RSAC™

Big Budgets, Accelerating AI: Agents and Post-Quantum Drive the RSAC 2027 Agenda

CYBERSECURITY

INSIGHTS & FUTURES

VOL 7 | NOVEMBER 2026

RSAC Authors:

Laura Koetzle
Head of Community Research

Athanasios Theocharis
Principal Researcher

Introduction

In this report, we synthesize several years of data from RSAC's research with CISOs, the RSAC™ Call for Submissions (including for the forthcoming RSA Conference™ 2027), and session attendance patterns. We use these signals to assess the state of the cybersecurity community in H2 2026 and to recommend steps CISOs and other senior leaders should take now to prepare for what lies ahead in 2027.

Key Takeaways

- Security for AI claimed an unprecedented nearly 20% share of RSAC Call for Submissions (CFS) entries for 2027
- Cybersecurity has grown as a proportion of firms' technology budgets; the largest share of CISOs now claim between 6 and 8% of those budgets
- Post-quantum security's share of CFS proposals grew by more than 50% between 2026 and 2027, catapulting Cryptography back onto the RSAC Top 10 Topics list
- Fortune 1000 CISOs are staying put; 60% report no plans to change roles within the next 12 months

RSAC Top-Level Topics

Figure 1

RSAC assigns all Call for Submissions entries (including the subset selected for our in-person events) to one of the following top-level Topics. We have made minor updates to the Topic list for this report: [1,2]

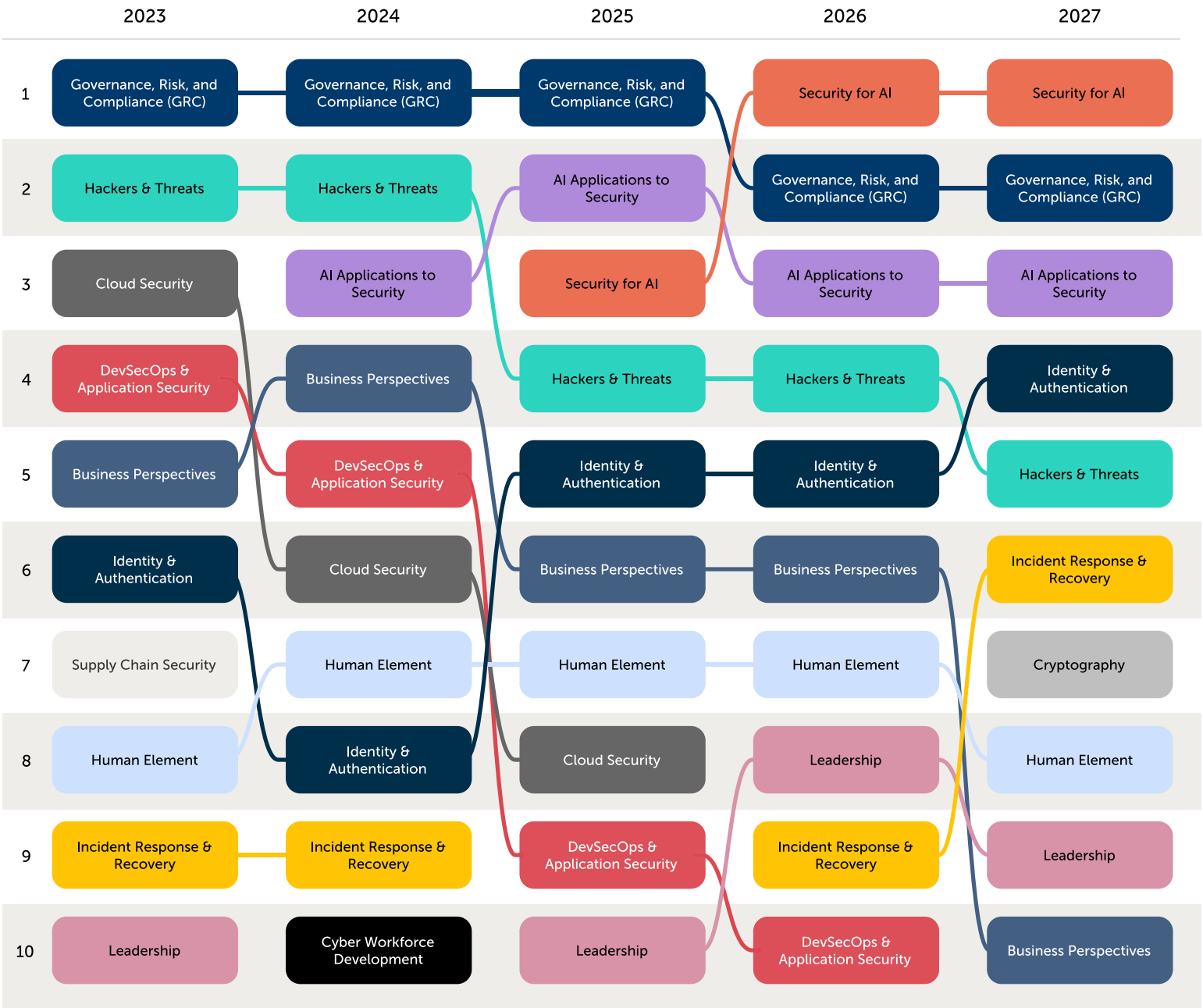
TOPIC	DEFINITION
AI Applications to Security	Use AI to perform security functions
Anti-Fraud	Detect, prevent, and respond to fraudulent activities that target financial & personal info
Business Perspectives	Understand the impact of cyber threats on business operations and align security strategies with business goals
Cloud Security	Protect cloud data, applications, and infrastructure
Critical Infrastructure	Protect essential systems (power grids, water supplies, etc) from cyber threats
Cryptography	Secure information by algorithmically transforming it into an unreadable format that only authorized parties can access
Cyber Workforce Development	Equip cybersecurity team members with the skills they need
DevSecOps & Application Security	Integrate security practices into the whole software development lifecycle
Digital Forensics	Collect, analyze, and preserve digital evidence while investigating cyber incidents
Governance, Risk, & Compliance (GRC)	Implement the frameworks and processes to manage risk and align cybersecurity practices with regulations
Hackers & Threats	Explore the tactics, techniques, and motivations of attackers and the threats they pose to target systems
Human Element	Harness human behavior to improve the effectiveness of security measures
Identity & Authentication	Verify the identity of users and devices to ensure that only authorized entities can access systems and data
Incident Response & Recovery	Processes and strategies for managing and mitigating the impact of cybersecurity incidents
Innovation & Startups	Examine how innovation flows into cybersecurity via the startup and funding ecosystems
Leadership	Develop the skills to lead cybersecurity organizations
Mobile & IoT Security	Secure mobile and Internet of Things (IoT) devices and ecosystems
Offensive Security	Use proactive measures like ethical hacking to identify and exploit vulnerabilities before malicious actors can
Physical Security	Shield physical assets and facilities from unauthorized access, damage, or disruption
Privacy and Privacy Enhancing Technologies	Protect personal data and implement technologies to preserve privacy in digital environments
Security for AI	Secure the AI models and applications themselves
Supply Chain Security	Safeguard the integrity and security of software and physical supply chains
Zero Trust	Implement the Zero Trust security model (grant no implicit trust, continually verify users and devices)

Security for AI Claims Cybersecurity Experts' 2027 Top Spot by a Mile

The 2027 dominance of "Security for AI" is unsurprising, given that RSA Conference 2026 attendees of all levels devoted the largest share of their learning time to it.[3] Further, the cybersecurity community has faced blizzards of AI-driven vulnerability discovery and consecutive months of record-breaking Microsoft Patch Tuesdays since the release of Mythos Preview in May 2026.[4] Security for AI entries already accounted for nearly 13% of Call for Submissions (CFS) entries in 2026, but their share still grew by 50% between 2026 and 2027 to arrive at nearly 20% of the total (See Figure 1). Further, frequent number one Topic "Governance, Risk and Compliance (GRC)" takes second place again for 2027 in large part thanks to AI governance-related proposals, which make up nearly 35% of the GRC Topic total. The "AI Applications to Security" Topic continued to grow to round out the top three; hence, just 3% of RSAC's CISO respondents aren't using AI for security use cases, and 54% reported that the number one benefit they received from using AI to perform security functions was improved team productivity (See Figure 2).[5]

The Top 10 RSAC Call for Submissions Topics, 2023-2027

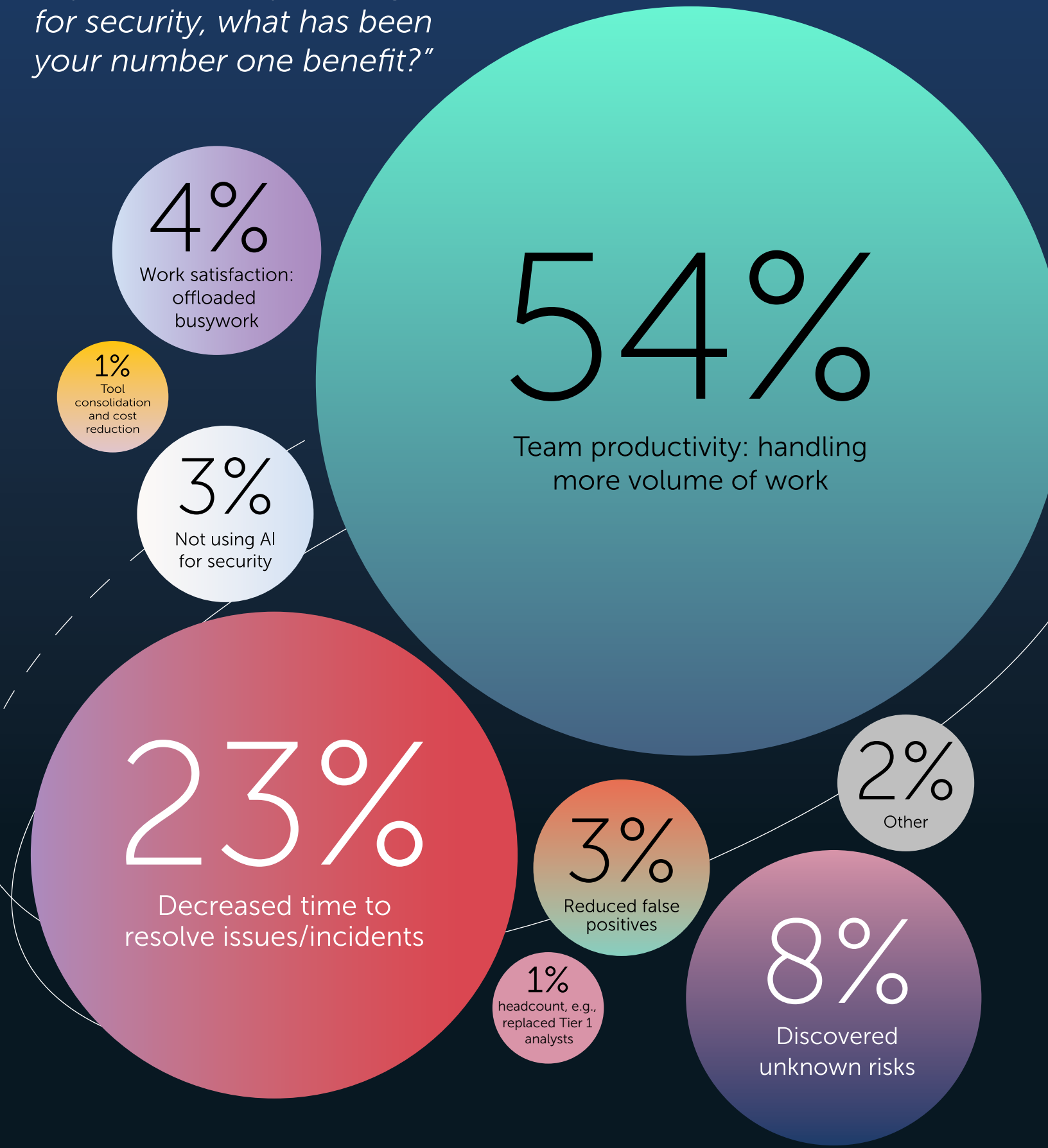
Figure 1



Security Teams' Number One Benefit of Using AI for Security Is Increased Productivity

Figure 2

"If your company is using AI for security, what has been your number one benefit?"



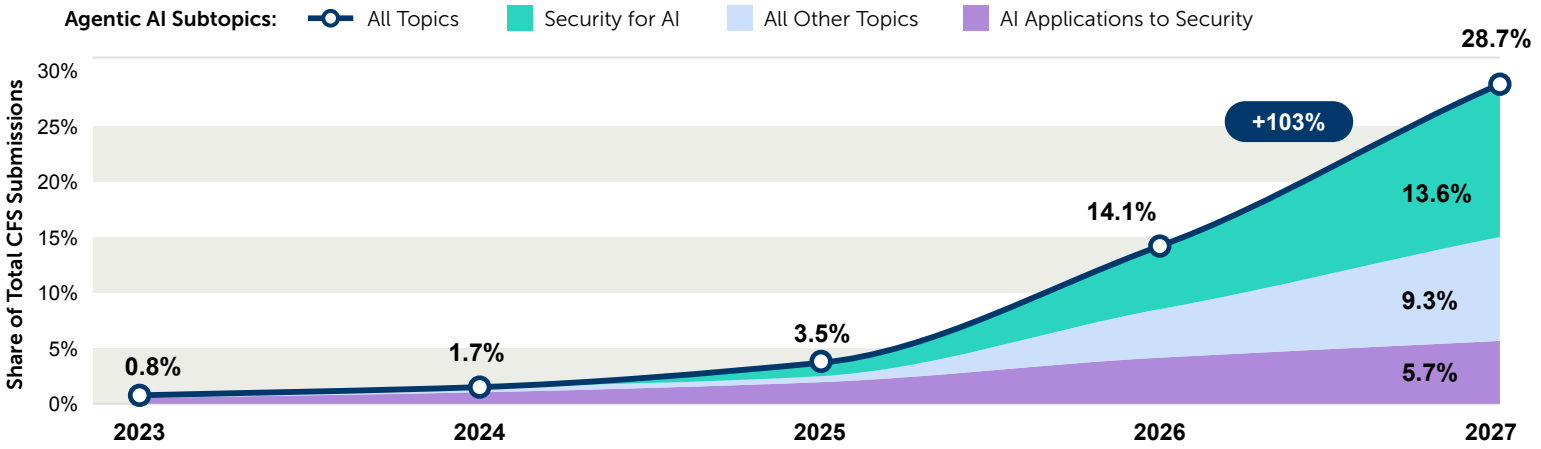
Base: 166 CISOs: 83 Fortune 1000 CISOs, 83 CISOs of firms with 500 or more employees

Agentic AI Security Consumes Nearly 29% of 2027 Proposals

When RSAC extrapolated from the 2026 Call for Submissions, we anticipated that Agentic AI Security's share would grow by at least 30% by 2027; in fact, it grew by nearly 103% (See Figure 3).[6] And at RSAC™ 2026, sessions on Agentic AI Security Subtopic "MCP Agent Security" already consumed the single largest slice of Senior Leaders' learning time.[7] Hence, it's no surprise that RSAC's Fortune 1000 CISO respondents spend a lot of time on Agentic AI, with overprivileged agents and manipulated agents topping their list of concerns (See Figure 4). Those CISOs' top security controls for Agentic AI include AI GRC, placing a Human-in-the-Loop (HITL) for high-risk decisions, and DLP (See Figure 5). However, skepticism of HITL as a viable control has since grown; a tone analysis of HITL-related submissions reveals that more than half of the RSAC 2027 proposals were decidedly negative ("why HITL fails/does not scale").

We Thought Agentic AI Was Already Everywhere in 2026; It More Than Doubled for 2027

Figure 3

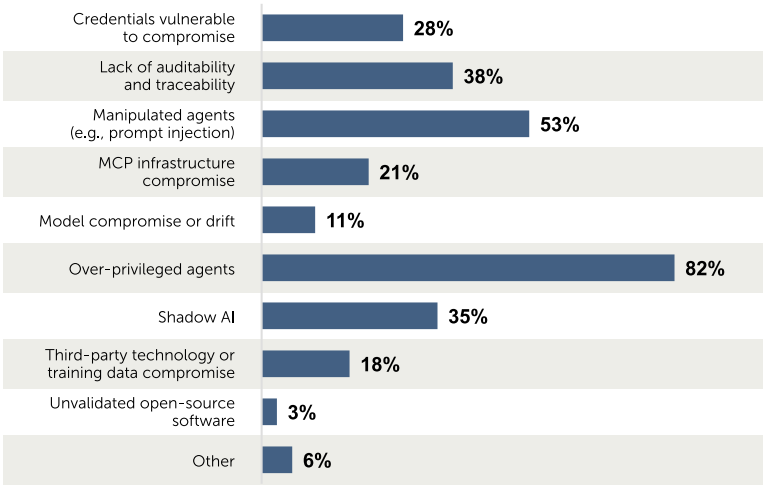


Base: RSAC Call for Submissions entries for 2023 (2,253), 2024 (2,524), 2025 (2,510), 2026 (2,532), and 2027 (3,430)[8]

For Agentic AI, CISOs Worry Most About Overprivileged Agents and Prompt Injection

Figure 4

"As your company increases agentic AI adoption, what are your top three security concerns? (Select up to three answers)"

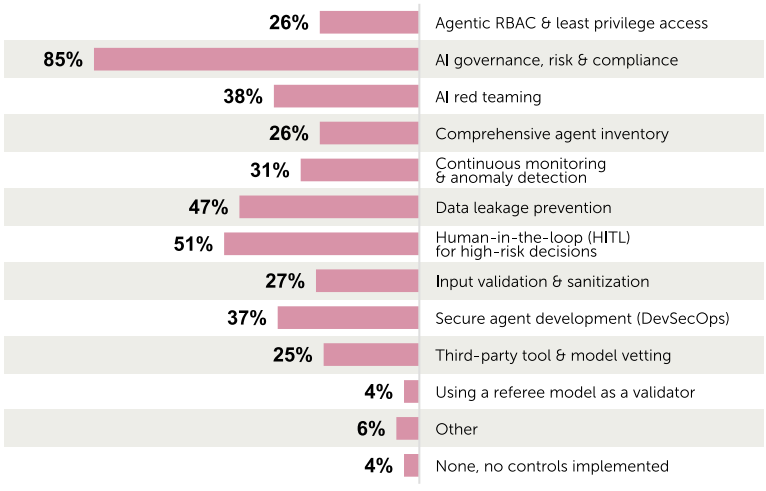


Base: 131 CISOs of Fortune 1000 firms

More Than Half of CISOs Add Humans-in-the-Loop to High-Risk Agent Decisions

Figure 5

"To manage the risks of agentic AI in your organization, which security controls have you implemented? (Select all that apply)"



Base: 123 CISOs of Fortune 1000 firms

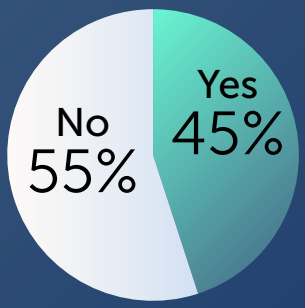
Post-Quantum Security Catapults Cryptography Back Into the RSAC Top 10

The RSAC 2027 Call for Submissions has taken RSA Conference back to our roots; Cryptography has rejoined the Top 10 Topics list for the first time since at least RSAC 2021. Why? Because the long-anticipated surge in detailed guidance on implementing cryptographic agility and sequencing the post-quantum transition has arrived; CFS entries on post-quantum security grew by more than half for 2027 (See Figure 7). And that focus extends to senior cybersecurity leaders; 45% of Fortune 1000 CISOs already include post-quantum risk in their reporting to their Boards of Directors (see Figure 6). Further, nearly 62% of Fortune 1000 CISOs and nearly 51% of CISOs of firms with 500 or more employees expect that their organizations will require the use of post-quantum algorithms within 3-5 years (See Figure 8).[9]

Figure 6

Nearly Half of Fortune 1000 CISOs Track Post-Quantum Risks for Their Boards of Directors

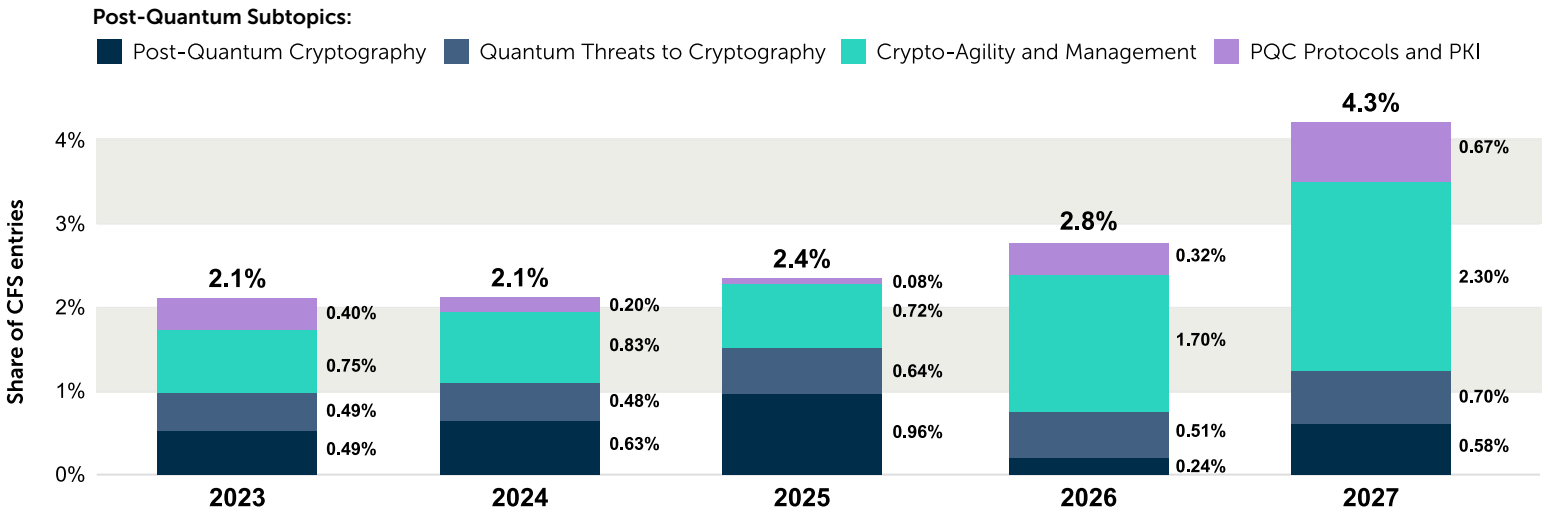
"Are you tracking the risk that post-quantum computing poses to cybersecurity and including it in your reports to the Board?"



Base: 144 CISOs of Fortune 1000 firms

Expert Proposals on Post-Quantum Security Grew by Nearly 54% Between 2026 and 2027

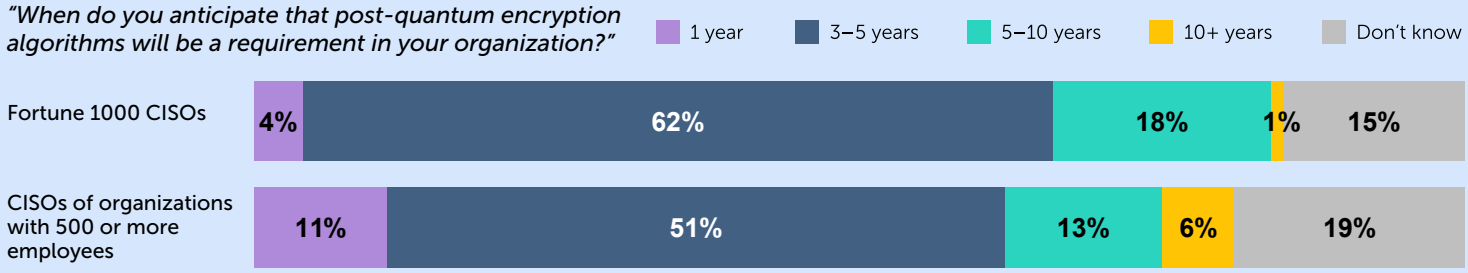
Figure 7



Base: RSAC Call for Submissions entries for 2023 (2,253), 2024 (2,524), 2025 (2,510), 2026 (2,532), and 2027 (3,430)[10]

Majorities of Both Groups of CISOs Expect Post-Quantum Encryption to Be Required Within Five Years

Figure 8

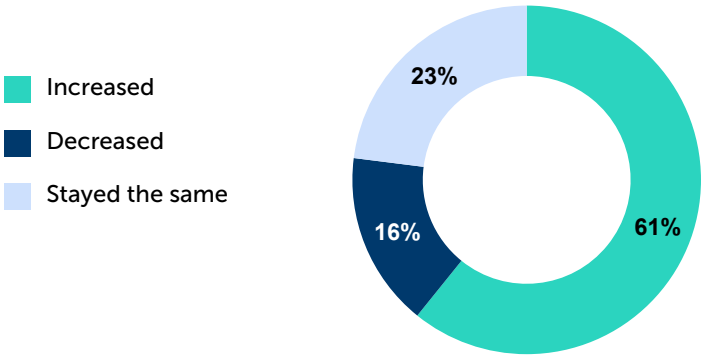


Base: 144 Fortune 1000 CISOs, 83 CISOs of organizations with 500 or more employees

More Than 60% of CISOs Saw Increases in Their Budgets Over 2025

Figure 9

"How does your 2026 information security budget compare to 2025?"

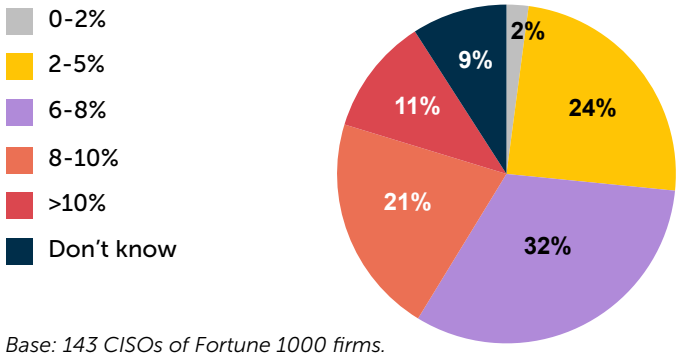


Base: 204 CISOs: 144 Fortune 1000 CISOs, 60 CISOs at organizations with 500 or more employees

Nearly a Third of Firms Allocated Between 6 and 8% of Their Technology Budgets to Security

Figure 10

"What is the ratio between your annual information security budget and technology budget (digital and IT) at your organization?"



Base: 143 CISOs of Fortune 1000 firms. Note that percentages may not total 100% due to rounding.

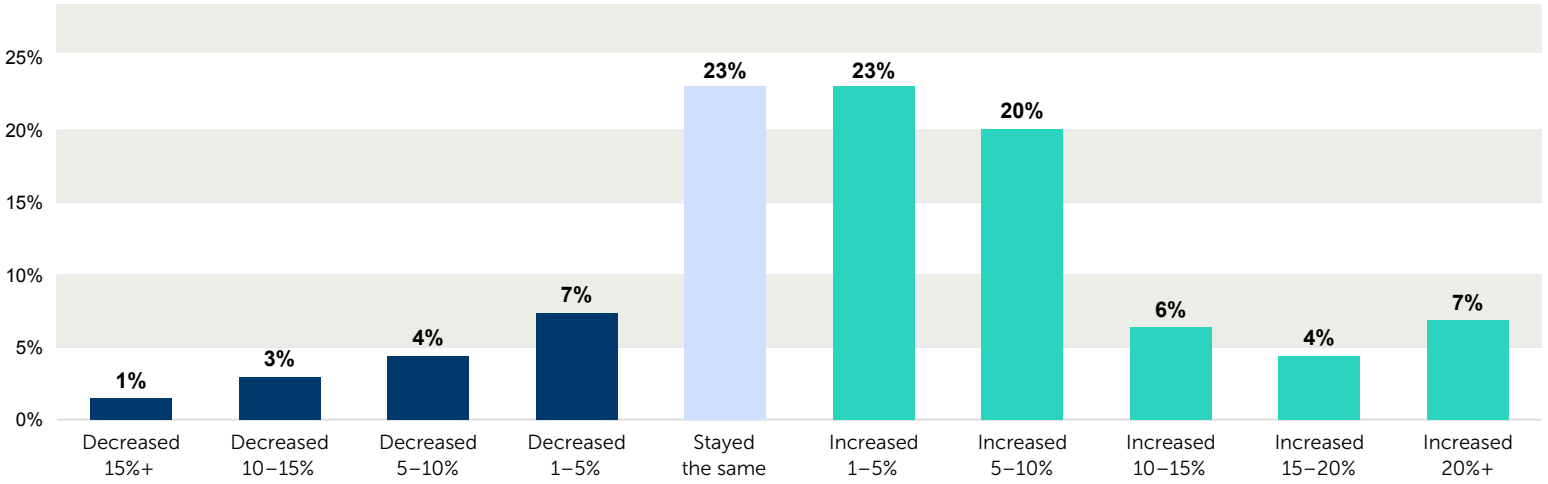
CISOs' Budgets Stay Buoyant in 2026, and Expand as a Share of Tech Budgets

While the security budget picture isn't quite as rosy as when we compared 2025 with 2024, a healthy majority of CISOs still saw increases to their budgets in 2026, and just 16% saw decreases (See Figure 9).[11] Nearly a quarter of CISOs received budget increases of between 1 and 5% over 2025 (See Figure 10). Information security budgets' shares of the technology budget (IT and digital) have also risen, with the largest group (32%) of Fortune 1000 CISOs reporting that their budget accounts for between 6% and 8% of the overall technology budget—whereas in 2024 and 2025, a share of between 2% and 5% was the most common (See Figure 11).

More Than 40% of CISOs' Budgets Increased by Between 1-10% from 2025 to 2026

Figure 11

"How does your 2026 information security budget compare to 2025?"



Base: 204 CISOs: 144 Fortune 1000 CISOs, 60 CISOs of organizations with 500 or more employees. Note that percentages may not total 100% due to rounding.

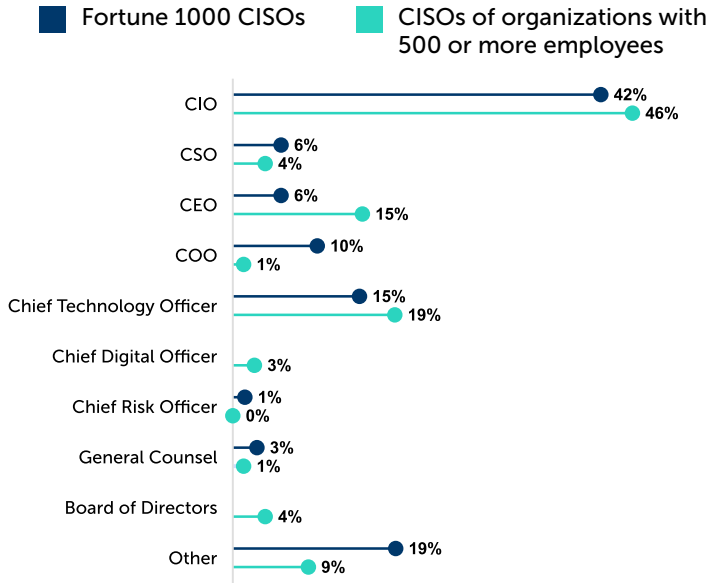
CISO Reporting Lines Have Hardly Shifted, and Team Turnover Remains Low

As in 2025, majorities of the CISOs that RSAC surveyed reported to either the CIO or CTO: 57% of Fortune 1000 CISOs and 64% of CISOs of firms with 500 or more employees did so in 2026, as compared with 60% of the combined group of CISO respondents from 2025 (See Figure 12).[12] Beyond the CIO/CTO reporting lines, the two groups of CISOs do differ modestly in 2026, with a larger share of Fortune 1000 CISOs reporting to the COO (10%), and a larger share of their counterparts at the smaller firms reporting directly to the CEO (15%). CISOs at the smaller firms were most likely to present to their full Boards of Directors quarterly (30%), while just 11% of Fortune 1000 CISOs do the same (See Figure 13). Turnover in security teams has remained low thus far; 71% of Fortune 1000 CISOs in RSAC's survey reported no required staff reductions related to restructuring in the previous 12 months (See Figure 14). Further, 69% of CISOs at the smaller firms reported that total turnover (meaning both voluntary and involuntary) for their teams had been less than 5% for the previous six months.

Nearly 60% of CISOs Report to the CIO or the CTO

Figure 12

"Who do you report to? (direct line)"

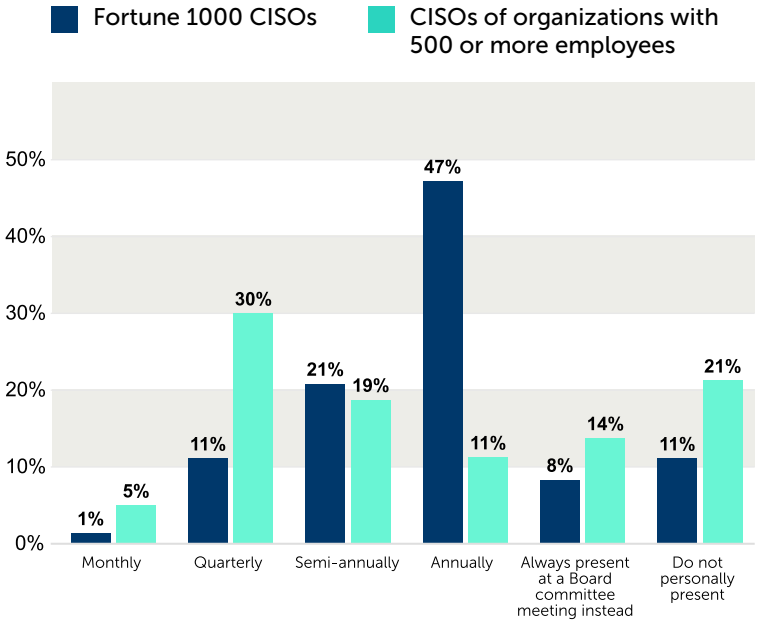


Base: 145 Fortune 1000 CISOs, 81 CISOs of organizations with 500 or more employees. Note that the Fortune 1000 CISO respondents were unable to select "Chief Digital Officer" or "Board of Directors," and note also that percentages may not total 100% due to rounding.

Fortune 1000 CISOs Most Commonly Report to Full Boards Annually

Figure 13

"How often do you personally present to the full Board of Directors?"

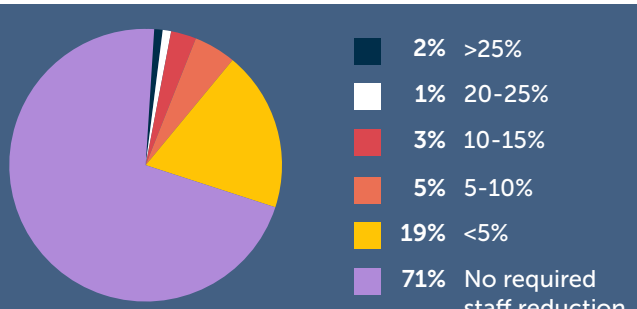


Base: 144 Fortune 1000 CISOs, 80 CISOs of organizations with 500 or more employees. Note that percentages may not total 100% due to rounding.

Figure 14

More Than 70% of CISOs at Fortune 1000 Firms Reported No Required Involuntary Turnover

"In the past 12 months, was there a required reduction in your security staff to meet your organization's restructuring objectives?"

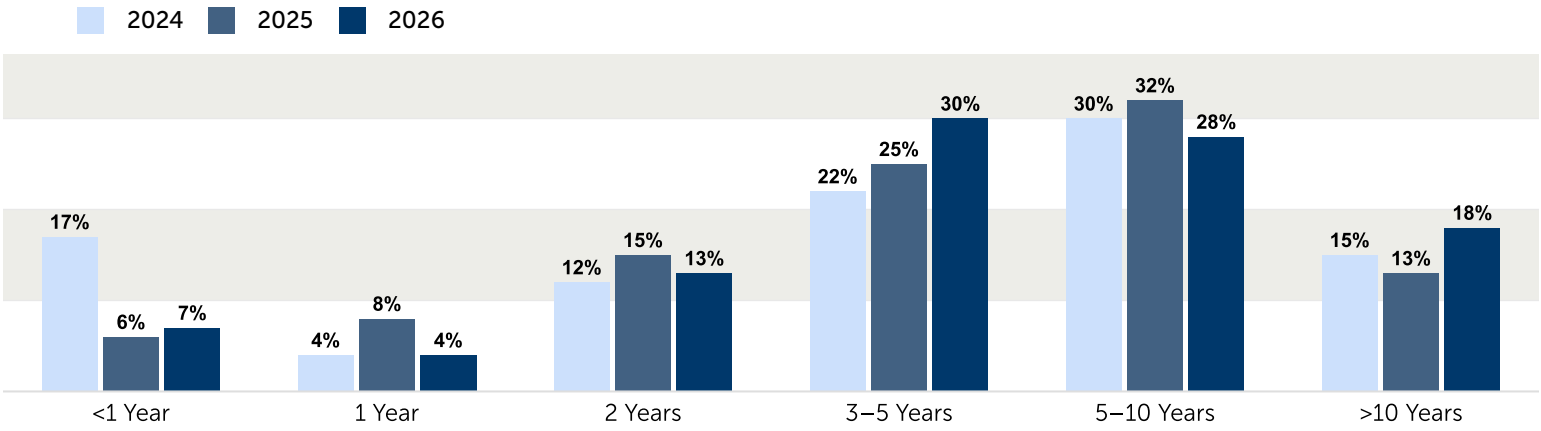


Base: 144 CISOs of Fortune 1000 firms. Note that none of the respondents reported a required reduction of between 15-20%, and note that percentages may not total 100% due to rounding.

More Than Three Quarters of Fortune 1000 CISOs Have Served in Their Current Roles for More Than Three Years

Figure 15

"How long have you been in a CISO role at your current employer? (where CISO = senior executive held accountable for cyber risk by the Board of Directors)"



Base: Fortune 1000 CISOs: 2024 (93), 2025 (94); 2026 (145). Note that percentages may not total 100% due to rounding.

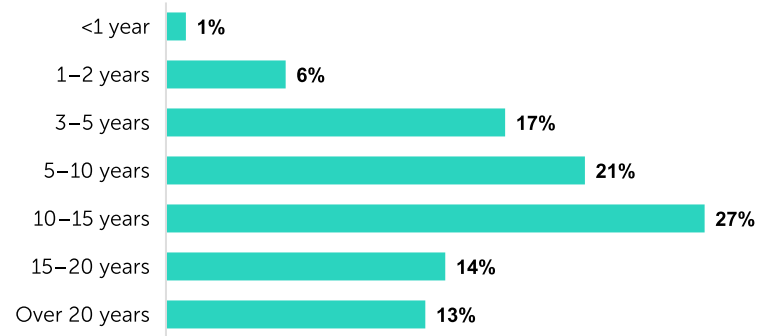
CISO Tenures Are Longer Than You Think, and Rising

Conventional wisdom holds that CISO tenures are short. However, our CISO data says otherwise; 76% of the Fortune 1000 CISOs that RSAC surveyed have occupied their current posts for three or more years, and that share has risen since 2024 (See Figure 15). Indeed, if we examine the arc of those Fortune 1000 CISOs' careers across multiple employers, more than half of them have been CISOs for more than 10 years (See Figure 16). Further, would-be new Fortune 1000 CISOs will find few open positions and stiff competition from sitting Fortune 1000 CISOs for the few roles that do open; 60% of the Fortune 1000 CISOs RSAC surveyed report they have no plans to move on within the next 12 months, while another 21% plan to take another CISO role (see Figure 17). That's changed since 2024, when a total of 65% of the Fortune 1000 CISOs RSAC surveyed were planning to change roles within the next 12 months.

Nearly 55% of Fortune 1000 CISOs Have Held CISO Roles for More Than a Decade

Figure 16

"How long have you been in a CISO role total, including at your current and previous employers?"

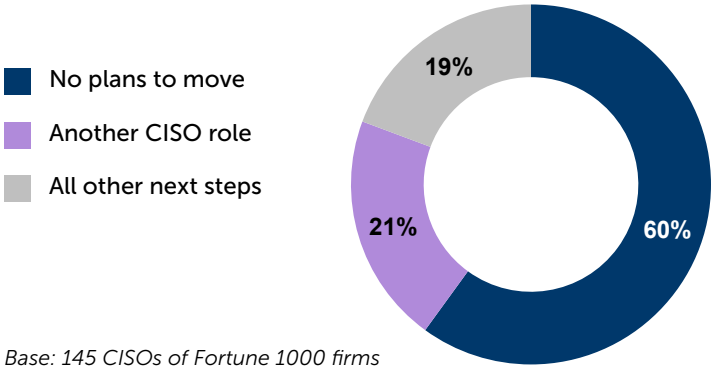


Base: 145 CISOs of Fortune 1000 firms. Note that percentages may not total 100% due to rounding.

A Solid Majority of Fortune 1000 CISOs Plan to Stay Put for at Least the Next 12 Months

Figure 17

"In the next 12 months, if you are considering moving from your current CISO role, what type of role will you be moving to?"



Base: 145 CISOs of Fortune 1000 firms



CISO Checklist

Next Steps

Here's what RSAC recommends that CISOs and other senior cybersecurity leaders do to prepare for what lies ahead in 2027:

NEXT WEEK

Double-Check Your AI Budget for 2027

For those on calendar year budgets, you're likely putting the finishing touches on your 2027 budget now. You've doubtless heard the cautionary tale of Uber chewing through its full-year token budget in about four months, and your company likely already has usage caps in place to minimize billing surprises (if not, work with the contract owners to add them!). If you're like the more than two-thirds of CISOs RSAC surveyed who are either already using AI coding agents to build more of your own tools or planning to do so within six months,[13] plan carefully for rising token costs—Anthropic's recent price structure changes were but the first of many.

WITHIN THE NEXT THREE MONTHS

Treat Your Humans-in-the-Loop as a Scarce Resource

Anthropic calculated that developers using Claude Code approve 93% of prompts, allowing unsafe actions to slip through. This "alert fatigue/vigilance decrement" phenomenon is well-documented; there are decades of studies that show similar behavior in everyone from physicians (overriding drug safety alerts) to radar operators (ignoring submarine signatures), and your cybersecurity team is just as susceptible (for example, a 2025 study found that overloaded SOC operators ignore 67% of alerts). As such, you'll want to carefully ration your AI system's approval prompts so that your security team has sufficient attentional resources and context to make good judgments. So you don't just need a token budget; you also need a "human approval budget."[14]

Give Your Designated Successor a Clear Roadmap and Timeline

If, like the majority of the Fortune 1000 CISOs we surveyed, you don't plan to move on anytime soon, be honest with your deputy CISO or other designated successor about that. If your deputy's timeline is more aggressive than yours, figure out how you can support him/her in finding the right next step outside your company. Further, collaborate with your deputy to develop his/her successor so that you'll have someone prepared to step in as deputy when the time comes.

WITHIN THE NEXT SIX MONTHS

Start Reporting Post-Quantum Risks to Your Board

As we mentioned in RSAC Cybersecurity Insights & Futures Volume 4, many national authorities (including Australia and the EU) have set interim milestones for cryptographic inventory, planning, and starting the post-quantum migration for 2026 through 2028.[15] If you're like the 55% of CISOs who aren't yet including post-quantum threats in your risk reporting for your Board, it's time.

WITHIN THE NEXT YEAR

Re-Examine Your AI Assumptions (and Repeat Every 8-12 Months)

The current rule of thumb holds that the capabilities of open-weight models run six months behind those of published closed-weight models. Further, the rising hardware costs (memory, GPUs, etc.) of self-hosting open-weight models—especially at scale—tip the scales in favor of consuming models via the hyperscalers' APIs.[16] But given rapid AI advancement and token cost growth, smaller, open-weight models will become viable options at some point, despite the hardware costs. Thus, it's worth regularly re-examining your core AI assumptions with your CTO, including: 1) Should you move some workloads to smaller local models? 2) For local models, would local hardware or buying capacity from a hyperscaler or a neocloud like Crusoe or Nebius be more cost-effective? 3) Have you shifted the maximum number of tasks to cheaper (non-frontier) models?

Endnotes

1. RSAC updated the data classification process when incorporating the 2027 Call for Submissions data. We preserved the raw CFS entries, excluded ineligible and test records, and deduplicated equivalent submissions for analysis. We used the 2027 data to discover emerging Subtopics, then reviewed the taxonomy for overlap, clear boundaries and coverage gaps. We classified submissions from 2021–2027 using GPT 6.1 Sol at medium reasoning effort, assigning a maximum of one Subtopic per submission where supported, and selectively reclassified affected submissions after consolidating overlapping subjects and repairing coverage gaps. We reviewed the least-used 15% of Subtopics against the underlying content, retaining useful distinctions and leaving submissions unclassified where no defensible fit existed. The final taxonomy contains 23 top-level Topics (as listed in Figure 1), and 207 Subtopics.

2. Here are the specifics on our minor updates to this list of 23 top-level Topics that we introduced in the RSAC Cybersecurity Insights & Futures Volume 1 report: 1) the "AI & ML Applications to Security" Topic is now called "AI Applications to Security"; 2) the "AI & ML Security" Topic is now called "Security for AI"; 3) we omitted "& ML" from those two Topics' definitions; and 4) we made a few further minor wording changes to other definitions for clarity.

3. See the Volume 6 report.

4. Microsoft's Patch Tuesday release for June 2026 was the largest ever, with 206 CVEs, and the release in July 2026 was larger still, with 570 fixes, followed by a slightly smaller release with 400 fixes in August 2026. Sources: Security Boulevard, Krebs on Security (July), Krebs on Security (August)

5. RSAC conducted internal research surveys of two cohorts simultaneously in Q1 2026. The first cohort consists of CISOs of Fortune 1000 and equivalently-sized non-US firms (the Fortune 1000 index is US-only). The second cohort is composed of CISOs of organizations with 500 or more employees (more than 90% of which are smaller than those in the first cohort). Hereafter, we'll refer to that first cohort as "Fortune 1000 CISOs" or "CISOs of Fortune 1000 firms" and the second cohort as "CISOs of organizations with 500 or more employees" for brevity's sake. These two surveys shared many identical questions, and no individuals responded to both surveys. In cases where the responses to the identical questions do not show a statistically significant difference using a two-proportion z-test, chi-square, or Mann-Whitney U test as appropriate ($p < 0.05$), we report the cohorts combined. Where there are statistically significant differences in the responses, we show those differences. Given the sample sizes, only relatively large differences between cohorts would be detected as statistically significant, so modest differences may exist on questions where results are combined. The number of respondents per question from each group may differ, so we've noted those per question. Because the CISOs responding to RSAC's surveys are not a randomly selected sample, they should not be considered representative of all CISOs.

6. See the Volume 4 report.

7. Where the Senior Leaders cohort includes Director-, Vice President-, and C-Level executives. See the Volume 6 report for the full Senior Leader profile.

8. The "Bases" listed for the 2023-2027 RSAC CFS entries in this Figure represent the total number of completed submissions per year. Note that the public "total numbers of submissions" figures that RSAC releases differ, because those public numbers also include partial submissions.

9. That difference is marginally statistically significant, so we've reported the two groups of CISOs separately.

10. See endnote 8 above.

11. See the Volume 3 report.

12. See the Volume 3 report.

13. From the preliminary results of a survey of CISOs of Fortune 1000 firms conducted by RSAC for an internal research study in Q4 2026.

14. For more on attention and the human factors research behind the idea of the "approval budget," see this Ready Solutions AI blog.

15. See endnote 17 in the Volume 4 report for further details.

16. On rising hardware costs, see for example: SDxCentral, TrendForce

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 36 years and counting at our flagship event, RSA Conference.

At RSAC, our mission is to unite the cybersecurity community to create a safer society. We do this through our RSAC™ Membership Platform and our annual Conference. RSA 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.

RSA 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. Through our Call for Submissions process, RSAC received more than 3,600 proposals from the global cybersecurity community for RSAC 2027.

Additionally, RSA Conference has become a launchpad for groundbreaking cybersecurity startups through initiatives like the RSAC™ Innovation Sandbox contest (ISB), 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. For ISB 2026, which was the 21st edition of the contest, RSAC received over 150 submissions from around the world to compete for an opportunity to be a Top 10 Finalist and ultimately one declared winner.

RSAC 2026 included 600 exhibiting companies, from startups to well-established platform providers. We offer RSAC™ Early Stage Expo for up and comers in the industry; RSAC™ Next Stage for rapidly growing startups; and a sprawling Expo with innovative solution providers from across the globe.

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 and similarly-sized global firms.

Why We Created This Report

The RSAC™ 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 $50.1B in Investments***

*Source: Crunchbase

RSAC™

CYBERSECURITY INSIGHTS & FUTURES
VOL 7 | NOVEMBER 2026

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.

OneRSAC.com

© 2026 RSA Conference LLC. All Rights Reserved.