines 2–3
	Standards/policies to implement to keep aligned with the evolution of trends and threats	Lines 1–2-3
Retraining	If employees fail internal phishing tests	Line 1
Continuous improvement approach	Following information sharing	Lines 1–2-3
	After follow-ups	
	After frequent discussions between internal stakeholders (and external ones, if needed)	

Table 3 (continued)

Panel D –Act: Modify and update controls based on internal feedback and change in the business environment		Lines of defense
Review/update	Internal policies	Lines 1–2–3
	Cybersecurity event procedures manual	
	Benchmarking	
Other adjustments	Following evaluations by external governance agencies or high-profile exfiltration cases	Line 2
	To cyber-risk management in strategic partnerships with third parties	
	To contracts with customers, with third party partners	
	To financial resources allocated for cybersecurity (optimal use—proportion vs. risk—see Panel A—Plan)	

51-201: National policy 51-201: Disclosure standards (CSA, 2013)

52-109: Regulation 52-109 respecting certification of disclosure in issuers' annual and interim filings (CSA, 2015)

CDP: Disclosure Insight Action https://www.cdp.net/en/guidance/guidance-for-companies

CMMI: Capability Maturity Model Integration https://cmmiinstitute.com

COBIT: Control Objectives for Information Technology (ISACA 2019)

CSAE (Canadian Standards on Assurance Engagements) 3416: Reporting on controls at a service organization relevant to user entities' internal control over financial reporting (CPA Canada 2019)

ESG: Environmental, Social and Governance Criteria

ISF: Information Security Forum https://www.securityforum.org

ISO27000: Information technology — Security techniques—Information security management systems—Overview and vocabulary https://www.iso.org/standard/73906.html

MSCI: https://www.msci.com/our-solutions/esg-investing/esg-ratings

NIST: National Institute of Standards and Technology—US Department of Commerce https://www.nist.gov

PCI: Payment Card Industry Security Standards Council https://www.pcisecuritystandards.org

SASB: Sustainability Accounting Standards Board https://www.sasb.org/about/

Table 4 Three lines of defense's involvement in relational mechanisms associated with cybersecurity

Relational mechanisms		Lines of defense
Management's vision	Of cyber risk tolerance	Lines 1–2
	For reporting (including cybersecurity)	
Collaboration	Close and regular between the three lines of defense on information security, including cybersecurity	Lines 1–2-3
	Between the person responsible for information security (CISO) and internal auditors and external auditors regarding information security, including cybersecurity	Lines 1–3
	Between the finance, IT, legal, and communications functions on reporting (including cybersecurity)	Lines 1–2
	Between the person responsible for the preparation of the ESG report and the parties involved in the topics reported, including cybersecurity	
Discussion/information sharing	Informal internal discussion/information sharing groups on cybersecurity best practices	Lines 1–2
	Formal external discussion groups/information sharing communities on information security, including cybersecurity (by industry or multi-industry)	Line 1
	Formal external discussion groups/information sharing community on internal audit, including information security such as cybersecurity	Line 3
Training	Formal training for all employees on new cybersecurity risks, given either by the IT or information security functions or by external consultants	Lines 1–2
	Formal or informal training of board members (or audit committee members) given by the IT or information security functions	Line 1

recognize the limitations of each of these frameworks for cybersecurity purposes.

> The statement "We're going to comply 100 percent with the NIST [National Institute of Technology] framework." That's not managing risk. Compliance and cybersecurity are two things. You don't manage your risk by being 100% compliant. That's not how it works. If you think it is, well, you're a bad cybersecurity practitioner. … NIST, ISO [International Organization for Standardization], any other framework, they're toolboxes that I use mainly to help myself, to figure out if I've overlooked something. (Participant 6, CISO)
>
> [The Payment Card Industry – PCI framework] is extremely well done because it's technically based. It's not only technically based, but it's scope-based because its scope is credit cards. You should know what the scope of NIST is and what the scope of ISO is. Well, the scope is everything. (Participant 6, CISO)
>
> There's NIST and its CSF [cybersecurity framework]. There's ISO 27 000. There's just one thing I've learned: there's no framework that works from A to Z. You have to pick and choose bits and pieces, then develop your framework to suit the maturity of your organization. There isn't one framework I can tell you: it's this one. It's really a combination of a little bit [of various frameworks]. (Participant 9, Director, Cybersecurity)

Indeed, as suggested by these practices, the internal audit function should rely on one of the cybersecurity frameworks (COBIT, NIST) to ensure consistency of benchmarks and terminology across the three lines of defense (Kahyaoglu and Caliyurt 2018). Alternatively, it can develop its own framework (Slapnicar et al 2022).

In the "plan" stage, efforts are made to identify quantifiable security/cybersecurity key performance indicators (KPIs) (first and second lines). Incorporating these targets into the executive compensation system could contribute to the achievement of objectives by stimulating management commitment in this regard, including allocation of sufficient financial resources to deal with cybersecurity risks.

> Let's face it, when the time comes to put a dollar value on a cybersecurity risk, it's not easy. That's when you shouldn't get caught up in details because you could spend a week detailing a risk in monetary terms. (Participant 16, Senior Manager, Internal Audit)
>
> Let's say 10% of your bonus, your compensation plan is linked to these objectives, believe me, you'll see change happen in the company! It'll speed us up by three years. That's the motivator. Money always talks. Always. (Participant 9, Director, Cybersecurity)

In addition to KPIs, internal criteria must be defined in advance to identify, for example, cybersecurity events or incidents that the organization would consider important (or material) because they generate a reputational risk or a loss of services or revenue (second line).

Forecasting cybersecurity investments is closely linked to the cybersecurity risk appetite of those responsible for governance (management [second line] and board of directors). A zero-tolerance goal (regarding cyber incidents, for example) is impossible to achieve in practice given the huge investments it would involve. Companies seek an optimal balance/dose of cyber risk tolerance and investments to properly manage this risk, and this may vary from one organization to another, depending on the risk tolerance of the board and management.

> [The president] says, "As for me, zero tolerance." I say, "But you can't have zero." He says, "Well, 99.99!" "OK. 99.99." I say, "But you have to be aware that if we're not able to achieve that the first five years what happens? And if it costs $100 million, $500 million to get to that number? You have to balance your appetite for risk, there's an investment to be made. It has to be doable." (Participant 9, Director, Cybersecurity)

Cybersecurity risks and practices are managed by cybersecurity action or improvement plans, internal audit plans with mandates that include or specifically address cybersecurity, risk management programs that include cybersecurity, and specific cybersecurity programs (all three lines).

> From an internal disclosure point of view, we have a risk management program, everything related to cybersecurity is always on what we call heatmaps because cybersecurity has been topical for a very long time. (Participant 16, Senior Director, Internal Audit)

Tools for managing cybersecurity risks include a cyber-incident procedures manual, a register of potential risks categorized by level of criticality as well as a register of cybersecurity events or incidents, and a cybersecurity operational dashboard recording risk monitoring activities in line with the regulatory framework (first line). One of the preferred means of risk governance/management is a risk assessment and impact grid forecasting the likelihood of events or incidents occurring and the estimated speed at which they would damage the organization's reputation or its assets (velocity) (second line).

"Do"

The "do" stage refers to the establishment, application, and maintenance of frameworks/standards (Nicho 2018).

Some organizations tend to centralize cybersecurity activities around a function such as IT, information security, or cybersecurity because of the specific skills and knowledge involved (first line). Common actions include access management, management of existing controls and cybersecurity incidents, and reporting problems through a centralized mechanism. Sometimes an internal team performs phishing tests or the IT/cybersecurity function manages breach tests.

A daily press review to keep abreast of national and international cybersecurity incidents helps in anticipating whether similar problems could occur in the organization and to establish procedures to remedy or correct the situation (first line). These incidents can affect partnerships with third parties.

One of the activities described is the formal or informal cybersecurity training given to employees, business unit managers, executives, and directors. It can be provided by the CISO, the head of internal audit, or their respective team members (first and third lines), or by external audit firms. The training is aimed at maintaining or improving cybersecurity risk management and governance. IT and cybersecurity training is also provided by external parties to in-house trainers such as internal auditors or the CISO.

> It includes cybersecurity awareness campaigns with our internal IT client and there is also mandatory eLearning on cybersecurity for employees. If they don't do the training, we cut off their access to their email. So, people take the training. (Participant 12, Vice President, Corporate Communications)

Other actions intended to maintain or improve cybersecurity governance and risk management consist in communicating to all the organization's members cybersecurity performance indicator trends, cybersecurity benchmarking and assessing the maturity of cybersecurity management (second line). The internal audit function (third line) can then assess any measures planned by the IT department/CISO (first line). In addition to the IT function, external consultants may be called upon to collaborate in these activities carried out by the second and third lines.

> Our IT department will actually go and get studies to find out where we stand on different criteria, either in terms of infrastructure or patching, various things. And they're able to either do it themselves, therefore we benchmark ourselves with the studies, or it's happened that we actually hired a subcontractor to do some kind of analysis, diagnosis to tell us where we stand. (Participant 15, Vice President, Internal Audit)
>
> The IT department itself has done maturity assessments over the years and what we did was to see if the roadmap of the initiatives worked with [the maturity assessments], to see the achievement of the organization's maturity in terms of cybersecurity management. And also, to look at the roadmap of the initiatives to see if there was alignment between the deficiencies, the priorities and to see if everything was well aligned. And based on that, we identified the areas where initiatives are close to being completed or are completed from a technical standpoint, that we can check to ensure that they have been properly implemented or that the areas are mature. So that's how we work. (Participant 4, Director, Internal Audit)

"Check" (audit/oversight)

The "check" (audit/oversight) stage refers to monitoring and measuring controls effectiveness (Nicho 2018).

The effectiveness of existing cybersecurity controls is subject to various forms of verification and oversight. The organization's self-assessment based on frameworks (e.g., NIST and ISO 27000) and internally defined policies and targets are common ways to monitor cybersecurity controls. The internal audit function, supported by external auditors, if necessary, plays a key role in this (third line).

In addition to testing the effectiveness of these controls, the internal audit function follows up on cybersecurity deficiencies/test results with management/IT (all three lines). It audits cybersecurity performance indicators or the third-party governance process. It evaluates cybersecurity action plans, which are submitted to senior management and subsequently transmitted to the appropriate officials for follow-up. It also reports to the board of directors and management through the risk management committee and the audit committee. The head of the internal audit function accompanies the CIO or CISO for cybersecurity presentations to the audit committee. The frequency of reporting to the board and its audit committee is an important quality characteristic of cybersecurity audits (Slapnicar et al 2022).

> [The organization] has a cybersecurity program to continually strengthen its controls. And we [the internal audit function] monitor this over time. In each of our assignments, we look at what improvements are coming, what the gaps are, and then we follow up on these action plans. (Participant 1, Senior Director, Internal Audit)
>
> Competitors in our field ... started experiencing fraud. So, really, since ... 2019 the board suddenly made cybersecurity a subject that people, basically, have to ask questions about…. So that's why we brought in our Senior VP [IT] to present to the audit committee ... [and] senior management. (Participant 15, Vice President, Internal Audit)
>
> We have a number of third parties that we do business with, and we have a policy for correctly managing our third parties, correctly managing our security risk and other risks with respect to our third parties. We also

> have a standard and an entire governance system with respect to our third parties. We have identified the most critical third parties, and for our critical third parties, we check some factors, including security. We also audit this third-party governance process. (Participant 1, Senior Director, Internal Audit)

The external auditors assess the cybersecurity control environment as part of their audit of annual financial statements. In doing so, they might use the internal auditor's tests of the effectiveness of cybersecurity controls (third line). They can also be asked to audit the governance of third parties.

Generally speaking, the board of directors (including the audit committee and the risk management committee) tends to receive information on cybersecurity via reports or presentations by the internal audit function, the CIO or CISO, or the cybersecurity manager (all three lines). In particular, the latter presents the cybersecurity priorities and KPIs. More proactive audit committees monitor the cybersecurity improvement plan and these performance indicators.

> We have several assignments, not just the cybersecurity assignment, but ones that require security checks. So, during the year, we perform these different assignments and then, following each one, we provide our conclusions. In our various reports, we detail what our findings are in terms of security. And our reports are always presented to the sector leaders. We also provide a summary in our quarterly report. Our quarterly report is presented to the audit committee. (Participant 1, Senior Director, Internal Audit)

Regulators such as the OSFI (Office of the Superintendent of Financial Institutions) or external governance agencies such as the SASB may monitor the organizations' current cybersecurity measures. The SASB or other agencies may ask the organization to complete a questionnaire, after which they assign a score or possibly conduct an audit. The organization can then follow up by establishing benchmarks based on the reports of external governance agencies to improve cybersecurity or take other actions (second line).

> When you answer the questionnaire [from an external governance agency], you have to substantiate what you say based on your public communications. So everything I disclose [to the external governance agency] has to be public and on the website or … in reports we issue. They take nothing for granted. (Participant 3, ESG Director)

"Act"

The "act" stage refers to the modification and update of controls based on internal feedback and change in the business environment (Nicho 2018).

For instance, a change in board's perception of the importance of cybersecurity affects subsequent actions to monitor the organization's alignment with the evolution of cyber threats.

> So, like most manufacturing companies, we felt that we were less at risk than banks are. This means that we have very little information, I would say, of a highly confidential nature. We don't really have credit cards. It's really more about our clients' bank accounts. ... [C] ompetitors in our field started experiencing fraud. So, it's really since 2019, the board, suddenly, in its list of questions to be asked by board members, appears to have made cybersecurity a subject that people, basically, have to ask questions about. So that's why we brought in our Senior VP [IT] to present to the audit committee ... [and] senior management. (Participant 15, Vice President, Internal Audit)

Indeed, the mechanisms surrounding the cybersecurity processes' stages labelled Plan, Do and Check (audit/oversight) lead to changes and updates in controls—in other words, changes to organizations' cybersecurity, which are then reflected in their actions.

Overall, the interviews revealed that adjusting controls ensures better management of cybersecurity incidents. The monitoring of cybersecurity maturity leads the audit committee to ensure that the necessary resources are available to remedy detected flaws (second and third lines), as illustrated in the following interview excerpts:

> I think it's four times a year ... that we'll go and present to the audit committee what's going on in terms of cybersecurity. .... It's a presentation that will be given by our senior VP IT directly to the members [of the audit committee]. ... It's four, five [slides] that mainly present specific cases [of cyber incidents] of what happened: if there were attempts [intrusion attempts] by people [external], what were they, what happened, how were they blocked. But above all, also, what we are doing in terms of infrastructure, then investment to, every year, increase ourselves in terms of cybersecurity protection to keep up to date on what's going on. (Participant 15, Vice President, Internal Audit)

In the same spirit, respondents justified an increase in the financial resources allocated to cybersecurity and said they would make the best use of the money but would consider risk tolerance in the process, as highlighted by Participant 9:

> I said [to the CEO], "We have to have a Risk Appetite Statement. We have to declare what our risk tolerance is."
> ... Then all the controls that are going to come in to support that statement flow from that.

> ... You have to balance your appetite for risk, there's an investment to be made. It has to be doable.
> .... So he [the CEO] has set himself a target [in terms of risk tolerance], knowing that there are investments to be made. (Participant 9, Director, Cybersecurity)

Interviews also suggested that the oversight activities regarding positioning and the standards/policies to implement in cybersecurity are shown to be aligned with trends and threats to cybersecurity (all three lines). Cybersecurity is managed with a view to continuous improvement through information sharing, follow-ups, and frequent discussions between internal (and, if necessary, external) stakeholders, as shown in the following interview excerpts:

> I do a lot of information sharing with other companies, other heads of internal audit. ... In all the companies [with which] I share information, cybersecurity is always on the heatmap. ... So, cybersecurity is a risk to watch out for for all companies, including us. (Participant 16, Senior Director, Internal Audit)
> Over the years, I've had many exchanges with external auditors, ... The old guard being very: "Okay, well, here are the controls. If you don't do it..." .... Versus the new guard, who are more committed to a dialogue, so that this dialogue, with the controls in place, brings them the assurance they're looking for. At the end of the day, they're looking for assurance that the data is well protected. (Participant 6, CISO)

This view of continuous improvement leads to reviews/updates in internal policies, the cybersecurity event procedures manual, and benchmarking measures (all three lines). In addition, failure on internal phishing tests forces employees to retake cybersecurity training (offered by first line).

> We have an external benchmark [of our cyber position] which we also carry out over time to see how we've improved and how we're positioned in relation to other financial institutions, whether banks or insurance companies. Following this, an analysis is carried out, and an improvement plan is put in place. The [audit] committee is used to monitor the progress of the plan, among other things. (Participant 10, Vice President, Internal audit)
> We do business with a Big Four firm, which has the operations and benchmarking. We provide our data. They come on site to do the interviews, look at our positioning. Then, for example, they look at the NIST framework and say... I'll just give you an example in terms of computer access. It's a maturity grid, from 0 to 4, then they determine where we are, then they show us where we were last time, then where the benchmark was two years ago, then where the benchmark is now. (Participant 10, Vice President, Internal audit)
> The other thing we've also done, that we're also doing: I was talking about learning from our own little [cyber] incidents that happened, but also learning from the market. We did a complete debrief, for example, of the Desjardins incident …: how we, our controls, our situation is in relation to what we learned that was faulty. (Participant 10, Vice President, Internal audit)
> The board came to push, to say: "I want to hear more about it [cyberrisk]", but we, internally, this famous risk which, in our top 50 was maybe at 120 a couple of years ago, well, every year it was going up! Then, at a given moment, more and more with the cases [of cyberincidents/cyberattacks], more and more as we set up integrated systems, oops, all of a sudden, this risk, which was ... very fragmented, all of a sudden took on more and more magnitude. (Participant 15, Vice President, Internal Audit)

Changes in cybersecurity governance/management are also made as a result of assessments by external governance agencies or high-profile exfiltration cases (second line). Adjustments to cyber-risk management in strategic partnerships with third parties have also resulted in changes to contracts with clients and third-party partners to include a cyber clause (second line).

> What I've noticed is that ... in everything we sign, in contracts, even now, this notion [cybersecurity] is going to be there. So, I'm often sent these contracts and asked: "Have there been any cases of cybersecurity? What are we doing in terms of cybersecurity?" because it's part of the standard forms, when you renew for all sorts of things. (Participant 15, Vice President, Internal Audit)

Relational mechanisms

In light of De Haes and Van Grembergen (2009), relational mechanisms involve, among other things, management's vision, partnerships, and informal meetings between the three lines of defense.

Management's vision of cyber risk tolerance determines the actions that will be taken by the first and second lines in the organization to counter cyber threats.

> We have to state our risk appetite [in regard to various cybersecurity issues]. These will be statements that the President will endorse. That's the starting point for all the controls that are brought in to support [these statements]. (Participant 9, Director, Cybersecurity)

The three lines of defense work together on information security, including cybersecurity. In some instances, there is collaboration with the business units.

> Internally, we try to be proactive while still observing our three lines, but we all work shoulder-to-shoulder in the organization to avoid [breaches]. (Participant 10, Vice-President, Internal Audit)
>
> We work with our business units to understand what their vision is, what their trajectory is. (Participant 11, CISO)

Some organizations have informal internal discussion/information sharing groups on cybersecurity best practices (first and second lines). Many CISOs and internal auditors are part of formal external discussion groups, information sharing communities on information security, including cybersecurity, or communities that audit related processes (first and third lines).

> We belong to groups and networks to keep up to date, professional groups. And, well, we receive newsletters from regulatory associations as well. (Participant 5, Director, Legal Services)
>
> Communities that my peers are part of, we share information with each other, which is not anti-competitive, in other words, it's not private company information. It's more like, "Hey, we're under attack. We think it's out of China or Russia.... Have you experienced that sort of attack?" Then the information goes around. (Participant 9, Director, Cybersecurity)

Organizations are also concerned with training their employees in information security to reduce this type of risk (first and second lines).

> The CTO team is an internal client of ours [communications function] regarding internal communications because we conducted cybersecurity awareness campaigns. (Participant 12, Vice President, Corporate Communications)
>
> We call it awareness training. So, what we do is we have an education and training campaign that we deploy, that we do every, almost every year. And as part of that, we also do a phishing campaign, we do tests to find out, let's say, how we're improving from a first-line perspective. Who's taking the bait, and also, is our training effective? Are we doing the right things to inform our various employees, our users? So, we have that type of campaign, and everyone has to do it. It's just as important as an ethics campaign, ethics training, occupational health and safety training. Our intention is to really ensure that the first line of defense, which is our users as such, is well trained in this area. We publish about this. In these training sessions, in those capsules, we cover the part about our security policies, how to report incidents, what the best cyber hygiene practices are, and so forth. It's part of our policies. (Participant 14, Chief Information Officer)

Members of the board of directors (or audit committee) receive formal training on information security, including cybersecurity. This training is often provided by the IT or information security functions (first line). The CISO can also provide informal guidance to audit committee members on issues that need to be addressed.

> Naturally, the training that [IT gives to board members] doesn't make anyone a specialist. It's to share the vocabulary, for example, the NIST framework, that sort of thing, where we stand. It's applied training, I would say. (Participant 10, Vice President, Internal Audit)

The internal audit function can indeed help organizations achieve an effective level of information security by cooperating with the IS function (Steinbart et al 2012, 2013, 2018; Wallace et al 2011). Findings suggest that its collaboration is part of the upstream actions implemented to inform cybersecurity reporting.

Cybersecurity external disclosure activities

Cybersecurity activities related to external disclosure are also supported by specific structures, processes, and relational mechanisms. These are presented in the following sections, and included in Tables 2, 3 and 4 respectively.

Structures

The audit committee is responsible for overseeing external disclosure in financial reports, including on cybersecurity. Internal auditors may assist audit committee members regarding any questions about cybersecurity disclosure (third line).

Another board of directors' committee, the governance committee, plays a role in cybersecurity disclosure as it is usually responsible for monitoring ESG disclosure. Indeed, cybersecurity information can fall under the Social (S) or Governance (G) component of ESG.

At the management level, the disclosure committee, composed of senior executives from the administrative functions (notably finance, legal, communications, and internal audit) and business units (first and second lines), is responsible for drafting the information disclosed in public information documents, including information on cybersecurity. This committee follows up quarterly on cyber incidents to determine whether they should be disclosed, and, if so, the extent of the disclosure. At the corporate level, the finance and legal functions are responsible for the risk factors presented in the MD&A, while the communications function is more specifically involved in ESG disclosure. The CISO and/or the internal audit function provide assistance with information on cybersecurity risk. The internal audit function is involved in auditing the cybersecurity aspects.

> That [writing information on cybersecurity] is really a team effort between the IT department and it's clear that if you look at the people involved, that would be the CISO, the Information Security Officer. There's the CIO, the Chief Information Officer. We also have our process for preparing all the information in the document. We have a disclosure committee. So everything we draft goes through a disclosure committee that includes the VPs of the different divisions, the corporate controller, all the senior people in the company who look at all the documents, who compare them, the MD&A, the annual information form. There's a lot of discussion on these points and ... between the finance team, which prepares the first drafts, and the IT teams, the CFO, before the draft goes to the disclosure committee. (Participant 4, Director, Internal Audit)

The ESG managers (second line) prepare the information in the ESG reports, including information on cybersecurity. They report to the Vice President, Corporate Services or the Vice President, Communications. They present ESG progress and priorities to the board of directors' governance committee.

Processes

In public disclosure, organizations use legal frames of reference (such as National policy 51–201, CSA, 2013) for financial report disclosure and external governance agencies for ESG disclosure (such as SASB) (second and third lines). In addition, a common strategy is to use benchmarks against the information communicated by organizations in the same sector, other sectors, or other regions (second line).

The organization's KPIs may be included in public disclosures and are of interest to external governance agencies for ESG compliance.

> [The external governance agencies for ESG compliance] ask me: how do you measure up, because I'm going to check up on you next year. What's your target? And also: did you go get an audit? So, let's say we release our diversity strategy this year. We say what we're going to do about the process. They're going to ask us what our targets are, then what our measurements are. Then they're going to ask us how we audit ourselves. And next year I'm going to get the same questions. (Participant 3, ESG Director)

Relational mechanisms

The nature and extent of the organization's public disclosure, including cybersecurity, reflects the management's vision (second line), often that of the CEO (senior management). The vision regarding reporting may focus on the satisfaction of the information needs of investors/shareholders or extend to satisfying the needs of other stakeholders, such as customers and suppliers. In the first case, public disclosure would be limited to complying with the prescriptions of financial regulators, while in the other case, it may include providing numerical data in relation to pre-determined performance indicators. However, organizations are concerned about the competitive, reputational, and litigation issues tied to voluntary disclosure.

> Every year, we go over the risk factors. We have [several dozen] risk factors. So that means we have a priority list because the law requires that we order them from most to least important. That's what 51-102 [regulation by Canadian Securities Administrators, CSA, 2023] requires, that our risks be in order of decreasing importance. (Participant 5, Director, Legal Services)
>
> We look at our entire value chain as well. So not just our operations. And then, what our impacts are. But it's not just the environmental ones, all the ESG issues, what our impacts are in that regard. And we want to disclose the information, we want to communicate all that's important to our stakeholders and us. (Participant 18, ESG Director)
>
> Anything that involves disclosure, if it's required by law, we do it, we have to do it. However, in terms of voluntary disclosure, when responding to stakeholders, what they ask for can be hard, it's sometimes not the information we want to give. Sometimes you say, "I don't mind my client knowing [this information], but I don't want my competitors to know!" (Participant 18, ESG Director)

The finance, IT, legal, and communications functions collaborate in the preparation of public disclosures required by laws and regulations (second line). These functions rely on IT staff for the preparation of information security-related information, including cybersecurity (first line).

> Typically, our communications teams are responsible for dissemination and they usually prepare the texts and we review them. And sometimes, when the information or details are more technical, or if information is missing, we provide it. (Participant 11, CISO)

Further, the person responsible for the preparation of the ESG report collaborates with the parties involved in the topics reported, including cybersecurity (first and second lines).

Issues raised by participants

Several participants pointed out that board members have insufficient knowledge to properly perform their oversight role over cybersecurity. This observation is consistent with the lack of board IT expertise highlighted by Ashraf et al (2020). In the three lines of defense model, the board of directors is responsible for determining the organization's risk appetite and exercising oversight of risk management (IIA, 2020), including cybersecurity risks. The results indicate that the recruitment of board members familiar with cybersecurity currently appears to be lacking in organizations applying the three lines of defense model. This is an area for improvement.

> I almost put all the words in [the board members'] mouths, unfortunately. Cyber is what they read in the news. It's mysterious to them. Because it was one of my mandates. What questions should the board ask the officers? I gave them about ten questions that they should ask us. (Participant 9, Director, Cybersecurity)

One participant felt that the regulatory environment did not foster collaboration and transparency:

> There's very little information sharing because of this notion of potential penalties for companies, such as litigation, non-compliance, reputational impacts in the media, all sorts of impacts. So, it's quite difficult for companies to share openly among themselves and even with the public because again, there can often be significant consequences. We've been going through this for years and years: we don't want to share the threats that we foresee, our vulnerabilities, our incidents, because of these conditions. (Participant 11, CISO)
>
> The government context isn't always helpful because if we want to be open, to share, well, there are potentially heavy impacts.... We haven't struck the right balance, meaning that if we want to create openness and collaboration for collective work and help each other, we have to have an environment where we can have impact-free sharing. (Participant 11, CISO)

Securities administrators (SEC, 2023 or CSA 2017, 2023) require that firms report material information. However, comparability between organizations is hampered by different considerations of materiality criteria, both quantitative criteria, such as cost implications for the organization, impact on share price, and number of customers who would be affected, and qualitative criteria, such as management's credibility or reputation. This can lead to inconsistencies in the application of reporting guidelines when determining which information to report.

> It's not just materiality thresholds because impacts on services can be loss of critical services, for example, a ransomware attack where a representative ends up being blocked for three months. Yes, for most types except reputation losses we can assign a value, we're able to assign a value to an operational loss and so forth. It's harder to say how much reputational loss costs us. (Participant 6, CISO)

The definition of the concepts of *incident* and *event* in cybersecurity is unclear and differs among organizations. This can lead to inconsistencies and difficulties when organizations are compared on the basis of their publicly reported cybersecurity information.

> Everyone has a definition of what an incident is, for example, some companies consider every virus, every malicious email, a phishing attack, each of these as an incident. So they'll consider that they've had thousands and thousands each year. We look at incidents where there's a potential impact. So, we have tools, they block emails, they detect events. We don't consider these incidents. But, for example, if an employee responds or ... discloses their password after a phishing email, that's an incident for us. So a virus that shows up on a workstation but is detected by the protection tool and immediately destroyed, that's not an incident for us, that's an event. But if the tool doesn't detect it and the workstation is affected, well, that's an incident. Others might say that every instance of a virus is an incident. There's no market definition of what an incident is. (Participant 11, CISO)

Some organizations believe that if they provide too much information, they could expose themselves to hackers, who are always eager to find new vulnerabilities. This observation is in line with the results of Ettredge et al (2018) regarding firms facing a higher probability of cybersecurity breaches after disclosing trade secrets.

Conclusion

This interview-based study conducted with 18 senior executives and senior managers from 13 organizations in seven activity sectors provides an overview of how the three lines of defense contribute to cybersecurity effectiveness. More specifically, using an IT/IS governance lens, it documents the actions of internal audit and other functions in respect of cybersecurity.

The participants clearly indicated that the rising level of cyber risks was part of their organizational priorities. Organizations deal with cybersecurity issues by using structures with varying degrees of maturity and by deploying a variety of processes. Collaboration between the various functions/lines of defense on information security, including cybersecurity, is key in implementing and monitoring controls and in preparing public disclosure. An analysis of the data indicates that the participating organizations are well aware of cybersecurity risks and have implemented several mechanisms to deal with them and contribute to cybersecurity effectiveness.

Contributions and practical implications

This study examined how public companies deal with cybersecurity-related issues. The research was based on interviews, consistent with Cram et al (2023), who have called for greater use of qualitative methods in cybersecurity research. The research helps fill the gap in studies on cybersecurity in public companies underlined by Haapamäki and Sihvonen (2019), and it makes the following contributions and has practical implications.

First, this study entered into the "black box" to document how different organizational functions are engaged and involved together in cybersecurity effectiveness. It offers new insights by providing details about what organizations actually do in that matter.

Second, by using IT/IS governance concepts for data coding and analysis, this study draws an overall picture of firms' organization of cybersecurity, i.e., their structures, processes, and relational mechanisms. The study also contributes to the cybersecurity management and IT/IS governance literature by looking not only at the three lines of defense in cybersecurity-related structures, as Slapnicar et al (2023) did, but also at processes and relational mechanisms.

Third, the insightful findings on the actions of internal auditors complement cybersecurity audit/assurance studies. For instance, auditors' assessment of the effectiveness of cybersecurity controls through different cybersecurity testing techniques (e.g., identifying vulnerabilities in information systems and penetration testing, as suggested by Caron 2021) can contribute to cybersecurity risk mitigation. Further, findings about internal auditors' collaboration with external auditors complement prior research about how independent internal and external auditors take into consideration cybersecurity issues (e.g., Frank et al 2019; Li et al 2019; Smith et al 2019) and can enhance the reliability of reporting. These results enrich the internal audit literature.

In addition, findings about the influence of executives on cybersecurity reporting add to prior corporate reporting studies (e.g., Alrazi and Mat Husin 2021; Plöckinger et al 2016).

In terms of practical implications, the detailed description of structures, processes, and relational mechanisms associated with cybersecurity is helpful in understanding how public firms deal with cybersecurity-related issues. It provides aspects that management, boards of directors, and internal audit and other functions can ponder so they can improve their cybersecurity effectiveness. The issues raised by participants can also help securities regulators reflect on the nature and extent of cybersecurity disclosure and the assurance to be provided in this regard. They bring out potential areas for improvements in the regulatory environment and cybersecurity reporting rules/guidelines.

Research avenues

Participants brought up interesting issues illustrating many promising research avenues that could be addressed by qualitative/interview-based studies with internal and external stakeholders. Their perceptions could provide the basis for extensive reflection on the issues raised below.

As suggested by our findings, boards of directors are engaged to a certain extent in dealing with cybersecurity issues and related oversight activities. Further, external auditors are sometimes indirectly involved in cybersecurity activities. Interviews with board members and external auditors may deepen the understanding of their respective roles in respect of cybersecurity effectiveness. In that spirit, extending the IIA's three lines of defense model would be an interesting research avenue, as the board of directors can be presented as a fifth line of defense (e.g., Slapnicar et al 2023) and external auditors could be considered a fourth line (e.g., ICAEW 2023).

Voluntary disclosure provides leeway for those who want to differentiate themselves and be seen as leaders. However, when a company is alone in making a specific type of disclosure, it can be judged negatively by its stakeholders. Mandatory disclosure makes it easier to compare companies, but clear definitions are needed (e.g., what constitutes a cyber event or incident). In the same spirit, an international effort to reflect on having "a common definition, common languages, common indicators" (Participant 11, CISO) is needed to ensure that cybersecurity comparisons would be feasible between organizations. Consistency of terminology and benchmarks is a crucial component in cybersecurity reporting effectiveness, as it would contribute to disclosure comparability. International studies would be needed to guide regulators on that matter.

Acknowledgements We thank the participants interviewed in this study for their insightful comments. We are grateful for the financial support of the Corporate Reporting Chair, ESG-UQAM, and the Autorité des marchés financiers (AMF – Québec).

References

Allen, B., T. Kelly, R. Loyear, A. Poole, A. Awojulu, A. Kmetetz, M. Rakotomavo, Z. Wang, H. Xu, M. Xu, and H. Yuan. 2018.

Security risk governance: A critical component to managing security risk. *Journal of Applied Business and Economics* 20(1): 132–146.

Alrazi, B., and N. Mat Husin. 2021. Chief financial officers' international experience and corporate reporting quality: Evidence from Malaysia. *Global Business and Management Research* 13(4): 1091–1111.

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

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

Bowen, P.L., M.-Y.D. Cheung, and F.H. Rohde. 2007. Enhancing IT governance practices: A model and case study of an organization's efforts. *International Journal of Accounting Systems* 8: 191–221.

Caron, F. 2021. Obtaining reasonable assurance on cyber resilience. *Managerial Auditing Journal* 36(2): 193–217.

Carré, J.R., S.R. Curtis, and D.N. Jones. 2018. Ascribing responsibility for online security and data breaches. *Managerial Auditing Journal* 33(4): 436–446.

Chambers, A.D., and M. Odar. 2015. A new vision for internal audit. *Managerial Auditing Journal* 30(1): 34–55.

Coleman, D., M. Conley, N. Hallas. 2022. Trends in cybersecurity breach disclosures. Audit Analytics report. https://www.auditanalytics.com/doc/AA_Trends_in_Cybersecurity_Report_April_2022.pdf. Accessed 9 November 2022.

Cram, W.D., T. Wang, and J. Yuan. 2023. Cybersecurity research in accounting information systems: A review and framework. *Journal of Emerging Technologies in Accounting* 20(1): 15–38.

CPA Canada. 2019. CSAE (Canadian Standards on Assurance Engagements) 3416: Reporting on controls at a service organization relevant to user entities' internal control over financial reporting.

CSA (Canadian Securities Administrator). 2017. Multilateral Staff Notice 51-347: Disclosure of cyber security risks and incidents. https://www.osc.gov.on.ca/documents/en/Securities-Category5/20170119_51-347_disclosure-cyber-security.pdf. Accessed 9 November 2022.

CSA (Canadian Securities Administrator). 2023. Regulation 51-102 respecting continuous disclosure obligations. https://lautorite.qc.ca/en/professionals/regulations-and-obligations/securities/5-ongoing-requirements-for-issuers-and-insiders-51-101-a-58-201/51-102-continuous-disclosure-obligations. Accessed 24 August 2023.

De Haes, S., and W. Van Grembergen. 2009. An exploration study into IT governance implementation and its impact on business/IT alignment. *Information Systems Management* 26(2): 123–137.

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

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

Gordon, L.A., M.P. Loeb, T. Sohail, C.-Y. Tseng, and L. Zhou. 2008. Cybersecurity, capital allocations and management control systems. *European Accounting Review* 17(2): 215–241.

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

ICAEW. 2023. The four lines of defence. https://www.icaew.com/technical/audit-and-assurance/assurance/what-is-assurance/four-lines-of-defence. Accessed 21 April 2023.

IIA (The Institute of Internal Auditors). 2013. Position paper: The three lines of defense in effective risk management & control. Altamonte Springs, FL: IIIA.

IIA (The Institute of Internal Auditors). 2016. Global technology audit guide (GTAG): Assessing cybersecurity risk: The three lines model. https://www.theiia.org/en/content/guidance/recommended/supplemental/practice-guides/assessing-cybersecurity-risk-the-three-lines-model/. Accessed 9 November 2022.

IIA (The Institute of Internal Auditors). 2020. The IIA's three lines model (an update of the Three Lines of Defense). https://www.theiia.org/globalassets/documents/resources/the-iias-three-lines-model-an-update-of-the-three-lines-of-defense-july-2020/three-lines-model-updated-english.pdf. Accessed 21 September 2023.

ISACA. 2019. COBIT: Control objectives for information technology.

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

Kahyaoglu, S.B., and K. Caliyurt. 2018. Cybersecurity assurance process from the internal audit perspective. *Managerial Auditing Journal* 33(4): 360–376.

Lainhart, J.W., IV. 2000. COBIT^{TM}: A methodology for managing and controlling information and information technology risks and vulnerabilities. *Journal of Information Systems* 14(S-1): 21–25.

Li, C., G.F. Peters, V.J. Richardson, and M. Watson. 2012. The consequences of information technology control weaknesses on management information systems: The case of Sarbanes-Oxley internal control reports. *MIS Quarterly* 36(1): 179–203.

Li, H., W.G. No, and J.E. Boritz. 2019. Are external auditors concerned about cyber incidents? Evidence from audit fees. *Auditing: A Journal of Practice and Theory* 30(1): 151–171.

Lois, P., G. Drogalas, A. Karagiorgos, A. Thrassou, and D. Vrontis. 2021. Internal auditing and cyber security: Audit role and procedural contribution. *International Journal of Managerial and Financial Accounting* 13(1): 25–47.

Miles, M.B., and A.M. Huberman. 1994. *Qualitative data analysis*, 2nd ed. Thousand Oaks, CA: Sage.

Nicho, M. 2018. A process model for implementing information systems security governance. *Information and Computer Security* 26(1): 10–38.

Patton, M.Q. 2015. *Qualitative research & evaluation methods*, 4th ed. Thousand Oaks, CA: Sage.

Plöckinger, M., E. Aschauer, M.R.W. Hiebl, and R. Rohatschek. 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.

SEC (Securities and Exchange Commission). 2023. SEC adopts rules on cybersecurity risk management, strategy, governance, and incident disclosure by public companies. https://www.sec.gov/news/press-release/2023-139. Accessed 21 August 2023.

Slapnicar, S., M. Axelsen, I. Bongiovanni, and D. Stockdale. 2023. A pathway model to five lines of accountability in cybersecurity governance. *International Journal of Accounting Information Systems* 51: 100642. https://doi.org/10.1016/j.accinf.2023.100642.

Slapnicar, S., T. Vuko, M. Cular, and M. Drascek. 2022. Effectiveness of cybersecurity audit. *International Journal of Accounting Systems* 44(3): 1–21.

Smith, T.J., J.L. Higgs, and R.E. Pinsker. 2019. Do auditors price breach risks in their audit fees? *Journal of Information Systems* 22(2): 177–204.

Stafford, T., G. Deitz, and Y. Li. 2018. The role of internal audit and user training information security policy compliance. *Managerial Auditing Journal* 33(4): 410–424.

Steinbart, P.J., R. Raschke, G.F. Gal, and W.N. Dilla. 2012. The relationship between internal audit and information security: An exploratory investigation. *International Journal of Accounting Information Systems* 13(3): 228–243.

Steinbart, P.J., R. Raschke, G.F. Gal, and W.N. Dilla. 2013. Information security professionals' perceptions about the relationship between the information security and internal audit functions. *Journal of Information Systems* 27(2): 65–86.

Steinbart, P.J., R.L. Raschke, G. Gal, and W.N. Dilla. 2018. The influence of a good relationship between the internal audit and information security functions on information security outcomes. *Accounting, Organizations and Society* 71: 15–29.

Turetken, O., S. Jethefer, and B. Ozkan. 2020. Internal audit effectiveness: Operationalization and influencing factors. *Managerial Auditing Journal* 35(2): 238–271.

Von Solms, B., and R. von Solms. 2018. Cybersecurity and information security—What goes where? *Information and Computer Security* 26(1): 2–9.

Wallace, L., H. Lin, and M.A. Cefaratti. 2011. Information security and Sarbanes-Oxley compliance: An exploratory study. *Journal of Information Systems* 25(1): 185–211.

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

Wilkin, C.L., and R.H. Chenhall. 2010. A review of IT governance: A taxonomy to inform accounting information systems. *Journal of Information Systems* 24(2): 107–146.

Sylvie Héroux Ph.D., M.Sc., CPA auditor is a full professor 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 Ph.D. is a full professor of accounting in the École des sciences de la gestion, Université du Québec à Montréal, Canada. Her research areas include 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, Advances in Accounting Behavioral Research, Sustainability Accounting, Management and Policy Journal, Journal of Information Systems, Information Systems Management, Accounting Perspectives, Australian Accounting Review, Journal of Accounting, Ethics & Public Policy, Accounting Education*.