Cybersecurity: Emerging Challenges and Solutions for the Boards of Financial Services Companies

BANK POLICY INSTITUTE

September 29, 2020

Table of Contents

Introduction

Cybersecurity has become a top concern for the boards of directors of financial services firms – one that seems to be growing day by day. With players seeking to create new digital customer experiences, applying sophisticated data analytics and investing in a wealth of other technology innovations, cyber risk management clearly requires governance at the highest levels. The advent of the COVID-19 crisis makes this mandate even more urgent, with millions of new interactions now taking place online, and questions arising about their security.

Well before the pandemic hit, the Bank Policy Institute began seeking to address these issues in a collaboration with McKinsey & Company. To gain deeper insights, we conducted a survey of top financial firms to assess current cybersecurity trends, challenges and solutions to help guide boards in their decision making.

We found that boards are spending a significant amount of new time on this issue and are appointing committees to deal with it specifically. However, while many are working to integrate cybersecurity resilience into their overall risk efforts, they have yet to achieve consistency in how to measure these risks and maximize value for money and resources spent on cybersecurity. Boards also find themselves in need of new, practical approaches to set a risk appetite for cybersecurity and then guide management on resourcing and spending to ensure they can address the consistent and persistent risk inherent in this area.

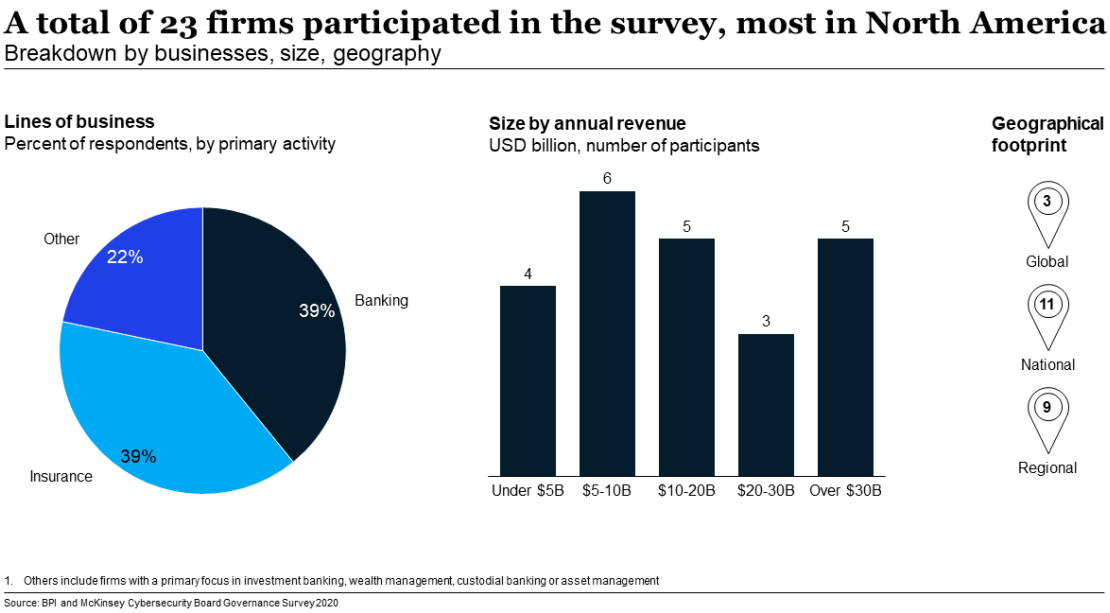
As boards look at their next moves, they can take cues from more advanced firms that are starting to adopt a cyber and technology risk management strategy in conjunction with business operations. These firms are integrating cyber and technology risks with operational risk and resilience. They are giving their boards new perspectives to help them assess cyber risks against the enterprise risk appetite, and they are ensuring board members have the knowledge to oversee these activities.

This report summarizes our survey findings and describes some of the actions that mature firms are taking now.

An Evolving and Increasing Role for the Board

A total of 23 financial services firms participated in the survey, most in North America, spread across a diversity of sizes and lines of business (Exhibit 1).

Exhibit 1



The survey had 14 questions across 3 broad areas:

- **Oversight.** The nature of board oversight of cyber risks, including which committees are responsible, who is on them and how often they meet.
- **Structure.** Whether boards are forming technology committees with a mandate that includes cyber oversight, and if they have, what are their structure and charter.
- **Awareness.** How boards are increasing their awareness and understanding of these risks along with their skills and expertise.

Oversight: More Frequent and Intense

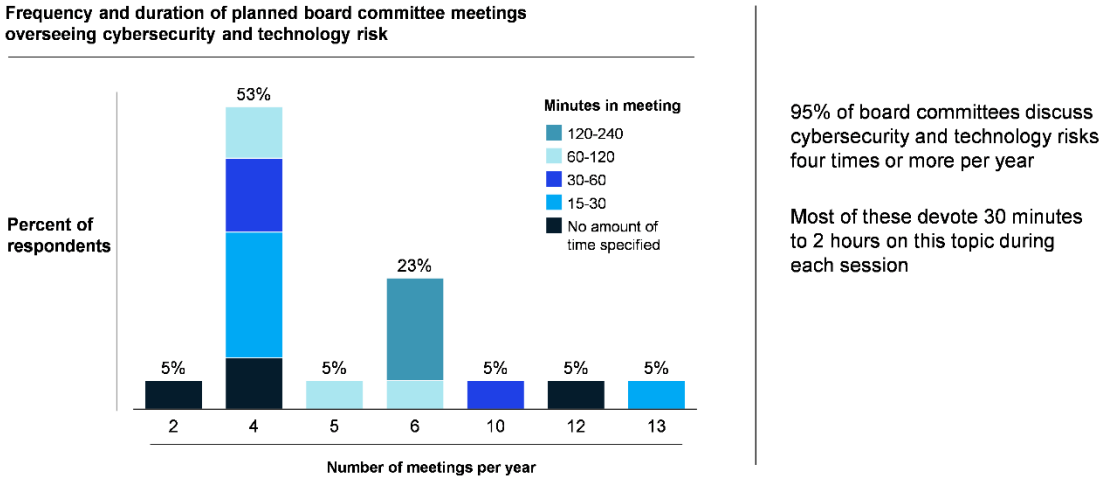
The increased attention all financial firms are devoting to cyber risk is reflected in actions by boards. For example, 95 percent of board committees reported discussing cyber and tech risks four times or more per year (Exhibit 2). One such firm reported success in holding optional deep-dive sessions the week preceding each quarter's board meeting. These sessions covered relevant topics such as updates on current threat intelligence for the company, case studies of any recent breaches that could impact the company or others in the industry and the impact of regulatory changes.

There has been a remarkable shift in board awareness of cybersecurity in the last few years. For example, earlier McKinsey research from 2017 suggested that only 25 percent of all companies would present information technology and security updates to the board more than once a year. More frequent and consistent communication between board

members and senior management on this topic, now, enables the board to understand the financial, operational and technological implications of emerging cybersecurity threats to the business and to guide direction accordingly.

Exhibit 2

Boards are putting a growing focus on cybersecurity, with an increased investment in their time



Source: Q1.c, How often do these committees meet a year and for what length of time (e.g., risk committee meets quarterly for an hour on cyber)? (n=23) (Due to rounding percentages don't always equal 100%)

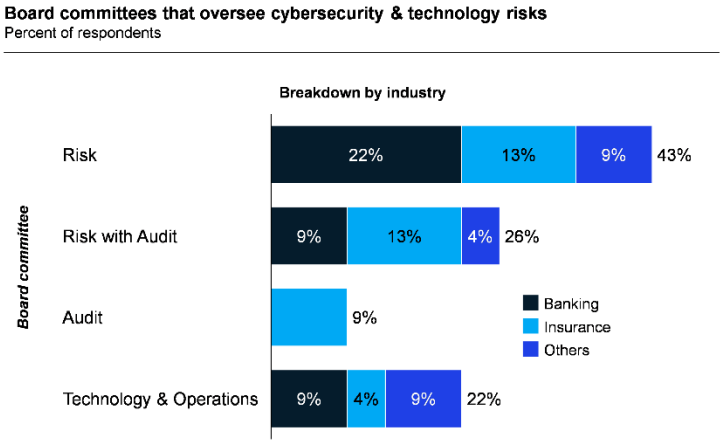
Firms are increasingly recruiting experts for these committees. For example, 65 percent said that they have at least one board director with expertise in cybersecurity and/or technology risk. Profiles of these directors include senior executives of top technology companies and executives with defense or intelligence agency backgrounds.

Structure: Appointing a Specialized Technology Committee

Risk and audit committees are the primary overseers of these risks, but a growing number of firms have a technology committee for cybersecurity oversight — now 22 percent, and as high as 35 percent in some segments (Exhibit 3).

Exhibit 3

Boards increasingly rely on a technology and operations committee



Source: Q1) Which Board committees currently oversee cybersecurity and technology risk management (n=23)
(Due to rounding percentages don't always equal 100%)

A desire for better cyber risk oversight is driving the formation of these committees, but the motivation goes beyond this alone. Examples of areas covered in their charter include:

- Integrating oversight of cyber risk and resilience with technology and operational resilience, including business continuity;
- Applying an expert focus on strategic technology choices, innovation, transformation initiatives and investments; and
- Better managing regulatory concerns and requests in these areas.

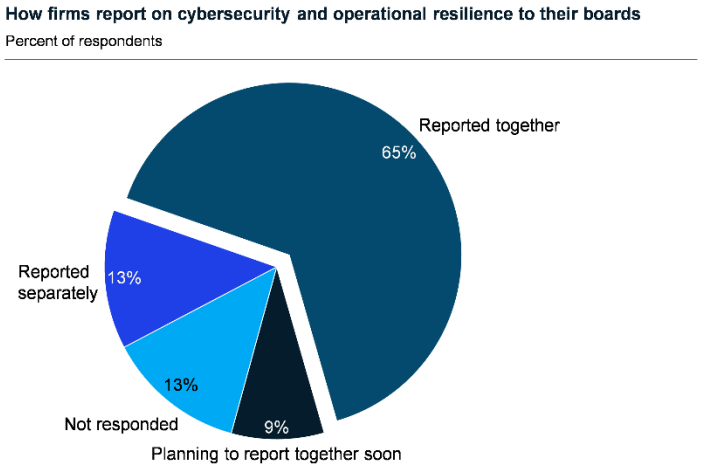
Awareness and Understanding: Growing, but Challenges Remain

The growing awareness and attention of boards to cybersecurity risks are reflected in a number of ways and are evident in how companies report on them to the board. These measurements and risks, however, remain a challenge for many.

For instance, 65 percent of firms integrate cybersecurity and operational resilience when reporting to the board. An additional 9 percent plan to soon. (Exhibit 4).

Exhibit 4

Companies increasingly view cybersecurity as part of overall operational resilience

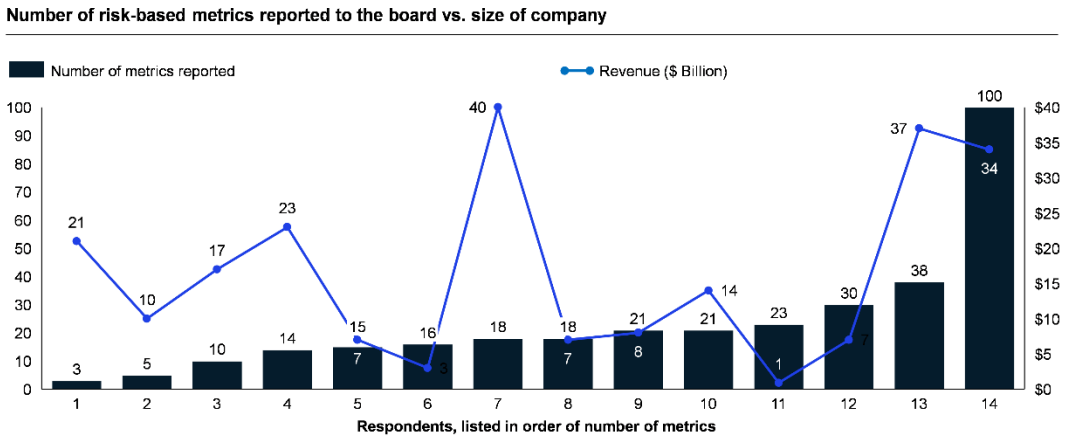


Source: Q3.b. Do you approach and integrate broader operational resilience (e.g., production technology risk) with cybersecurity resilience when reporting to board? (n=23)

However, firms reported little consistency in this area. There is a wide variance in the type and number of metrics that firms use to report to the board on cyber risk — and the higher number of metrics does not correlate with the size of the firm (Exhibit 5).

Exhibit 5

Firms' use of risk-based cyber metrics varies widely in board reports



Eight additional firms responded that they do not have standard metrics but are in the process of standardizing, or they use a rotating set of metrics based on the topic of discussion.

Source: Q3c) Do you use a consistent set of risk-based metrics in your periodic report to the board? If yes, how many such metrics do you typically track and report? (n=22)

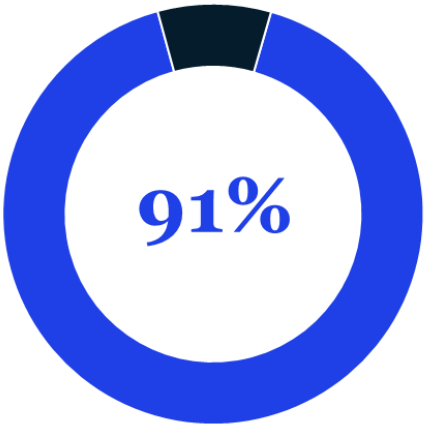
More advanced firms report on a standard set of key risk or performance indicators that are relevant to them and indicate resilience in the context of their business and industry risk exposure.

Some firms said they focus on technical metrics such as malware detections. Eight said they do not have standard metrics, but are in the process of standardizing, or they use a rotating set of metrics based on the topic of discussion.

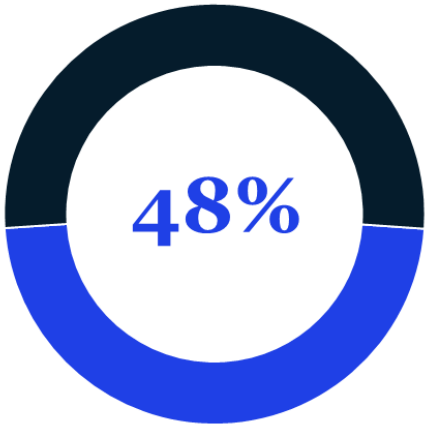
Nearly all firms see value in keeping the board regularly aware of the ongoing risks: 91% of them provide updates at least annually or more frequently (Exhibit 6).

Exhibit 6

Companies providing regular updates on cybersecurity to the full board



Companies periodically involving the board in cybersecurity exercises



3) Do you provide regular updates or conduct regular education sessions for the board on cybersecurity and technology risk? (n=23)
Q3.b) Do you involve board members in cybersecurity exercises? (n=23)

These are usually led by the responsible board committees or by the chief information security officer.

Nearly half the firms (48%) conduct regular "tabletop" cyber exercises with the board to raise awareness and knowledge. The timing of a cybersecurity crisis may be unpredictable, but most crisis events evolve in predictable ways. The first set of actions that are taken shape much of the outcome, and getting those early steps right is core to emerging stronger. Firms see these simulation exercises as enabling the board to understand the business risk of a specific cybersecurity crisis and the firm's capabilities to respond.

Advanced Boards Maintain a More Integrated Cybersecurity Strategy

Advanced boards are shifting their role in cybersecurity and are actively involved to understand the cyber risk to the company and helping set the direction on risk and investment strategy. A number of factors such as the rising number of cyber breaches making headlines, regulators increasingly holding companies accountable for addressing gaps in cybersecurity resilience and the increase in cybersecurity and technology investments are causing this shift in boards' involvement. Boards looking for direction can take cues from those who have already begun to pursue a cybersecurity and technology risk management strategy that is integrated with business operations. These strategies have three major elements:

Integrating Cyber and Technology Risks With Operational Risk and Resilience for the Board

- These boards are focusing on how to secure their digital agenda. They are integrating cybersecurity considerations as part of their technology strategy including oversight of technology investments, digital transformation programs and the development of differentiated customer experiences.
- They are separating cyber threats from cyber risks. Cyber threats are technical cybersecurity exploits such as privilege escalation, vulnerability exploitation or phishing, while cyber risks are potential risks to the enterprise due to loss of confidentiality, integrity and the availability of digital assets.

Giving the Board Tools to Help It Assess Cyber and Technology Risks Against the Enterprise Risk Appetite

- This includes implementing a common risk terminology to measure cybersecurity resilience and maximize risk reduction at different levels of investment (as a complement to qualitative discussions).
- These firms are also pioneering an effective, efficient approach to cyber risk reporting to the board, and thereby allowing members to conduct meaningful problem-solving on which risks are within tolerances, which are not, and why.
- With an understanding of cyber risks, mature firms are setting the cyber risk appetite and then steering cyber investment decisions to optimize the risk reduction impact. Such "cost-risk optimal" defenses provide the same level of overall protection to critical assets, but in a more lightweight way that is less expensive and enables better productivity.
- They are also streamlining metrics and linking key performance indicators (KPIs) and key risk indicators (KRIs). To do this, they are implementing metrics to measure both inputs and outputs. Inputs are the company's risk-reduction efforts and outputs are the resulting reduction in enterprise risk. For example, in the context of data protection, the critical assets requiring data protection coverage can become the

output metric, or KRI. Assuming that the KRI is not 100 percent, then the linked input metric, or KPI, could be the proportion of critical assets covered since the last reporting period vs. the total expected to be covered.

Ensuring the Board Has the Knowledge and Skill to Understand Cyber and Technology Risk and Resilience in the Business Context

- Leading firms ensure the board is aware of cyber and tech risks, their potential impact on the firm and how the firm's leadership is addressing them. They update the board on these at least quarterly, with additional awareness and education sessions as needed.
- They use simulations and tabletop exercises to prepare the board and test the capabilities of senior leadership to respond to a major cyber incident. For example, they will simulate a cybersecurity-related crisis scenario such as a ransomware demand that may result in a customer data breach. Through such simulations, senior executives become better prepared to make high-stakes decisions under pressure and the board gains a deeper understanding of the firm's capabilities. The insights generated from the simulation are used to refine the crisis response playbook, as well as build the type of "muscle memory" required to make appropriate decisions in real time with limited information.

Conclusion

Cyber risks are diverse, difficult to predict and quantify and growing. Mature boards are taking a comprehensive approach to cyber risk management, developing strategies integrated with the rest of the business to increase board awareness, understanding and skills, and making the board an important and valuable partner with management in increasing firm-wide resilience.


bpi
BANK POLICY INSTITUTE