RSAC Cybersecurity Insights & Futures, Volume 3

For 2025-2026, Identity and Data Protection Are CISOs' Top Areas for Increased Investment

Authors:

Laura Koetzle
Head of Community Research
RSAC

Richard Eng
Senior Principal Security Researcher
RSAC

Øystein Fladby
Principal Security Researcher
RSAC

Chris Gates, PhD
Director, Research
RSAC

Felix Leder, PhD
RSAC

Dario Pasquini, PhD
Principal Researcher
RSAC

NOVEMBER 6, 2025

For 34 years, the data that the community purposefully shares with each other has allowed RSAC to serve as a window into the industry's future. Highlights of this third edition of RSAC™ Cybersecurity Insights & Futures include:

- Most CISOs' budgets increased between 2024-2025
- CISOs need practical passwordless implementations
- CISOs seek solutions to old and new data protection problems
- Burnout remains a problem
- Smaller firms are far less likely to indemnify CISOs
- Most CISOs report to the CIO or CTO
- Turnover in most CISOs' teams remains low, but will climb

The Data That Inspired This Report

Cybersecurity is too big and complex to be solved alone. It requires a collective, global effort across all disciplines to tackle rapidly evolving threats. This is why RSAC has brought hundreds of thousands of the most diverse minds in cybersecurity together for 34 years and counting at our flagship event, RSAC™ Conference.

RSAC's mission is to unite the cybersecurity community to create a safer society. We do this through our RSAC™ Membership Platform and our annual Conference. RSAC Conference is the largest and most influential event in the cybersecurity industry, bringing together industry leaders, researchers, and innovators to discuss the latest advancements and challenges in cybersecurity.

RSAC Conference selects presentations through a rigorous process. Our independent Program Committee consists of 150+ cybersecurity experts from enterprise, government, academia, and the vendor community, who evaluate submissions based on relevance, originality, and impact. All content selected for the program must meet strict neutral and educational guidelines. In 2025, **more than 2,800 submissions** were received from the cybersecurity community across the globe through our Call for Submissions process.

Additionally, RSAC Conference has become a launchpad for groundbreaking cybersecurity startups through initiatives like the RSAC™ Innovation Sandbox (ISB) contest, which has helped emerging companies secure funding and gain industry recognition. This environment fosters innovation, making RSAC a key destination for companies looking to showcase cutting-edge security solutions. 2025 was the 20th anniversary of the ISB and **more than 200 submissions** were received from across the globe to compete for an opportunity to be a Top 10 Finalist and ultimately one declared winner.

RSAC 2025 Conference had **more than 650 exhibitors**, from start-ups to well-established platform providers. We offer RSAC™ Early Stage Expo for up and comers in the industry; RSAC™ Next Stage for rapidly growing start-ups; and a sprawling Expo with innovative solution providers from across the world.

RSAC also hosts specialized programs for cybersecurity executives at key stages in their careers such as: 1) CISO Boot Camp (CBC) for aspiring CISOs; 2) Cyber Leaders Forum (CLF) for CISOs of mid-sized enterprises; and 3) Executive Security Action Forum (ESAF) for CISOs of Fortune 1000 firms. At RSAC 2025, 375 executives participated in these programs.

Why We Created This Report

This vibrant community has grown into the convening authority of the cybersecurity industry. Through reports like this, we aim to educate and empower the community to stay ahead of emerging threats—and to inspire and support one another in times of need. Everything we do is for the community and by the community, to enable collaboration and foster growth. Find more Insights & Futures reports like this one here.

Who We Serve

The RSAC™ Community is represented by:

140+ Countries

4,500+ Contributing Experts

40,000+ Annual Conference Participants

Global 1000 Security Executives

Senior Government Decision-makers

Top Anti-fraud Executives

Innovation Sandbox Participants Boasting $17.8B in Investments*

*Source: Crunchbase

The State of the CISO, 2025

RSAC conducted studies of CISOs of companies ranging in size from 500 employees to some of the largest firms in the Fortune 1000 in Q2 2025. Here's what's on their minds:

- **Most CISOs' budgets increased between 2024 and 2025...**
- **…And their top areas of investment for 2025-2026 are identity and data protection**
- **CISOs recognize the toll the job takes on themselves and their teams…**
- **…And are engaging with it seriously**
- **Smaller firms are far less likely to protect their CISOs from personal liability for security breaches**
- **Senior leaders focus on legal accountability for security breaches**
- **Sixty percent of CISOs report to the CIO or the CTO**
- **Cybersecurity staffers are sticking with their teams… for now**

CISO Priorities and Challenges: A Deep Dive

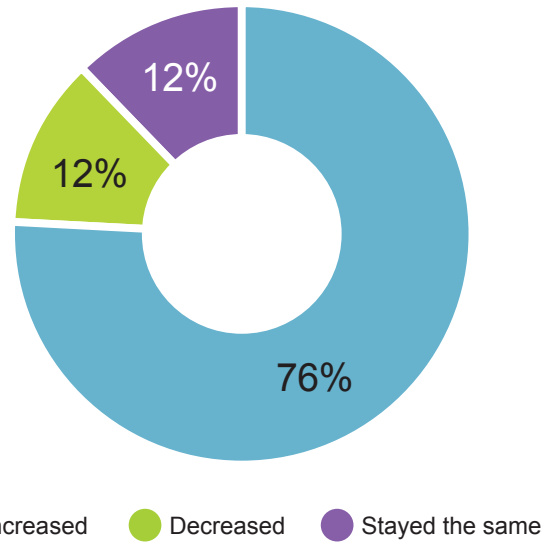
Nearly a century of social science research has demonstrated large gaps between what people say they do in surveys and their actual behavior.[1] Hence, RSAC analyzed our session attendance and exhibitor visit data from RSAC Conference to see how closely the broader population of senior cybersecurity leaders' patterns of "voting with their feet" lined up with our CISO respondents' stated priorities. And they matched to a surprising degree overall:

Most CISOs' budgets increased between 2024 and 2025... In Q2 2025, RSAC asked CISOs how their budgets had changed from the previous year, and 76% reported that their budgets had increased, while just 12% saw their budgets decrease (See Figure 1).[2] The most common budget increase was between 5 and 10% (See Figure 2).

…And their top areas of investment for 2025-2026 are identity and data protection. Nearly 25% of CISOs select identity and access management as their number one area for increased investment over the 12 months starting from Q2 2025 (See Figure 3). If we separate out the Fortune 1000 CISO cohort, the emphasis on identity proves even more pronounced: 32% of those CISOs choose identity as their top investment priority. Hence, it's no surprise that senior cybersecurity leaders at RSAC 2025 overall prioritized learning about identity;[3] they were nearly 38% more likely than average attendees to attend those sessions.[4] Data protection was the second most popular top investment area at 15%, but senior leaders were very slightly *less* likely (about 4%) than average attendees to spend time in sessions on topics like how CISOs and data protection officers can work most effectively together and data-centric security.[5]

Figure 1: More Than 75% of CISOs Saw Increases in Their Budgets from 2024

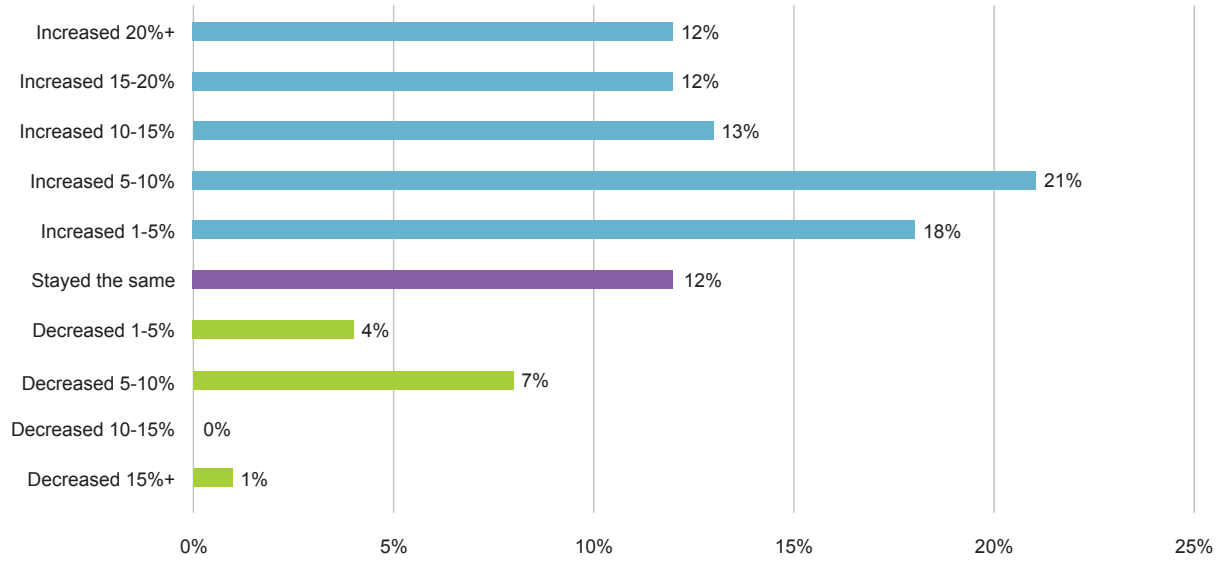
"How does your 2025 information security budget compare to 2024?"



Base: 68 CISOs at organizations with 500 or more employees

Figure 2: The Most Common Budget Change Was an Increase of Between 5% and 10%

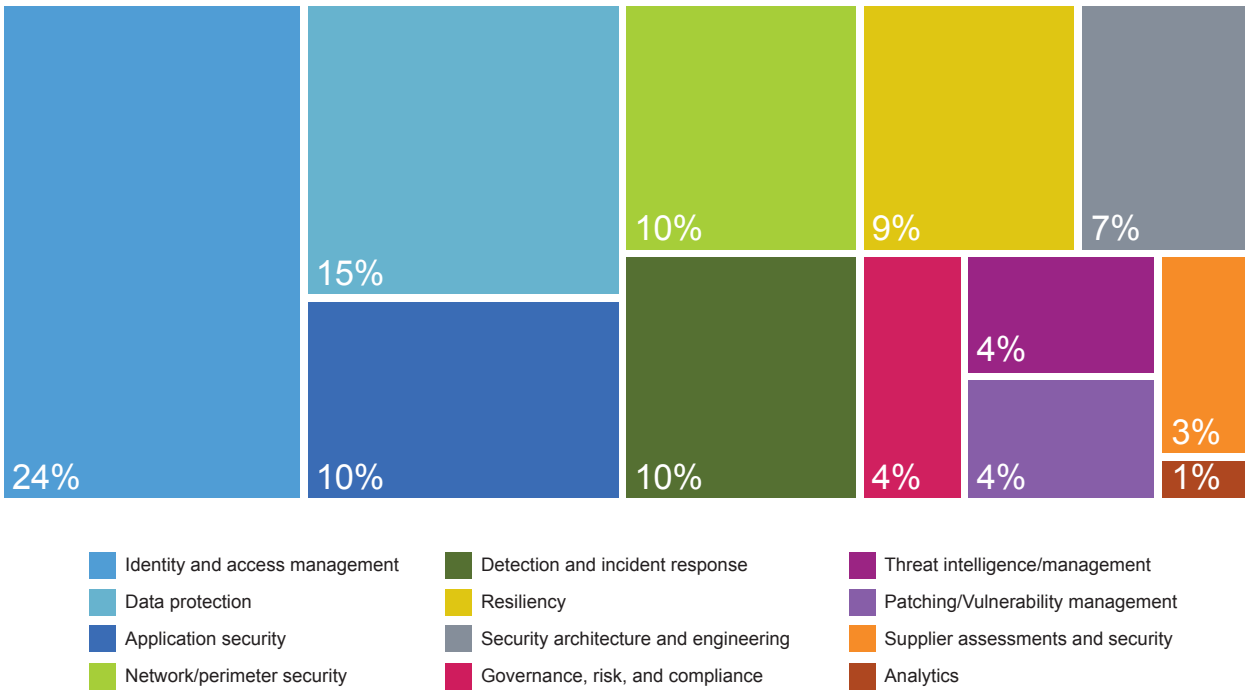
"How does your 2025 information security budget compare to 2024?"



Base: 68 CISOs at organizations with 500 or more employees

Figure 3: CISOs Prioritize Investments in Identity and Data Protection for 2025-2026

"In the next 12 months, what will be your number one area for increased investment?"



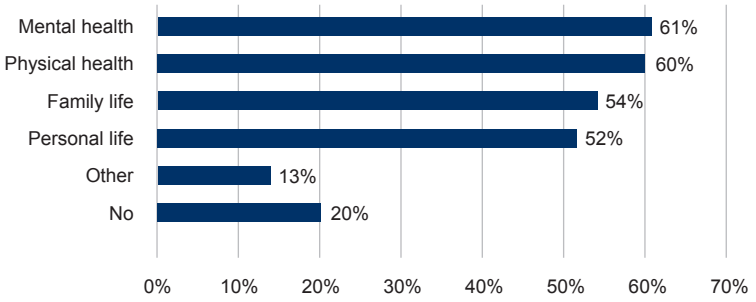
Base: 178 CISOs at organizations with 500 or more employees

CISOs recognize the toll the job takes on themselves and their teams... In Q2 2025, RSAC asked a cohort of Fortune 1000 CISOs whether the stress of their jobs was taking a toll on any aspect of their lives, and just 20% said "No" (see Figure 4).[6] At least 60% of this group report that their mental or physical health has been affected by being a CISO. CISOs serve as their companies' public armor, but in private, they wear the weight of expectations and obligations heavily.[7] And their cybersecurity team members are in the same boat. A 2024 study found that a worrying 78% of respondents were at serious risk of burnout, and the preliminary results from the 2025 study remain concerning, with 66% at risk.[8]

…And are engaging with it seriously. When examining RSAC Conference attendance at sessions on mental health and employee burnout, we found that senior cybersecurity leaders were consistently more likely than average attendees to spend time on those sessions (See Figure 5).[9] RSAC 2021—which was exclusively virtual because of the COVID-19 pandemic—boasted the highest percentage of Call for Submissions proposals on mental health and employee burnout, but it was in 2022 that senior leaders were most keenly interested in the topic (they proved 45% more likely than the average attendee to join those sessions at the 2022 event).

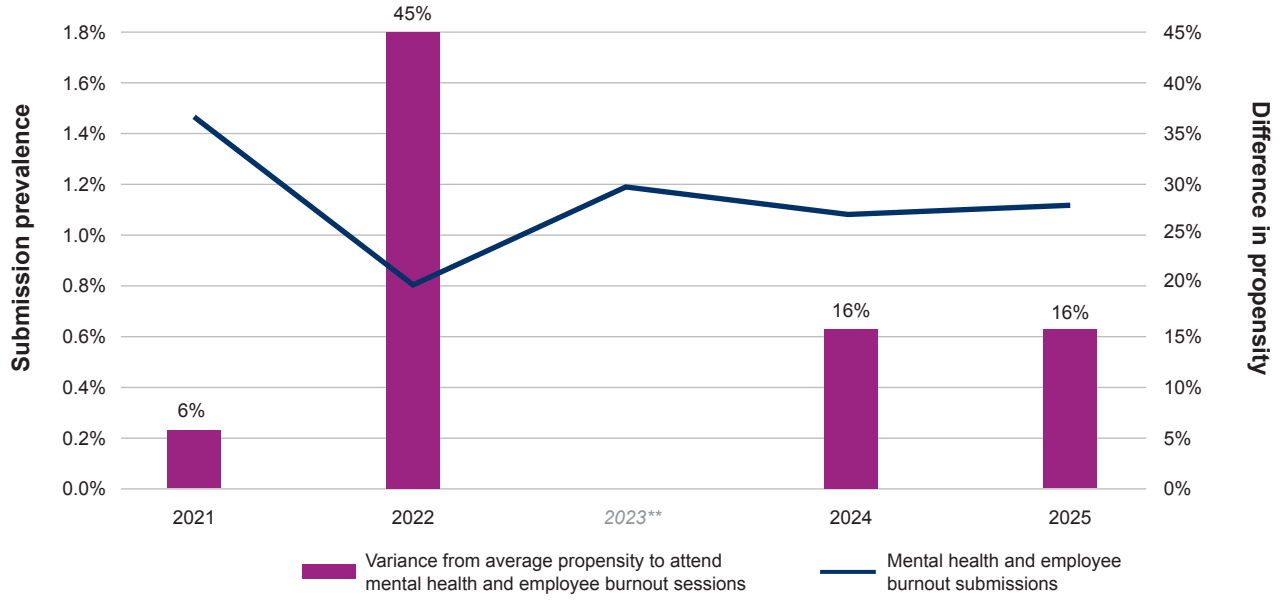
Figure 4: Just 20% of CISOs Think the Stress of Their Jobs Isn't Adversely Affecting Other Aspects of Their Lives

Is the stress of being a CISO taking a toll on any aspects of your life? (select all that apply)



Base: 90 CISOs at Fortune 1000 companies

Figure 5: Cybersecurity Community Mental Health and Employee Burnout Submission Prevalence (left axis) vs. Senior Leaders' Comparative Propensity to Attend Those Sessions (right axis)*



*In the column portion of this chart (right axis), we've measured the senior leaders' propensity to attend the group of mental health- and employee burnout-focused sessions compared with the propensity of the average attendee. All of these percentages are > 0 (except for 2023's; see note ** below) which means that senior leaders were that percentage more likely than average attendees to join those sessions.

**RSAC 2023 Conference did not present any sessions on mental health and employee burnout (none of the entries from the Call for Submissions process were selected for the program).

Unlocking a Cure for Burnout: A Cyber Leaders Forum Case Study

Devon Bryan

SVP, Global Chief Security Officer
Booking Holdings

Dianna Moore

CEO/Managing Partner
Moore Joy Group

Devon, before:

Burnout: Physically and mentally depleted

- **Always on, reactive, no boundaries: Working seven days a week**
- **Inconsistent sleep and exercise**
- **Eating out too often**
- **Health indicators deteriorating, nearly requiring medical intervention**
- **Only work-related development**

Devon and Dianna worked together to do two things:

1) Acknowledge the things Devon cannot control: nation-state adversaries, incidents, emerging threats, regulations, and budget constraints.
2) Take charge of the things he can control: create new, healthier habits (morning/evening routines, nutrition-rich breakfasts, planned workouts), set boundaries, and be intentional about what he says "Yes" to.

Key realization: *"Your capacity to lead under pressure, decision-making clarity, and emotional resilience aren't luxuries. They're prerequisites for your sustained high performance."*

Devon, after:

Breakthrough: Disciplined and healthy

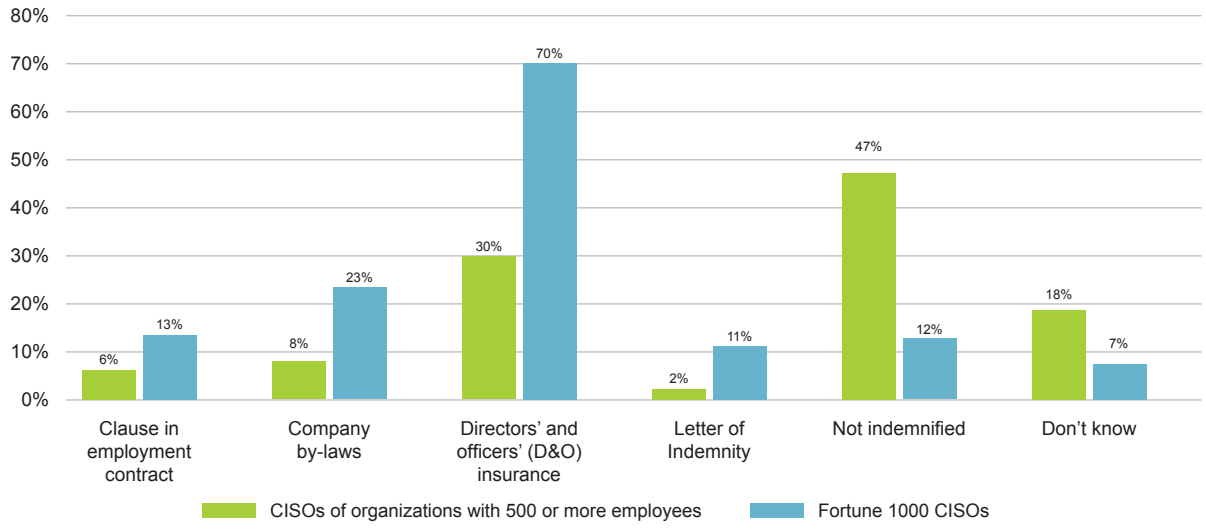
- **Saying "No" more often**
- **Good sleep hygiene, regular exercise**
- **Preparing more meals at home**
- **Health indicators returned to "green"**
- **Prioritizing personal development**

Smaller firms are far less likely to protect their CISOs from personal liability for security breaches. CISOs have worried about personal liability for security breaches at least since 2020, when Uber CISO Joseph Sullivan was criminally charged in relation to the firm's 2016 data breach. In Q2 2025, RSAC surveyed two different cohorts of CISOs on this topic: 1) CISOs from Fortune 1000 companies, and 2) CISOs from organizations with 500 or more employees.[10] Just 12% of that first group say that they're not indemnified by their companies, while 47% of the second group report that they're not indemnified (see Figure 6).[11] Directors' and officers' (D&O) insurance is the most common indemnification vehicle for both groups, and 70% of our Fortune 1000 CISOs report being covered by it.

Senior leaders focus on legal accountability for security breaches. Readers of our RSAC™ Cybersecurity Insights & Futures Volume 1 report may recall our puzzlement that despite 2023's bonanza of legal and regulatory activity (the EU NIS2 Directive came into force, and the US SEC adopted new cybersecurity rules and charged Solar Winds CISO Timothy K. Brown with fraud), C-Level executives at RSAC 2024 were just 7% more likely than average attendees to join sessions about CISO personal liability.[12] That changed at the 2025 event, where nearly 71% of the attendees of those sessions held titles of Director level and above, and senior leaders were 127% more likely than average attendees to join those sessions.[13]

Figure 6: Nearly Half of CISOs of Smaller Organizations Aren't Indemnified

"In your role as CISO, how are you indemnified? (select all that apply)

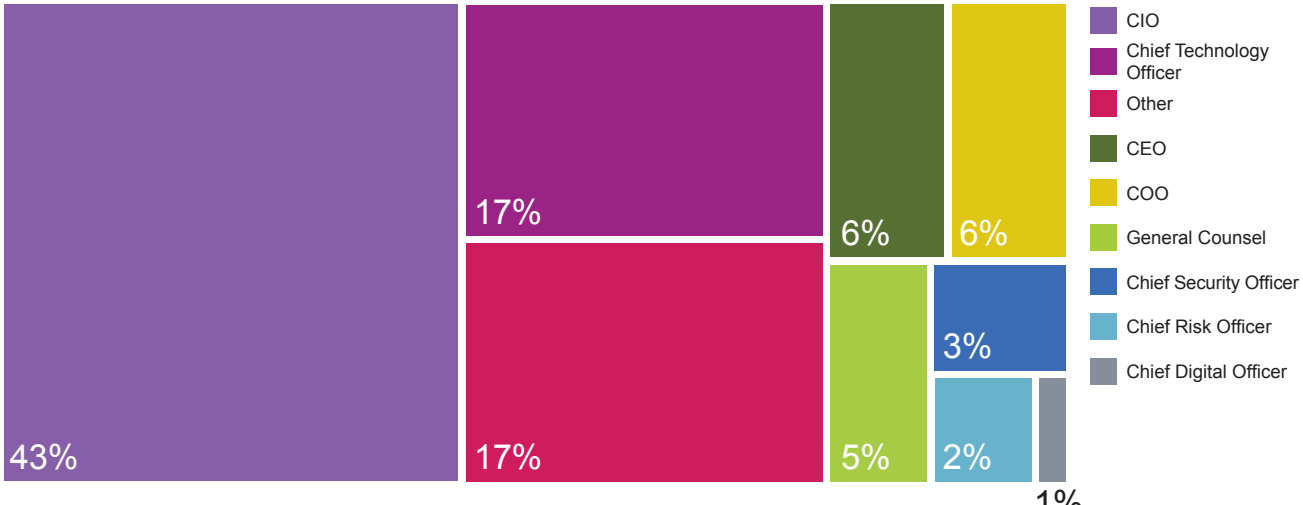


Base: 83 CISOs at organizations with 500 or more employees and 84 CISOs at Fortune 1000 companies

Sixty percent of CISOs report to the CIO or the CTO. The debate over where CISOs should report in the organization (to the CIO or elsewhere?) is a long-running one—and indeed, one of the Top-Rated sessions from RSAC 2025 focused on the impact of CISOs' reporting lines.[14] But who reviews the CISO's performance has remained remarkably consistent. A 2020 global CISO study found that 51% of CISOs reported into the CIO or CTO,[15] and in RSAC's Q2 2025 CISO survey, 60% did so (See Figure 7).[16] And as to the oft-repeated claim that larger firms place their CISOs higher in the organization, the data doesn't support it; if we separate out the Fortune 1000 CISO respondents to our survey, 58% report either into the CIO or CTO. Further, 67% of those Fortune 1000 respondents sit two layers below the CEO. But that doesn't mean the CISO is invisible; 57% of that Fortune 1000 CISO cohort present to committees of their companies' Boards of Directors at least quarterly (see Figure 8).

Figure 7: A Healthy Majority of CISOs Still Report to the CIO or the CTO

"To whom do you report? (direct line)"

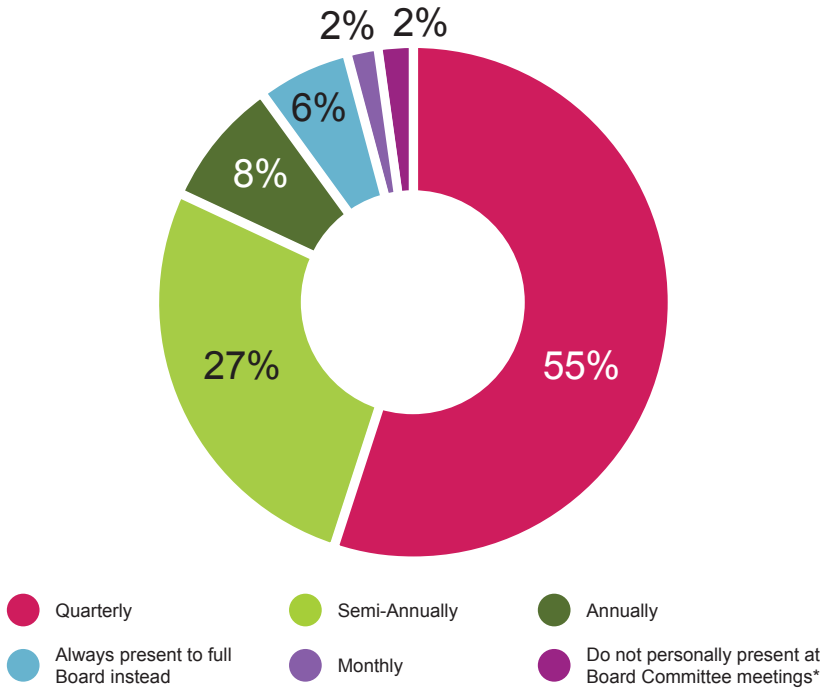


Base: 174 CISOs at organizations with 500 or more employees

Cybersecurity staffers are sticking with their teams… for now. As of Q2 2025, 67% of the CISOs that RSAC surveyed reported that turnover on their security teams for the previous six months had been less than 5% (See Figure 9).[17] But this isn't because security professionals are thrilled with their jobs; RSAC believes that this low turnover primarily reflects the relative softness of the cybersecurity job market that we discussed in Volume 2 of this series.[18] For example, in Q2 2025, nearly half of hiring managers reported that they were able to fill even senior cybersecurity roles—meaning roles that demand 10 or more years of experience—in three months or fewer.[19] But familiar challenges lurk beneath the surface; salaries remain the biggest challenge to retaining security staff, and dissatisfaction with benefits and lack of training opportunities also figure prominently.[20]

Figure 8: A Majority of Fortune 1000 CISOs Present to Board Committees Quarterly

"How often do you personally present at a Board Committee meeting? (regular cadence)"

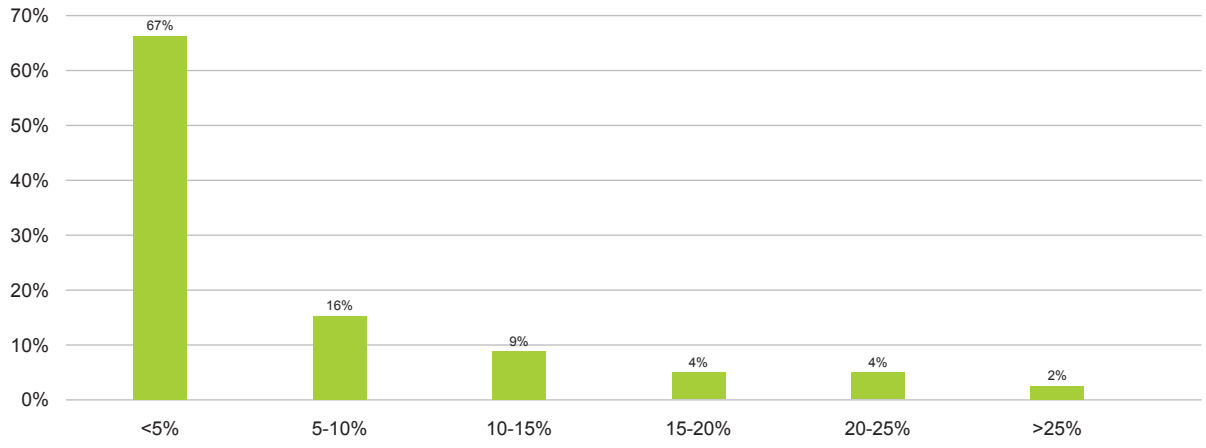


*Covers situations where the CISO may provide written updates and/or another executive (e.g. the CIO) presents at Board Committee meetings.

Base: 86 CISOs at Fortune 1000 companies

Figure 9: Security Team Turnover Is Currently Low

*"Over the last six months, what was the turnover rate for your information security team?"**



Base: 57 CISOs at organizations with 500 or more employees
*Percentages may not total 100% due to rounding.

The Implications: Next Steps for CISOs and Senior Cybersecurity Leaders, and for Technology Suppliers

Here's what RSAC recommends that different segments of the cybersecurity community should do in response to those priorities and challenges:

CISOs and Senior Cybersecurity Leaders

- **Invest in your own resilience.** Readers of Volume 2 in this series may remember that we encouraged leaders to spend more time improving their own skills. That investment should extend beyond new leadership practices to include the tools to establish boundaries and recover from the stress of the role.

- **Monitor yourself and your team members for signs of burnout.** Telltale indicators include irritability, indecisiveness, isolation, emotional exhaustion, and fatigue.[21] If you see those signs, don't jump straight into trying to solve the immediate problem; instead, find the root causes and address them.[22] You should model setting limits, asking for help, balancing workloads, and taking time off to recover for yourself so that your team sees that they have permission to do the same.[23]

- **Protect yourself against liability stemming from a security breach.** In Volume 1 of this series, RSAC predicted that US CISOs will need to worry less about personal legal accountability for security breaches in 2026 because of changes in US SEC enforcement priorities. For US CISOs who aren't indemnified yet, use this breathing space to rectify that. For European CISOs who've thus far been less concerned about individual liability, the Dutch investigation of Clearview AI's directors changes that calculus. Work with your General Counsel and your Head of HR to protect yourself; if your firm offers directors' and officers' insurance, that's likely the easiest route.

- **Don't expect today's low team turnover to last.** In Volume 2 of this series, we also posited that the cybersecurity job market will improve in 2027. To avoid losing your essential people, work with them to define and document their desired growth trajectories. Find out what they value most for that time horizon (it isn't always a raise or a promotion!) and make sure that the chosen path will provide it.

Technology Suppliers

- **Senior buyers seek solutions that use generative AI to improve identity management and crave detailed roadmaps for deploying passwordless authentication...** At RSAC 2025, more than 36% of senior cybersecurity leaders who visited the Expo spoke with two or more identity solution providers. They also flocked to sessions on generative AI and identity, both as a tool for defenders (automating identity governance tasks, authenticating and delegating safely to AI agents) and as misused by attackers ("better" deepfakes), and to sessions that featured detailed case studies of practical passwordless implementations.[24]

- **…And they're also searching for answers to data protection problems old (DLP) and new (securing generative AI systems).** At RSAC 2025, more than 37% of senior visitors to exhibitors spent time with two or more providers of data protection or data security solutions. Senior cybersecurity leaders spent their learning time in sessions on topics from applying generative AI to data loss prevention (DLP) to protecting data in multi-agent AI systems to keeping on top of the latest legal developments.[25]

- **You still need good answers for your prospective customer's CIO or CTO.** Rumors of CISOs reporting directly to Boards or to CEOs have been exaggerated. Because 60% of your CISO buyers report to the CIO or CTO, your proposed solution must demonstrate that it matches the CIO/CTO's overall technology strategy and availability commitments.

Endnotes

1 See for example: 1) LaPiere, R. C. (1934). Attitudes vs. Actions. *Social Forces*, *13*(2), 230-237; and 2) Wicker, A. W. (1969). Attitudes versus Actions: The Relationship of Verbal and Overt Behavioral Responses to Attitude Objects. *Journal of Social Issues, 15*(4), 41-78.

2 From a survey of CISOs at organizations with 500 or more employees conducted by RSAC for an internal research study in Q2 2025.

3 Here and throughout this report, we'll use "senior cybersecurity leaders" to mean people with titles of Director, Vice-President / Senior Executive, or C-Level / President / Member of the Board of Directors.

4 These sessions primarily belong to the "Identity & Authentication" Topic in our RSAC™ Cybersecurity Atlas: Map of Topics toolset.

5 The data protection sessions are more widely distributed across the Topics in our RSAC Cybersecurity Atlas: Map of Topics toolset, but some of the most common Topics where you'll find them are "Zero Trust," "AI & ML Security," "AI & ML Applications to Security," and "Privacy & Privacy Enhancing Technologies."

6 From a survey of Fortune 1000 CISOs conducted by RSAC for an internal research study in Q2 2025.

7 Source: RSAC 2025, "Unlocking Burnout Cure - Secrets from a 5x CISO and 360 Integrated Executive Coach."

8 Sources: 1) 2024: Forrester Research (2024); 2) 2025: Jinan Budge, Forrester Research (2025)

9 These sessions primarily fall under the "Burnout and Employee Retention" Subtopic of "Cyber Workforce Development" and the "Mental Health in Cybersecurity" Subtopic of "Human Element" in our RSAC Cybersecurity Atlas: Map of Topics toolset.

10 There were 84 respondents in group 1), and 83 respondents in group 2).

11 To date, European CISOs have been less concerned about personal liability for security breaches because although the EU NIS2 and some of the member states' additional provisions associated with the EU GDPR offer the possibility of being held personally liable, in practice it's been quite rare. However, there are early signs this is changing. For example: The data protection regulator in the Netherlands is investigating whether it can hold Clearview AI's management personally responsible for GDPR violations, having already fined the company.

12 These sessions primarily belong to the "CISO Accountability and Legal Challenges" Subtopic of "Governance, Risk, and Compliance (GRC)" in our RSAC Cybersecurity Atlas: Map of Topics toolset.

13 See for example: 1) RSAC 2025, "A Deep Dive into the New SEC Cybersecurity Disclosure Requirements"; and 2) RSAC 2025, "The SolarWinds CISO Litigation and What It Means for Your InfoSec Program"

14 See RSAC 2025 Conference, "Reporting Lines Matter: The 2025 CISO's Place in the Org Chart"

15 Source: Heidrick & Struggles

16 From a survey of CISOs of organizations with 500 or more employees conducted by RSAC for an internal research study in Q2 2025.

17 From a survey of CISOs of organizations with 500 or more employees conducted by RSAC for an internal research study in Q2 2025.

18 See also for example: Dice.com

19 Source: ISC2

20 Source: SANS | GIAC

21 Sources: 1) RSAC 2025, "Unlocking Burnout Cure - Secrets from a 5x CISO and 360 Integrated Executive Coach"; 2) Forrester Research; 3) Cybermindz

22 Source: RSAC 2025, "Mental Health In Cybersecurity: Balancing the Scales"

23 Sources: 1) RSAC 2024, "Burnout in Cybersecurity"; and 2) RSAC 2025, "We Will Work 5000 Hours"—One Bank's Journey to Conquer Burnout in Cyber"

24 See for example: 1) RSAC 2025: "AI Era Authentication: Securing the Future with Inclusive Identity"; and 2) RSAC 2025, "Dude, Where's My Password? The Challenges of Getting to Passwordless"

25 See for example: 1) RSAC 2025, "Classify It: Developing a Classification Engine for Data Loss Prevention"; 2) RSAC 2025, "Zero Trust AI: Securing Multi-Agent Systems for Private Data Reasoning"; and 3) RSAC 2025, "Navigating the Legal Landscape: Cyber Law 2025"

RSAC Cybersecurity Insights & Futures, Volume 3 | November 6, 2025

We look forward to bringing you many more reports like this one.
Find all our Insights & Futures reports here.

Visit the library in the RSAC Membership Platform for additional cybersecurity resources.

RSAC
Cybersecurity, Together™

OneRSAC.com