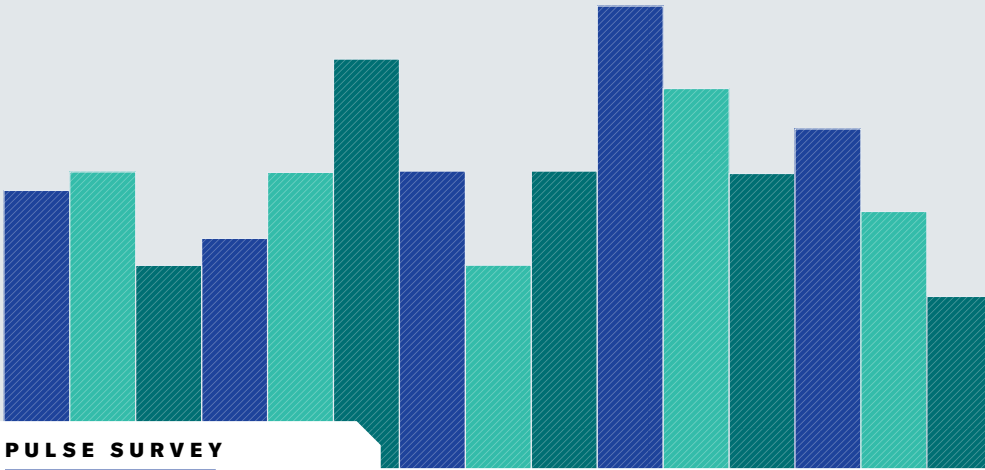




**Harvard  
Business  
Review**

ANALYTIC SERVICES



**PULSE SURVEY**

# Organizations Struggle to Measure and Monitor Cyber Risk



Sponsored by



## SPONSOR PERSPECTIVE

Cybersecurity efficacy has always been of chief importance but perhaps has never been as complicated as it is today. This is especially true for risk posture. Ad hoc or infrequent scanning for vulnerabilities cannot keep up with a rapidly changing, complex IT environment. Remediation or mitigation efforts are hindered by reliance on tools that are disconnected from risk analysis and overall security performance.

Nonetheless, odds are high that boards of directors will have even more questions for security leaders regarding sensitive data, risk levels, risk reduction, and security investments. There's a significant communication gap between the two groups. In reality, most executives don't have strong technology backgrounds, and they struggle to understand the metrics being presented by their security counterparts.

Chief information security officers (CISOs) struggle to explain the value and performance of security investments, which puts them in jeopardy of falling out of sync with business priorities or gives executives a false sense of confidence about security readiness. Lack of consistency and creating patchwork reports from a variety of security point tools also hamper the ability of security leaders to offer executives a comprehensive, real-time view of risk across their organization.

In addition to the type of data, the way that data is conveyed also matters. Security leaders may also be too focused on presenting metrics that aren't actionable or are centered on security tools rather than security effectiveness. Risk data must align with business objectives if it's going to make sense to boards.

Bridging this communication gap requires security leaders to identify and communicate the metrics that matter to both sides.

This move starts by taking a proactive, data-driven, and continuous approach to managing risk exposure with a real-time view of risk posture. With access to real-time risk scoring, security leaders have the ability to see and communicate key trends, improvements, and industry benchmarks that produce insights that boards and security teams can act on together while taking into account people, processes, and technology.

We sponsored this Harvard Business Review Analytic Services report to showcase the disconnect between security and executive management about cybersecurity efficacy and performance. Through a quantitative survey and interviews with experts, it illuminates how security teams should explain cyber risk and security performance to the C-suite and the board—and the extent to which this communication is adequate and effective—and explores ways to improve it.



**Chris Hallenbeck**  
**CISO, Americas**  
**Tanium**

# Organizations Struggle to Measure and Monitor Cyber Risk

**WHEN IT COMES TO CYBER RISK**, most organizations have a communication problem. The consequences of inadequate executive governance of that risk have never been greater. Yet translating the technical intricacies of cybersecurity into how a business should reduce its cyber risk has proved to be a challenge.

“You can’t govern what you don’t understand,” says Bob Zukis, founder and CEO of the Digital Directors Network (DDN), an organization with a mission of helping boards understand and govern cyber risk—and helping security technologists’ ability to present risk in business terms.

A survey of 180 respondents by Harvard Business Review Analytic Services sheds light on this gap and its consequences. Despite showing broad agreement about the importance of cybersecurity, the survey reveals that the executives making decisions on cyber-risk investment may not be getting the information they need.

Effective cyber-risk oversight is hampered by a mutual shortage of knowledge; executives don’t know enough about what the technology means, and cybersecurity experts don’t know how to put cyber risk in a relevant context. That shortage of knowledge is compounded by other factors, including inconsistent or indirect lines of reporting, various methods of measuring cyber risk, and a lack of context showing how and why such measures matter.

## Digital Innovation, Cyber Risk

The pandemic accelerated digital transformation. The World Economic Forum expected that 60% of global gross domestic product would be digitized by 2022<sup>1</sup> and that 70% of new value created in the economy over the next decade will be based on digitally enabled platform business models.<sup>2</sup>

Digital innovation creates value and competitive advantage—but it also creates risks that can threaten that value, says Zukis, who founded the DDN in 2017 after a 30-year career at PwC. So far, most organizations have focused on the former but not the latter. “We’ve done a much better job of innovating

### HIGHLIGHTS



70% of survey respondents somewhat or strongly agree that senior business executives at their organization should be **more concerned about their organization's cybersecurity**.



68% somewhat or strongly agree that **information technology could do more to make sure senior executives are better informed** about their organization's cyber risk/cybersecurity.



51% report that the CEO or equivalent is **responsible for final cybersecurity investment decisions** in their organization.

Due to rounding, some figures in this report may not add up to 100%.

and creating digital value,” says Zukis. “We’ve done a much less effective job of protecting that digital value.”

Criminals are taking advantage. In the Harvard Business Review Analytic Services survey, 57% of respondents report an increase in cyber attacks since the pandemic began, with 38% saying attacks have increased some, and 19% saying attacks have increased significantly. Organizations dramatically expanded attack surfaces as they rushed to send employees home to work, and many organizations didn’t secure all their new connections and endpoints immediately, says Emily Mossburg, global cyber leader at Deloitte.

Financial losses mounted with the increasing cybercrime that resulted. The FBI’s Internet Crime Complaint Center reports that losses totaled \$4.2 billion in 2020, up from \$3.5 billion in 2019.<sup>3</sup> The amount paid in ransomware attacks rose in 2020 by more than 300%, to \$350 million, according to the Ransomware Task Force Report.<sup>4</sup>

Most organizations recognize the rising level of risk and increasing importance of cybersecurity, but executives may not have the information they need to manage that risk. Some 66% of respondents to the Harvard Business Review Analytic Services survey say it is extremely important that their organization has strong cybersecurity; 27% say it is very important. A great majority (93%) of respondents somewhat agree (18%) or strongly agree (75%) that “it’s important that senior business executives are well-informed about their organization’s cybersecurity and cyber risk.” Yet far fewer, 69%, somewhat agree (35%) or strongly agree (34%) that “senior business executives at my organization are well-informed about the organization’s cybersecurity and cyber risk.”

A similar proportion (70%) also somewhat or strongly agree that senior business executives at their organization should be more concerned about their organization’s cyber risk/cybersecurity. In addition, 68% somewhat agree (30%) or strongly agree (38%) that “IT could do more to make sure our senior business executives are better informed about the organization’s cyber risk/cybersecurity.”

### Lost in Translation

These results indicate a disconnect between the business and technology sides of the house. Several factors contribute to this gap: lack of translation between business and technical language, opaque organizational and reporting structure, infrequency of updates, lack of appropriate context, and inconsistent use of metrics.

Technology and business executives or corporate directors often speak different languages. Chief information security officers (CISOs) tend to talk about technical metrics that other executives and directors may not understand. When business executives sit politely and listen to a litany of

technical metrics, they may get a false sense of security, says Zukis. What executives do understand, and focus on, is business value. “That’s why you have to talk about cyber risk in economic terms,” he notes.

Reporting between those implementing cybersecurity and those deciding how much to invest in cybersecurity can be muddy. In the survey, over half (51%) of respondents report that the CEO or equivalent is responsible for making final cybersecurity investment decisions in their organization. **FIGURE 1** Thirty-seven percent say that responsibility rests with the CISO/chief information officer (CIO)/chief technical officer (CTO) or equivalent, and 31% say it rests with the board of directors.

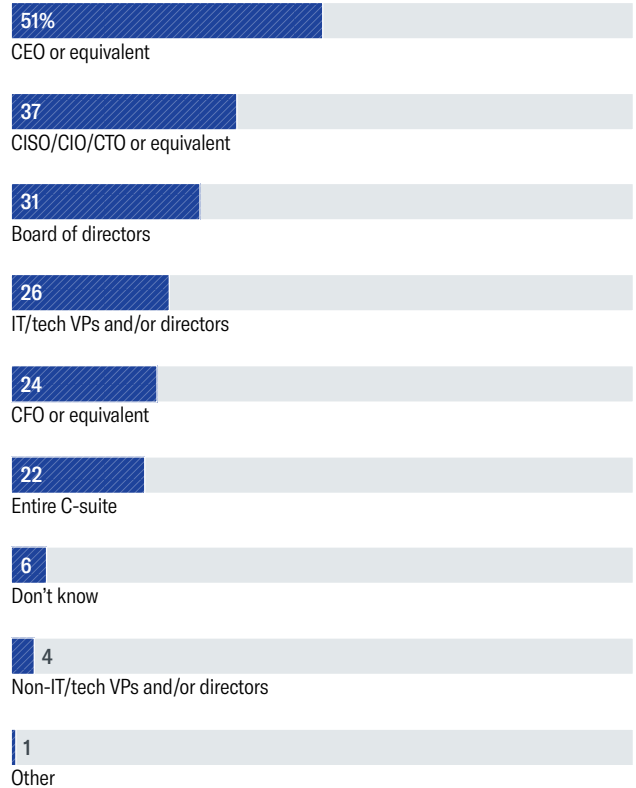
CISOs are rising in organizational charts, says Deloitte’s Mossburg. A Deloitte survey of executives found that 33% of

FIGURE 1

### Holders of the Purse Strings

Cybersecurity spend is controlled primarily by the head of the organization, technology leaders, and the board.

Which groups are responsible for making final cybersecurity investment decisions at your organization? [SELECT ALL THAT APPLY]



Source: Harvard Business Review Analytic Services survey, September 2021

CISOs globally and 42% in the U.S. now report directly to the CEO. That’s up from 32% in the U.S. in 2019.<sup>5</sup>

Zukis believes CISOs should report directly to the CEO, or even the board of directors. Yet far too many CISOs still report to the CIO, he says. “That’s not ideal, because there are inherent conflicts,” he says. The CIO is typically responsible for creating value through technology; having the CISO under the CIO could subordinate the protection of that value.

Some boards are creating committees focused on cybersecurity, which could draw a direct line to the CISO. Fewer than 10% of boards today have a dedicated cybersecurity committee overseen by a qualified board member, according to Gartner, which predicts that percentage will increase to 40% by 2025.<sup>6</sup>

At Mastercard, the chief security officer (CSO) is a member of the CEO’s management committee, says Alissa Abdullah, deputy chief security officer and senior vice president of emerging corporate security solutions. The CSO can bring technical detail and expertise to the committee but should primarily serve as a filter at the CEO and board levels, talking in terms of high-level trends to enable management to think strategically about cybersecurity and cyber risk, she says.

The CSO regularly reports to Mastercard’s board. The frequency of such updates varies from one organization to another. Asked how regularly those responsible for implementing and monitoring cybersecurity provide updates to their organizations’ senior business executives, 24% of respondents to the Harvard Business Review Analytic Services survey say they do so quarterly. **FIGURE 2** The largest proportion of respondents (33%) report on an “ad hoc” basis. Such a



“We’ve done a much better job of innovating and creating digital value. We’ve done a much less effective job of protecting that digital value,” says Bob Zukis, founder and CEO of the Digital Directors Network.

lack of regularly scheduled business-level oversight could mean executives hear about risk levels only when there is a problem. More encouraging is the second-largest proportion of responses—29% say senior business executives are updated monthly. Some 7% say “annually,” and 7% say “rarely or never.”

As important as regular updates, if not more so, is the information the updates provide. That communication presents one of the trickiest challenges: how to present important technical information on cyber risk that grabs executives’ attention.

### Mixed Measurements

Some organizations use metrics to assess cyber risk, and others don’t. The survey asked those respondents who say their senior business executives are regularly updated on cyber risk to choose from a list of update descriptions. **FIGURE 3** Fifty-two percent indicate they use some measurement to gauge risk levels over time, selecting “overall status/level of risk including some metrics/benchmarks.” The second-largest proportion of respondents (44%) describe updates as “general, overarching status/current level of risk, little or no metrics/benchmarks,” which could mean these executives are not monitoring cyber risk in much depth. But some executives are going deeper; 13% of respondents chose “a comprehensive review including many metrics/benchmarks.”

These results aren’t surprising, given that there is no single standard framework for measuring cybersecurity and cyber risk. Each organization chooses its preferred model. “There is resistance to a single approach,” Mossburg notes. “I think it may be because there is such a contextual element to cyber. Anytime you try to create a framework, it’s hard to make sure every context can be incorporated.”

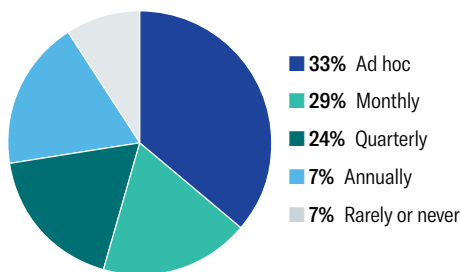
That reality contrasts starkly with the black-and-white measurement of finance, where clear accounting standards lay out exactly how to quantify and report financial information.

FIGURE 2

### The “Squeaky Wheel” Schedule

The largest proportion of respondents indicate that senior executives receive only ad hoc updates, which may mean only when there is a problem.

How regularly do those responsible for implementing and monitoring cybersecurity update senior business executives on the status of cyber risk in your organization?



Source: Harvard Business Review Analytic Services survey, September 2021

**“There is resistance to a single approach [to measuring cyber risk]. I think it may be because there is such a contextual element to cyber. Anytime you try to create a framework, it’s hard to make sure every context can be incorporated.”**

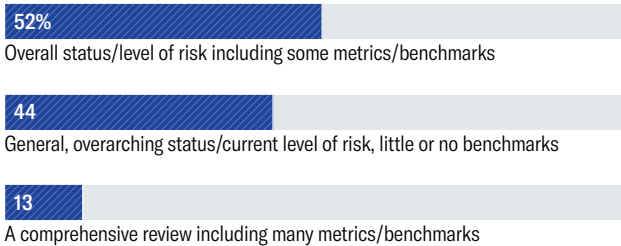
**Emily Mossburg, global cyber leader, Deloitte**

FIGURE 3

### Differing Levels of Detail

Most respondents say cyber risk updates to executives include at least some metrics.

Which of the following best describes the level of information senior business executives are provided in these updates?



Source: Harvard Business Review Analytic Services survey, September 2021

Organizations usually follow one of three approaches to cyber risk, says Mossburg. The first is maturity assessments, which are often based on the National Institute of Standards and Technology’s cybersecurity framework, a guide on managing cyber risk. The second is risk quantification, in which organizations identify their top risk scenarios, examine how a cyber attack could hurt value, and make sure their cybersecurity program mitigates those specific risks. The third approach relies on the experience of cyber leaders, who are likely using specific technical metrics, “which makes it hard for executives to understand the true business impacts,” she says.

### A Plethora of Metrics

When the Harvard Business Review Analytic Services survey asked those who say their business executives review some or many metrics to select the type of metrics used, the most common response was technical metrics. Some 68% of respondents characterize the metrics as measuring “technical vulnerability to attack.” **FIGURE 4** Almost as many, 63%, characterize them as measuring “damage in terms of reputation, customers/customer trust, and press.” In third place, 56% say they measure “potential monetary damage,” and the fewest, 41%, say they measure “potential legal ramifications.”

Many technical metrics aren’t helpful to executives and boards gauging cyber risk, especially when CISOs or their equivalents present them with little context. “What we see happening is CISOs come in with a presentation deck, saying, ‘Here are the threats that we identified, here are the results of our phishing tests, this is how many attacks we identified,

this is the percentage that we stopped,’” says Zukis. What they should be telling executives, he says, is what those metrics mean in terms of protecting the value of the organization. “Most CISOs don’t make that business value connection yet,” says Zukis.

Even financial metrics are unhelpful if they aren’t presented in the right context. “The question a lot of business leaders ask is ‘What are we spending on cybersecurity, and is that the right number or not?’” Zukis says. “There really is no right number, and that question is the wrong question.” Rather, executives should be identifying the value at risk in the organization and asking if they are spending enough to protect that value and how secure the organization is for what they are spending.

Adding to the confusion is that organizations often switch metrics or frameworks. “One of the biggest challenges I see is that organizations mix and match them rather than consistently applying one approach,” Mossburg explains. “One quarter, they talk about maturity. The next quarter, they talk about risk quantification, and the next, they talk about certain metrics.”

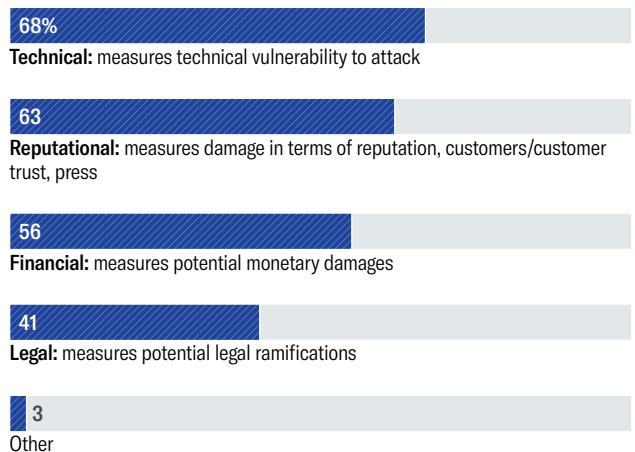
She thinks such switches may be attempts to improve understanding, as CISOs present information in different forms to see what hits home with executives. There may be value in offering different perspectives on risk, but this mixing usually just confounds boards and executives. “They don’t

FIGURE 4

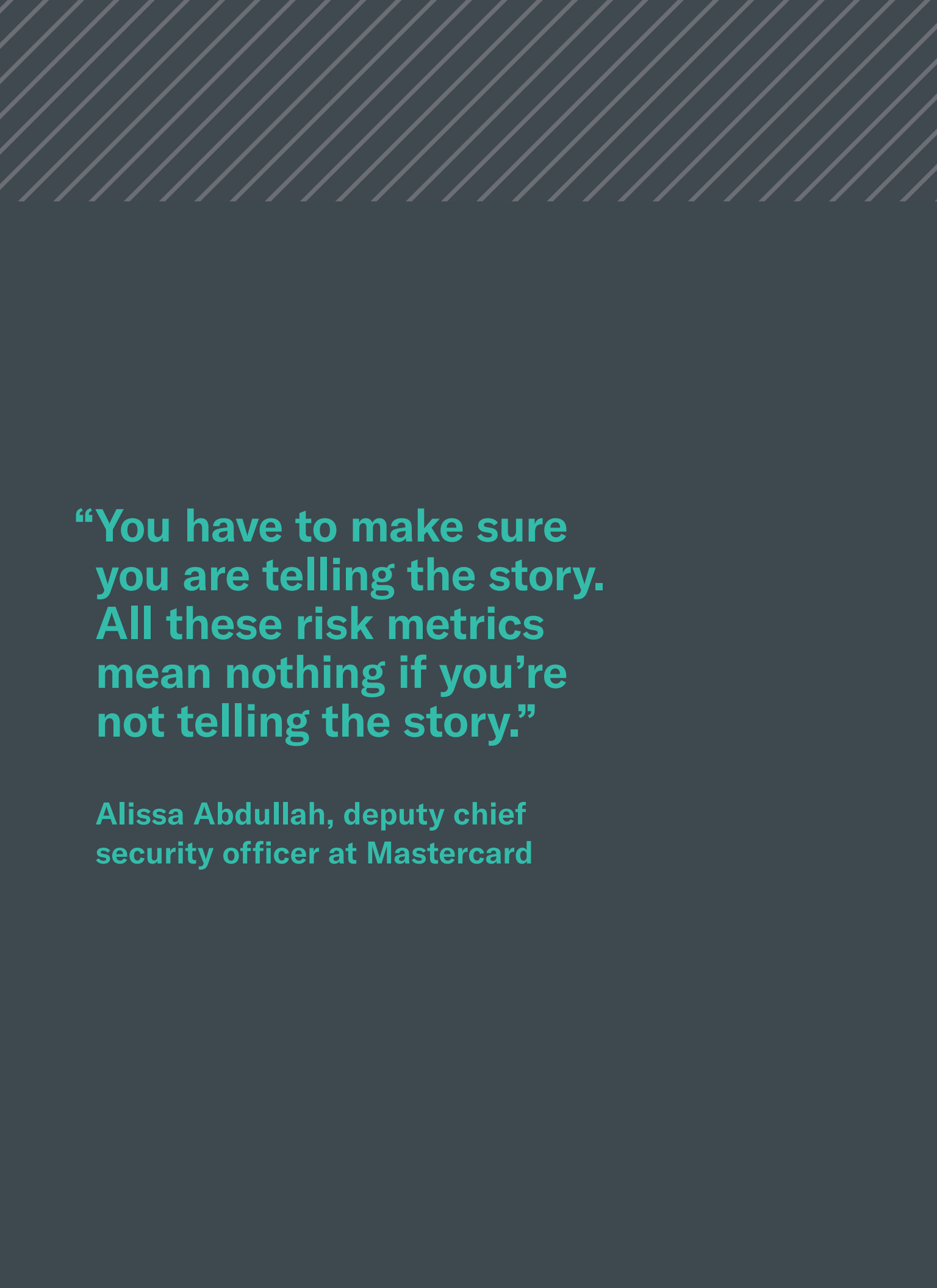
### Mixed Metrics

Respondents report that executives receive a variety of metrics, but more are technical than financial.

Which of the following best describes the types of metrics senior business executives are provided in these updates? [SELECT ALL THAT APPLY]



Source: Harvard Business Review Analytic Services survey, September 2021



**“You have to make sure  
you are telling the story.  
All these risk metrics  
mean nothing if you’re  
not telling the story.”**

**Alissa Abdullah, deputy chief  
security officer at Mastercard**



know whether the organization is doing better or worse from one quarter to the next,” she says.

An important aspect of context is aligning risk appetite with risk tolerance, says Zukis. He uses a Las Vegas metaphor to explain; a gambler may understand the odds of winning a particular type of game, “but that’s only half the equation. What really matters is the odds of the game and how much money you’re betting—a few dollars or the mortgage on your house.”

Risk appetite and tolerance are part of Mastercard’s process. The company uses a framework called Factor Analysis of Information Risk (FAIR) to quantify risk, according to Mastercard’s Abdullah. Executives including the CSO define risk appetite, apply factors such as the likelihood of a cyber attack, and determine which cybersecurity measures are in place to mitigate that risk.

In updates, executives and the board see a visual representation of risk levels as a grid. “Anything in the top right quadrant of the grid is really high risk,” Abdullah says. She stresses that assessment is continuous. “It’s dynamic risk management rather than just assessment. We are looking at the magnitude of impact at any given time,” she says. “When we introduce new projects into our infrastructure, for example, we look at the risk and the potential magnitude of impact.”

## Keeping Cyber Risk on Executive Radar

At the same time, it’s important to avoid getting too far into the weeds. “You have to make sure you are telling the story,” says Abdullah. “All these risk metrics mean nothing if you’re not telling the story.”

A compelling story can help keep risk top of mind with business executives. It’s easy for something as technical as cyber risk to drop from their list of top priorities. Even though 81% of respondents in the Harvard Business Review Analytic Services survey say cybersecurity is a high or extremely high priority in their organizations, some 70% also agree that other aspects of the business take greater priority.

Those other aspects nearly always concern revenue. That’s why the surest way to keep executive attention on cyber risk is to put it into financial terms, says Zukis, and an emerging discipline called cyber economics does exactly that.

Mossburg sees the power struggle “when there is a choice of getting a product or service to market and producing revenue versus something controls-oriented that does not lead to immediate revenue.” That’s why she advises clients to build in security from the start. “If a product or service has cybersecurity as a design requirement, that inherently minimizes risk,” she says. “That makes security a part of the innovation rather than making it look like an extra cost.”

One way Mastercard keeps cyber risk high on executives’ radar is by including them in crisis simulations. “They need

to have that ‘Oh, no’ moment,” says Abdullah. “Once they’ve lived it, they understand it and remember it.” She also walks management and the board through an actual cyber attack, helping them understand the theories on a practical level. “Cybersecurity can be overwhelming,” she says. “But if you show them how available hacking tools are on the dark web, then they get it.”

## Conclusion

Experts agree that the communications gap is narrowing. Executives and boards are paying more attention to cyber risk than ever before. CISOs and other cybersecurity professionals are exploring better ways of quantifying and explaining risk in business terms.

But there’s still room for improvement. “Have we gotten the language clear and crisp on how to talk about cyber risk and how to quantify cyber risk? Do business executives and boards understand completely? I think the industry still has work to do there,” says Mossburg.

CISOs need to cut back on technical metrics and put cyber risk in economic terms. Executives—on the technical side and the business side—should agree on a framework and use consistent measures and scoring from quarter to quarter. And the cybersecurity discussion should focus not on whether but on when an attack will happen. “Cyber risk management needs to be more of a conversation about impact and less about likelihood,” says Mossburg. With cybercrime rising exponentially during the pandemic and threatening to get worse, even the best organizations with top-tier security can become victims. The point should be to anticipate and minimize the negative impacts.

Executives and boards need to be less passive and more proactive, beefing up their general knowledge of cybersecurity and assigning executive responsibility for cyber risk. And they need to bring cybersecurity into product, service, and other business discussions.

When executives hear reports on the latest innovations or product roadmaps, they should ask how the designers are embedding cybersecurity to protect the value they’re creating. “It’s not just what CISOs say when they update the board,” Mossburg says. “It’s also about making cybersecurity a part of the innovation process.”

## Endnotes

- 1 World Economic Forum, "Our Shared Digital Future: Responsible Digital Transformation - Board Briefing," February 2019. <https://www.weforum.org/whitepapers/our-shared-digital-future-responsible-digital-transformation-board-briefing-9ddf729993>.
- 2 World Economic Forum, "Shaping the Future of Digital Economy and New Value Creation," <https://www.weforum.org/platforms/shaping-the-future-of-digital-economy-and-new-value-creation>.
- 3 Internet Crime Complaint Center, "2020 Internet Crime Report," March 17, 2021. <https://www.fbi.gov/news/pressrel/press-releases/fbi-releases-the-internet-crime-complaint-center-2020-internet-crime-report-including-covid-19-scam-statistics>.
- 4 Institute for Security and Technology, "Combating Ransomware: A Comprehensive Framework for Action: Key Recommendations from the Ransomware Task Force," April 2021. <https://securityandtechnology.org/wp-content/uploads/2021/04/IST-Ransomware-Task-Force-Report.pdf>.
- 5 Deloitte, "Deloitte Global 2021 Future of Cyber Survey Finds Rapid Increase in Cyberattacks Driven by Organizations' Embrace of Digital Transformation," October 2021. <https://www2.deloitte.com/global/en/pages/about-deloitte/press-releases/deloitte-global-2021-future-of-cyber-survey-finds-rapid-increase-in-cyberattacks-driven-by-organizations-embrace-of-digital-transformation.html>.
- 6 Gartner, "Gartner Predicts 40% of Boards Will Have a Dedicated Cybersecurity Committee by 2025," January 28, 2021. <https://www.gartner.com/en/newsroom/press-releases/2021-01-28-gartner-predicts-40--of-boards-will-have-a-dedicated->.

## METHODOLOGY AND PARTICIPANT PROFILE

A total of 180 respondents drawn from the HBR audience of readers (magazine/ newsletter readers, customers, HBR.org users) completed the survey.

### Size of Organization

**28%**  
Fewer than 100 employees

**12%**  
500 - 999 employees

**14%**  
1,000 - 4,999 employees

**9%**  
5,000 - 9,999 employees

**25%**  
10,000 or more employees

### Seniority

**28%**  
Executive management

**34%**  
Senior management

**35%**  
Middle management

All other grades less than 2% each.

### Key Industry Sectors

**15%**  
Technology

**13%**  
Financial services

**14%**  
Manufacturing

**10%**  
Government/ not-for-profit

All other sectors less than 8% each.

### Job Function

**18%**  
General/executive management

**11%**  
IT

**11%**  
Consulting

**8%**  
Sales/business development/ customer service

All other functions less than 8% each.

### Regions

**34%**  
North America

**27%**  
Asia/Pacific/ Oceania

**23%**  
Europe

**8%**  
Latin America

**7%**  
Middle East/Africa

Figures may not add up to 100% due to rounding.



# Harvard Business Review

ANALYTIC SERVICES

## ABOUT US

Harvard Business Review Analytic Services is an independent commercial research unit within Harvard Business Review Group, conducting research and comparative analysis on important management challenges and emerging business opportunities. Seeking to provide business intelligence and peer-group insight, each report is published based on the findings of original quantitative and/or qualitative research and analysis. Quantitative surveys are conducted with the HBR Advisory Council, HBR's global research panel, and qualitative research is conducted with senior business executives and subject matter experts from within and beyond the *Harvard Business Review* author community. Email us at [hbranalyticservices@hbr.org](mailto:hbranalyticservices@hbr.org).

**[hbr.org/hbr-analytic-services](https://hbr.org/hbr-analytic-services)**