How CISOs Can Talk Cyber Risk So That CEOs Actually Listen

MAY 10, 2022

While the usual activities to measure and mitigate cybersecurity risk remain vital, an ongoing challenge for chief information security officers (CISOs) today involves communicating the current situation in a language their senior bosses can understand and act on.

Most C-suite and board members who review cybersecurity preparedness don't have a strong tech background. As they sit through cybersecurity briefings, they often struggle to make sense of a swirl of technical jargon, metrics, and data about network vulnerabilities, **threat hunts**, **phishing tests**, **software patches**, and **risk scores**.

To communicate more effectively, CISOs need to think like CEOs and put the fire hose of information they present to stakeholders in a broader context. After all, senior leaders can't manage what they don't understand.

Download: Organizations struggle to measure and monitor cyber risk

The language of the C-suite or boardroom is all about the bottom line, argues Bob Zukis, founder and CEO of Digital Directors Network, an organization dedicated to enhancing communication between enterprise leaders and security technologists. "You have to talk about cyber risk in economic terms," Zukis said in a **recent report** by *Harvard Business Review* Analytic Services, sponsored by Tanium.

The report surveyed 180 respondents from middle, senior, and executive management levels at enterprises of different sizes across a range of industries and regions. It includes interviews with experts immersed in the world of digital risk.

While the current communication breakdown leaves CISOs frustrated, executives puzzled, and actionable data lost in translation, cybercriminals are taking advantage. More than half of survey respondents (57%) reported an increase in cyberattacks since the start of the pandemic, with 19% noting that such attacks have increased significantly.

> **You have to talk about cyber risk in economic terms.**
>
> Bob Zukis, founder and CEO, Digital Directors Network

The pandemic-related shift to working from home only added fuel to the fire, as many organizations suddenly found themselves managing a wave of new endpoints and connections they often failed to secure appropriately.
CISOs must bridge the gap between what they say and what executives hear. The good news, say experts, is that both sides are willing to learn, and there are signs the gap is narrowing. Here are three core ideas successful CISOs have relied on to find a common language that everyone can understand.

Joseph V. Amodio

Joseph V. Amodio is a veteran journalist, television writer, and the Editor-in-Chief of *Focal Point*. His work has appeared in *The New York Times Magazine*, *Men's Health*, *Newsday*, *Los Angeles Times*, *Chicago Tribune*, CNN.com, and Barrons.com, and has been syndicated in publications around the world. His docudramas have aired on Netflix, Discovery, A&E, and other outlets, and he has appeared on *Good Morning America*, NBC 4 New York, and NPR's *Morning Edition*.

Key takeaways

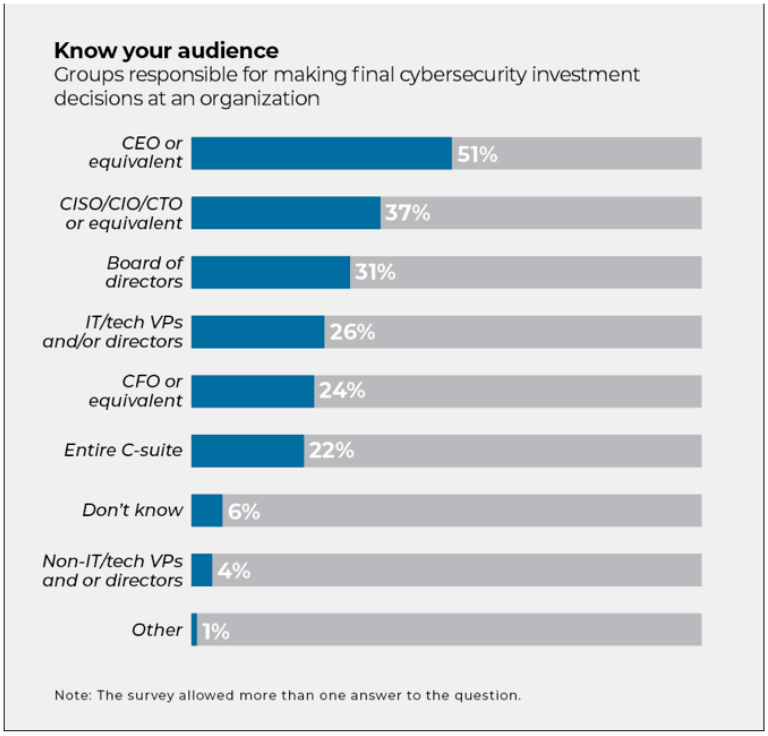
- Lighten up on jargon; keep language clear, accessible, and focused on the bottom line.
- Stick to a common framework and use consistent measures of risk scoring each quarter.
- Make sure all your metrics and presentations tell a story, so your message hits home in a visceral way.

Focal Point

Dedicated to helping business executives and IT leaders effectively use technology to connect with customers, empower employees and achieve better results.

Communicating cyber risk means focusing more on business value

The majority of those who make the ultimate decisions about cybersecurity investment come from outside the field. According to the *HBR* survey, cybersecurity spending is controlled at the CEO level in just over half the companies surveyed (51%). Technology leaders like CISOs, chief information officers (CIOs), and chief technical officers (CTOs) hold the purse strings at a little over one-third of organizations (37%); VPs and directors focused on IT or tech weigh in at about a quarter (26%) of firms.



When it comes to head counts, supply chains, and regulations, CEOs and boards are used to talking numbers. But when CISOs do the numbers, they often tie them to harder-to-decipher technical metrics, such as zero days identified or percentages of phishing attacks foiled. Things go further awry when they mix in acronyms and jargon like DDoS (**distributed denial of service**), XEM (**converged endpoint management**) or AWS EC2 (**Amazon Web Services Elastic Compute Cloud**).

It's a bit like describing a cricket match to a baseball fan. Both games feature a bat, a ball, and people running around. But cricket uses its own insider vocabulary like "grubbers," "nurdles," and "dibbly-dobbly bowlers."

> **Are we spending too much or too little on cybersecurity? That is the wrong question.**
>
> Zukis

Instead of loading up on jargon, experts recommend keeping language clear, accessible, and focused on the bottom line.

CISOs make headway with higher-ups when they rely on metrics that are actionable and are tied not only to security tools but also to security effectiveness. For example, they explain how phishing percentages or XEM systems can protect and enhance the value of an enterprise. Still, many CISOs don't illustrate that connection to business value.

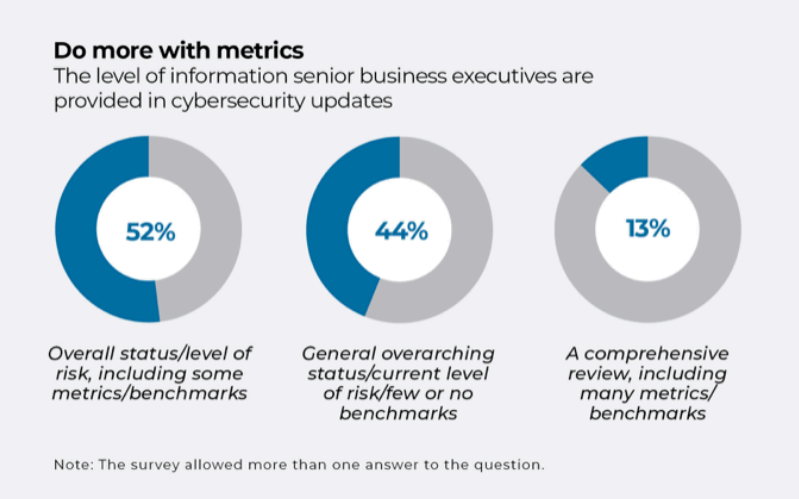
[Read also: 3 cyber hygiene practices that federal CISOs must adopt]

Even familiar financial metrics can be misleading without context. While business leaders may ask, "Are we spending too much or too little on cybersecurity?" the truth is less black and white. "There is no right number," Zukis explains in the report, "and that is the wrong question."

Rather, leaders must take a radically different view of investment. Using data from **asset discovery and inventory** and **automated endpoint management** systems, among other tools, CISOs can help senior executives identify the value at risk in their enterprise, how much of that value is protected based on existing spending, and how protection may change over time.

Cyber risk scoring is clearest when it's consistent

While an overreliance on technical metrics can confuse senior leaders, a significant number of enterprises offer few metrics at all. Of the executives updated regularly on cyber risk, nearly half (44%) in the *HBR* survey received only a general overview, with little or no metrics or benchmarks. Only 13% received a comprehensive review, featuring a variety of metrics and benchmarks.



Security leaders often switch up the metrics they present, further complicating matters. In one meeting, they may focus on maturity, the next on risk quantification, and later on a different metric. "Organizations mix and match them rather than consistently applying one approach," says Emily Mossburg, global cyber leader at Deloitte. She argues in the *HBR* report against such a scattershot approach.

CISOs may offer different perspectives on risk or test new ways to present information in order to interest executives or improve understanding. But the end result may leave them even less certain about risk. Executives don't know whether the organization is doing better or worse from one quarter to the next.

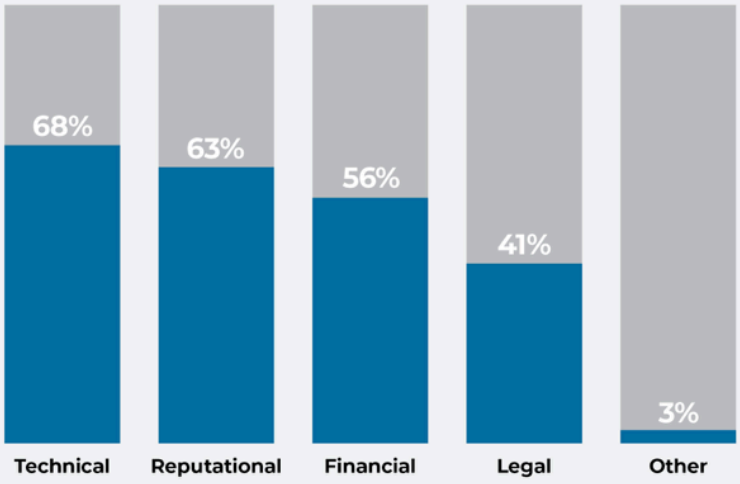
[Read also: As cyber crisis mounts, CISOs and boards must learn to communicate]

A more productive approach is to help executives from the technical and business sides agree on a common framework and use consistent measures of risk scoring from quarter to quarter.

Endpoint vulnerability must be calculated, predicted, and—most of all—*felt*

Among business executives briefed with metrics, most (68%) are weighted down with technical data, according to survey respondents. Reputational metrics (63%) also receive a lot of attention, with financial metrics only a factor at about half (56%) of the organizations surveyed.

Tell a story
Types of metrics senior business executives are provided in cybersecurity updates



Note: The survey allowed more than one answer to the question.

Boosting financial metrics may help, but the last word on metrics is that they're not the last word. The problem with metrics, experts warn, is that it's too easy to get lost in them.

"You have to make sure you are telling the story," says Alissa Abdullah in the *HBR* report. As deputy chief security officer and senior vice president of emerging corporate security solutions at Mastercard, she's used to winning over skeptical execs. "All these risk metrics mean nothing if you're not telling the story," she says.

> **All these risk metrics mean nothing if you're not telling the story.**
>
> Alissa Abdullah, deputy chief security officer and senior vice president of emerging corporate security solutions, Mastercard

For executives focused on top-line revenues and bottom-line profits, getting a sexy new product or service to market will always seem more appealing than spending money on something as abstract as cybersecurity. Storytelling can help combat that tendency. At Mastercard, management and the board join in crisis simulations, and also walk through an actual cyberattack, so that what might seem theoretical hits home on a visceral level.

"Cybersecurity can be overwhelming," Abdullah admits. She urges security executives to share stories and experiences that will stick with their audience. "They need to have that 'Oh, no' moment," she says. "Once they've lived it, they understand it and remember it."