MIS Quarterly Executive

Volume 22 | Issue 4 Article 6

December 2023

The Importance of Board Member Actions for Cybersecurity Governance and Risk Management

Jeffrey G. Proudfoot

W. Alec Cram

Stuart Madnick

Michael Coden

MIS Quarterly Executive

The Importance of Board Member Actions for Cybersecurity Governance and Risk Management

Boards of directors are increasingly responsible for providing guidance and oversight on cybersecurity risk, yet are often unequipped to do so. This critically important mandate introduces novel challenges to what is already a complex governance environment. Drawing on in-depth interviews with board members and executives, we describe four core cybersecurity challenges that boards encounter and provide 10 recommended actions they can take in response. These actions enable boards to optimize their ability to provide meaningful, effective governance to address cybersecurity risk.[1,2]

Jeffrey G. Proudfoot
Bentley University/MIT Sloan School of Management (U.S.)

W. Alec Cram
University of Waterloo (Canada)

Stuart Madnick
MIT Sloan School of Management (U.S.)

Michael Coden
Boston Consulting Group/MIT Sloan School of Management (U.S.)

Board-Level Cybersecurity-Related Challenges

"Boards are still not prioritizing cyber like they should be. ... I think every company needs to live in a proper amount of paranoia about this, and we have turned into an economy that is driven by information—if we don't protect that, it is the equivalent of leaving the door of the store open at 1:30 in the morning and leaving anyone to walk in and [steal]." Board Member, Interview No. 10[3]

"I think it is important for the board to get more active. It is part of the mission now: You should know this. Every company is a tech company! You can't say 'I don't want to know.' You need to know ... boards are freaked out ... I can be found personally liable." Board Member, Interview No. 2

1 Joe Peppard, Blaize Horner Reich and Martin Mocker are the accepting editors for this article.

2 This research was supported by the members of the Cybersecurity at MIT Sloan (CAMS) initiative (https://cams.mit.edu/) and the Social Sciences and Humanities Research Council (SSHRC) under grant 435-2021-0437.

3 The interview participants and their industries are listed in the Appendix.

DOI: 10.17705/2msqe.00084

> *"Every board knows that cyber is a threat and cyber is a risk. How they manage it is still the wild west."* Board Member, Interview No. 3

Boards of directors face a variety of technology-related challenges in the organizations they oversee. Chief among these challenges is navigating the ever-increasing threat of cybersecurity incidents, including denial-of-service attacks, breaches of private customer data, theft of intellectual property, cyber-physical destruction and the most urgent concern, ransomware. Despite the ongoing concern about a lack of board expertise on cybersecurity issues,[4] stakeholders have high expectations for boards to provide an important governance and risk management presence that can help protect the organization from cybersecurity incidents.[5]

Many boards find themselves at a critical crossroads in their approach to cybersecurity. On the one hand, basic "checklist" guidance has begun to be disseminated for board members to follow (e.g., put cybersecurity issues on the board agenda, follow essential cybersecurity procedures and develop a plan of response for when an attack takes place).[6] This approach may provide a minimum standard for addressing the most basic cybersecurity concerns, but doesn't fully engage with the more complex consequences and risk management dependencies that cybersecurity can generate. On the other hand, more sophisticated, forward-looking boards are committing to addressing cybersecurity governance and risk management by facing the challenges head-on.

The purpose of this article is to *provide an overview of the most salient cybersecurity challenges facing board members in today's organizations and to provide recommended actions for responding effectively.* Our insights and guidance are drawn from in-depth interviews with 35 cybersecurity experts and current board members, including business executives, chief information security officers (CISOs), chief technology officers (CTOs), compliance officers and board advisors. The interviewees were drawn from a range of industries, including finance, technology, communications, media, healthcare, critical infrastructure and insurance, and included representatives from large Fortune 100 companies as well as smaller enterprises.[7]

In this article, we first provide an overview of the four categories of cybersecurity-oriented board challenges identified in our research: 1) board attitudes and governance, 2) board-executive interaction dynamics, 3) board cybersecurity expertise, and 4) expanding cybersecurity regulations. Based on the interview data, we then describe the pressing concerns for boards in each of these categories. Finally, we provide 10 recommendations that board members can take in response to these challenges. Together, these actions form a solid foundation for effective oversight of cybersecurity issues at the board level.

The Changing Role of Boards in Mitigating Cybersecurity Risks

The role of boards in organizational cyber risk mitigation has changed, with some of the most meaningful changes happening in the last few years. Our interviews with board members and executives helped us to understand: 1) how board engagement with cybersecurity has evolved over time and 2) the current state of affairs. This understanding provides a contextual backdrop for our discussion about the key cybersecurity challenges boards are facing and our recommended actions for addressing these challenges.

As recently as 10 years ago, many boards were not technologically engaged and were not exposed to consistent reporting or discussion about organizational cybersecurity issues. Moreover, relatively few directors had technical or cybersecurity skills and therefore did not know the relevant questions to ask or how to interpret

4 For example, see *The Director's New Playbook: Taking on Change*, PwC's 2021 Annual Corporate Directors Survey, available at https://www.pwc.com/us/en/services/governance-insights-center/assets/pwc-2021-annual-corporate-directors-survey.pdf.

5 Schinagl, S. and Shahim, A. "What Do We Know about Information Security Governance? "From the Basement to the Boardroom": Towards Digital Security Governance," *Information and Computer Security* (28:2), January 2020, pp. 261-292.

6 For example, see Rothrock, R. A., Kaplan, J. and van der Oord, F. "The Board's Role in Managing Cybersecurity Risks," *MIT Sloan Management Review* (59:2), Winter 2018, pp. 12-15.

7 The Appendix provides detailed information on our research methodology.

cybersecurity metrics or reporting tools. Instead, boards focused on providing key strategic guidance for the organization, financial reporting and ensuring they carried out their fiduciary duties.

However, with the widespread proliferation of technology in most industries and organizations and the accompanying increases in cybersecurity risk associated with organizations' digital transformations, many boards have begun to prioritize cybersecurity as a key risk area. This heightened focus has also been driven by growing government requirements for board-level oversight of cybersecurity,[8] the increasing and more overt use of cybercrime and cyberwarfare[9] (with implications for economic activity and critical infrastructure) and new rules introduced by the U.S. Securities and Exchange Commission (including requirements for companies to share information about board involvement with cyber risks).[10,11,12]

For example, a recent report on boards and cybersecurity reported that two-thirds of board members considered their organization at risk of an impactful cyberattack, with the top three concerns being: email fraud (business email compromise or BEC), cloud account compromise and ransomware.[13] Our interviewees repeatedly stressed how the commonality of high-profile cybersecurity breaches has been a catalyst for increasing board attention. They also noted that nothing motivates boards to prioritize cybersecurity more rapidly than experiencing a breach within their own organization, especially when regulators get involved (with the potential for punitive measures, such as fines, being taken against the organization).

The growing prioritization of cybersecurity is evidenced in several ways. Most prominent is that boards are now requesting reports on their organizations' cybersecurity measures several times a year at scheduled board meetings. These reports are supplemented with committee meetings in which more nuanced discussions can take place on specific topic areas (e.g., risk). Cybersecurity accountability can be assigned to different committees depending on the preferences of the board, but it is most commonly found in audit, technology, risk or operations committees. (Committees can also meet together for expanded conversations that span a broader scope than of a single committee.) Though less than 10% of boards have a dedicated cybersecurity committee, some estimates[14] suggest this could increase to as high as 40% by 2025. Some boards have also formed a temporary committee in response to a specific incident or serious vulnerability, which is subsequently disbanded or merged with another committee.

Boards are also increasingly engaging with executives to ask what cyber issues need to be addressed and what resources the organization needs to effectively address those issues. As a consequence, many organizations have substantially increased resource allocation for cyber initiatives. Boards, however, are not always mindful of the fact that however much is spent on cybersecurity, this investment can never guarantee full protection from a cyber incident, and therefore they must also focus on cyber-resiliency, or the ability to detect, respond and recover from a successful cyberattack.[15]

Another emerging trend is for boards to more carefully compile a variety of skillsets in the boardroom—particularly cybersecurity

8 For example, see Uberti, D. "Fearing More Cyberattacks, Congress Requires Key Businesses to Report Digital Breaches," *The Wall Street Journal*, March 17, 2022, available at https://www.wsj.com/articles/fears-of-cybersecurity-attacks-may-increase-disclosure-requirements-for-businesses-11647444384.

9 See Stupp, C. and Nash, K. S. "Ukraine War and Upcoming SEC Rules Push Boards to Sharpen Cyber Oversight," *The Wall Street Journal*, January 3, 2023, available at https://www.wsj.com/articles/ukraine-war-and-upcoming-sec-rules-push-boards-to-sharpen-cyber-oversight-11671723827.

10 See Pearlson, K. and Hetner, C. "Is Your Board Prepared for New Cybersecurity Regulations?" *Harvard Business Review*, November 11, 2022, available at https://hbr.org/2022/11/is-your-board-prepared-for-new-cybersecurity-regulations.

11 See Rundle, J. "Boards, Security Chiefs Face Challenges Over New Cyber Rules," *The Wall Street Journal*, April 15, 2022, available at https://www.wsj.com/articles/boards-security-chiefs-face-challenges-over-new-cyber-rules-1165001500.

12 *SEC Adopts Rules on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure by Public Companies*, Securities and Exchange Commission Press Release, July 26, 2023, available at https://www.sec.gov/news/press-release/2023-139.

13 *Cybersecurity: The 2022 Board Perspective*, proofpoint, 2022, available at https://www.proofpoint.com/us/resources/awareness-materials/cybersecurity-2022-board-perspective-key-findings-and-executive.

14 See *Gartner Predicts 40% of Boards Will Have a Dedicated Cybersecurity Committee by 2025*, Gartner Press Release, January 28, 2021, available at https://www.gartner.com/en/newsroom/press-releases/2021-01-28-gartner-predicts-40--of-boards-will-have-a-dedicated-.

15 Coden, M., Reeves, M., Pearlson, K., Madnick, S. and Berriman, C. "An Action Plan for Cyber Resilience," *MIT Sloan Management Review*, January 4, 2023, available at https://sloanreview.mit.edu/article/an-action-plan-for-cyber-resilience/.

talent. In the past, board members were often selected based on their political connections or high-level executive experience, or on existing board members' networks. Some boards are now more intentionally constructed to build a holistic team that can respond to heightened market competition and a more complex and interconnected risk environment. Others use survey tools to regularly assess the expertise of each board member to guide future board appointments. Yet others are more generally trying to increase their cybersecurity awareness and knowledge through training for all directors or by involving external consultants or cybersecurity experts.

In general, board interactions with executives about cybersecurity issues are becoming more frequent and meaningful.[16] Many boards receive information on phishing exercise results, cybersecurity maturity, results of tabletop exercises, etc. Executives are also increasingly presenting extensive reports to the board detailing risk areas. In many cases, these reports use color-coded or graphical dashboards to summarize the performance of the organization in different risk areas (our interviewees repeatedly compared these reports to Sarbanes-Oxley compliance reports).

Boards are being encouraged to further enrich their communication about cybersecurity with executives and to focus more on cyber-resilience (i.e., how can the organization effectively respond to, and recover from, an attack rather than only focusing on preventing one).[17] CISOs are beginning to get more access to boards yet board-CISO interaction dynamics can sometimes be ineffective and problematic.[18] In our interviews, board members with extensive experience of reviewing cybersecurity reports shared examples of the types of questions boards are starting to ask executives, including "How many outages or attacks have happened?" "How robust is our infrastructure?" "What are the crown jewels and how are we protecting them?" "What is our recovery plan?" and "Are we doing more than our peers?" Because of the need for boards to be more formally guided on what they should be asking, researchers are beginning to provide advice on the key questions.[19]

Despite these advances in boards' understanding of cybersecurity, challenges remain. Though these challenges span a broad range of topics, we found that our interviewees' comments coalesced around four key areas: 1) board attitudes and governance; 2) board-executive interaction dynamics; 3) board cybersecurity expertise; and 4) expanding cybersecurity regulations. Below, we describe these challenges in detail, along with representative quotes relating to the challenges captured during our interviews.

Four Cybersecurity-Related Challenges for Boards

Though growing board attention to cybersecurity risk mitigation is a positive trend that should improve organizational cybersecurity outcomes, we have found that the way boards are operationalizing this newfound emphasis on cybersecurity risk can be inconsistent, haphazard and potentially problematic, unlike the systematic approach taken to financial risk decisions.[20,21] Our interviewees consistently highlighted a variety of challenges that they had observed in the boardroom on cybersecurity issues. We have organized these challenges into the four key areas described in detail below.

Challenge 1: Board Attitudes and Governance

Though there was consensus across the interviewed board members that organizations are generally beginning to prioritize cybersecurity, there are many industries and individual organizations that remain complacent. Some boards are still not taking cybersecurity

16 Pearlson, K. and Hetner, C., op. cit., November 11, 2022.

17 Uberti, D., op. cit., March 17, 2022.

18 Vance, A. and Lowry, M. "How CISOs Can Wield More Power in Organizations," *The Wall Street Journal*, December 5, 2022, available at https://www.wsj.com/articles/information-security-officers-power-companies-11670015448.

19 For example, see Pearlson, K. and Neto N. N. "7 Pressing Cybersecurity Questions Boards Need to Ask," *Harvard Business Review*, March 4, 2022, available at https://hbr.org/2022/03/7-pressing-cybersecurity-questions-boards-need-to-ask.

20 Coden, M. *Yes Virginia, There is a Way to Calculate ROI on Cyber Investments*, Forbes.com, May 9, 2019, available at https://www.forbes.com/sites/forbestechcouncil/2019/05/09/yes-virginia-you-can-calculate-roi-for-cybersecurity-budgets/.

21 Ramachandran, S., Yousif, N., Bohmayr, W., Coden, M., Frankle, D. and Klier, O. *A Smarter Way To Quantify Cybersecurity Risk*, Boston Consulting Group, August 9, 2019 available at https://www.bcg.com/capabilities/digital-technology-data/smarter-way-to-quantify-cybersecurity-risk.

seriously and are adopting a "security-through-obscurity" mentality (i.e., with so many organizations out there to be targeted, the chance that we will be the organization that is targeted is minimal; we are therefore safe). Our interviewees suggested that one reason why some board members are not prioritizing cybersecurity properly is that they feel that they have little to lose personally if a breach occurs. In other words, if there is no risk for board members when a breach occurs, board-level attention to cybersecurity will likely be minimal.

Board attitudes to cybersecurity can also be heavily influenced by the information that is distributed to board members about cybersecurity operations. One of our interviewees noted that cybersecurity briefings handed out to board members often include key metrics and dashboard-inspired graphics, with green, yellow and red shading to signify the current state of various cybersecurity operations as being good, moderate or poor. However, handouts dominated with green shading can instill a false sense of protection in the board and breed complacency that the organization is secure and that no additional security actions, investments or interventions are needed. The boards of companies that have experienced fairly minor consequences from a previous breach may be ignoring the fact that the next breach might have much more severe consequences. That many boards lack the proper attitude and sense of urgency concerning cybersecurity risk was reinforced by one of our CEO interviewees:

> *"Any board that is unaware ... [even though] they have all read about these hacks and incidents—[and does] not have [cybersecurity] as a fundamental part of board oversight is just inconceivable. I guess if you're planting oranges in a grove and picking oranges, then the board doesn't need to worry, but just about every company needs to worry [about cybersecurity] as we move to digital from analog."* CEO, Finance Company, Interview No. 1

Another aspect of this first board challenge is determining the proper scope of the board's involvement with organizational cybersecurity initiatives. The board's mission is not to tell management how to do its job but to make sure that management is doing a proper job. Operating at too high a level can result in poor oversight, whereas operating too granularly is not the board's mandate and can result in ignoring other risk areas. Such governance may put undue pressure on executives and top security practitioners in the organization, who may perceive this oversight as overstepping by the board. A specific context where the issue of board scope was consistently referenced by our interviewees is breach response. Many organizations do not have clearly articulated response plans prescribing how various internal stakeholders in each tier of leadership will operate and/or collaborate when a breach occurs.

Inappropriate scope of board involvement can also result in boards being subjected to detailed, overly technical generic reports that may not be understood or may overwhelm board members, resulting in a lack of proper prioritization of risk and thus poor oversight. The following example from one of our board member interviewees illustrates the problems that can arise from providing boards with overly long and complex reports, especially for reviewing cybersecurity operations:

> *"I have seen these lists—my company used to create them; voluminous things, and what do I do with that long list of stuff? And then the cyber portion; cyber is always on the list ... and essentially, you could probably pull them off the server and change three words and you would see the same list. The question is what the hell do you do with it and how do you prioritize the few things that you should really worry about as opposed to the long laundry list, the bibliography, of things that are out there?"* Board Member, Food Services Company, Interview No. 7

Another aspect of this first challenge is board oversight of organizational investments in cybersecurity initiatives. Despite boards' increasing awareness of cybersecurity as a critical risk area, justifying investments for cybersecurity continues to be difficult because these investments are made with the hope that nothing happens (i.e., no breach occurs). When there are opportunities for other potentially more impactful investments with enticing tangible

benefits (e.g., product research and development, acquisition of talent, more sophisticated marketing campaigns), cybersecurity can quickly become an afterthought. A board member of a finance company commented as follows on the need for proper cybersecurity investment and provided an example of a specific organization that was made aware of its poor cybersecurity yet continued to be complacent:

> *"There was a company that I used to advise that decided not to [deploy] this [cybersecurity] reporting tool, and I said, 'this is your problem, not my problem, and your score is a C, and if you look at your vendors, because you can do reports on vendors, 90% of them are vulnerable.' I never heard back. I don't understand it. … Anyone who is pennywise on this stuff is nuts. If you want to save money on something, save it on lunch. Don't save it on cyber, for God's sake."* Board Member, Multiple Industries, Interview No. 11

Challenge 2: Board-Executive Interaction Dynamics

A second core cybersecurity challenge facing boards is the nature of their interactions with company executives. As the CISO is often the primary conduit through which boards are exposed to organizational cybersecurity performance information, the ability of board members to effectively provide cybersecurity governance depends heavily on board-CISO interaction dynamics. One of the most important factors identified by our interviewees is the board's perceived competence of the CISO, which is heavily determined by the CISO's ability to effectively communicate. On the one hand, a CISO who may have unparalleled technical expertise and leadership abilities, but who cannot clearly and plainly communicate with the board on cyber issues, may be perceived as incompetent or ineffective. Poor communication skills may also deter board members and other executives from engaging in meaningful discourse on cyber issues. On the other hand, a marginally qualified CISO who appears credible, but may lack the proper expertise and leadership skills, may (dangerously) be perceived as highly qualified and effective, thereby triggering a sense of complacency among board members.

These risks highlight the importance of organizations hiring not just the most skilled CISO from a technical or operational standpoint—perhaps more important is the ability of the CISO to interact with the various stakeholders of the organization effectively, especially regarding interactions with the board. The following quote reinforces the importance and impact of having a CISO with the right skillset:

> *"The challenge is how good is your CISO in explaining in plain terms some of the technology challenges around cyber. If you have a really good CISO who can explain things, then the conversations are great because you can still drill down into the details but also have substantive conversations with board members. … When you don't have that and people don't know how to present to boards or executives, that is when you get the blank stares and no follow-up questions."* Board Member, Technology Company, Interview No. 5

We also identified several other important factors that boards are grappling with in their interactions with CISOs. First, though the CISO is the executive in the front line when a cybersecurity event takes place, CEOs are increasingly being held accountable when breaches occur (as evidenced by CEOs commonly participating in press releases and interviews as a part of breach response). Related to this trend, we found a lack of more formal measures for consistently holding CEOs accountable for cybersecurity performance (e.g., having the CEO regularly sign off on the organization's cybersecurity arrangements). However, a recent report predicted that high-level executives will, by 2026, have "performance requirements related to risk built into their employment contracts."[22]

Another factor influencing board-CISO interaction dynamics is the limited time that boards allocate to engaging with cybersecurity topics during regular board meetings. Brief presentations by CISOs and discussion sessions

22 See *Gartner Unveils the Top Eight Cybersecurity Predictions for 2022-23*, Gartner, June 21, 2022, available at https://www.gartner.com/en/newsroom/press-releases/2022-06-21-gartner-unveils-the-top-eight-cybersecurity-predictio.

are insufficient for the board to carry out due diligence. Unfortunately, many boards are still not addressing this challenge through more consistent and informal information flows between board members and the CISO outside of traditional but limited boardroom interactions.

Finally, board-CISO interactions can sometimes be strained if board members are too aggressive, confrontational or in any way undermine the CISO, which can lead to a less than constructive partnership in the future. Boards don't always appreciate the possible ramifications of handling their cyber governance mandate in a way that could compromise its effectiveness. Reflecting on the challenges of engaging with top executives as a part of the board's cybersecurity governance mandate, a board member with experience in multiple industries stated:

> *"Don't show up the CEO. If you have an issue, take it out of the meeting and bring it up. But in my case, we were quite good, but not great, so I brought it up during the board meeting. And I said, 'you put me on the board to be honest, so here is the honest answer.' And everyone took it well."* Board Member, Multiple Industries, Interview No. 11

Challenge 3: Board Cybersecurity Expertise

Another prominent challenge that boards are encountering is ensuring they have the proper level of cybersecurity knowledge and understanding how to effectively replace or increase that expertise when a board member is replaced. Board-level cyber expertise can either be centralized with a single highly specialized board member or decentralized with several board members having basic cyber expertise. As the importance of board governance of cybersecurity issues has rapidly increased, many boards have been uncertain about the best way to respond. Board turnover can be slow, thus impeding an agile response to rapidly changing demands such as increasing cybersecurity threats and regulations.

There is clearly a lack of proper cyber knowledge and expertise on many boards today, and having at least one person on the board with cyber knowledge is critical. Moreover, many boards are composed of individuals with siloed areas of expertise, which often translates to tension and a lack of cross-functional perspectives on governance decisions, especially when it comes to cybersecurity initiatives. One former CEO made the following observation about how board composition and expertise have evolved to become an integral aspect of a board's cybersecurity governance:

> *"If you think back 15 years ago, it would be fair to say that there were very few boards highly technically engaged or that review[ed] or[received] reports [on cybersecurity], or even [had] a committee that worried about cybersecurity. ... It is interesting looking over time how that topography of importance to the board has changed and one of the most notable ones is cybersecurity. For the more sophisticated companies, it also tends to coincide with looking for board members who have some familiarity with the space as well. ... Most board members are not that familiar with cybersecurity issues; [when you] talk about patching they think you are in the garment industry."* Board Member/CEO, Multiple Industries, Interview No. 12

There are also more specific issues complicating the general challenge of configuring cyber expertise on boards. For example, despite boards' growing interest in cybersecurity risk, many are onboarding directors without assessing their cybersecurity knowledge.[23] Failing to assess the cyber capabilities of new directors is a missed opportunity that can lead to cyber expertise being underused or the failure to identify a lack of expertise that should be remedied with future additions to the board. However, the lack of cyber expertise on a board can be difficult to address because of the typically slow pace of board turnover.

Though there are increasingly more options for boards seeking cybersecurity education and training, many boards are still not taking advantage of these resources. A board member in

23 For an analysis of director expertise and skills, with cybersecurity rated as the weakest area, see Kabanov, I. and Madnick, S. "Applying the Lessons from the Equifax Cybersecurity Incident to Build a Better Defense," *MIS Quarterly Executive* (20:2), June 2021, pp. 109-125.

the media industry made the following comments about the lack of cyber talent on boards, the need to train board members, the level at which boards should be trained and the inclusion of third parties to evaluate organizational cybersecurity:

> *"[In a typical corporate board with] nine board members, [I] would be hard pressed [to find] one or two [who] really understand the nuances [of cybersecurity]. That is my experience. I think it is about training the board members themselves, but more important than that, [training them on] the risks to the organization [and] how well the risks are being managed throughout the organization. … Part of what I would want on a board is someone at least understanding the programmatic execution of cybersecurity throughout the organization. There is the leadership. There is operational follow-up. And a comfort level that perhaps is codified by giving a symbol of approval of a third party."* Board Member, Media, Interview No. 10

Challenge 4: Expanding Cybersecurity Regulations

The final core challenge boards are facing is the expanding landscape of cybersecurity regulations. The problem is that directors tend to conflate the regulatory compliance of their organization with sufficient cybersecurity practices/investment while, in reality, there is often a disconnect between compliance and security appropriate for the business. Though board members must ensure their organization complies with cybersecurity regulations, including those originating from overseas jurisdictions that are not highly advanced or sophisticated in terms of technology and cybersecurity expertise, they should be aware that compliance may not provide sufficient cybersecurity for the business. When questioned about the cybersecurity disclosure rules introduced in the U.S. by the Securities and Exchange Commission (SEC), a highly experienced board member (who was also the CEO of a Fortune 100 company) made the following statement about the quality and relevance of cybersecurity regulations:

> *"How much money would you bet that there is not a single person developing that SEC rule who has ever sat in a corporate boardroom or ever run a company? Do you want to take that bet? I have worked in the government. I have said … everyone ought … to spend at least two years at a high enough level in a government agency to see what the hell they do. Anyone who thinks expertise is lodged in the federal bureaucracy, I mean, God bless them, but it is just not true."* Board Member/CEO, Multiple Industries, Interview No. 12

Another pitfall is that boards can easily become fixated on the operational level of regulatory compliance. Focusing on this level can reduce attention to other risk areas, resulting in a misalignment of the priorities for cybersecurity risk vs. other risk areas. Overemphasizing regulations can be triggered by boards focusing on extensive compliance checklists coupled with a box-ticking mentality to ensure that the organization is compliant. This tendency can also result in a lack of attention to incident response (an essential component of cyber resilience) or to thinking creatively about how regulatory response can be a catalyst for improving security (vs. simply doing the minimum to be compliant). One board advisor made the following statement about cybersecurity regulations and organizational cybersecurity response:

> *"The analogy that I always use is safety. … If it weren't for OSHA [Occupational Safety and Health Administration] regulations, we probably wouldn't have safe working environments. We wouldn't have safe electrical appliances. … Without regulations, companies will not do the right thing, which is unfortunate, but with regulations, companies will do an approximation of the right thing or at least something close to it. The question is: how to get them to do what is really right while satisfying the regulators? Companies turn around and say, 'How do I get the regulators to recognize that my situation is slightly different and allow them to do X instead of Y?' I think it is insurmountable."* Board Advisor, Multiple Industries, Interview No. 8

Table 1: Board Challenges and Recommended Actions

Board Cybersecurity Challenge	Recommended Board Actions
Challenge 1: Board Attitudes and Governance	Action 1: Acknowledge that cybersecurity is an enterprise operational risk, and thus a concern for the entire board.
	Action 2: Gauge the organization's cybersecurity maturity.
	Action 3: Be clear on the possible enterprise and personal consequences of a significant cyber incident.
Challenge 2: Board-Executive Interaction Dynamics	Action 4: Don't "get into the weeds" on cybersecurity, but focus on the business implications.
	Action 5: Demand clarity and understandability in executive communications.
Challenge 3: Board Cybersecurity Expertise	Action 6: Determine the board's appetite for bringing in cyber experts, as either a board member or through an advisory or consulting role.
	Action 7: Seek out cybersecurity training and education opportunities, including tabletop cyberattack simulations.
Challenge 4: Expanding Cybersecurity Regulations	Action 8: Know the cybersecurity and related privacy regulations that affect your industry, organization and countries of operation, and their potential costs (fines).
	Action 9: Appreciate that compliance with regulations doesn't (necessarily) equate with sufficient cybersecurity.
	Action 10: Understand the tension between what cybersecurity regulations aim to achieve vs. the business and legal implications following an incident.

Recommended Actions for Board Members

Below, we set out our 10 recommended actions that board members should take in response to the four cybersecurity challenges that boards face (see Table 1 for a summary of the actions). Actions 1, 2 and 3 address board attitudes and governance challenges. Actions 4 and 5 relate to the response to board-executive interaction dynamics. Actions 6 and 7 are the responses to the board cybersecurity expertise challenge. Actions 8, 9 and 10 are our recommendations for responding to the challenge of expanding cybersecurity regulations. Though we recognize that the situation of each board is unique, and that one size does not fit all, these actions represent common themes that emerged from our research across different industries and in different contexts.

Responding to Challenge 1: Board Attitudes and Governance

Action 1: Acknowledge that cybersecurity is an enterprise operational risk, and thus a concern for the entire board. Though nearly every board member acknowledged that cybersecurity is an important issue for their organization, not all boards approach the issue in the same way. In some cases, board members unfamiliar with cyber issues may be inclined to assign responsibility to a single, expert board member or a particular committee (e.g., audit, IT). This approach allows the board to seemingly distribute responsibility elsewhere and get it "off the hook," without needing to directly confront the challenge. Instead, we recommend that boards move beyond thinking about cybersecurity as only a specialist, technical issue and acknowledge that it is a fundamental business issue on par with climate change, leadership succession and social issues like diversity and inclusion. In the same way that

boards consider legal, audit and operational organizational risks, they should govern cybersecurity with the same broad mindset that allows for a thorough analysis of cyber risks alongside other risks.

Assessing and clarifying the risk appetite for cybersecurity threats will help to make cyber risks an integral part of the enterprise's overall risk profile. In some cases, this assessment could leverage insights from members of the cybersecurity committee (if one is in place), but care must be taken to avoid inadvertently marginalizing the topic by subsuming it within the more general concerns of audit or IT. Indeed, one of our board member interviewees stated: "You want the whole board looking at cybersecurity." We understood this to mean that even though not every board member may be an expert on the topic, the pervasiveness of cybersecurity risk is such that it may permeate other areas of the business in which board members do have expertise. Effective boards consider the consequences of cybersecurity risk across the enterprise and avoid relegating it as an issue that can be confined and managed as a technical issue.

Action 2: Gauge the organization's cybersecurity maturity. Deciding how much attention to cybersecurity is "enough" is admittedly no easy task. Just as company executives and managers need to determine the depth and breadth of their investment in cybersecurity tools, training and oversight, the board members we interviewed reported that they were keen to fulfill their fiduciary duties but also wanted to find the right balance of time, effort and investment relative to cybersecurity risks. One helpful approach frequently mentioned was for the board to gauge the organization's cybersecurity maturity by making comparisons with industry peers. This approach can help the board get a clearer sense of where the organization currently is with cybersecurity and where it wants (or needs) to be. Indeed, considering how the organization is managing cybersecurity relative to established metrics and/or competitors can provide board members with clues about how much attention they should dedicate to advocating the allocation of cybersecurity resources in the short term vs. the medium/long term. Comparison with peers can also trigger a broader discussion with management about the organization's cybersecurity strategy.

Several tools are available to measure an organization's cybersecurity capabilities, including the COBIT framework's[24] maturity models (ranging from 0: lacking basic capabilities to 5: well-defined, measured and continually improved capabilities), and the NIST Cybersecurity Framework[25] and derivatives such as the CRI Profile,[26] with implementation tiers ranging from 1: *ad hoc* to 4: *adaptive*. Using these frameworks to assess and quantify cyber risks can help prioritize where the enterprise and the board should focus its energy.[27,28] Though we acknowledge that boards will only occasionally initiate such assessments, an organization's internal audit function or external consultants may be well positioned to undertake such evaluations to share with board members.

Action 3: Be clear on the possible enterprise and personal consequences of a significant cyber incident. Media coverage of cybersecurity incidents is constantly highlighting the financial and reputational damage to organizations targeted by the continuing rise in ransomware and denial-of-service attacks.[29] Though board members are broadly aware of these business-oriented consequences, our interviewees highlighted several areas where the implications of a significant cyber incident were less clear to boards. In particular, we recommend that board members get advice on the personal

24 COBIT is promoted by ISACA (Information Systems Audit and Control Association). For information about ISACA and COBIT, see isaca.org. ISACA also promotes the Cybersecurity Maturity Model Certification (CMMC) framework, which was developed by Carnegie Mellon University and purchased by ISACA.

25 For information about the NIST Cybersecurity Framework, see nist.gov.

26 For information about the CRI Profile (provided by the Cyber Risk Institute), see: 1) https://cyberriskinstitute.org/the-profile/; and 2) Coden, M. *Cutting The Cost And Complexity Of Cybersecurity Compliance*, Forbes.com, January 13, 2022, available at https://www.forbes.com/sites/forbestechcouncil/2022/01/13/cutting-the-cost-and-complexity-of-cybersecurity-compliance/?sh=4b335cdf51f9.

27 Coden, M., op. cit., May 9, 2019.

28 Ramachandran, S., Yousif, N., Bohmayr, W., Coden, M., Frankle, D. and Klier, O., op. cit., August 9, 2019.

29 See, for example: 1) Rundle, J. "Cyberattack on ION Derivatives Unit Had Ripple Effects on Financial Markets," *The Wall Street Journal*, February 10, 2023, available at https://www.wsj.com/articles/cyberattack-on-ion-derivatives-unit-had-ripple-effects-on-financial-markets-11675979210?page=1; and 2) *Amazon "Thwarts Largest Ever DDoS Cyber-Attack*," BBC, June 18, 2020, available at https://www.bbc.com/news/technology-53093611.

liability that they may be exposed to following a cybersecurity incident. Generally, board members are expected to undertake:

> *"reasonable care and diligence in running the company, including exercising appropriate oversight over the company's cybersecurity program. Investors or other stakeholders could pursue such claims against directors … to seek to remedy the harms suffered by the company as a result of director or officer negligence. Under securities law, directors and officers can be held liable for omissions or misrepresentations in the company's public disclosure, which could include disclosures about the status of cybersecurity incidents, risks and preventative measures."*[30]

Legal proceedings at T-Mobile,[31] Caremark[32] and Yahoo[33] have highlighted the increasing concern in this area for board members. Though organizations commonly carry cybersecurity insurance and directors/officers insurance, due to the changing nature of the legal environment, we recommend that board directors clarify both their personal responsibilities and the level of potential exposure following a cybersecurity incident.

Responding to Challenge 2: Board-Executive Interaction Dynamics

Action 4: Don't "get into the weeds" on cybersecurity, but focus on the business implications. Despite the growing attention of board members to cybersecurity issues, many of our interviewees stressed the importance of not "getting into the weeds" on the topic. They reinforced the view that management is responsible for running the company and that the role of board members is to push management to do a better job and provide them with the necessary resources. To achieve this aim, some of our interviewees went so far as to advocate that board members refrain from asking management technical questions or attending low-level incident response exercises. Their view was that such activities are fundamentally operational in nature, that direct involvement by board members does not facilitate better governance and that delving into unnecessary detail can impede effectiveness.

For example, one board member made the following statement about the need for boards to avoid the minutiae of operational cybersecurity issues:

> *"[Boards] do ask [detailed questions] because it is seductive. … 'Why did you pick this company? Why did you go with this strategy?' It is seductive to ask the technology questions because there is an answer. It's not easy to say 'What is your strategy?' and then make an evaluation if we as the board think they made the right [strategy] decision. Board members need to ask questions to make sure that the operational managers are doing the best they can. It is not the board members' role to say: 'You made the wrong decision by picking company X over company Y.'"* Board Member, Healthcare, Interview No. 3

Action 5: Demand clarity and understandability in executive communications. Boards typically formally communicate with the executives tasked with managing cybersecurity several times a year, perhaps for as little as 10-15 minutes per session. For instance, the CISO may provide a brief, quarterly report to the board on high-level issues and initiatives. Consistent with Action 4, we recommend that such reports avoid low-level details and unnecessary technical depth. Instead, boards should aim to facilitate a dialogue with the CISO about the key issues and demand clarity and understandability in the related communications. Board members should not simply take executive reporting at face value or treat the perceived

30 Himo, J., Reynolds, M., Caparelli, C. M., DiPaolo A. and Butt, A. *Director and Officer Liability for Cybersecurity Breaches in Canada and the U.S.*, Torys Quarterly, Spring 2022, available at https://www.torys.com/en/our-latest-thinking/publications/2022/04/director-and-officer-liability-for-cybersecurity-breaches-in-canada-and-the-us#:~:text=Under%20securities%20law%2C%20directors%20and,incidents%2C%20risks%20and%20preventative%20measures.

31 Sullivan, V. "Personal Liability for Directors Who Disregard Cybersecurity," *CPO Magazine*, May 23, 2022, available at https://www.cpomagazine.com/cyber-security/personal-liability-for-directors-who-disregard-cybersecurity/.

32 Ferrillo, P., Zukis, B. and Veltsos, C. *Boards Should Care More About Recent "Caremark" Claims and Cybersecurity*, Harvard Law School Forum on Corporate Governance, September 15, 2020, available at https://corpgov.law.harvard.edu/2020/09/15/boards-should-care-more-about-recent-caremark-claims-and-cybersecurity/.

33 Edwards, B. P. "Cybersecurity Oversight Liability," *Georgia State University Law Review* (35:3), 2019, pp. 663-677.

credibility of the CISO as sufficient, as evidenced by the following comment from a board member:

> *"I always feel that the management team, whoever it is, is always on audition. And if the person giving the presentation, [whether] the CIO or head of counsel or head of technology/security, comes across as credible and on top of their game, the board is kind of done with the issue. It becomes a relatively surface-level understanding of these issues."* Board Member, Media, Interview No. 10

Though board-executive interaction dynamics will be partly determined by the level of board expertise (see below), directors should push back on cybersecurity executives who use excessive jargon and technical terminology while insufficiently focusing on the business and risk consequences. Recent articles in management publications[34] have highlighted the strategic aspects of cybersecurity and the quantification of cyber-risk, and this is the level of discussion that board members require. By better understanding the CISO's objectives and goals, board members can gain a clearer view of how cybersecurity fits into the organization's overall strategic framework and better support management by ensuring they get the resources to do their job effectively.[35],[36]

However, some more technically inclined CISOs may struggle to fulfill the board's needs in terms of sufficiently clear communications. This can be particularly challenging in smaller companies with a part-time CISO, where board-CISO interactions will likely be less frequent. In such cases, we recommend that boards seek input on cybersecurity issues from another executive, such as the chief financial officer, who may share the board's prioritization of risk management issues. Overall, however, by ensuring it receives clear communications on cybersecurity issues, pitched at the right level, the board will be in a stronger position to better understand the issues at hand.

34 See, for example Hepfer, M. and Powell, T. C. "Make Cybersecurity a Strategic Asset," *MIT Sloan Management Review* (62:1), Fall 2020, pp. 40-45.

35 Coden, M., op. cit., May 9, 2019.

36 Ramachandran, S., Yousif, N., Bohmayr, W., Coden, M., Frankle, D. and Klier, O., op. cit., August 9, 2019.

Responding to Challenge 3: Board Cybersecurity Expertise

Action 6: Determine the board's appetite for bringing in cyber experts, as either a board member or through an advisory or consulting role. One of the most contentious issues we discussed with current board members was the role of cyber experts serving on (or advising) the board. This is becoming a key issue for many boards, as the recently introduced SEC rules[37] include a provision that requires "periodic disclosures of the board of directors' cybersecurity expertise, if any, and its oversight of cybersecurity risk."[38] In general, we recommend that boards ensure that their members have a diversity of experience and expertise. However, we heard differing views on whether one or more board members should have extensive technical familiarity with cybersecurity issues. The overriding concern raised was that boards do not need to include experts who tell the company how to operate but rather members who know the questions to ask that will challenge company executives.

In fact, boards that include cyber experts may have a false sense of comfort. Instead of having an expert on the board, they can bring in consultants to do an evaluation if a "deep dive" is required. However, we recognize that the decision of whether to employ consultants is determined by the specific company context, in terms of industry, country and company size.

Despite the lack of consensus on the precise level of cyber expertise that should be in place at the board level, it is clear that board member expertise should go beyond a surface-level understanding of the issues, but as mentioned in Action 4, they should not "get into the weeds" of cybersecurity. Though many boards would find it easiest to simply defer to a qualified individual or a committee tasked with cyber governance, we recommend that each board member develop at least a basic competency in terminology and risks associated with the topic in order to understand the key issues.

37 *SEC Proposes Rules on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure by Public Companies*, U.S. Securities and Exchange Commission Press Release, March 9, 2022, available at https://www.sec.gov/news/press-release/2022-39.

38 *Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure*, U.S. Securities and Exchange Commission, 2022, available at https://www.sec.gov/rules/proposed/2022/33-11038.pdf.

Action 7: Seek out cybersecurity training and education opportunities, including tabletop cyberattack simulations. To improve the board's cyber expertise, board members who are currently unfamiliar with cybersecurity governance and risk management would benefit from appropriate training and education. This training and education will equip them with the confidence to ask management tough questions. On the topic of training board members on cybersecurity issues, one of our interviewees said:

"Where do you get the experts to fill those [board] seats? And it's like, okay, we have to figure out how we do this training. And then here's the key from the regulatory side you're talking about. It can't be this watered-down training. ... It has to be real training geared to the board members on their responsibilities and outlining what their duties are. ... So how do you get the trainers to do that? And how do you multiply that?"

Though our interviewees cautioned that basic board training is not a replacement for true cybersecurity expertise, it can play a key role in raising the level of sophistication at which the board can operate when interacting with management on key cyber issues. Some of this training could be facilitated internally, but the number of external offerings is growing, including those from the National Association of Corporate Directors (https://www.nacdonline.org) and MIT Sloan Executive Education (https://exec.mit.edu/). We have observed that board members, like most people, learn more by doing than by being instructed in a lecture. In our experience, having board members participate in a business-oriented tabletop exercise simulation of a cyber breach is a very effective training and education tool.[39,40]

One of our interviewees (a board member) noted that "What you want ... is [to] have a board that is aware that the cyber stuff creates systemic risk for the firm and that needs to be carefully managed." Providing a diverse group of non-expert board members with a solid understanding of (nontechnical) cybersecurity concepts will equip them to balance the business and risk management issues of interest to the board with the cybersecurity concerns that face the organization. This is especially important when there is a lone cybersecurity expert on the board, who can become overpowered or ignored by other directors prioritizing different risk areas or competing board initiatives.

Responding to Challenge 4: Expanding Cybersecurity Regulations

Action 8: Know the cybersecurity and related privacy regulations that affect your industry, organization and countries of operation, and their potential costs (fines). Many of the board members we interviewed expressed uncertainty about precisely which cybersecurity and privacy-related regulations required their organization's compliance. This is not entirely surprising, based on the increasing quantity and extent of regulations. We recommend that board members pay more attention to this issue, perhaps as part of training activities (Action 7), to ensure they are better informed about the organization's regulatory responsibilities. The recent SEC regulations (noted above) are of particular interest to boards of companies with a U.S. presence and were generally welcomed positively by our interviewees. However, the expanding range of other competing cybersecurity regulations that organizations are obligated to follow introduces a complex balance involving not only understanding what an individual regulation requires but also how these regulations align or conflict with one another. These other regulations include the Health Insurance Portability and Accountability Act (HIPAA), General Data Protection Regulation (GDPR), Personal Information Protection and Electronic Documents Act, Federal Information Security Management Act, California Consumer Protection Act (CCPA), and similar acts in Virginia and pending in 40 other U.S. states, as well as acts already made law in 156 countries globally.[41,42]

39 Pearlson, K., Thorson, B., Madnick, S. and Coden, M. "Cyberattacks Are Inevitable. Is Your Company Prepared?" *Harvard Business Review*, March 9, 2021.

40 Coden, M. *Table-Top Attack Simulations: Cyber Resilience's Swiss Army Knife*, Forbes.com, March 12, 2019, available at https://www.forbes.com/sites/forbestechcouncil/2019/03/12/table-top-attack-simulations-cyber-resiliences-swiss-army-knife/?sh=1124000f7f11.

41 Coden, M., op. cit., January 13, 2022

42 Bartol, N., O'Malley, B., Bickford, J. K. and Coden, M. *Radically Simplifying Compliance in Cybersecurity*, Boston Consulting Group, February 08, 2019, available at https://www.bcg.com/capabilities/digital-technology-data/simplifying-compliance-in-cybersecurity.

In addition, it is now customary for purchase contracts to include cybersecurity maturity and notification requirements. We observed that, in some companies, each customer had different requirements in its purchasing contract, requiring management to construct a database of reporting requirements for each of its customers. Though the practicalities of doing this is a management responsibility, boards need to ensure that the issue is dealt with effectively. They can only do so by developing a clear understanding of which regulations are relevant to the organization.

Action 9: Appreciate that compliance with regulations doesn't (necessarily) equate with sufficient cybersecurity. We found that board members widely acknowledge the importance of ensuring compliance with relevant cyber regulations, but we also note that simple compliance does not necessarily mean that their organization's cybersecurity defenses are sufficient. For example, one board member stated: "I think there is an overlap between a board's fiduciary duty and the compliance side because the board wants to make sure the company is in compliance—but just because you are compliant doesn't mean you are secure." Indeed, prior research[43,44] has highlighted regulations that are out of date or ill-suited for particular types of organizations.

We recommend that board members push management to undertake cybersecurity initiatives not only to fulfill basic regulations but also to ensure that the specific cybersecurity risks faced by the organization are adequately managed. Moreover, regulators should recognize the power they hold and the potential they have to help organizations make compliance impactful, and not just establish a regulation and do nothing to proactively facilitate meaningful compliance. On this topic, one of our board member interviewees commented:

> *"It is fascinating but not [helpful] for the government to come in and say 'ok companies, we expect you to do ABCDEF' and then do nothing really to help; well, they do do something, that is too strong, but not do much on collaborative efforts within industries to prevent these events from happening, and that is true to this day."* Board Member/CEO, Multiple Industries, Interview No. 12

Action 10: Understand the tension between what cybersecurity regulations aim to achieve vs. the business and legal implications following an incident. We found that board members generally hold a positive view of the objectives that cybersecurity regulations aim to achieve (e.g., protect customer information), though some highlighted the potential disconnect with the actual enforcement of the regulations and the related organizational consequences. In particular, some directors view regulators as not effectively following through on their mission due to an inflexible approach to enforcement. The challenges of out-of-date regulations, conflicting regulatory guidance and regulations that fail to fulfill current best practices mean that organizations are left in the difficult situation of either simply meeting what the regulations require or going beyond the minimum standard with the risk that this will be seen as a noncompliant approach.

From a board member perspective, this tension presents a unique opportunity to challenge managers not only on their approach to overseeing numerous cybersecurity regulations but also in terms of how the organization interacts and communicates with regulators during enforcement activities. As new cyber regulations continue to emerge and are refined by governments around the world, board members are in an ideal position to guide executives and managers toward an effective balance between meeting compliance expectations, while also mitigating any residual risks not covered by current guidelines.

Concluding Comments

Members of corporate boards are increasingly aware of the risks associated with cybersecurity. However, for those without expertise in the area, it remains challenging to move beyond simplistic inquiries of management toward a more sophisticated, value-adding role. Our research

43 For example, see Bayard, E. E. "The rise of cybercrime and the need for state cybersecurity regulations," *Rutgers Computer and Technology Law Journal* (45:2), 2019, pp. 69-96.

44 Sterns, R. Q. "Complementary approaches or conflicting strategies? Examining CISA and New York's DFS Cybersecurity Regulations as Harmonizing Framework for Bilateral Approach to Cybersecurity," *Richmond Journal for Law and Technology* (26:1), 2020, pp 1-35.

Second Study Interview Participants

Interview No.	Role	Industry	Interview Length (mins:secs)
1	CEO	Finance	41:49
2	Board Member	Finance/Education/Technology	34:11
3	Board Member	Healthcare	50:24
4	CISO	Communications	56:57
5	Board Member	Technology	28:05
6	Board Advisor	Technology	47:40
7	Board Member	Food Services	25:21
8	Board Advisor	Multiple Industries	21:48
9	Board Member	Communications	38:25
10	Board Member	Media	27:05
11	Board Member	Finance/Technology/Insurance	35:36
12	Board Member/CEO	Multiple Industries	38:40
13	Board Member	Technology/Finance	45:59

brings clarity to this issue by drawing on the insights of 35 cybersecurity and board experts, including current board members, business executives, CISOs, CTOs, compliance officers and board advisors. We have identified four specific cybersecurity challenges that currently face boards of directors and recommend 10 actions that directors can take in response. Following these recommendations will enable boards to more effectively navigate the current cybersecurity environment and contribute to improved enterprise risk management and governance.

Appendix: Research Methodology

Our investigation into cybersecurity governance and risk management for boards of directors used a qualitative research method based on a total of 35 interviews. We conducted an initial round of semi-structured interviews with 22 cybersecurity executives and practitioners, including executives and senior managers, to compile insights and perspectives on the operationalization of cybersecurity regulations in organizations. Participants were volunteers sourced through an international forum for cybersecurity. To ensure that our findings were comprehensive and generally applicable, the interviewees represented a broad range of industries, including technology, finance, consulting, government and industrial control systems. The interviews ranged from 35 to 65 minutes with an average of 57 minutes.

We then used an inductive coding approach to analyze over 300 pages of interview transcripts, which revealed several emerging themes. One theme was an emphasis by 11 of our initial 22 interviewees on the importance of effective interactions between executives and the board to maximize meaningful cybersecurity governance and oversight. This insight triggered our interest in conducting a follow-up study to more closely examine the role boards play in overseeing cybersecurity within their respective organizations.

The secondary data collected from the follow-up study forms the core of this research study. This second study aimed to gather insights directly from board members on their evolving role in cybersecurity governance and risk management, and complements our first dataset based on executives' perspectives. We conducted 13 semi-structured interviews, 11 of which were with board members and two with people

serving in an advisory role to a board. (Two of these additional interviews were with high-ranking technology executives who had extensive experience interacting with boards.) As with the initial data collection, participants for this secondary data collection were also sourced via an international cybersecurity forum. The second round of interviews ranged from 21 minutes to 56 minutes, with an average of 37 minutes. The table on the previous page lists the role, industry and interview length for each participant in the second study.

About the Authors

Jeffrey G. Proudfoot

Jeffrey Proudfoot (jproudfoot@bentley.edu) is an associate professor in the Computer Information Systems Department at Bentley University and a research affiliate in the Cybersecurity at MIT Sloan (CAMS) center at MIT. His research focuses on information security topics, including deception and insider threat detection, security policies and compliance, and on cybersecurity regulations. Jeff's work has been published in several premier journals, including *MIS Quarterly, MIS Quarterly Executive, Journal of Management Information Systems, Journal of the Association for Information Systems, European Journal of Information Systems and Information Systems Journal.*

W. Alec Cram

Alec Cram (wacram@uwaterloo.ca) is an associate professor in the School of Accounting and Finance at the University of Waterloo, Canada, where he holds the J. Page R. Wadsworth Junior Chair in Accounting and Finance. His research focuses on how information systems control initiatives can contribute to improving the performance of organizational processes, including cybersecurity and algorithmic management.

Stuart Madnick

Stuart Madnick (smadnick@mit.edu) is the John Norris Maguire (1960) Professor of Information Technologies at the MIT Sloan School of Management, a Professor of Engineering Systems at the MIT School of Engineering and the Founding Director of Cybersecurity at MIT Sloan (CAMS). He has been active in the cybersecurity field since co-authoring the book Computer Security in 1979. His work has been published in journals such as *ACM Transactions on Management Information Systems, ACM Transactions on Internet Technology, IEEE Transactions on Dependable and Secure Computing, Journal of Database Management, Journal of Management Information Systems and MIS Quarterly Executive.*

Michael Coden

Michael Coden (mcoden@mit.edu) advises boards, CEOs and CISOs on technology, transformation, cyber strategy and resilience, and cyber technology companies on product design and marketing. He is co-founder and Associate Director of Cybersecurity at MIT Sloan (CAMS), CEO of DBOS, Inc., Managing Partner of Magjic Technology & Cyber Consulting LLC, Senior Advisor to Boston Consulting Group, and on the advisory boards of Safe Security Inc. and The Decision Lab. Michael assisted the White House in developing the NIST CSF, has appeared on Bloomberg radio and PBS television, published many articles and a book, is a sought-after speaker and has 17 patents.