McKinsey & Company

Risk Practice

Cybersecurity: Emerging challenges and solutions for the boards of financial-services companies

Mature boards are making themselves valuable partners for management in the effort to make firms more resilient.

by Tucker Bailey, Soumya Banerjee, Christopher Feeney, and Heather Hogsett

October 2020

Cybersecurity has become a top concern for the boards of financial-services firms, and the level of concern seems to be growing day by day. With organizations seeking to create new digital customer experiences, applying sophisticated data analytics, and investing in a wealth of other technology innovations, cyberrisk management clearly requires governance at the highest levels. The advent of the COVID-19 crisis makes this challenge even more urgent.

Well before the pandemic hit, the Bank Policy Institute and McKinsey began to address these issues. To gain deeper insights and help guide boards in their decision making, we collaborated on a survey of top financial firms to assess current cybersecurity trends, challenges, and solutions. We found that boards are not only spending a significant amount of time on cybersecurity challenges and ways to address them but also assigning committees to deal specifically with these issues. However, though many boards are working to integrate cybersecurity resilience into their overall risk efforts, they have not yet learned to measure these risks consistently and to maximize value for money. Boards also need practical new approaches to set their risk tolerance for cybersecurity and to guide management's resourcing and spending so that they can address the consistent and persistent risks inherent in this area.

As boards look at their next moves, they can take their cues from more advanced firms starting to adopt a cybersecurity and technology risk-management strategy informed by business operations. These firms are integrating their efforts to control cybersecurity and technology risks with operational risks and resilience. They are giving their boards new views of information to help them assess cyberrisks against the risk tolerance of the enterprise and ensuring that board members have the knowledge to oversee these activities.

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

An evolving and increasing role for the board

A total of 23 financial-services firms, mostly in North America, participated in the survey. They included a diversity of sizes and lines of business. The survey had 14 questions in three broad areas:

— *Oversight.* What is the nature of board oversight of cyberrisks—including which committees are responsible, who serves on them, and how often do they meet?

— *Structure.* Are boards forming technology committees with a mandate that includes cyberoversight and, if they have, what is their structure and charter?

— *Awareness and understanding.* How are boards becoming more aware of these risks, understanding them better, and increasing their skills and expertise?

A growing number of firms—22 percent overall, and as many as 35 percent in some segments—have a technology committee to oversee cybersecurity.

Oversight: More frequent and intense

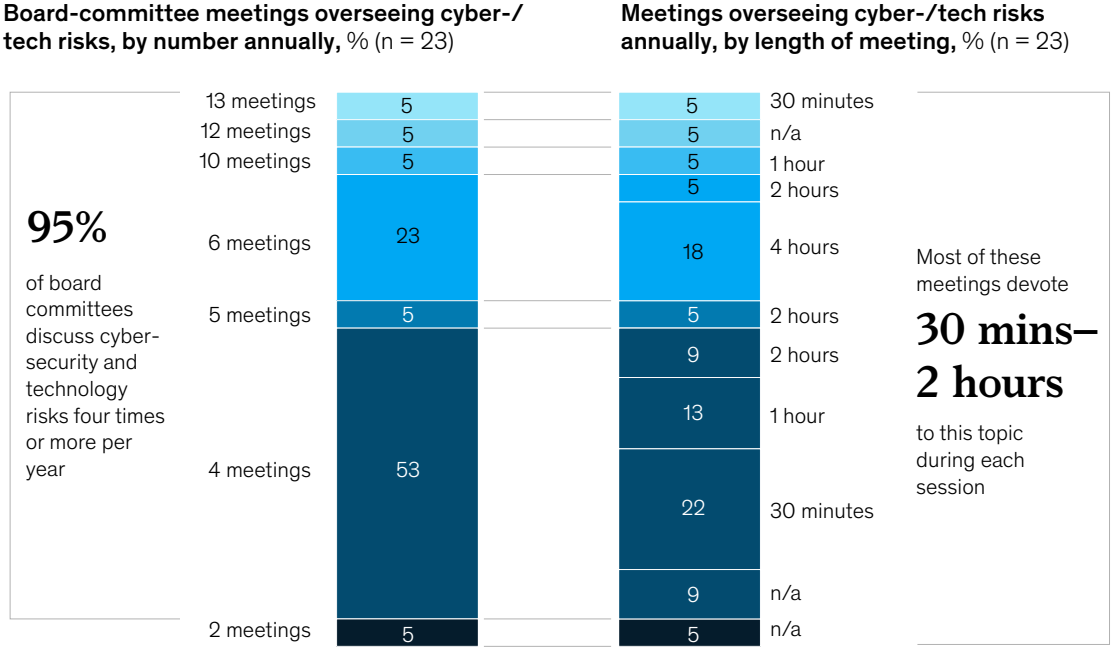
Actions by boards reflect the increased attention all financial firms are now devoting to cyberrisk. Ninety-five percent of board committees, for example, discuss cyberrisks and tech risks four times or more a year (Exhibit 1). One such firm holds optional deep-dive sessions the week before each quarter's board meeting. These sessions cover relevant topics, such as updates on the current intelligence on threats, case studies of recent breaches that could affect 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 past few years: for example, earlier McKinsey research, from 2017, suggested that only 25 percent of all companies gave their boards information-technology and security updates more than once a year. More frequent and consistent communication between board members and senior management on this topic now enables boards to understand the financial, operational, and technological implications of emerging cybersecurity threats for the business and to guide its direction accordingly.

Firms increasingly recruit experts for these committees. Sixty-five percent of them, for example, have at least one board director with expertise in cybersecurity, technology risk, or both. These directors include senior executives of top technology companies and executives with defense or intelligence backgrounds.

Exhibit 1

Ninety-five percent of board committees discuss cyberrisks and tech risks four times or more a year.



Note: Figures may not sum to 100%, because of rounding.
Question: How often do these committees meet a year and for what length of time (eg, risk committee meets quarterly for an hour on cyberrisk)?
Source: BPI and McKinsey Cybersecurity and Board Governance Survey, August 2020

Structure: Appointing a specialized technology committee

Risk and audit committees are the primary overseers of these risks, but a growing number of firms—22 percent overall, and as many as 35 percent in some segments—have a technology committee to oversee cybersecurity (Exhibit 2).

A desire for better cyberrisk oversight is part of the reason for the creation of such committees—but not the only reason. The areas covered in their charters include these:

— integrating the oversight of cyberrisk and resilience with technology and operational resilience, including business continuity

— applying an expert focus to strategic technology choices, innovation, transformation initiatives, and investments

— better managing regulatory concerns and requests in these areas

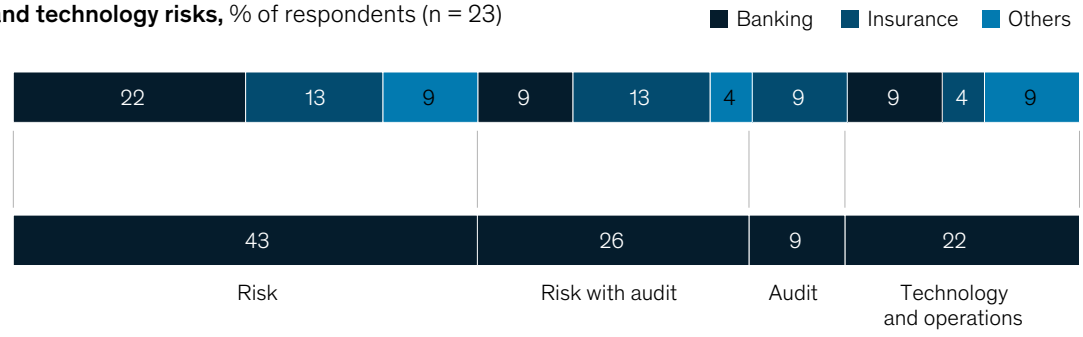
Awareness and understanding: Growing, but challenges remain

The growing awareness and attention of boards to cybersecurity risks is reflected in a number of ways—for example, how companies report on such risks to their boards. These reports nonetheless remain a challenge for many. True, 65 percent of firms integrate cybersecurity and operational resilience in reports to the board. An additional 9 percent plan to do so soon (Exhibit 3). However, the types and

Exhibit 2

Boards increasingly rely on a technology and operations committee.

Board committees that oversee cybersecurity and technology risks, % of respondents (n = 23)



Note: Figures may not sum to 100%, because of rounding.
Question: Which board committees currently oversee cybersecurity and technology risk management?
Source: BPI and McKinsey Cybersecurity and Board Governance Survey, August 2020

Exhibit 3

Companies increasingly view cybersecurity as part of overall operational resilience.

How companies report on cybersecurity and operational resilience to their boards, % of respondents (n = 23)

Question: Do you approach and integrate broader operational resilience (eg, production-technology risk) with cybersecurity resilience when reporting to the board?
Source: BPI and McKinsey Cybersecurity and Board Governance Survey, August 2020

number of metrics firms use to report to their boards on cyberrisk vary widely among firms—and a higher number of metrics does not correlate with the size of the firm (Exhibit 4).

More advanced firms report a standard set of key risk or performance indicators relevant to them and indicate their level of resilience in the context of their business and industry risk exposure. Some firms focus on technical metrics, such as malware detections. Eight are standardizing their metrics or use a rotating set, depending on the topic under discussion.

Nearly all firms see value in keeping the board regularly aware of the ongoing risks: 91 percent of them provide updates at least annually (Exhibit 5). These are usually led by the board committees responsible or by the chief information-security officer. Nearly half of the firms (48 percent) conduct regular "tabletop" cybersecurity exercises with the board to raise awareness and knowledge. The timing of cybersecurity crises may be unpredictable, but most of them evolve in predictable ways. The first responses shape much of the outcome. Getting the early steps right is the heart of efforts to emerge stronger. Firms believe that these simulations enable their boards to understand the business risks of specific cybersecurity crises and their ability to respond.

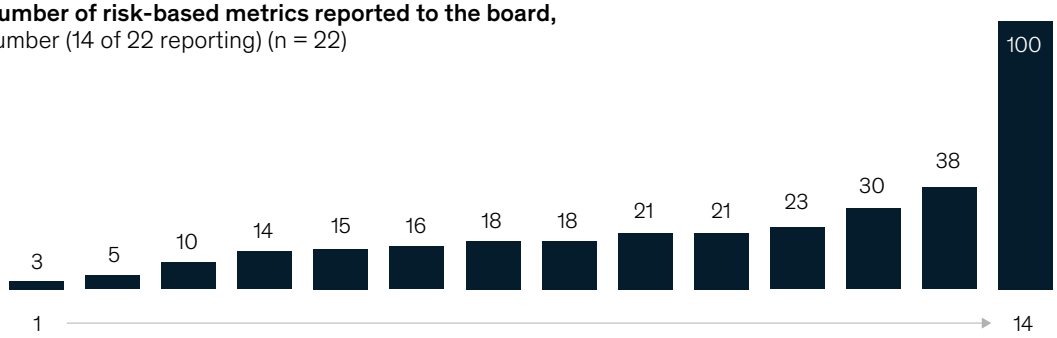
Advanced boards: A more integrated cybersecurity strategy

Advanced boards are shifting their role on cybersecurity by actively trying to understand the cyberrisks to their companies and helping to set the direction on risk and investment strategy. A number of factors are causing this shift in the involvement of boards—for instance, the rising number of cyberrisk breaches making headlines, regulators who increasingly hold companies accountable for addressing gaps in their cybersecurity resilience, and the increase in the level of cybersecurity and technology investment. Boards looking for direction can take

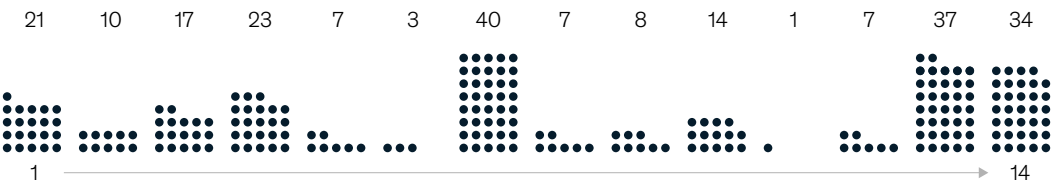
Exhibit 4

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

Number of risk-based metrics reported to the board, number (14 of 22 reporting) (n = 22)



Revenue by firm, $ billion (14 of 22 reporting)



Question: 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?
Source: BPI and McKinsey Cybersecurity and Board Governance Survey, August 2020

Exhibit 5

Companies recognize the importance of keeping the board aware of and building cybersecurity knowledge.

Companies providing regular updates on cybersecurity to the full board, % of respondents (n = 23)

Companies periodically involving the board in cybersecurity exercises, % of respondents (n = 23)

Question: Do you provide regular updates or conduct regular education sessions for the board on cybersecurity and technology risk?
Source: BPI and McKinsey Cybersecurity and Board Governance Survey, August 2020

cues from those that have already begun to pursue a cybersecurity and technology risk-management strategy integrated with business operations. These strategies have three major elements.

Integrating cybersecurity and technology risks with operational risk and resilience

Advanced boards are focusing on the digital transformation of their companies. For one thing, they are integrating cybersecurity into their technology strategies, including the oversight of technology investments, digital-transformation programs, and the development of differentiated customer experiences. They are also separating cyberthreats from cyberrisks. Cyberthreats are technical cybersecurity exploits, such as privilege escalation, vulnerability exploitation, or phishing. Cyberrisks are potential threats to the enterprise as a result of a loss of confidentiality, integrity, and the availability of digital assets.

Giving the board the right tools to assess cybersecurity and technology risks

Advanced firms in this area implement a common risk terminology to measure their cybersecurity resilience and maximize the reduction of risk at different levels of investment (as a complement to qualitative discussions). They are also pioneering an effective, efficient approach to reporting cyberrisks to their boards and thus allowing directors to determine which risks are within tolerances, which are not, and why.

Thanks to this understanding of cyberrisks, mature firms are determining their tolerance for them and then steering cyberinvestment decisions to optimize the risk-reduction impact. Such “cost–risk optimal” defenses provide the same level of overall protection for critical assets as the traditional risk-based approach for managing cyberrisks, but in a more lightweight, less expensive way that improves productivity.

Mature firms are also streamlining their metrics and linking KPIs and key risk indicators (KRIs) by implementing metrics that measure both inputs and outputs. Inputs are a company’s risk-reduction efforts, and outputs are the resulting reduction in enterprise risk. In the context of data protection, for example, the critical assets requiring data-protection coverage can become the output metric, or KRI. Assuming that it is not 100 percent, the linked input metric, or KPI, could be the proportion of critical assets covered since the last reporting period and the total number of critical assets the firm expects to cover.

Ensuring that the board has the necessary knowledge and skill

Leading firms ensure that boards know about cybersecurity and tech risks in the business context, their potential impact, and how the leadership is addressing them. Such firms update the board on these issues at least quarterly, with additional awareness and education sessions as needed. They use simulations and tabletop exercises to prepare the board and test the ability of the senior leadership to respond to a major cyberincident: for example, they will simulate a cybersecurity-related crisis, such as a ransomware demand that may expose customer data. Such simulations help 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 by the simulation help refine the crisis-response playbook and build the type of "muscle memory" required to make appropriate decisions in real time with limited information.

Cyberrisks are diverse, difficult to predict or quantify, and growing. Mature boards are taking a comprehensive approach to managing cyberrisks by developing strategies integrated with the rest of the business to increase their awareness, understanding, and skills. In this way, they are making themselves important, valuable partners for management in the effort to increase the resilience of their firms.

Tucker Bailey is a partner in McKinsey's Washington, DC, office, and **Soumya Banerjee** is a cybersolutions expert in the New York office. **Christopher Feeney** is executive vice president and **Heather Hogsett** is senior vice president, technology and risk strategy, of the Bank Policy Institute, in Washington, DC.

Designed by McKinsey Global Publishing