The CISO Report

The path to digital resilience starts with your board

splunk>
a CISCO company

CISOs live and breathe risk every day. We combat malware, stop malicious insiders, and enforce compliance.

But being out of step with your board presents another kind of risk. If we can't articulate the potential impact of security issues, they'll probably continue to pose a threat.

This is the quintessential challenge for CISOs and their boards — telling our security story at the right altitude to people who can support our vision. In this year's CISO Report, we put this relationship under a microscope to find out what each thought about their other half. The survey confirmed a trend we've been seeing in recent years that CISOs are interacting more with boards.

However, there are still many areas of misalignment, including what skills are most important for CISOs to develop, how CISOs spend their time, and what strategies are effective in persuading our boards for additional budget.

To bridge these gaps, CISOs will have to speak the same language as their boards. In my experience, that means getting a lot more face time with them and other company leaders to understand the business better and make security a business enabler. CISOs who can attach security to revenue and know what keeps the board up at night will demonstrate they have skin in the game and can offer solutions — not just problems they need the board to solve.

We hope that The CISO Report will be a resource for you to tell your story, bridge communication gaps, and earn the board's support for your security program.

Michael Fanning

CISO, Splunk

Contents

The start of a beautiful friendship?

Oil and water. Mars and Venus. Whatever the metaphor, CISOs and their boards are inherently different beings whose backgrounds can feel worlds apart.

Business leaders' bottom-line concerns often conflict with CISOs' insistence on vital cybersecurity investments. Even a slight misunderstanding of priorities can cause sizable divisions down the road, and CISOs and boards will end up in very different places than they intended.

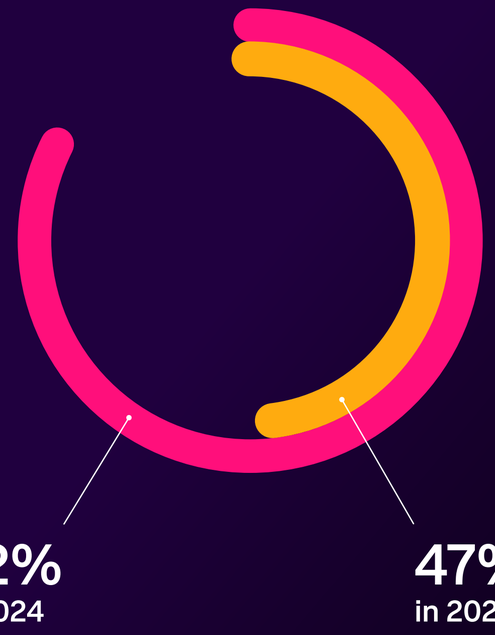
The CISO-board relationship is deepening as they have more opportunities to engage on matters of cybersecurity and enterprise risk. Most CISOs (82%) now report directly to the CEO, a significant increase from 47% in 2023. The two are like neighbors evolving from acquaintances to close friends, discovering common interests over time as they chat in the driveway.

Despite the gaps, they share a duty to safeguard the company. Boards protect profitability and stock price; CISOs protect data and systems. This is something to build on. But it will take communication, understanding, and a generous dose of patience to come together.

To thrive, each party will have to step out of their comfort zone and learn the other's language. For CISOs, that means understanding the business beyond the surface and finding new ways to convey the ROI of security initiatives to their boards. For board members, it means committing to a security-first culture and consulting the CISO as a primary stakeholder in decisions that impact enterprise risk and governance.

When CISOs and boards realize their joint mission, they become unstoppable allies who can propel the organization on its path to digital resilience.

More CISOs are reporting to the CEO



CISOs settle into the C-suite

As more CISOs report directly to the CEO, they cement their place in the C-suite and the boardroom, weighing in on strategic business decisions. This elevated status, however, has had its share of growing pains. Like many relationships, one partner thinks they have a slightly better rapport than the other.

Looking broadly at how CISOs measure up, 84% of board respondents claim CISOs meet their expectations. That sounds positive at first glance. Given security chiefs' complex challenges, is it enough to meet boards' tough standards of excellence? Presumably, CISOs who go above and beyond would generate more confidence, but only 8% of board respondents said CISOs exceed expectations.

When we dig into the relationship details, survey data shows that CISOs consistently think they're better positioned with the board on core responsibilities. Compared to board respondents, CISOs feel they're on firmer ground on everything, including hiring and training the security organization, budgeting adequately, and aligning on strategic cybersecurity goals.

CISOs overrate their relationships with boards in key areas

Respondents who said the relationship was *very good* or *excellent*

Boards are business leaders who are very good at managing the business and financial outcomes. But they materially don't understand that their dependency is on technology and the security ramifications of how they're managing technology.

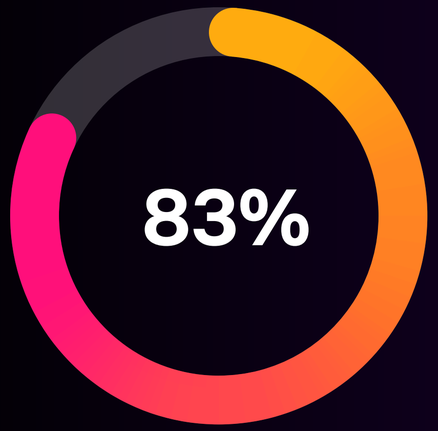
Christopher Kennedy, CISO, Group 1001

But the door swings both ways. CISOs are not exactly confident about the board's cybersecurity prowess. While 60% acknowledge that board members with cybersecurity backgrounds more heavily influence security decisions, not all boards have an authority like that in the room. Only 29% of CISOs said their board includes at least one member with cybersecurity expertise.

These foundational board relationships are where much of the future division starts. A minor disconnect here can grow wider downstream in critical areas like incident response and business growth.

However, some of these perceptions may change given that 83% of CISOs now participate in board meetings *somewhat often* or *most of the time*. It's conceivable this evolution will shape how boards address cybersecurity policy and organizational culture.

Fortunately, the current gaps are not insurmountable. CISOs' regular presence in the boardroom and their counsel on enterprise risk will strengthen board confidence and alignment.



of CISOs now participate in board meetings *somewhat often* or *most of the time*

When I started as a CISO, the big thing was getting a seat at the table with the board. That's changed. Now, there's no argument, discussion, or debate about whether the CISO role should be giving reports directly to the board.

Bruce Foreman, CISO, UMass Memorial Health

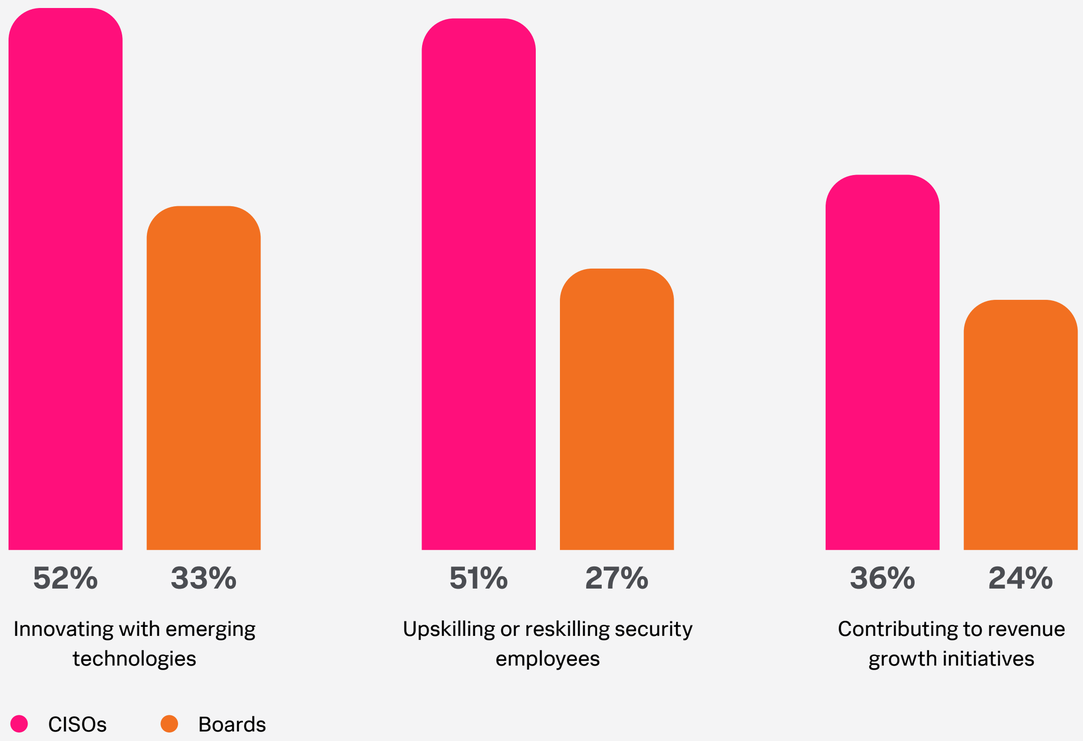
CISOs and boards mind the gaps

Our survey indicates the gap may be narrowing between boards and CISOs on certain security priorities. For example, they are strongly aligned on protecting sensitive company information — 70% of boards and 68% of CISOs say it is *very important* or *of top importance*.

However, serious gaps persist. CISO priorities match up with their technical expertise, shaping how they execute those priorities and ultimately achieve their long-term and short-term goals.

Largest gaps in priorities between CISOs and boards

Responses ranked as *very important* or *of top importance*



Boards want to know: Where does the time go?

With some of the most significant priorities at odds, CISOs and boards also diverge on how CISOs and security teams should use their time and energy to make their goals actionable.

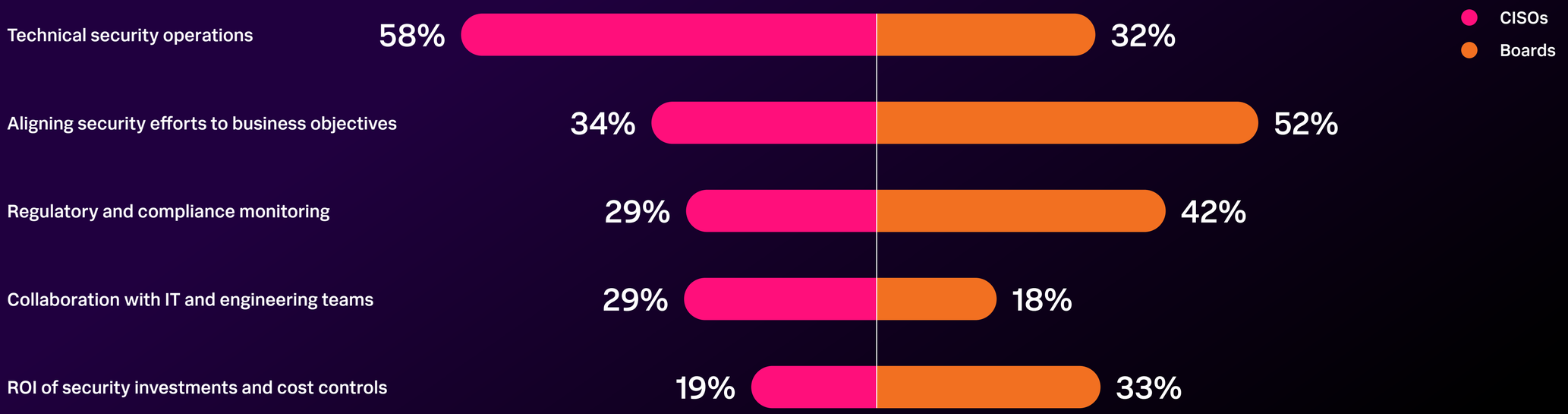
So, what exactly are CISOs doing all day? While 63% of CISOs and boards are aligned, saying CISOs devote the lion's share of their time to security posture and risk mitigation, their perceptions part ways after that. Fifty-two percent of board respondents believe CISOs spend the most time enabling the business — aligning security efforts to business objectives — compared to only 34% of CISOs. In reality, the technical aspects of cybersecurity take up far more of the CISO's time than the board realizes. According to 58% of CISOs, the bulk of their and their team's time goes to choosing, installing, and operating technology.

If a company is not used to the high cost of cybersecurity, then a CISO needs to explain the full duties of the security team to the board and map how security responsibilities are woven through the fabric of the entire business.

Christopher Kennedy, CISO, Group 1001

Perception vs. reality

How CISOs and their teams spend the majority of their time



Business skills help CISOs branch out

Boards have high hopes for CISOs, the biggest one being that they become better business leaders. However, CISOs might view that ambition differently or take alternate paths to get there.

More so than CISOs, board respondents emphasized business acumen and soft skills like empathy and communication as the top skills to work on. For CISOs, collaboration with IT and engineering teams and compliance knowledge were more important development areas.

"Adding on new skill sets to learn and deepen makes the CISO's job more complex, and arguably more challenging," said Marcus LaFerrera, director of SURGe security research team.

This could be why 53% of CISOs say their responsibilities and expectations have become more difficult since they took the job.

Despite CISOs' stature in the executive ranks and boards' desire for them to develop business savvy, boards still may not see beyond their technical credentials. CISOs can change this perception, however. "Unless the CISO has the wisdom and the wherewithal to argue for a more appropriate place in the hierarchal pecking order, I think CISOs are still considered a tech whizzbang role that can 'solve my problems with tech' versus materially understand how our tech drives our business," said Christopher Kennedy, CISO, Group 1001.

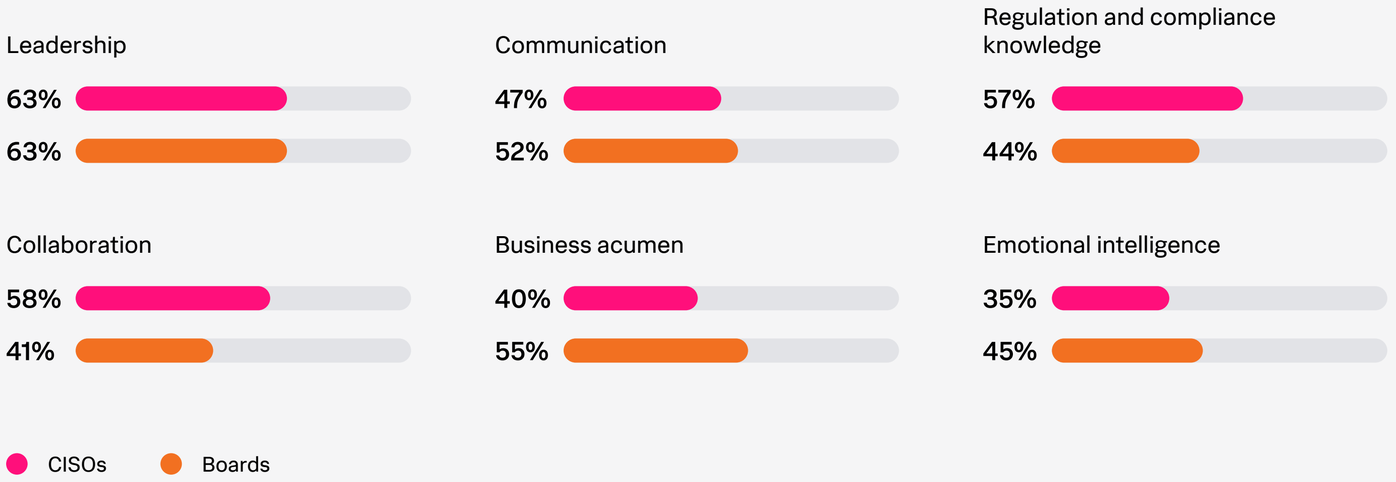
It will be up to CISOs to increase their awareness of business and board priorities and how they relate to revenue and growth objectives. They can bridge divides through proactive and effective upward communication and cultivation of a deeper understanding of the organization's strategy. Once they see the big picture, they can determine how a security strategy should fit into it.

"The CISO has to collaborate and partner with other functions across the company. Security should not be an isolated department. We need to work together with legal, with risks, with heads of business. So the CISO has to be a good communicator," said Chenxi Wang, general partner at Rain Capital and board member at MDU Resources.

53%

of CISOs say their responsibilities and expectations have become more difficult

The skills most important for CISOs to develop



To CISOs and boards, success looks different

In general, boards and CISOs agree that core cybersecurity KPIs, like the number of material security incidents and timeliness of vulnerability management, are important. However, most boards and CISOs (79%) say KPIs for their security teams have changed substantially over recent years.

"The business is changing. We have aspirations to enter into new business models and new business areas, and then we are going to be dealing with consumer data and personal data. My stance has changed because now I see security as a bigger risk than two years ago," said Prasanna Ramakrishnan, global CISO at Clarios.

Boards also have specific standards for evaluating a CISO's performance, like the ROI of security investments. This is likely one reason boards expect CISOs to be strategic rather than tactical, communicating more holistically about how their initiatives impact the business.

"We won't consider moving a security investment forward unless it's a minimum 15% ROI. Otherwise, it will be difficult to justify," said a board member at a U.K.-based multinational banking group.

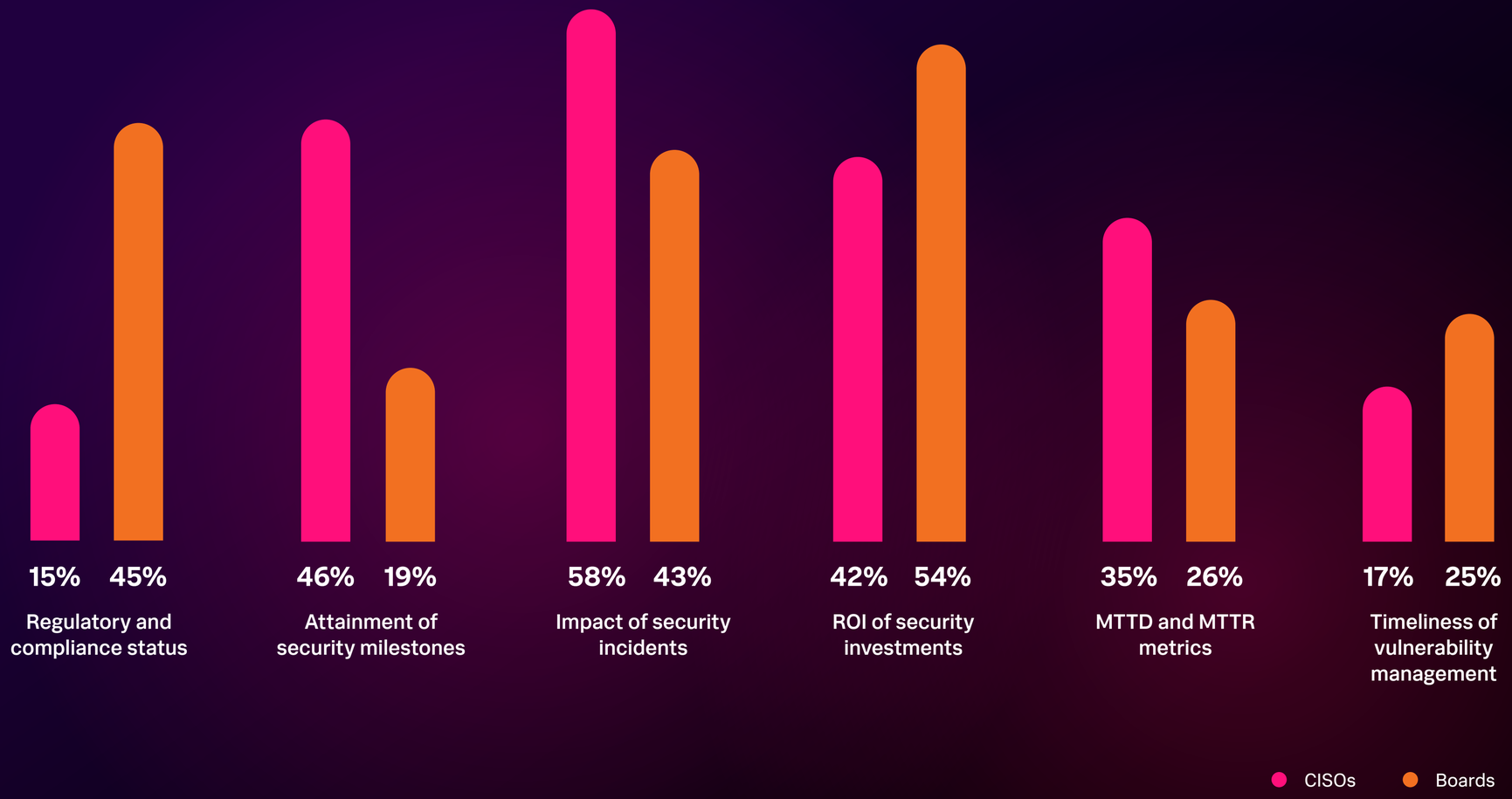
The net-net? For one, boards don't want fire-fighting heroics from CISOs. They're looking for mature, strategic, proactive leadership and business enablement, not just damage control when an incident inevitably occurs. CISOs who can educate the board on how their security KPIs can benefit the business will find more success.

When presenting estimates for future initiatives, CISOs can persuade boards by emphasizing that expenses incurred from lost revenue and reputational damage will likely be less than the cost of downtime from a security incident.

CISOs also need to switch up their tactics to be better heard, using their precious board time to justify the ROI of their security investments and elevate security to a business enabler, not just a cost center.

Kirsty Paine, Field CTO and Strategic Advisor, Splunk

CISOs and boards measure success differently

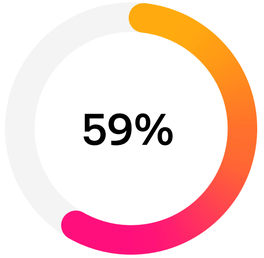


Compliance is getting personal for CISOs

Regulatory environments have become more complex, expansive, and punitive, requiring faster incident reporting and placing more liability squarely on CISOs' shoulders. As a result, they are taking a more rigorous and personal approach to compliance.

Will they or won't they? The friction of reporting non-compliance

It's hardly surprising that CISOs take their organization's compliance posture seriously — a lot is riding on their decisions. After all, CISOs, not boards, will be held most accountable for security incidents. CISOs face more regulatory scrutiny, legal liability, steep financial penalties, and the possibility of losing their jobs if found in violation.



of CISOs would become a whistleblower if their organization was ignoring compliance requirements

Perhaps even more shocking, 21% of CISOs revealed they had been pressured not to report a compliance issue. Thankfully, the majority of CISOs surveyed are willing to step up and do the right thing — 59% said they would become a whistleblower if their organization was ignoring compliance requirements.

"Pressuring CISOs not to report issues, rather than being open and transparent about any failings and lessons to learn, means that risk-based decisions can't be made — the right people don't have the real information. That can be really dangerous," said Kirsty Paine, field CTO and strategic advisor for Splunk, a Cisco company.

Of course, when an incident is considered "material" (and the definition is squishy), companies must report it to authorities within hours to days, depending on where in the world they are operating. Recent mandates, including the U.S. SEC cybersecurity ruling, Europe's NIS2, and DORA, impose much narrower reporting windows — as short as 24 hours in NIS2 — for disclosing cybersecurity incidents. Similarly, Australia's Security of Critical Infrastructure (SOCI) Act requires mandatory reporting within 12 hours after discovering an incident.

When reporting incidents and other compliance protocols, CISOs should work on crisis management well before any crisis occurs. A proactive plan will help align expectations with the board and have a set response for the broader business.

"I think everybody who serves as head of security or in the boardroom for public companies should be concerned about personal liability if they're not doing the right things.

Chenxi Wang, General Partner, Rain Capital and Board Member, MDU Resources

21%

of CISOs have been pressured not to report a compliance issue

CISOs lean into compliance … to a point

In today's rigorous regulatory environment, compliance is becoming an outsized part of a CISO's job. This could explain why 57% ranked "depth of knowledge related to regulations and compliance" as a top skill to develop.

And while maintaining compliance is vital to the business, CISOs don't necessarily think it's the best way to measure their success in overseeing security. Only 15% of CISOs ranked compliance status as a top performance metric, a significant disconnect compared to 45% of boards. Historically, CISOs have not perceived it as a strategic security activity.

This disconnect can mean boards and CISOs talk past each other on compliance. "While boards know compliance is important, many may not fully realize or understand the work required to achieve it. With a lack of day-to-day insight, it's not surprising that board members think it should be 'easy' or are confused when CISOs and their teams take excessive amounts of time to achieve and sustain a strong compliance posture," said Kirsty Paine, field CTO and strategic advisor for Splunk, a Cisco company.

> **"HIPAA and any other compliance — they're check boxes. 'You did this, you're compliant.' But it doesn't mean you're secure, of course. It's a baseline, but I think it's a very low baseline.**
>
> Bruce Foreman, CISO, UMass Memorial Health

Bring better evidence to the budget debate

Cyber budgets reflect inconsistent support and misalignment, dampening CISOs' expectations, frustrating boards, and widening the chasm between them.

Only 29% of CISOs say they receive the proper budget for cybersecurity initiatives and accomplishing their security goals, compared to 41% of board members who think cybersecurity budgets are adequate. Justifiably, CISOs are concerned about how this lack of support will affect their organization's security posture, and 64% reveal that the current threat and regulatory environment make them concerned that they're not doing enough.

When you go to the board to say that we have a potential cyber threat, it's difficult to justify the investment. The usual problem that I face is with the certainty of an investment versus the likelihood of a threat which may not happen.

A board member, U.K.-based multinational banking group

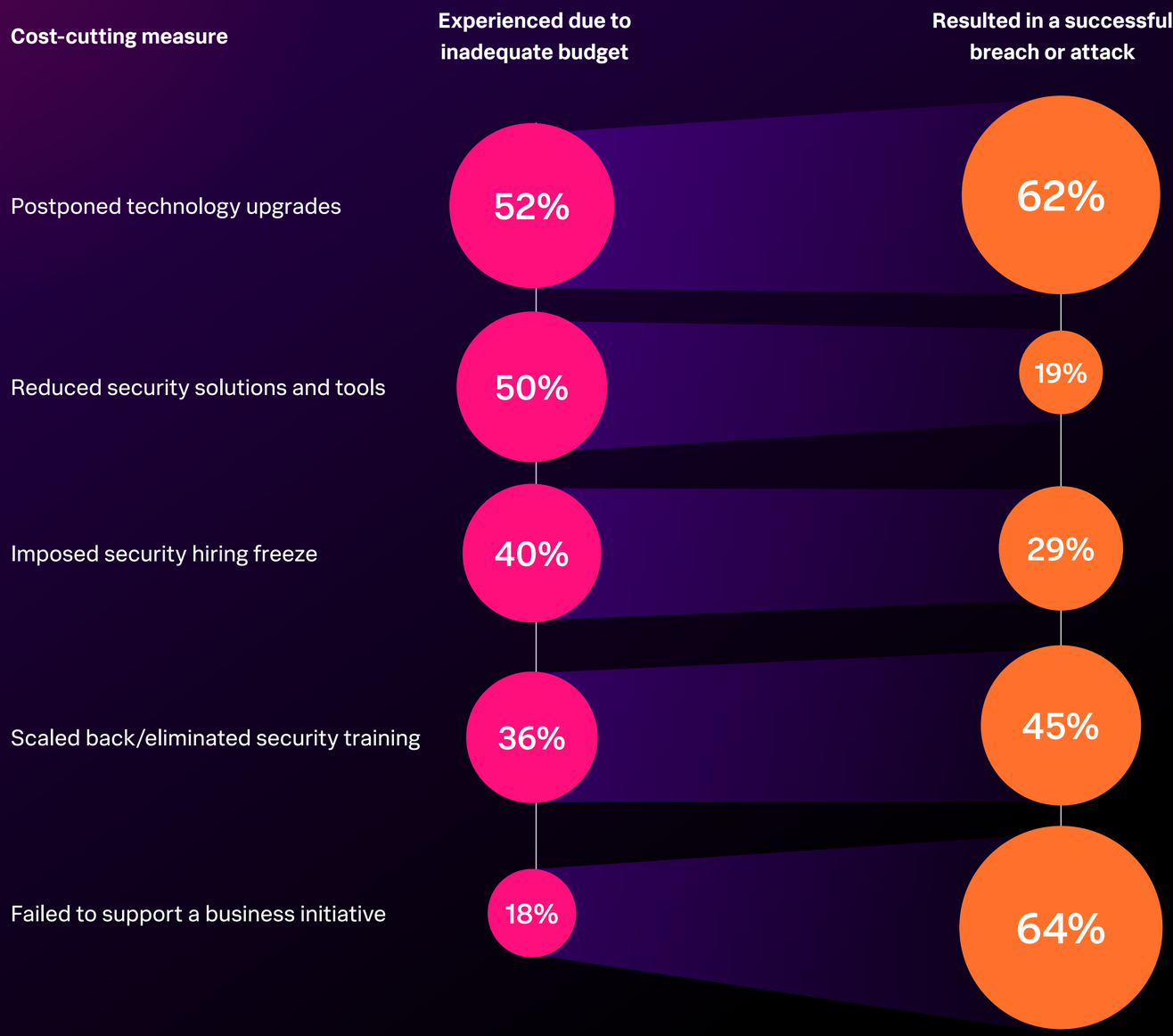
Small cutbacks, serious consequences

Many CISOs enacted cost-saving measures due to inadequate budgets. Some of the most substantial cuts included postponing a security update, reducing the number of solutions to reduce license costs, and freezing promotions, raises, and hiring. But these security cutbacks don't simply fly under the radar — they often come with severe consequences, such as successful security attacks or data breaches.

Meanwhile, cyberattacks show no signs of slowing down. A whopping 94% of CISOs report being victims of a disruptive cyberattack. The majority, 55%, report experiencing them at least *a couple of times*, and another 27% said they were victims *many times*.

Proper funding will be crucial to ensure adequate cyber defenses, with CISOs maintaining that the most significant area of future investment will be in cyber risk management (64%). These and other new investments in infrastructure, tools, solutions, and services will be key in helping CISOs and their teams protect their organizations' data and systems.

Inadequate security budgets come with consequences



CISOs champion security by speaking “board”

So what really convinces boards to open their wallets? Many boards state that they prioritize business growth (44%) over strengthening the cybersecurity program (24%), which means they’re inclined to back cybersecurity initiatives that provide the most value to shareholders and the organization. Presenting security as a business enabler is the most potent argument by far, with boards at 64%. But only 43% of CISOs claim they engage in this practice.

To get what they want, CISOs will have to learn how to evangelize what they need in a way that is compelling to the board. In short, they need to learn how to speak board — fluently.

CISOs can get boards to listen and respond to budget requests by presenting them with concrete calculations on direct and secondary costs of downtime, including lost revenue, SLA fines, and factors that will impact shareholders. Downtime costs Global 2000 companies $400 billion annually, averaging $200 million per company, or about 9% of profits.

Forty-six percent of boards say these types of costs are convincing in budget discussions. While 39% of CISOs already do this, there are still ample opportunities for them to refine their powers of persuasion, such as presenting cyber risk metrics and recommendations that guide management decisions and educating the board on the impact of cyberattacks.

As the old adage says, money talks. And, if allocated correctly, it can prevent costly breaches and compliance violations that can potentially save your organization’s reputation and millions of dollars down the road. The winning communication strategy is to explain how security drives ROI, helps the business grow, and protects share prices. That will get your board’s attention, every time.

CHAPTER 5

AI empowers defenders and adversaries

For CISOs and boards alike, AI is fraught with both uncertainty and potential. They agree it is worthy of current and future investment. Still, a significant portion of CISOs feel they aren't moving fast enough on AI to stay competitive or keep pace with innovation.

AI can be a security force multiplier for malware analysis, threat detection, configuration standards, and other functions — but only if CISOs help their boards see the possibilities and motivate them to invest further in infrastructure, training, and governance.

AI gives cyber adversaries an edge

AI still presents a threat on the cyber frontier, with 53% of CISOs believing it will give attackers a slight or significant advantage. However, that group is noticeably shrinking from 70% in 2023.

The most worrisome perceived AI threats are more realistic phishing attacks and deep fakes (57%), followed by new malware strains (44%), adaptive social engineering attacks (40%), and exploitation of existing generative solutions (40%). And the fear, especially regarding the threat of deepfakes, isn't unfounded. Social engineering is already the most common attack vector experienced in the past year at 67%. It's conceivable this type of attack will grow as AI continues to emulate human behavior and speech more convincingly.

The most concerning generative AI threats for CISOs

- **57%** Highly realistic phishing emails
- **44%** New malware that can evade cybersecurity
- **40%** Adaptive social engineering tactics
- **40%** Exploitation of gen AI tools used by company
- **38%** More automated and efficient attacks
- **33%** Faster brute force attacks
- **30%** Realistic voice and image deep fakes

AI's endless possibilities

Despite their concerns about AI in the hands of threat actors, the majority of CISOs recognize its promise, calling AI *appropriately hyped* (70%) or even *underhyped* (21%).

CISOs and their teams often get so caught up in a defensive game of whack-a-mole with cyber attackers that daydreaming about future investments can sometimes feel like an indulgence. As luck would have it, the rise of AI as a cyber defense tool will allow them to be more forward-thinking.

Twenty-two percent of CISOs say AI will give cyber defenders a slight advantage over attackers. Most CISOs (53%) also believe they're adopting AI at the right pace, although more than a third (38%), believe they're not moving fast enough. Boards also maintain that their organizations are either currently using AI for cybersecurity (24%), have immediate plans to use it in the next year (41%), or have an interest in doing so (33%).

Many CISOs are laying the groundwork for new, AI-driven cyber defenses. Almost two-thirds (65%) of CISOs are actively training security teams on prompt engineering. Additionally, more than half (56%) are establishing protocols to determine which tasks are appropriate for AI and which are better suited for humans.

Looking ahead across use cases, AI will be a hefty area of future investment for CISOs and their boards. Thus, CISOs have many chances to highlight the ROI of this tool as a business enabler. Showing that AI will increase competitiveness and time to market will go a long way toward getting board buy-in. It might even increase budget allocation.

Top security use cases for generative AI according to CISOs

47%
Malware analysis, threat detection, and alert enrichment

39%
Creating security software configuration standards

32%
Creating threat detection rules

30%
Analyzing data sources to reducing alert noise

30%
Proactive threat hunting

28%
Creating security reports for internal communication

25%
Developing cybersecurity policies

CHAPTER 6

It’s magic when CISOs and boards align

As cybersecurity has grown into a standard component of business decisions, having a board member or two with security expertise is advantageous. By virtue of proximity, having a CISO on the board or one with cybersecurity expertise is prone to strengthen the CISO-board relationship. Because of their deep security knowledge, board members with a CISO background might feel more confident about the organization’s security posture — they are far less likely than other board members to express concern they are not doing enough to protect the organization (37% versus 62% survey average).

Having their feet in both worlds allows them to paint an accurate picture of the organization’s security posture, make a better case for future investments, and illustrate how cybersecurity drives the business forward.

However, simply putting a CISO on the board won’t necessarily be a panacea for security shortcomings. It’s likely that a company that takes security seriously will also have a CISO or someone with a security background on the board, which reflects a dedication to improving security culture and a willingness to adopt related initiatives.

But whether they sit on a board or not, CISOs in good standing with their board get noticeably more mileage from their relationships.

Having board members with a CISO background is a relationship advantage

Areas where relationships were ranked as *very good* or *excellent*

Communication boosts collaboration … and budget

It's not just board relationships that function better when CISOs regularly interface with the board, albeit those relationships clearly benefit both parties. CISOs with healthy board relationships benefit from better collaboration throughout the organization, reporting particularly strong partnerships with IT operations (82% versus 69% of other CISOs) and engineering (74% versus 63% of other CISOs). This may be because they can effectively communicate the board's business needs and strategies to more technical departments in a way that connects them to the rest of the organization.

CISOs with good board relationships are also bestowed greater trust to test and explore new technology investments. They are more likely to be given the ability to pursue use cases for generative AI, such as creating threat detection rules (43% versus 31% of other CISOs), analyzing data sources (45% versus 28% of other CISOs), incident response and forensic investigations (42% versus 29% of other CISOs), and proactive threat hunting (46% versus 28% of other CISOs).

CISOs are critical liaisons, translating the language of technology-driven departments and championing security in a way that boards can understand and vice versa. Going forward, they'll have even more opportunities to build upon and strengthen those relationships. Boards have shown they are willing to learn simply because it makes sense for their business strategy, practices, and investments. That means CISOs can lean further into shaping the business through cybersecurity.

CHAPTER 7

Clear the path to partnership with your board

The journey continues for CISOs and boards. They have made great strides to harmonize goals, priorities, and business strategies. Yet, there is an opportunity to narrow gaps.

Here are a few fundamental steps CISOs can take to help drive alignment and ensure stronger, healthier, and more productive board relationships.

1

Educate your board on what you're doing (and why)

There is always room for boards to sharpen their security expertise. That especially holds true when discussing strategy around incident response, which will not only give them a window into standard procedures at any given time but will also illuminate the value of those procedures when facing auditors or during a crisis.

So, create tabletop exercises to make it real. Use visuals and storytelling to make your message land. Then develop a strategy and cadence, and follow through on your plan with iterative sessions.

2

Boost trust (and budget)

It won't hurt to practice speaking "board." While boards benefit from your cybersecurity expertise, it's on you to make them understand your needs and priorities. Emphasize ROI over MTTD and learn how to communicate the value of your investments and the importance of resource allocation effectively. (Maybe it's harder to do, but when was security ever easy?)

You'll also want to dive deep into topics like protecting revenue and shareholder value, minimizing business disruptions, improving brand trust, and delivering secure and seamless customer experiences. Boards care about growing the business, so speak to their KPIs.

3

Own compliance and know your personal liability

CISOs face a more rigorous and punitive regulatory environment, so it's wise to be prepared. That means knowing your personal liability, potentially retaining a lawyer in the event of an incident, and taking a strategic and well-documented approach. Articulate risks to the board and why material events require reporting in the first place.

You should also know what boards expect in a crisis, codify these expectations in writing, and make sure all parties agree before an incident occurs, not during. Re-read your employment contract, and if there are any gaps, close them.

4

Expand your scope to include business strategy

We know that stepping out of your comfort zone isn't easy. However, by taking on the role of business strategist, you'll discover how to balance business needs while protecting your organization. Because if you want to grow security, you must show how security grows the business.

And it's not just developing business acumen, although you will need that in spades. Develop your soft skills. This includes honing more effective means of communication and understanding how your board prefers to receive information. Refining emotional intelligence will also go a long way.

5

Build leadership across the business, not just within security

CISOs and boards agree on the importance of leadership skills. This means managing up by understanding what matters to the board and why. It also involves effective communication with HR, legal, and the C-suite, who are crucial to advancing your priorities and securing larger tech investments.

To build strong relationships, map out stakeholders, spend time with them, and show genuine interest in their work and challenges. Collaborate on major initiatives so that when a crisis arises, your colleagues will already see you as a team player and be eager to support your efforts.

Become a security leader with Splunk

Perspectives by Splunk — by leaders, for leaders

Looking for more thought leadership and insights from CISOs? Learn how security leaders address today's most critical challenges, including regulatory compliance, AI, and the evolving threat landscape.

Get executive insights

State of Security 2024: The Race to Harness AI

Discover how security leaders and professionals navigate opportunities and obstacles such as compliance mandates, talent shortages, and the rise of generative AI.

Read the report

Industry appendix

Manufacturing

Compared to their industry counterparts, manufacturing CISOs feel less supported by their C-suite, generally expressing less optimism about their collaboration and cybersecurity budgets. This lack of support could be a factor in why manufacturing experiences more cyberattacks than other industries.

CISOs are less likely to say their C-suite supports the cyber team's strategy and advocates for its policies (41% versus 57% of CISOs in all industries). And they are also less likely (52%) to feel like their cyber teams' KPIs are important to their boards, versus 64% across all industries.

As for cybersecurity funding, only 20% of manufacturing respondents say their organizations provide adequate cybersecurity budgets, and just 50% feel like they can convince their boards to increase their teams' budgets when needed. Manufacturing's spending lags behind the global average, with $65 million in expected annual spending versus $75 million.

With limited support and less strategic buy-in for cybersecurity, manufacturing organizations may be increasingly prone to vulnerabilities such as stolen credentials (reported by 58% of their CISOs) and undefined incident response processes (44%), which have led to successful attacks. Ninety-five percent of the sector report being hit with cyberattacks multiple times in the past 12 months (compared to 82% of organizations across all sectors). Despite these attacks, just 9% of boards in the industry cite strengthening their cyber program as the most meaningful future investment.

It may be that manufacturing boards are more preoccupied with the geopolitical landscape. Thirty-six percent of them (compared to 25% across all industries) perceive geopolitical instability as the greatest risk to the organization, possibly because manufacturing is globally distributed and affected by supply chain disruptions.

To get on the same page with their boards, manufacturing CISOs have opportunities to increase focus on regulatory compliance. Sixty-four percent of boards cite compliance as a top metric for CISOs' success, yet just 26% of CISOs report their team spends extensive time and effort on legal and regulatory issues.

Financial services

CISOs in financial services tend to have more successful relationships with their boards than other industries. They understand that the ROI of security investments indicates their success (60% agree) — an essential metric boards use for assessing CISO performance (64%).

But the industry is not without its share of struggles. Financial services are more likely than any other industry to fall victim to ransomware attacks, with 65% experiencing at least one in the past year, compared to 48% of organizations across all industries. As ransomware attackers eye lucrative prizes, boards in this sector prioritize strengthening their cyber programs. Fifty-five percent will focus on cybersecurity as their number one investment priority, compared to 24% of boards across all industries — with some of the widest gaps including third-party and supply chain security (68%) and cloud infrastructure (56%).

CISOs often have a seat at the table, as 42% participate in board meetings most of the time (compared to 20% of CISOs from all industries). And when they collaborate on the cybersecurity budget, their boards are more likely to rate this aspect of their working relationship positively. Seventy-three percent think the board-CISO partnership is effective, compared to just 32% of boards from all industries. The health of this partnership may influence the sector's greater level of investment in cybersecurity. Financial services organizations average $105 million in annual cybersecurity spending, well ahead of the $75 million average for all industries.

Another area where financial services leads is generative AI. FSI respondents were likelier to believe that cyber defenders would gain an advantage over adversaries when using the new technology (44% versus 25% of respondents from all sectors). This optimism translates to greater generative AI adoption, as 46% of boards in financial services say their cybersecurity teams are using generative AI, compared to only 24% in all industries.

Communications and media

The CISO-board relationship in the communications and media sector is complex. While CISOs have some direct contact, they don't often participate in board meetings. And though cybersecurity teams seem to get adequate funding, many organizations in the industry haven't made investments in proper cybersecurity measures that would prevent successful attacks.

While most CISOs in the communications and media industry are meeting their boards' expectations, a troubling 9% are "significantly underperforming" (compared to 1% of CISOs across all industries). This may be driven by how communications and media CISOs are less likely to align their team's priorities to the board's security priorities (51% do so versus 62% of CISOs across all industries).

CISOs also struggle to communicate progress against their security goals to their boards. Thirty-five percent of CISOs say this area of their working relationship is very good or excellent, while only 27% of their boards say the same. This misalignment could be rectified if CISOs had more face time during board meetings to provide greater transparency into cyber initiatives and ensure that they align with the board's priorities. While 78% of CISOs have "at least some direct contact" with their boards, only 7% of communications and media CISOs participate most or all of the time in board meetings.

Despite CISO-board challenges, communications and media boards are willing to increase investment in cybersecurity, with 100% saying they will likely boost funding for cybersecurity over the next three years (versus 89% across all industries).

Going forward, steady financial support from the board will be critical. Over the last 12 months, 49% of communications and media organizations experienced disruptive cyberattacks many times, versus 27% across all industries. The most common attack types include social engineering (69%), DDoS (44%), and account takeovers (40%). To address these threats, CISOs and boards would benefit from prioritizing better security training aimed at improving password hygiene and helping employees recognize phishing scams and other social engineering attacks.

Public Sector

In many areas, public sector CISOs and their boards aren't in step when it comes to cybersecurity. While 80% of boards think their CISOs spend extensive time on business enablement, only 26% actually do. And although 51% of CISOs think they're able to successfully create a plan of record with their boards, only 20% of their boards agree.

To improve consensus and alignment, public sector CISOs need to understand how strongly their boards value operational efficiency. Eighty of public sector boards rank it was *very important* or *of top importance*, compared to 29% of all boards who say the same. Prioritizing operational efficiency makes sense, considering the sector often struggles with limited budgets and staffing. Public sector cybersecurity spending averaged $55 million in 2024, compared to $75 million across all industries.

When evaluating CISOs' performance, boards emphasize the ROI of security investments as a key metric (80% of public sector boards versus 54% across boards of all sectors). Looking ahead, CISOs will need to better communicate the value of their security investments, a shift that will set them up for success with their boards as they present KPIs, advocate for future investments, and create security roadmaps. Aligning on how to advocate for the budget will also help CISOs and their teams address the deluge of social engineering attacks, the most common attack type affecting 72% percent of public sector organizations.

Future cyber defense strategies could also include AI. CISOs and boards in the public sector are on the same page about investing in that technology and speeding adoption. While none are currently using generative AI for cybersecurity use cases, 100% of public sector boards state they are either planning to or interested in doing so over the next twelve months.

Region appendix

North America

CISOs in North America typically have strong working relationships with their boards. With greater alignment on priorities and budgeting compared to those in other regions, 71% of North American CISOs report being directly aligned with their board's priorities, compared to 62% globally. North American boards are also more sympathetic to the challenges of their CISOs' jobs than their global counterparts, with 67% observing that CISOs' responsibilities and expectations have become more complex.

When the board understands the CISO's role, and when the CISO, in turn, understands the board's priorities, their working relationship improves — and so does the budget. North American organizations said their cybersecurity budgets are adequate (44% versus 31% globally). Their CISOs also say they can convince boards to increase the budget if needed (68% versus 59% of CISOs globally). Indeed, North American organizations have fuller purses, with expected annual cybersecurity spending to average $110 million, compared to $75 million globally.

Since CISOs in North America seem to understand what boards value, they can better deliver and meet their boards' expectations. Fifteen percent of boards in North America say their CISOs are overperforming, compared to 8% globally. There is, of course, opportunity for progress. CISOs in North America can better succeed by emphasizing the ROI of their security investments during conversations with board members. While 55% of their boards cite this as a metric to evaluate CISO success, just 35% of CISOs rank it as a top performance indicator.

To stay competitive on the global stage, North American organizations will need to increase generative AI adoption. Just 15% of board members in the region use the technology for cybersecurity, compared to 24% worldwide. This finding contrasts with how more than half (54%) of respondents in the region believe generative AI will give cyber adversaries an advantage. Looking ahead, North American CISOs may need to prioritize AI adoption to keep pace with competitors and outpace cyber attackers.

Europe

Compared to CISOs globally, European CISOs can better champion their respective cybersecurity organizations and invest in advanced technologies like generative AI. European boards are more likely to have a subcommittee focused on cybersecurity (55%) than other global counterparts. CISOs in Europe are also more likely to participate in board meetings at least somewhat often (87%) than their counterparts in other regions.

Despite these positive trends, CISOs in Europe have room for improvement when advocating for cybersecurity initiatives and funding increases. Forty-nine percent are less likely to report that their working relationship with the board is going well, lower than the global average. Most think the best way to champion investments is by discussing cyber risk metrics and recommendations (55%) and compliance requirements (49%). However, their boards are more likely to approve budget increases when CISOs demonstrate security as a business enabler (58%) and outline the costs of downtime (56%).

Some of these budget increases might be directed toward generative AI adoption for cybersecurity, an area in which Europe is ahead. Thirty-nine percent of organizations in Europe have implemented AI for cybersecurity initiatives, compared to 24% globally. European CISOs are also ahead in establishing protocols to determine the tasks best handled by AI and those better addressed by team security members.

When it comes to ransomware attacks, European organizations are also better insulated. Just 3% of those who experienced a ransomware attack pay the ransom directly (lower than the global average), and 23% say cyber insurance covers them in the event of an attack (more than respondents from all other regions).

APAC

APAC CISOs tend to have weaker relationships with their boards than their global counterparts, seeing less success when championing cybersecurity and advocating for budget increases. Few say their boards are very likely to support increasing the organization's investment in cybersecurity over the next three years (18% of APAC CISOs versus 27% globally).

Meanwhile, APAC boards are less likely to rate strengthening their cyber program as a high investment priority for the next 12 months (9% of them versus 24% of boards globally). Instead, the C-suite in APAC is more focused on business growth, with 38% citing it as the number one priority.

One advantage that APAC CISOs have is that they participate more frequently in board meetings, as 22% indicate they are present at most or every board meeting. If they refocus their conversations to educate boards on cyber threats, their boards may be more likely to support budget increases or back a new cybersecurity initiative.

Another challenge APAC organizations face is compliance. Twenty-eight percent of CISOs in this region say they've been pressured not to report an incident or compliance issue, the highest of any region. This may be partly because APAC lags in establishing clear governance for cybersecurity incident reporting; 40% of organizations in the region have defined clear incident reporting protocols, which falls behind both other regions.

When asked to what extent their organization uses generative AI for cybersecurity today, 18% of boards in APAC report using it somewhat, lagging behind the global average. But that may change very soon. Forty-four percent of boards plan to apply generative AI for cyber defense purposes within the next 12 months, and another 35% expressed interest in the idea.

Methodology

Oxford Economics researchers surveyed 600 respondents (500 CISOs, CSOs, or equivalent security leaders and 100 board members) in June and July of 2024. Respondent categories included CISOs who self-identified as board members. Respondents were in Australia, France, Germany, Italy, India, Japan, New Zealand, Singapore, the United Kingdom, and the United States. They also represented 16 industries: agriculture, business services, construction/engineering, education, energy and utilities, financial services, government, healthcare, life sciences, information services, technology, manufacturing, retail, consumer goods, telecom, and media and communications. Oxford Economics also conducted eight in-depth interviews with CISOs and board members for qualitative insight.

About Splunk

Splunk, a Cisco company, helps make organizations more digitally resilient. Leading organizations use our unified security and observability platform to keep their digital systems secure and reliable. Organizations trust Splunk to prevent infrastructure, application, and security incidents from becoming major issues, recover faster from shocks to digital systems, and adapt quickly to new opportunities.

Keep the conversation going with Splunk.

splunk> a CISCO company

25_CMP_report_CISO-report-2025_v12