The CISO Report

Emerging trends, threats and strategies
for today's security leaders

splunk>

Executive summary

Splunk sits at the heart of Security Operations for many of the world's largest and most complex organizations. We spend our days helping CISOs and their teams get ahead of emerging threats, respond quickly when incidents inevitably occur, and succeed as business enablers. But we also wondered, what do global security leaders really think about AI? Is our hypothesis true that CISOs are becoming central members of the C-suite? Do boards and CISOs speak the same language?

In The CISO Report, we share the results of our original research and offer insights on how leaders can evolve along with the cybersecurity landscape. Here are some of the most significant takeaways.

1. Love it or hate it — AI is here to stay

Seventy percent of CISOs believe AI gives the advantage to attackers over defenders, yet 35% are already experimenting with it for cyber defense, e.g., malware analysis, workflow automation and risk scoring. But augmentation doesn't start with AI: Ninety-three percent of CISOs have extensively or moderately implemented automation into their processes, and AI will only increase that percentage in the future.

2. CISOs often speak a different language than their board

While CISOs' and their board's priorities are moving closer together, there is still misalignment. Eighty-four percent of CISOs maintain that their board or governing body cares more about regulatory compliance than security best practices. Thirty-one percent say that projects have been delayed due to lack of funding while 30% say that the security team was unable to support a business initiative.

3. CISOs are now the C-suite

Forty-seven percent of CISOs now report directly to their CEO. Boards are becoming more active security stakeholders. CISOs are being asked to justify their investments, but this isn't a bad thing. It indicates their leaders are listening and overwhelmingly allocating more budgets for the year ahead (even if it's still not enough).

4. Most pay ransomware demands

Ninety percent of CISOs report that their organization experienced at least one disruptive attack last year. Even more shockingly, 83% paid attackers in the wake of a ransomware attack — directly, via cyber insurance or with a negotiator — with more than half paying at least $100,000.

5. Boards prioritize security funding

Ninety-three percent of CISOs expect an increase in their cybersecurity budget over the next year, yet 83% see cuts in other parts of their organization. Economic challenges are impacting security, but not in the way you might expect: Eighty percent say they have noticed their organization has faced a growing number of threats coinciding with the declining economy.

6. There is no resilience without collaboration

Levels of cybersecurity collaboration are highest with IT operations — likely because those integrations are more established — with 36% maintaining that collaboration was good, and another 40% saying it was good, but improvement was desired. CISOs also hail collaborations with software engineering/application development (42%), the cloud team (40%) and enterprise architecture (27%) as vital to ensure resilience throughout the organization.

About the authors

Ryan Kovar

Distinguished Security Strategist and leader of SURGe

Ryan is a distinguished security strategist and leader of SURGe, Splunk's security research arm. With over 20 years of experience as a security analyst, threat hunter, defender and Unix plumber, Ryan loves traveling the world and researching the biggest problems for Splunk's customers. Prior to Splunk, he worked at DARPA, US Navy, the UK Home Office and other organizations as a security practitioner and leader. Ryan has an MSc in Cyber Security from the University of Westminster.

Kirsty Paine

Field CTO and Strategic Advisor, Technology and Innovation (EMEA)

Kirsty Paine (she/her) is a strategic advisor to Spunk customers. As an experienced technologist, strategist and security specialist, she thrives on understanding difficult problems and finding creative solutions. Kirsty's background in cyber security stems from her mathematical roots, built over years working at the UK National Cyber Security Centre, specializing in security, privacy and internet technologies.

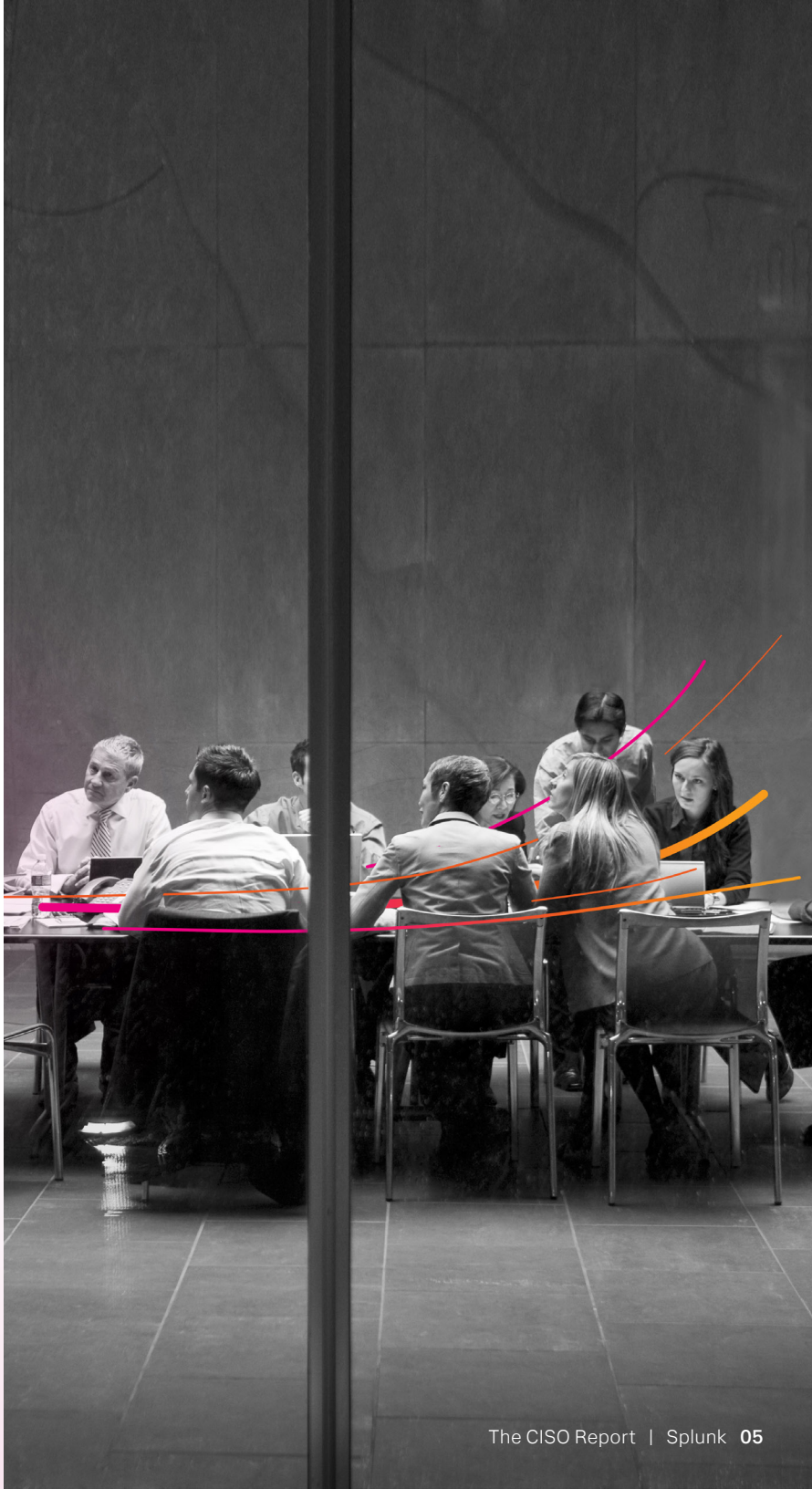
Today's CISO: On the front lines of change

The role of today's Chief Information Security Officers (CISOs) is complex and rapidly changing. Eighty-six percent say that the role has changed so much since they became a CISO that it's almost a different job. They are emerging as strategists and leaders who have a louder voice in the boardroom. And a growing number of them — now 47% — report directly to their CEO.

Of course, their most critical priorities still revolve around defending the organization against an increasingly complex threat landscape. Ninety percent of CISOs have faced a disruptive attack in the last year. And while they're adapting to stay ahead of cyber attackers, they aren't getting much sleep at night.

The CISO story, then, is about the constant struggle they face enabling the business to go fast while walking a daily tightrope between oft-competing priorities — the board's allegiance to business success metrics and the practical realities of securing the organization. For many of them, this means constantly justifying their teams' value to the C-suite and the board, while also filling security gaps caused by staffing shortfalls and finding new ways to mitigate organizational risk. The balancing act isn't easy.

The research illustrates a complete picture of the CISO: the issues, challenges and opportunities they face on a daily basis. Yet despite an increasingly sophisticated threat landscape and an uncertain economic outlook, many are optimistic. More than ever before, they have an opportunity to become champions who can effectively change the security culture of their organization. Boards and CEOs are not only listening, but relying on them for guidance. And as CISOs look ahead, their focus will be on collaborating with teams across their organization, working together to become more resilient so they can not only weather any storm, but thrive in its aftermath.



Generative AI elicits genuine insights

"We are trying to stay ahead of generative AI."

— CISO, government organization

We found that the overwhelming majority of CISOs (70%) believe that generative AI will create an asymmetrical battlefield that will inevitably be tipped in favor of cyber adversaries. We are more optimistic than that, though. We know 35% of CISOs are already using AI for positive security applications, and 61% will likely use it in the next 12 months.

Predictably, CISOs thought the highest ranking malicious use cases would be faster and more efficient attacks (36%), voice and image impersonations for social engineering (36%) and extending the attack surface of the supply chain (31%).

Many of these concerns are still theoretical, driven by media reports or as part of researchers' proof-of-concepts. At the time of writing this report, we haven't seen generative AI used extensively in real-world attacks or with any more success than human-written phishing scams.

"We are trying to stay ahead of generative AI. We know it is a technology that is being used. Instead of blocking the technology, we are trying to put as many guardrails around it as possible."

— CISO, government organization

Generative AI fills critical gaps in cyber defense

Will AI replace jobs? Not entirely. Eighty-six percent of CISOs believe that generative AI will alleviate skills gaps and talent shortages that they have on the security team. That means instead of replacing jobs, generative AI will more likely be used to fill in labor-intensive and time-consuming security functions that security professionals are reluctant to do anyway (writing policy documents, perhaps?), freeing them up to be more strategic. The reality is that there aren't enough cybersecurity professionals to meet demands. AI might give organizations the ability to supplement staff with everything from documentation to basic ticket triage.

So when it comes to fears that AI might "steal your job," try thinking of it in the same way as automation — augmenting, rather than replacing, talent. And when it comes to automation, 93% of CISOs say they have extensively or moderately implemented automation into their processes, giving them a lot of room for innovative use cases in the future.

"I don't know that anybody working in the cybersecurity space has got it easy right now regarding recruiting and retention," says the CISO of a government organization.

So when it comes to how AI can be used for cyber defense, CISOs have lots of ideas. AI is yet another tool that can address challenges ranging from strategic to deeply technical. It's not surprising that CISOs are queuing up mundane technical tasks for AI. But we were also excited to see AI opportunities span into strategic functions: challenges around data quality assurance, enriching and prioritizing alerts, and managing security posture analysis and internal communications. While security problems might not be new, AI offers the potential for new solutions.

AI also provides opportunities to elevate staff's skill sets and education. Forty-six percent plan on getting security teams up to speed on effective prompt engineering. Other policy efforts include training employees to better understand the threats posed by generative AI (39%) and establishing protocols to determine the types of tasks appropriate for AI bots (37%) as opposed to those that should be done exclusively by humans.

"We learn in cyber after the fact, with AI and GAI we can be more proactive, and it may help us with skills shortages."

— CISO, higher education

How Companies Are Using Generative AI for Cybersecurity

35% Security hygiene and posture management analysis and prioritization

27% Data enrichment of alerts and incidents

26% Internal communications

26% Analyzing data sources to determine which ones should be optimized or eliminated

25% Malware analysis

23% Creating detection rules

23% Creating secure configuration standards

22% Workflow automation

22% Threat hunting

20% Risk scoring

20% Policy creation

19% Incident response and forensic investigation

CISOs and the board get priorities straight

"The board has gotten fairly serious about looking at risk, and cyber is a form of risk."

— CISO, transportation, tourism and shipping

How do CISOs know if they're doing a good job? We asked them for their success metrics — what they prioritize and what they think their board cares about the most. There is sometimes a wide variance in those two answers, resulting in misalignment and frustration when executed in the field.

"You can buy all the technology in the world, but if the users are not well trained then things can go bad," says one technology CISO in an organization of more than 11,000 employees.

CISOs also point out more fundamental differences in values and understanding."Some of the board understands the importance of security," adds the CISO of an outsourcing company. "Some do not."

When they speak about quantifying risk, business value and return on investment, however, CISOs are slowly getting the ear of the board/C-suite:

- **26% say that they share results of security testing, indicating to boards the best places for intervention and demonstrating smart, proactive leadership.**
- **27% say that they prioritize reporting the ROI of security investments, indicating where interventions and money have already helped, and paving a way to speak directly to the CFO and gain support for future investments.**
- **25% say that the ability to purchase cyber insurance might be the best way to tell boards how 'safe' they are; and/or justify the investment elsewhere, too.**

"I think the awareness regarding the importance of pentesting and cybersecurity is higher than it was three years ago due to recent events in industry," says a CISO of a healthcare organization.

This validates another surprising finding: the biggest responsibility for 86% of CISOs is to ensure their governing body/board sees value in funding security investments. As one CISO in transportation puts it, "What the board really wants is risk quantification. They want it in dollars and cents."

Yet only 20% of boards rated "ROI of security investment" as a measure of success, possibly because they lack the understanding around how ROI impacts risk, relying instead on other metrics indicating security posture improvement.

Requirements for ROI are no doubt tougher. Almost a third (31%) of our respondents say that projects have been postponed or delayed due to lack of funding, while 30% also say the team was unable to support a business initiative.

Also, 84% of CISOs say that their governing board/body equates strong security with regulatory compliance rather than best practices, which might account for the slight disparity in the importance placed on "status and results from internal and/or regulatory compliance audits." It is not surprising, then, that 90% of CISOs say their governing body/board cares about different KPIs and security metrics today than it did two years ago. "My board loves a number," says the CISO of a transportation and logistics company. "But the problem with cyber is that it is super hard to come up with one figure that says how good or bad we are."

For CISOs and board members alike, it's time to refresh your approach and ensure you're still aligned.

CISOs expand board presence, own their influence

Overall, our research showed that CISOs are formalizing their seniority: Forty-seven percent of CISOs report directly to the chief executive officer (CEO), followed by 40% reporting to the chief information officer (CIO).

Interestingly, Western Europe is leading this trend, with 54% reporting directly to the CEO and 48% in APAC, while AMER trails at 41%. This is likely due to European legislation, both existing and incoming, that makes the CEO personally liable for security and penalizes them for negligence. In short, ignorance is no longer a defense in the face of a cyber attack.

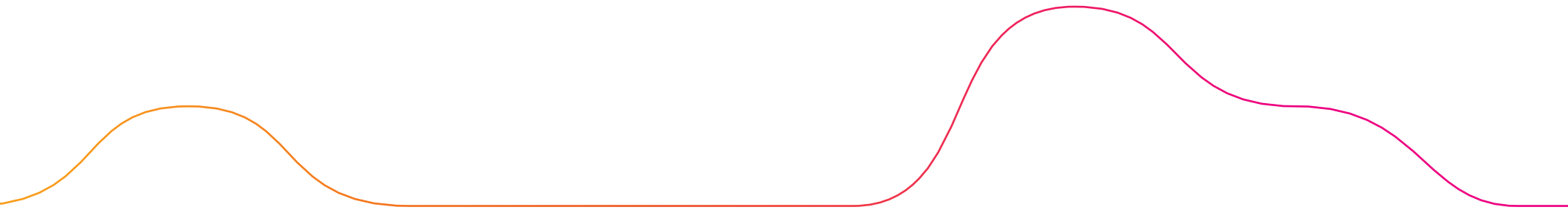
This shift in reporting illustrates how CISOs are changing their focus toward the business and formalizing their executive roles. Forget closer relationships with the C-suite. They are the C-suite. This trend reflects that security is now as important to organizations as finance (CISO and CFOs work side-by-side). And security risk has become just as costly, litigious and as impactful to share prices as financial risk is.

Driving a culture change

These days, cyber risk is business risk. Organizations often integrate security into their existing business systems and processes. As testament to its importance in the boardroom, a vast majority of organizations (78%) now report having a subcommittee or audit committee focused on cybersecurity, privacy or cyber-risk. This could be due, in part, to Europe's legislation, which makes the CEO personally liable for security.

Little by little, CISOs are driving change in security culture within their respective organizations, from improving employee awareness to building security requirements into software development and business decision making.

"It takes time to change the culture," the CISO of a transportation, tourism and shipbuilding company says. "It has very, very little to do with the technology itself and it's the hardest part of the job." They might be pushing on an open door, or their efforts are finally paying off, but it's clear that their influence on culture extends past their direct sphere of control: Eighty-eight percent report that their governing board or body is making a concerted effort to educate themselves on cybersecurity.



CISOs and Boards Rank Success Factors*

There is close alignment on the factors that indicate a successful cybersecurity program

CISO	Board	
27%	20%	ROI of security investments
17%	23%	Status and results from internal and/or regulatory compliance audits
26%	21%	Results of security testing
23%	18%	Risk exposure rate or patching/ tooling percentage coverage
23%	19%	Feedback from LOB executives / C-suite / Board
22%	18%	Percentage of systems with up-to-date patches
17%	21%	Attainment of security roadmap milestones
16%	19%	Alert inspection and investigation rate
16%	18%	Mean time to respond or remediate (MTTR)
21%	23%	Progress in security/maturity model assessment certifications
20%	18%	Average time it takes to patch a vulnerability
20%	18%	Percentage of systems consistent with policies for security controls
19%	17%	Number of high priority incidents, breaches and other reportable events
18%	20%	Asset and software inventory coverage
25%	23%	Ability to purchase cyber insurance
22%	21%	Percentage of employees completing security awareness training
17%	17%	Number of vulnerabilities identified
14%	14%	Mean time to detect (MTTD)

* Factors ranked in order of largest to smallest difference

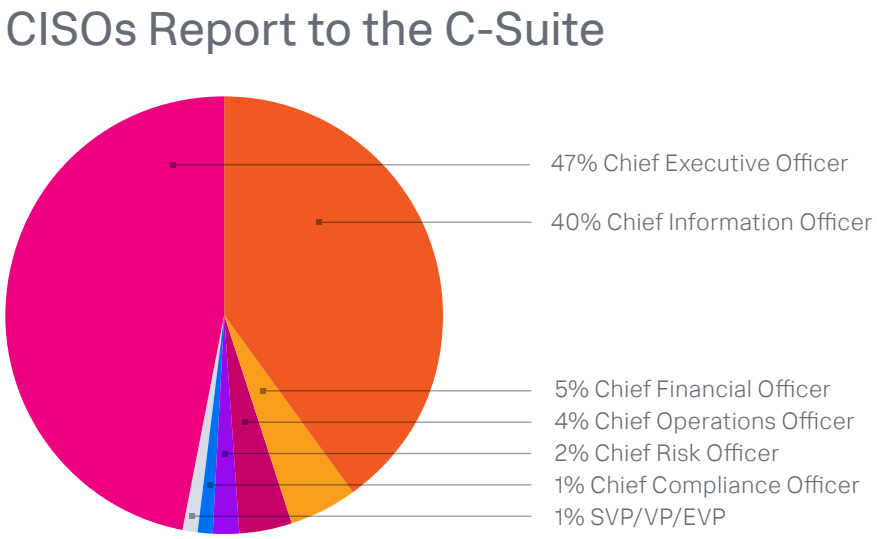
CISOs embrace — yet question — evolving role

Whistle-blowing is still trendy; eighty-two percent of respondents say that if their organization was wilfully ignoring security best practices and compliance mandates and putting the business at risk, they would consider becoming a whistleblower. This speaks to a responsibility above their employment, a strong sense of morality and perhaps some lessons learned after shouldering the blame for their organization's security mishaps.

To say that they are scapegoats might not be an exaggeration: Eighty-four percent agree or strongly agree that they're worried about their personal liability for cybersecurity incidents. Our experts recommend that you get a personal lawyer (not a company-provided one) that you can call on short notice, should you ever need to.

And when it comes to purchasing decisions, you could do worse than the tried-and-tested, safe options if you need to impress your board: Ninety percent say their governing body/board puts a high degree of faith in industry analyst recommendations.

Many boards and CEOs know that the liability landscape has shifted, but they feel powerless to effectively respond to these new dynamics. This opens an opportunity for CISOs to educate their board and ultimately improve the security posture of their organization. Ultimately, CISOs now have a bigger seat at the table and a louder voice in the room. The C-suite and the board are listening. Security leaders can use their growing platform to create the change they want to see in the industry.



CISOs submit to ransomware

"My goal: Not to be at the helm when we have a major cyber breach."

— CISO, company in the banking industry

CISOs are likely going to face a major attack — *a staggering 90% reported suffering at least one disruptive attack in their organization over the last year* (43% at least once, 34% "a couple of times," and 13% "several times.")

It should be no surprise that social engineering, OT/IoT, and ransomware are top-of-mind concerns for CISOs — threats that are not only featured prominently in the media, but are also financially devastating. "Your decisions impact how the business runs," says the CISO of a healthcare organization. "If you make bad choices, you might kill the business."

reported at least one disruptive attack

Most Concerning Cyber Threats

40% Social engineering attacks

37% Operational technology (OT) and Internet of Things (IoT)

33% Ransomware

30% Insider threats

29% Third-party risk

24% Distributed denial of service attacks

24% Destructive malware

24% Errors and misconfigurations

24% Cryptomining

21% Account takeovers

20% Fraud

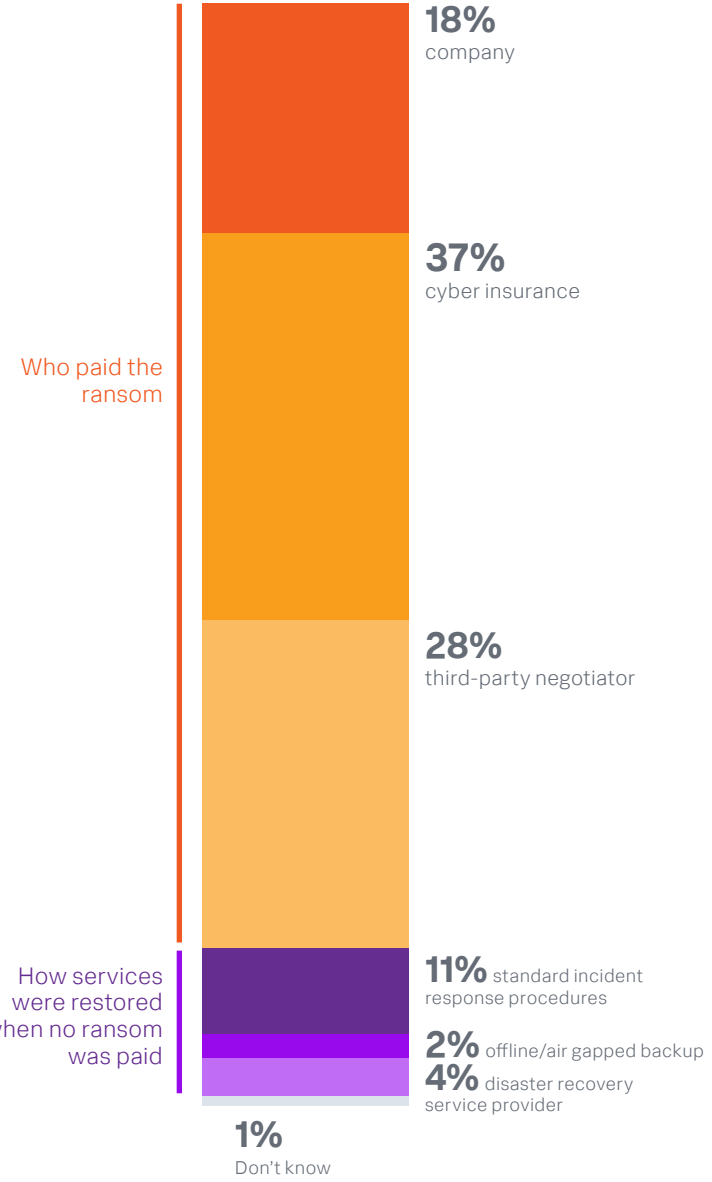
Ransomware: Attackers get a payday

All but 4% of our respondents report suffering a ransomware attack, with 52% experiencing one that significantly impacted their business systems and operations.

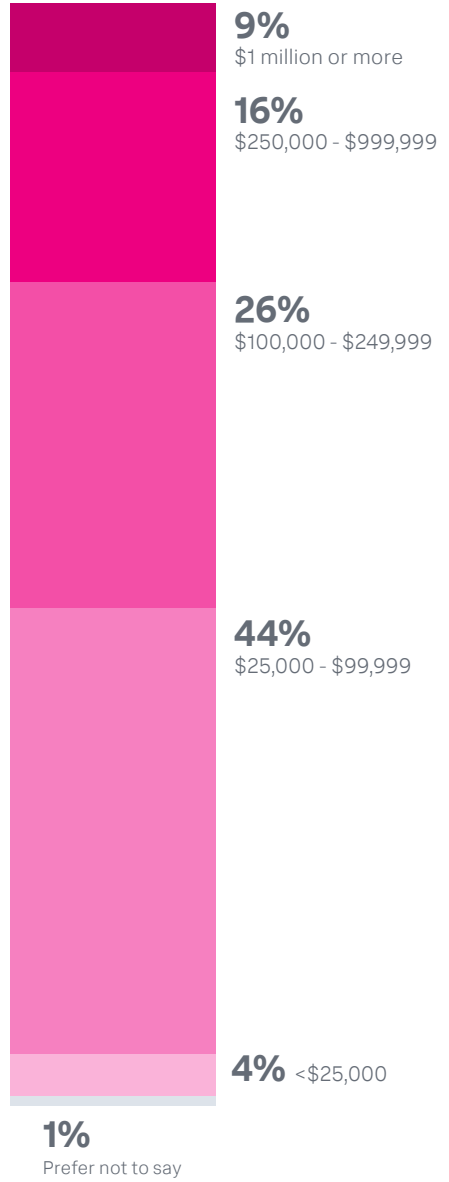
While 96% is significant, prepare yourself — 83% of those who answered said they paid the ransom. Of those who paid, 18% paid the ransom directly, 37% paid through cyber insurance and 28% paid through a third party.

And it's not cheap. The most significant number paid somewhere between $25,000 to $99,999 (44%), while more than half of respondents paid more than $100,000, a stunning 9% of respondents (or one in 11) paid $1 million or more. That's a lucrative business for ransomware gangs — and many desperate organizations gamble with their reputations in the hope of decrypting their data, recovering their systems and preventing the release of sensitive material.

Ransomware Remediation



Ransomware Payouts



The majority of CISOs (69%) maintain that paying a ransom makes them vulnerable to legal exposure in the future. Yet even after payment, organizations are often unable to fully recover their lost capabilities — there's no honor among thieves. And cyber insurance is no silver bullet; it's often difficult to obtain while falling short of full reimbursement.

The net-net? Make sure you have offline, regularly-tested, segregated back-ups. Designate maintenance responsibility and conduct regular checks that they're successfully executed. Additionally, run a board-level exercise to exert some real-yet-safe pressure on those systems.

And don't think boards aren't watching. Seventy-three percent of CISOs say they feel that their governing body/board is overly concerned about ransomware and the potential threat it poses to their organization. And the majority say that when they faced successful ransomware attacks, the governing body/board required regular updates as they sought to resolve the issue. That scrutiny likely won't go away anytime soon — but it does give you even more reasons to run exercises with the board.

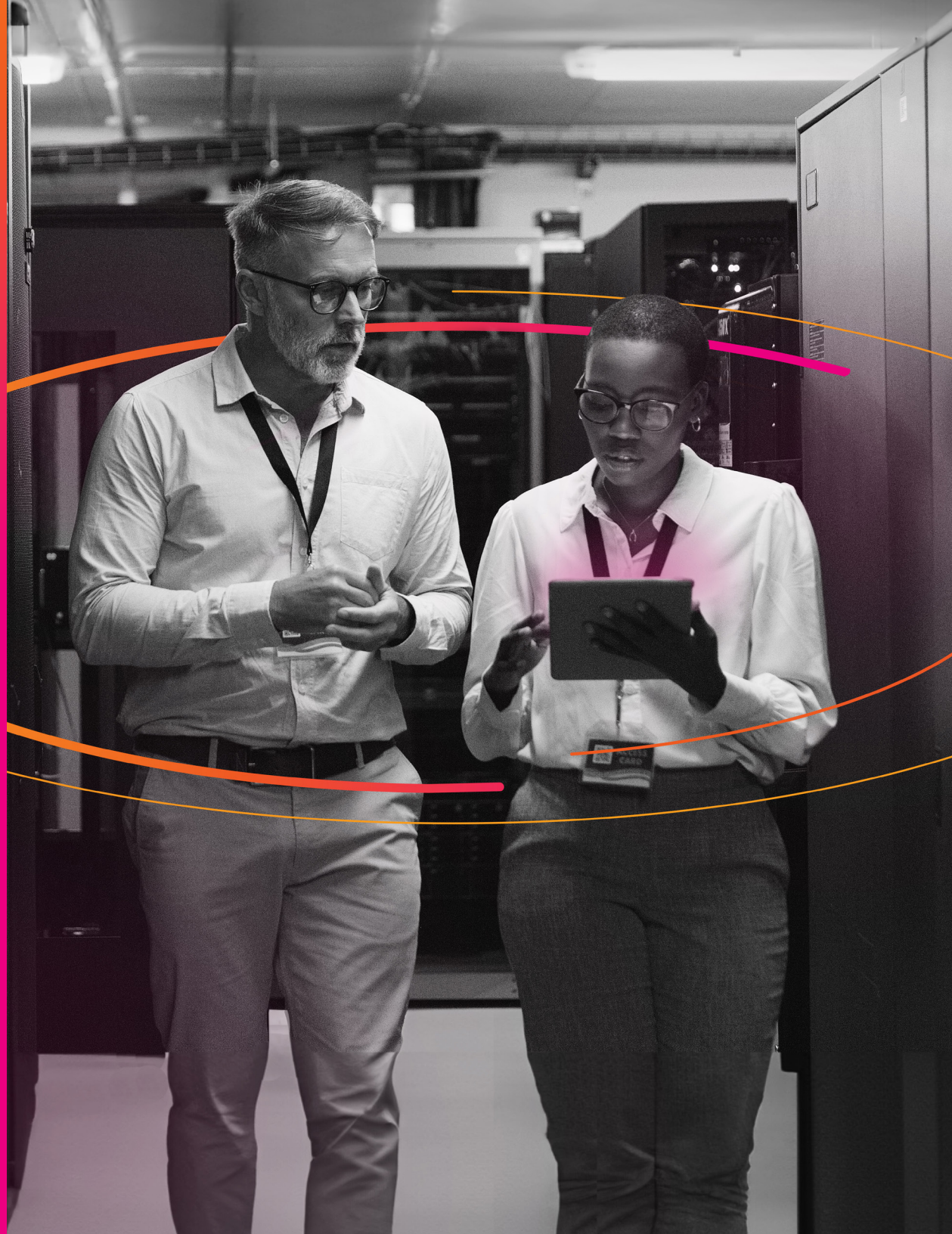
"The cyber insurance process has changed over the past few years. It is getting to the point where we are wondering if it is worth our time."

— CISO, finance company

Security investment on the rise

"Resources are my only real weakness — actually having enough hours in the day and having enough people to handle all the responsibilities."

— CISO, financial services company



Ninety-three percent of organizations actually expect to increase cybersecurity spending, either significantly or somewhat, over the next year. This is great news for security teams, as 85% percent of CISOs say a reduction in spending would hamper their ability to respond to threats, and 80% say they have noticed that their organization has faced a growing number of threats coinciding with the declining economy.

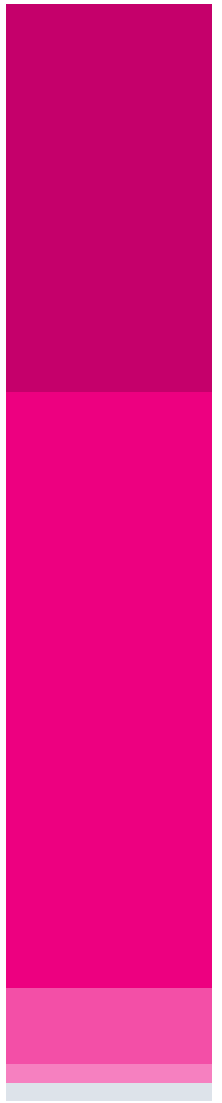
Yet 83% of CISOs see the cuts in other parts of their organization, and 85% say that they're worried about the macroeconomic uncertainty and its potential impact on their team.

Almost a third (31%) say that projects have been delayed or eliminated due to a lack of funding. While 87% say they've demonstrated a business case for increased budget year-over-year, only 35% say that their boards allocate adequate cybersecurity budgets. With security budgets expected to rise, there's reason to be optimistic. However, despite increased investment, the additional funding is still not enough for many CISOs wrangling their technical debt.

We saw CISOs are justifying ROI for security investments to the board, and some of them have a focus on tool sprawl. The vast majority (88%) say they see a need to rein in security analytics and operations tools with solutions like SOAR, SIEM and threat intelligence, to address issues of tool sprawl and complexity, with only 2% disagreeing that they need to consolidate their tools. This is a message that always lands well with a CFO — and helps to justify ROI.

of CISOs expect increases in cybersecurity spending

2024 Cybersecurity Spending



34% Increase significantly

59% Increase somewhat

6% No change

1% Decrease somewhat

1% Don't know, too early to say

> **"My CFO has said my budget will always be sufficient … as long as I can justify funding, then I will get it."**
>
> — CISO, banking industry

Collaboration is key to building resilience

"A great resiliency program is one that is always questioning itself and trying to make itself better. Never staying stable and always pushing against the program and questioning."

— CISO, telecommunications company

In our conversations with CISOs in the Forbes Global 2000 and beyond, we have advocated for a culture of cross-functional collaboration between security teams, IT and engineering organizations. That's because we've seen repeatedly that collaborative organizations with teams working together can better prevent issues from becoming major disasters, more quickly remediate incidents and ultimately become more adaptable to changing environments. It stands to reason then that 27% of CISOs call out cross-team collaboration between IT operations, security operations and software engineering/development as a significant means of building, expanding and sustaining resilience in their organization.

Collaboration opens doors, breaks down walls

While it's an incremental culture shift, we've seen that teams within organizations are becoming more collaborative. Levels of cybersecurity collaboration were highest with IT operations — likely because those integrations are more established — with 36% maintaining that collaboration was good, and another 40% saying it was good, but improvement was desired. CISOs also hail collaborations with software engineering/application development (42%), the cloud team (40%) and enterprise architecture (27%) as vital to ensure resilience throughout the organization.

Benefits of Collaboration

44%
Greater integration between security and IT operations tools and processes

42%
Faster time to understand, quantify and prioritize the risk associated with new business initiatives

40%
Greater knowledge transfer between groups

37%
Greater collaboration on procurement deployment and operations of security technologies

37%
Greater visibility across the attack surface

33%
Faster time for risk mitigation

31%
More career opportunities for individuals to move to and from the security department

29%
Less inter-team conflict/finger pointing

Other notable areas of solid cybersecurity integration include:

- **Application development**
- **Observability**
- **Customer experience/digital experience**

In all three areas, between 73% and 76% of respondents say collaboration was good — either good with no improvement or good with some desired improvement. However, executing on functions collaboratively is often different in practice than in theory. The CISO of a finance company describes the relationship between IT and security as respectful but fractious: "They never challenge what we want to do, but they mutter obscenities under their breaths as they walk away."

Although it takes some time and effort, there is no downside to collaboration. CISOs extoll the many benefits of collaboration, the biggest being the general integration of security and IT operations tools and processes (44%), which also helps with budget — and justifying ROI.

Building resilience into the future

A significant number of CISOs also say that they will continue to hone the organization's competencies around resilience by further developing comprehensive incident response plans that clearly outlines the steps their teams will need to take in the event of a security incident. As part of that effort, they also will be defining and automating incident response processes across different teams and individuals (25%).

These practices are nothing new for CISOs, who often see resilience as an extension of their security practices — because CEOs tie resilience to risk and response to attacks, it often falls within CISOs' purview. However, many security responses rely on IT to implement changes, in turn, compelling some CISOs to use resilience as a means of working more closely with IT. And the result is improved digital response.

Creating and building a culture of resilience is a monumental undertaking. CISOs believe that collaboration on digital resilience needs to be foundational, from planning and product modernization to business and product strategy. To that end, 55% percent maintain that they have opportunities to integrate security into all aspects of the software development life cycle, and 50% say that security should be an integral part of the modernization process. CISOs also maintain that resilience collaboration efforts will help explore unusual or anomalous system or network behavior (48%) as well as improve how an organization responds to degradation of critical applications (44%) — reinforcing the need for integrated security and observability functions.

Collaborative Resilience Activities

55%
Integrating security into the full software development lifecycle

50%
Modernization projects

48%
Exploring unusual or anomalous system or network behavior

44%
Observability, and how the organization responds to degradation of critical applications or services

38%
Crisis management process and protocols

A new era of resilience

The era of CISOs working in bubbles and independent silos is over. CISOs, and in turn the C-suite, are realizing it will "take a village" to become stronger, more secure and ultimately, more resilient. Strategic collaboration with engineering and IT is vital to this mission.

The data in this report makes it clear that CISOs have more face time and influence with CEOs and boards than ever before. And while CISOs might have to work harder to justify technology investments, their leaders are also paying attention and allocating more budget. Little by little, CISOs and their boards are learning to speak the same language.

At the same time, we can't ignore the unprecedented new challenges and pressures CISOs face. Stringent security regulations, such as updated Security and Exchange Commission rules in July of 2023, intensify risk for security leaders, potentially making them liable for cyber incidents. AI is opening the door to new opportunities, but can just as easily fall into the hands of cyber adversaries who will leverage it to propel deep fakes, disinformation and more elaborate social engineering schemes. And ransomware continues to introduce complex dilemmas about whether to contain the malware or silently pay off the attackers in hopes that the threat disappears.

CISOs will navigate these headwinds differently, but they can't go it alone. While there is precedent for integrating security with IT operations, there are signs this type of collaboration is expanding. Security functions work more closely with application development, observability and customer experience, creating opportunities to learn and be more effective across the organization.

While it won't happen overnight, teams across the organization will become more communicative, collaborative and integrated to expand visibility and increase overall effectiveness, setting them up for even greater success. And as leaders increasingly understand that cyber risk is business risk, the CISO will champion a security-first paradigm that will usher in a new era of resilience.

Appendix

Regional highlights

By region, we divided our respondents into the following categories: North America (41%), Asia-Pacific/Japan 30% and Western Europe (29%). Their responses to the various topics are as follows:

The role of the CISO

- Western Europe had the largest percentage of CISOs who reported directly to their CEOs (54%) followed by APAC/Japan (48%) and North America (41%), averaging 47% of total respondents.
- North America reported the highest percentage of respondents whose role as CISO had changed so much it was almost a different job at 90% (agree or strongly agree) followed by APAC at 89% and Western Europe at 76%.
- APAC had the highest percentage of respondents whose focus had shifted from controls and implementation to strategy (94%). APAC was followed by North America at 90% and Western Europe at 88%.
- CISOs' success metrics vary greatly by region. It's interesting to note that North America had the highest percentage of respondents (25%) who considered the number of high priority breaches, incidents and reportable events as a success metric. By contrast, a significant number of Western European respondents considered feedback from line-of-business executives, C-suite and the board as the most important measure of success (29%).

Board of directors

- Misalignment of board and CISO priorities is a source of frustration around the globe, although not consistent across regions. Forty-three percent of North American respondents reported that the security team was unable to support a business initiative compared to only 15% of Western European respondents, likely due to comparatively more stringent regulation in Europe than in the U.S. Thirty-three percent of APAC respondents reported that they had to cut back on cybersecurity staff because of misaligned priorities, compared to only 18% of Western European respondents.
- Misalignment of board and CISO success metrics is also inconsistent across regions. Thirty percent of North American CISOs say that progress in the security maturity model is most indicative of success to their board, compared to only 16% of respondents in Western Europe. Meanwhile 28% of respondents in APAC say that the percentage of systems consistent with policies for security controls (MFA, WAF, encryption, etc.) was a measure of success for their boards, compared to only 11% of respondents in Western Europe. The largest concentration of respondents in Western Europe (27%) cited status and/or results from internal regulatory compliance audits as the most important success metric for their boards.

Digital resilience

- North American respondents placed a higher priority on cybersecurity education in their digital resilience strategy than regional counterparts: 30% of North American respondents said educating cybersecurity staff on best practices and ongoing training is most important to ensure digital resilience, compared to 19% respectively in both APAC and Western Europe.

The rise of generative AI

In all regions, early opinions on generative AI's applications in security are generally optimistic.

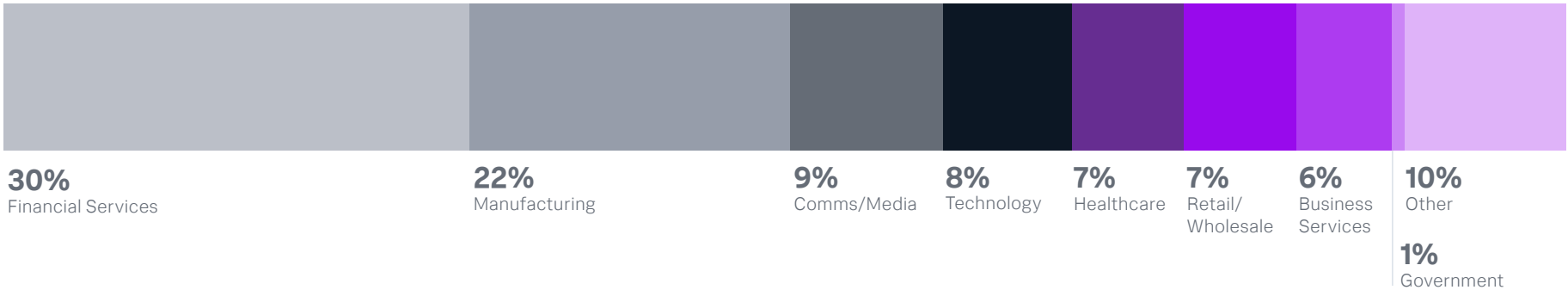
- 84% agree or strongly agree that they will develop their own language models or other AI-based solutions for cybersecurity.
- 89% agree or strongly agree that they will adopt generative AI for cybersecurity through vendor produced products/ functionality.
- 86% believe that generative AI will alleviate skills gaps/ shortages they have on the security team.
- 82% believe that generative AI bots will take jobs/activities done by humans today.
- APAC expresses the most hope for AI to be used as a defensive tool, with 24% believing that it would give them either a slight or significant advantage over cyber criminals, compared to 12% of respondents from North America and 17% of Western Europe. That said, all regions express that generative AI would give cybercriminals a slight or significant advantage.
- It stands to reason then, that respondents from APAC (23%) are most likely to be using generative AI for cybersecurity today, compared to only 11% in North America or Western Europe.
- Respondents in Western Europe express the most interest in using generative AI for cybersecurity over the next 12 months (57%) compared to 39% of North American respondents and 35% of respondents from APAC.

The threat landscape

- APAC and Western Europe report seeing the most security gaps in cloud infrastructure at 57% and 51% respectively, compared to North American respondents at 40%.
- Respondents in APAC are most afraid of attacks on operational technology (OT) and IoT (46%) compared to Western Europeans at (25%).
- While all regions were affected by ransomware, respondents in APAC (64%) and North America (53%) were more likely to experience an attack that significantly affected their systems and business operations, compared to Western Europeans (38%).
- All regions similarly report paying the ransom, whether directly, through cyber insurance or a third party. Respondents in North America (39%) were more likely to pay between $100,000 and $249,999 than Western Europe (20%) or APAC (14%). However, APAC was more likely to pay $1 million or more (17%) compared to North America (3%) or Western Europe (7%).

Industry highlights

Respondents by Industry



The role of the CISO

CISOs across numerous industries now report directly to the CEO, including:

- 84% in healthcare
- 63% of communications and media
- 44% of manufacturing
- 34% of financial services

1. Regulatory compliance is the most important priority to CISOs in the retail sector (56%) followed by technology (29%). Data privacy represents the biggest priority for CISOs in communication and media (59%), followed by technology (50%).
2. Almost half of CISOs in the retail sector (48%) cite the number of high priority incidents as the metric most indicative of success. A significant percentage of CISOs in communications and media (34%) cite progress in the security maturity model as the most important success metric. For CISOs in technology (39%), success was associated with the ability to purchase cybersecurity insurance.
3. Across industries CISOs feel like their role has changed so much it was almost like a different job. The CISOs in industries that are the most affected include:
   - Communications and media: 93%
   - Financial services: 92%
   - Technology: 89%
   - Retail/Wholesale: 85%
   - Healthcare: 84%

4. CISO are most concerned about their personal cybersecurity liability in the following industries:
   - Financial services: 94%
   - Technology: 93%
   - Business services: 86%
   - Healthcare: 84%
5. In almost all industries, CISOs say that (they agree or strongly agree) their role had transitioned from one of implementation and controls to security strategist:
   - Government: 100%
   - Retail/wholesale: 97%
   - Financial services: 95%
   - Business services: 91%
   - Manufacturing: 89%
   - Communications and media: 87%
   - Healthcare: 84%
6. When weighing in on most in-demand skills, CISOs in communications and media point at cloud security the most (47%). CISOs in retail express that they need more senior-level cybersecurity positions (41%).

The board of directors

1. Financial services (92%) and healthcare (92%) are the most likely industries to have a dedicated board-level cybersecurity committee, followed by retail/wholesale (85%) and manufacturing (84%).
2. The retail/wholesale sector is also most likely to have a board that provides adequate budgets to ensure cybersecurity measures are in place (59%), likely attributed to PCI and other customer data privacy regulations. Business services (62%) and financial services (51%) are most likely to have a board that has established governance requirements to ensure cybersecurity incidents are reported. 100% of government CISOs say that their biggest responsibility is to ensure their board sees value in their security investments.
3. Numerous CISOs across many industries regularly participate in board meetings, including:
   - Technology: 100%
   - Government: 100%
   - Communications and media: 94%
   - Healthcare: 88%
   - Manufacturing: 86%
4. CISOs in numerous sectors say their boards equate security with regulatory compliance — representing a source of frustration for CISOs.
   - Financial services: 89%
   - Communication and media: 87%
   - Manufacturing: 87%
   - Healthcare: 84%
   - Business services 81%
5. To reinforce value to their boards, the majority of CISOs in retail/wholesale (59%) say that they provide their governing body with cyber risk metrics and ask them to make risk-based decisions. The majority of CISOs in business services (52%) say that they position security as a business enabler.

Digital resilience

- CISOs in numerous industries are employing resilience strategies with teams across the organization. One hundred percent of government CISOs, and 59% of retail CISOs say security operations (SecOps) will drive digital resilience. Seventy-nine percent of technology CISOs and 56% of manufacturing CISOs say that IT operations have a high degree of responsibility for digital resilience.
- CISOs in business services (76%) and communications and media (63%) cite integrating security into the full software development lifecycle as a major resilience strategy. Fifty-nine percent of CISOs in communications and media say that they consider observability and how the organization responds to application degradation as an activity that builds resilience.

The rise of generative AI

CISOs in industries that express the most fear that generative AI would give either a strong or slight advantage to cyber adversaries included healthcare (88%), manufacturing (76%) and financial services (72%). Fifty-one percent of CISOs in financial services say that they planned to implement specific cybersecurity controls to mitigate AI security risks.

Industries that have the biggest interest in adopting generative AI over the next 12 months include retail (59%), healthcare (56%) and manufacturing (51%).

The majority of CISOs in most industries say that AI will take jobs that currently belong to cybersecurity professionals. But CISOs in manufacturing (80%), financial services (91%) and business services (85%) strongly express that it will alleviate the cybersecurity skills shortage.

The threat landscape

CISOs call out cloud applications and infrastructure as having the biggest security coverage gaps across industries. CISOs in business services (71%), healthcare (64%) and technology (64%) point to cloud applications, while manufacturing CISOs (64%) see the most significant security gaps in cloud security. Financial services (57%) see the biggest gaps in third party/supply chain security.

Ninety-six percent of healthcare organizations and 90% of manufacturing businesses report experiencing at least one disruptive attack over the last year.

A significant percentage of communications and media CISOs (44%) point to incident response processes or communication issues that made the attackers' job easier. A significant percentage of CISOs in technology (42%) cite vulnerable systems that were unknown, unmanaged or misconfigured.

Numerous industries experienced ransomware attacks that significantly impacted their systems and business operations, including financial services (59%), retail (59%) and healthcare (52%).

Perhaps contrary to popular belief, the industry most likely to pay the ransom is retail, with 95% of those reporting that they either paid directly, through cyber insurance or a third party.

Retail was most likely to pay a ransom between $25,000 and $99,999. The majority of communications and media organizations attacked by ransomware (56%) paid between $100,000 and $249,999.

Methodology

An independent research firm conducted two separate studies: quantitative and qualitative. The quantitative study targeted 350 CISOs, CSOs and other qualified executive security leader equivalents. The qualitative research targeted 20 CISOs, CSO and security leaders in 60-minute in-depth phone interviews.

Geographic Regions

The quantitative survey was distributed between North America, (United States, Canada) EMEA (UK, Germany, France) APAC (Australia, New Zealand, Japan, Singapore, India). Qualitative surveys were conducted in the United States, Canada and the UK.

Industries

Respondents in both qualitative and quantitative surveys represented 17 industries, including financial services (banking, securities, insurance), manufacturing, media and communications, technology, healthcare, retail/wholesale, business services, government/public sector, education (K-12, secondary, college/university), agriculture/forestry, construction/engineering, consumer packaged goods, life sciences, mining/oil/gas, telecom, transportation, utilities.

Perspectives by Splunk — by leaders, for leaders.

Get more executive viewpoints on security, IT and engineering at our online publication, Perspectives by Splunk. You'll hear from Splunk's own leaders and experts, as well as guest contributors from the industry. We aim to deliver interesting, provocative and actionable insights by people who have done your job at some of the largest companies in the world.

Visit Perspectives by Splunk

Keep the conversation going with Splunk

splunk>

23-295950-Splunk-The CISO Report-EB-123