# RSAC Cybersecurity Insights & Futures, Volume 2

## In 2026, AI Drives More Than Half of All Application Security Startups and Cyber Insurance Premiums Rise


Authors:

**Laura Koetzle**
Head of Community Research
RSAC

**Dario Pasquini, PhD**
Principal Researcher
RSAC

**Chris Gates, PhD**
Director, Research
RSAC



JULY 29, 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 second edition of RSAC™ Cybersecurity Insights & Futures include:

- Executives invest in their own leadership skills
- Leaders find cybersecurity hiring easier
- Cyber insurance premiums rise
- CISOs wrangle with regulators and suppliers about DORA fines
- Fewer startups focus solely on securing the cloud
- Supply chain security rejoins the top 10 list
- Application security uses AI to improve AI-generated code

## 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.

## 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 $16.4B in Investments***

*Source: Crunchbase

# RSAC's Predictions: What CISOs Should Expect, 2026-2028

Planning season often starts for cybersecurity in July and August, so it's an excellent moment for leaders to examine what's likely to happen in 2026 (and selected projections for 2027 and 2028!) and decide on their approach. Here's what RSAC predicts that cybersecurity executives will face, divided into sections:

## Leadership, talent, risk management, and regulation

- **Increased focus on senior leadership skills**
- **A temptation to underinvest in cybersecurity workforce development...**
- **...Leading to costly team departures in 2027 and a snap-back of investment in 2028**
- **Higher cyber insurance premiums, again...**
- **...Driven by rebounding ransomware payouts**
- **Financial services CISOs will tangle with regulators and technology suppliers over EU DORA fines**

## Technology shifts and attacker practices

- **More attackers will get hired as remote workers under false pretenses**
- **Fewer startups will focus solely on securing the cloud**
- **Stricter supply chain security requirements for software and hardware**
- **AI will drive more than half of all application security startups**

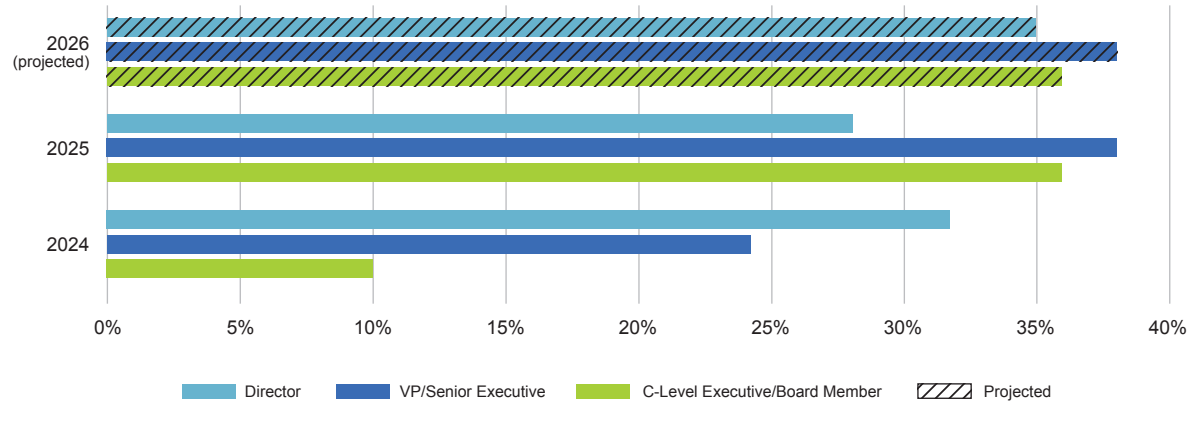
# The Proof: The "Why" Behind Our Predictions

To arrive at our predictions, RSAC synthesized several years of data from our Call for Submissions, Innovation Sandbox competition, Exhibitor descriptions, session attendance patterns, and session evaluations—including data gathered at the most recent RSAC 2025 Conference—and used our RSAC™ Cybersecurity Atlas toolset.

## Leadership, talent, risk management, and regulation

**Increased focus on leadership skills.** *Executives concentrated on refining their leadership skills in 2025, and that trend will continue in 2026.* RSAC Conference attracts many senior cybersecurity leaders—43% of the 2025 event's 44,000 attendees held Director-level or higher positions. At the 2024 event, C-level Executives and Board Members proved only slightly more interested in leadership development than the average attendee (see Figure 1). In 2025, however, they were 36% more likely than average to prioritize those skill-building sessions, and Vice Presidents and Senior Executives were 38% more likely than average to do the same. In 2026, RSAC expects CISOs and VPs to continue that level of investment in leadership acumen, and for Director-level attendees to spend more time on personal development.

**Figure 1: VPs and C-Level Executives' Increased Focus on Leadership in 2025 Will Continue into 2026**



**A temptation to underinvest in cybersecurity workforce development...** *Because a weaker job market is making recruiting easier, CISOs will continue to deprioritize staff development in 2026.* For the past decade, the so-called cybersecurity "talent shortage" has been a top concern for leaders. Whether that talent shortage is real or an artifact of a wish-list approach to hiring, RSAC would have expected cybersecurity executives to prioritize team retention and skills development efforts (see Figure 2). But C- and VP-level participants at the RSAC 2025 event were less likely than the average attendee to spend time attending sessions on team development (see Figure 3).[1] RSAC believes that's because CISOs have lately found recruiting capable staff less difficult than in prior periods, thanks to a combination of: 1) the increased availability of both former US Federal government cybersecurity staff in the US and cybersecurity professionals laid off by large tech firms globally; and 2) the successful adoption of more AI & ML and automation in areas like security operations and application security testing.

## Figure 2: Overspecified Job Postings Worsen the Cybersecurity Talent Shortage

**Director, Information Security**
**Location: Chicago, IL, USA : (full-time onsite)**

Wish list
~~JOB DESCRIPTION~~

**Requirements:**
✓ PhD in computer science or cybersecurity
✓ Certifications: CISSP, CISM
✓ Minimum 17 patents held
✓ Fluent Mandarin or Russian, both preferred

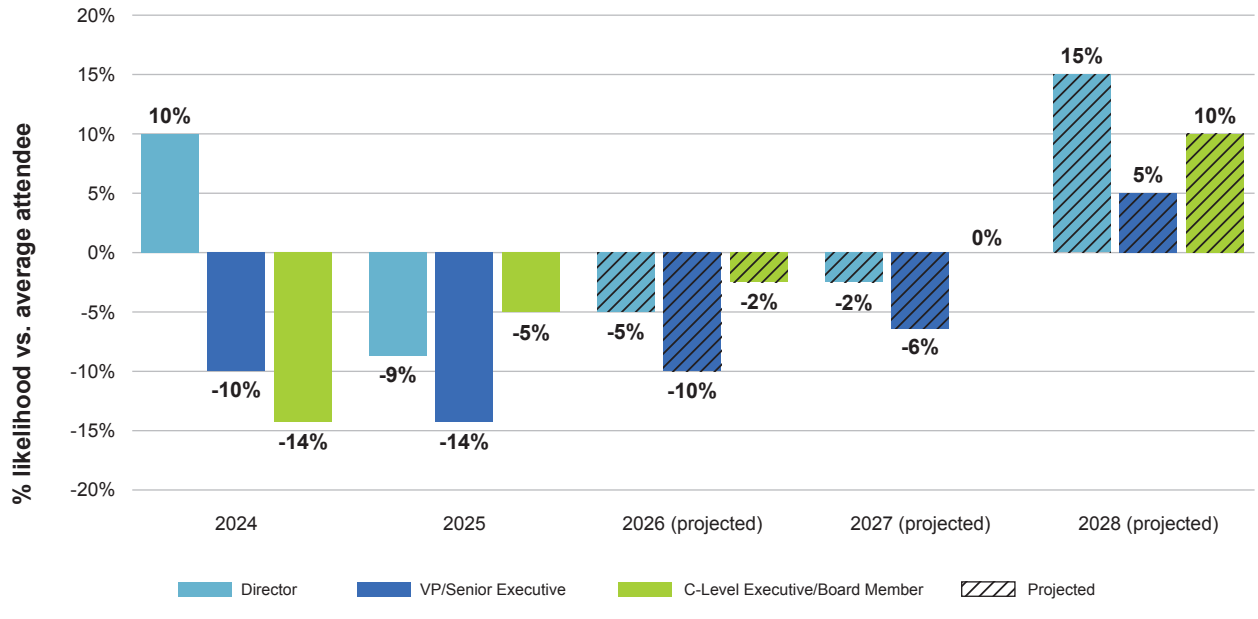
**Experience required:**
• 15 years cloud security
• 12 years forensics
• 10 years threat hunting
• 15 years Zero Trust architecture
• 3 years Agentic AI for security tasks

**Salary: USD $140K - $185K**

Apply | Save Job

**... Leading to costly team departures in 2027 and a snap-back of investment in 2028.** *Executives who ignore staff development in 2026 will suffer in 2027, and they'll return to spending more time and money on workforce development in 2028.* Here's how RSAC predicts this will play out: in H2 2025 and in 2026, some CISOs will be lulled into complacency by the combined impact of that softer job market plus AI & ML-driven time savings that reduce the pressure to add new staff. But cybersecurity leaders who succumb to these temptations will regret it later in 2027; as challenges pile up and the job market improves, they'll lose valuable people who they'll struggle to replace. With the usual caveats about projecting three years into the future in a volatile field like cybersecurity, RSAC expects CISOs to flood back into sessions on upskilling and promoting their teams at RSAC 2028 Conference.

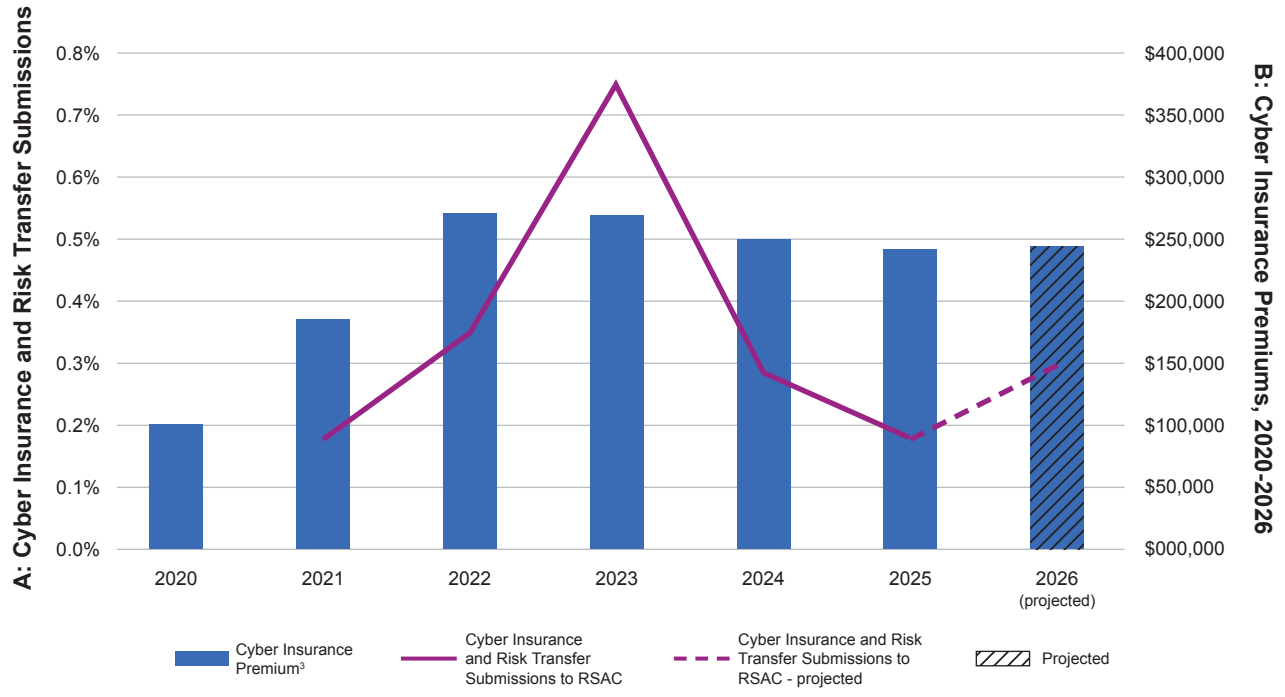
## Figure 3: Costly Team Departures in 2027 Will Drive Executives to Invest in Cyber Workforce Development Again in 2028



**Higher cyber insurance premiums, again...** *In 2026, a firm will pay an average of 145% more than it did in 2020 for the same level of coverage* (see Figure 4). Here's the history that has led us to this point: cyber insurance premiums surged by an average of more than 80% in 2021 and 41% in 2022.[2] To put that in financial terms, if we assume a starting premium of US $100K in 2020, that same company would have paid US $264K for the same level of coverage in 2022.[3] These enormous rises in cost reflect cyber insurers scrambling to recoup their large ransomware-related losses of 2020 and 2021.[4] Cybersecurity community experts' interest in cyber insurance has broadly correlated with changes in premiums, so it's no surprise that cyber insurance's share of RSAC™ Call for Submissions proposals more than doubled between the 2022 and 2023 events.[5]

**...Driven by rebounding ransomware payouts.** *RSAC expects cyber insurance premiums to move from modest declines from mid-2023 through 2025 to increasing by 1% in 2026.*[6] Insurers returned to profitability in 2022;[7] premiums began to decline slightly in the second half of 2023, and that continued in 2024.[8] But in RSAC Cybersecurity Insights & Futures Volume 1, we predicted that ransomware payouts will rise to more than $1.3B for the full year 2025, and insurers will see this impact in H2 2025. Hence, RSAC also expects the 2026 Call for Submissions share of proposals on cyber insurance to return to just above its 2024 level.

**Figure 4: Cyber Insurance Premiums vs RSAC Submission Prevalence, 2020-2026**




**Financial services CISOs will tangle with regulators and technology service providers over EU DORA fines in 2026.** *Given that the EU's Digital Operational Resilience Act (DORA) became applicable in January 2025, RSAC expects regulators to announce their first enforcement actions against violators by April 2026.*[9] DORA applies to all companies that provide financial services to European clients and all technology firms that provide ongoing Information and Communications Technology (ICT) services to EU financial entities; expert estimates of possible maximum fines range from €10M to 2-5% of global revenue.[10] DORA makes financial services firms "fully responsible" for compliance with the regulation even when they've outsourced much of the technology.[11] But "critical ICT third-party service providers" (including public cloud hyperscalers) also receive extra scrutiny under DORA, so financial services CISOs are likely to find themselves in triangular arguments with regulators and cloud service providers about who's at fault for what. GRC was already the most popular topic among financial services attendees at the 2024 and 2025 RSAC Conference events; wrangling over DORA fines will ensure that GRC retains its top spot at the 2026 event.[12]

## Technology shifts and attacker practices

**More attackers will get hired as remote workers under false pretenses.** *RSAC expects cybersecurity experts to continue to spend time hunting these bad actors (many of whom are based in North Korea) in 2026.*[13] From 2021-2024, cybersecurity expert interest in remote work (as reflected in the RSAC Call for Submissions process) correlated with changes in the share of the Canadian, European, and US workforce that worked remotely for a significant number of hours (see Figure 5).[14] We estimate that remote work rates will: 1) decline slightly in the US and Canada for 2025, and increase fractionally in Europe; and 2) rise modestly in all three regions in 2026.[15] However, because of the continued influx of would-be fake IT workers, RSAC predicts that in 2026, cybersecurity experts' focus on securing the remote workforce and remote identity proofing will rebound to its highest level since 2022 (see Figure 6).

**Figure 5: Percent of Workforce Working Remotely, by Region**

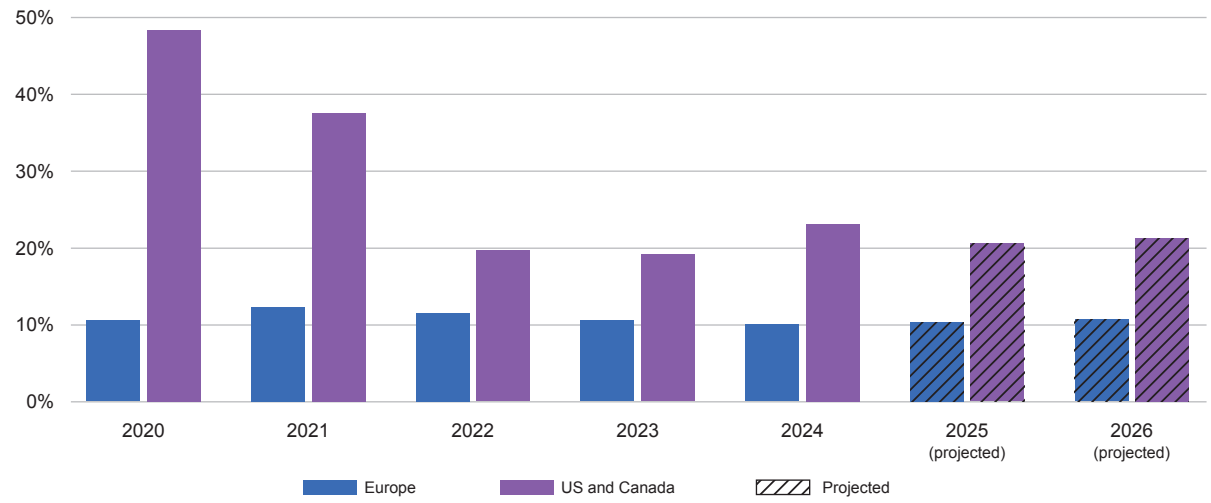
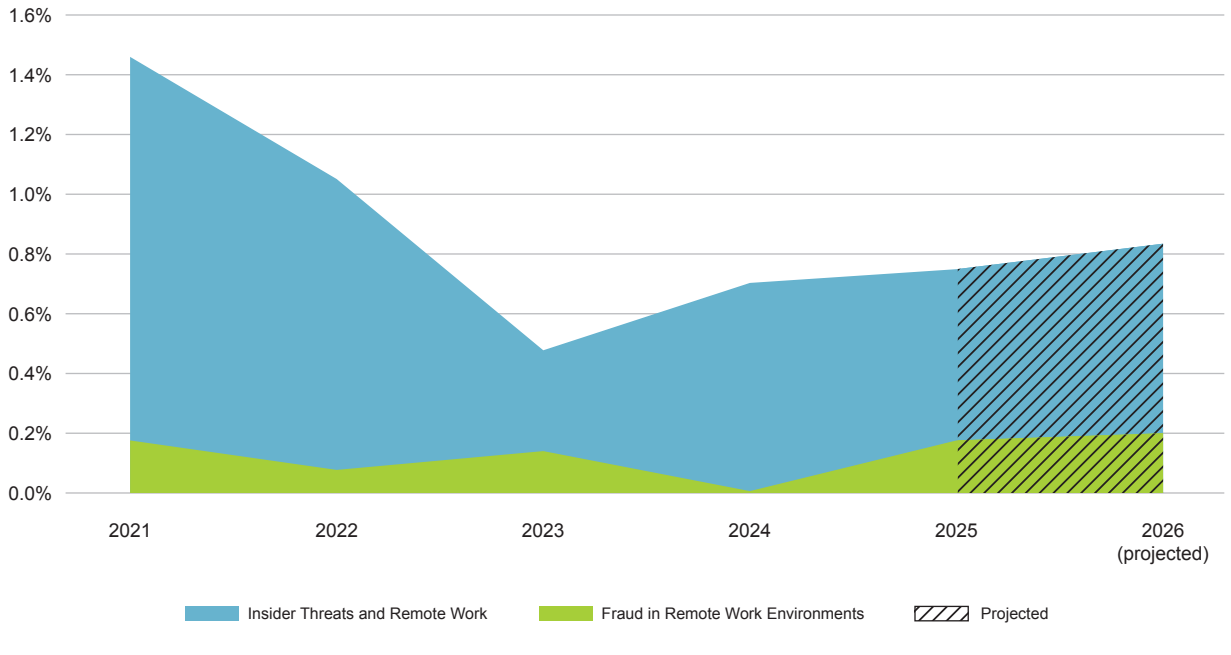
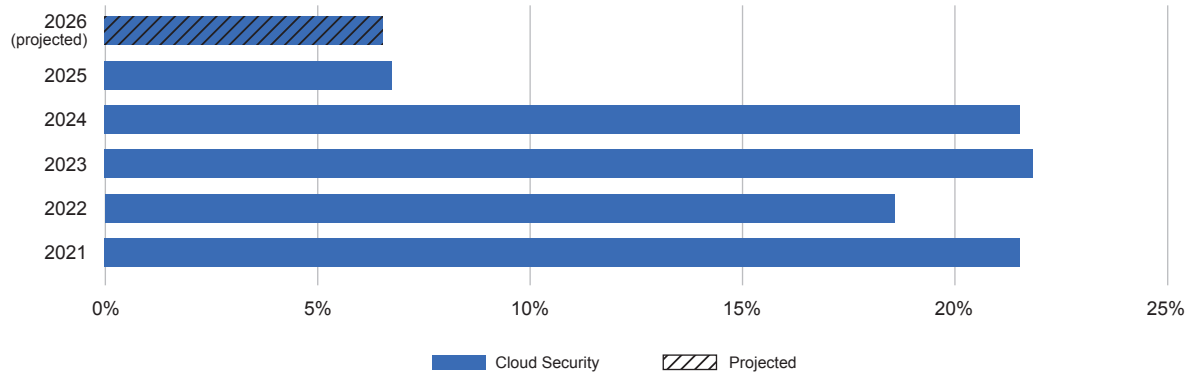



**Figure 6: Remote Work and Cybersecurity Submissions Will Rise in 2026 Despite a Slight Decline in Remote Working**



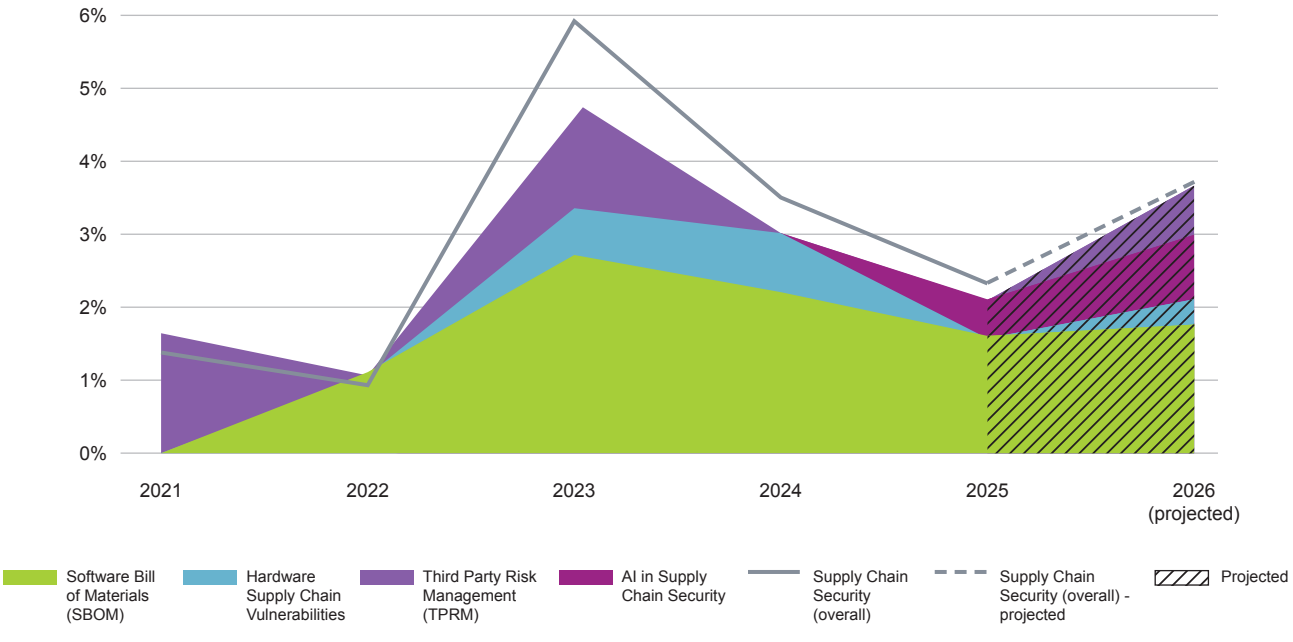
**Fewer startups will focus solely on securing the cloud in 2026.** *Instead, they'll focus on securing AI agents and other applications that live in the cloud.* In 2023, more than 22% of the startups competing in the RSAC Innovation Sandbox contest were cloud security solutions. That share fell to less than 7% by 2025, and we expect it to fall slightly further in 2026 (see Figure 7). This doesn't mean that cloud security is less important, but rather that it, like the cloud, is everywhere. Similarly, in a large study of US cybersecurity recruitment, cloud security's share of posted cybersecurity roles fell steadily from 2022-2024.[16] RSAC considers this healthy; it means that professionals throughout cybersecurity teams are successfully incorporating aspects of cloud security into their work.

**Figure 7: Cloud Security's Share of Startups Declines—and That's a Sign of Maturity**

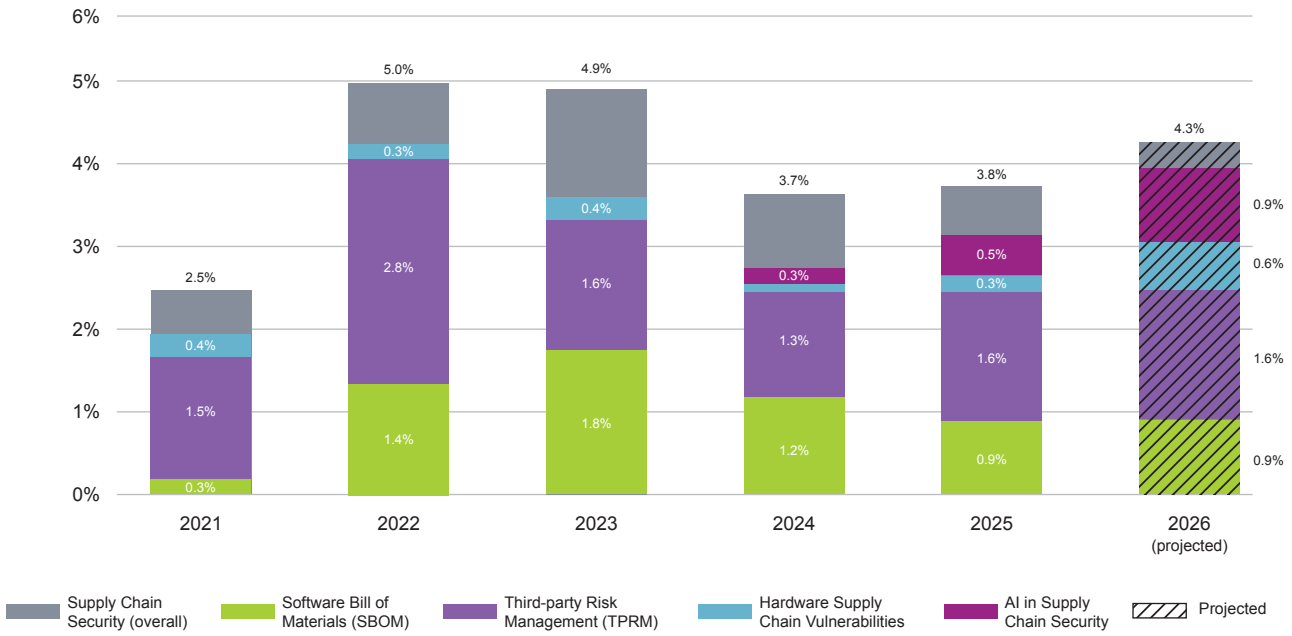



**Stricter supply chain security requirements for software and hardware.** *RSAC expects supply chain security to re-emerge as a top 10 priority for the cybersecurity community in 2026.* Further, we predict that in 2026, supply chain security will account for nearly 3.7% of Innovation Sandbox startups and nearly 4.3% of the Call for Submissions total (see Figures 8 and 9). We rely on several assumptions to make these predictions, including that: 1) cybersecurity experts will continue to grapple with the impact of AI & ML applications on the software supply chain; 2) the rapid proliferation of LLM-generated code will raise new third-party risk management concerns; and 3) hardware and software manufacturers must prepare for EU Cyber Resilience Act reporting in September 2026 and enforcement in December 2027.[17]

**Figure 8: Supply Chain Security Startups Will Rebound in 2026**

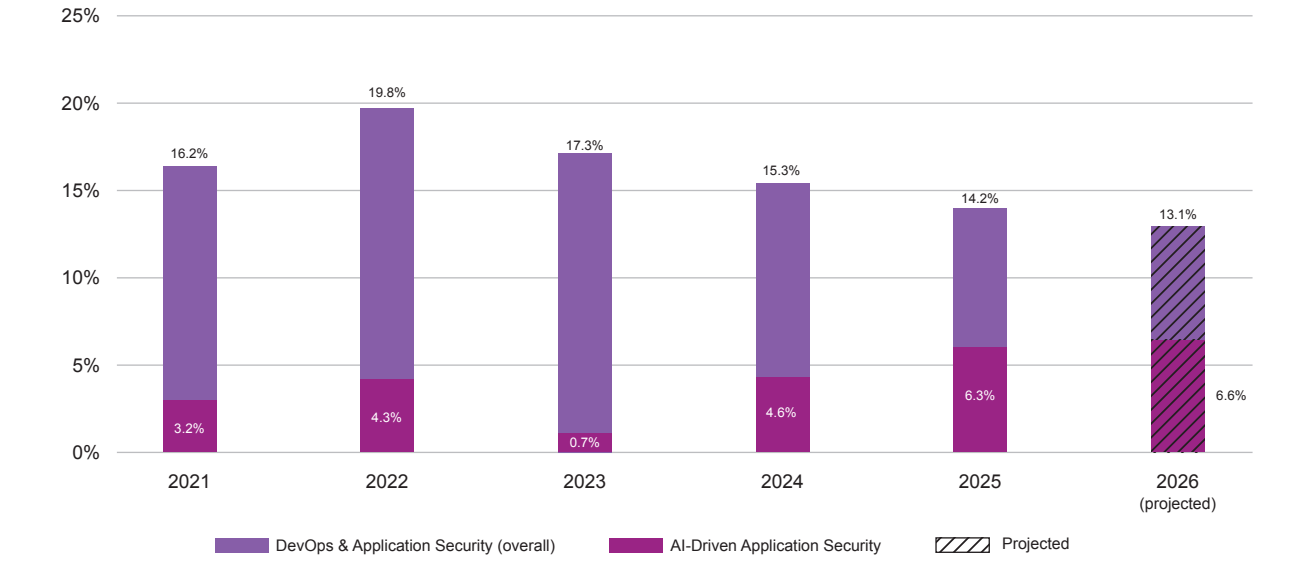


## Figure 9: Expect More Community Focus on Hardware and Software Supply Chain Security in the 2026 RSAC Call for Submissions




**AI will drive more than half of all application security startups in 2026.** *RSAC predicts this will be true of both our Innovation Sandbox contestants and of the cybersecurity industry overall.* Application security startups represented the largest or second largest group of RSAC Innovation Sandbox participants every year from 2021-2025. And we expect that more than 13% of the entries for Innovation Sandbox 2026 will be application security startups, but that slightly more than half of those (i.e. 6.6% of the total) will focus on "AI-Driven Application Security" (see Figure 10).

## Figure 10: In 2026, More Than Half of Innovation Sandbox Application Security Startups Will Be AI-Driven



# RSAC's Recommendations: What CISOs Should Prioritize in 2026-2028

Here's what RSAC recommends that cybersecurity leaders should do in response to our predictions:

## Leadership, talent, risk management, and regulation

- **Spend *more* time on improving your own skills.** Cybersecurity professionals are perpetually living in interesting times, and CISOs must be able to lead effectively through rapid change and keep their best people from burning out. Modest executives might be tempted to view resources spent on increasing their own leadership acumen as selfish, but the reverse is true: a better-equipped leader benefits the whole team.
- **Invest *more* in cybersecurity team talent development.** Resist the temptation to deprioritize team talent development as recruitment becomes temporarily easier and AL & ML help existing staff achieve greater productivity. Leaders who continue investing time and money in their team's skills will avoid expensive departures when the job market improves in 2027, and they'll be able to scoop up additional talent from firms that unwisely throttled spending on team upskilling.
- **Start negotiating with your cyber insurer early to lock in a lower premium *before* rates start to rise.** Leaders with cyber insurance renewals scheduled for April 2026 or later should pull them into Q1 2026 or earlier. Some insurers offer incentives for early renewals, and firms that renew in Q1 2026 should be able to avoid the predicted 1% premium rise. We realize that 1% doesn't sound like much, but remember that this is another 1% on top of the more than 143% average increase since 2020 that companies had to swallow at their last yearly renewals!
- **Financial services: Meet with the relevant European national authority for DORA to clarify its approach to issues that involve both a covered firm and a critical ICT third-party service provider.** This won't come as a surprise to CISOs at large banks and insurers who are used to meeting with European regulators, but for CISOs at fintechs and other firms less accustomed to working with them: the primary regulator will be happy to meet with any firm it supervises to answer questions. Good connections with the regulator will make it easier to collaborate during an investigation or a dispute with an ICT service provider.

## Technology shifts and attacker practices

- **Give recruitment, HR, service desk, and finance colleagues the insight they need to help spot attackers masquerading as remote workers.** These colleagues can help cybersecurity teams spot fake remote workers who pose a threat to the company. Recruiters should insist on in person or live video interviews and compare identification documents with video.[18] HR and service desk staff who process new employees should flag changes to corporate device delivery addresses as signs that new employees require further investigation, and payroll accountants should look for bank deposit details that change after hiring.[19]
- **Continue investing in cloud security skills for all team members.** Given the ubiquity of public cloud deployment, don't hire more cloud security specialists—instead, invest in cross-training and upskilling for as many of your cybersecurity team members as possible.
- **Ask suppliers whose applications incorporate generative AI for details in a defined format that builds on Software Bill of Materials (SBOM).** There's no universal standard for documenting generative AI applications yet, but extending SBOM with projects like AI Bill of Materials (AI BOM) and SBOM for AI is a good start. And firms subject to the EU AI Act and the EU Cyber Resilience Act will need to be able to provide this detail.
- **Allocate budget to skills development and tools for application security specialists who need to vet AI-generated code.** As of May 2024, more than 63% of professional developers reported that they were already using generative AI in their work, so CISOs should expect a large chunk of the code making its way through their development pipelines to be AI-assisted.[20] The good news? The "Sec" part of DevSecOps can use these tools too; they're great for use cases like enforcing secure coding standards and automating risk assessments as part of the delivery pipeline.[21] CISOs should make sure that application security teams are well-versed in, and able to implement guardrails for, the AI Code Assistants that the firm's developers use.[22]

## Endnotes

1 These sessions primarily fall under the "Cyber Workforce Development" top-level topic in the analysis that feeds our RSAC Cybersecurity Atlas: Map of Topics toolset, and they're listed under the "Professional Development & Personnel Management" category in the RSAC Membership Library for 2024 and earlier.

2 Sources: 1) 2021 increase: Insurance Journal, Marsh (2021); 2) 2022 increase: Cybersecurity Dive, Marsh (2022)

3 Data on actual cyber insurance premiums paid by large US enterprises (with more than US $1B in revenue) in 2020 is quite sketchy. RSAC is deliberately using a lowball estimate of US $100K for US $68M in coverage, which is rounded from the US $101K that we calculated as a straight multiple of the USD $1,485 per year paid by smaller enterprises with $1m in revenue for $1m in coverage with a $10K deductible, as our example to demonstrate the effects of premium rises. Sources: a) For the US $1,485 paid: AdvisorSmith; b) For the US $68M in coverage, extrapolated linearly from the figures for 2019 and the percent change from 2018: Business Insurance

4 Loss ratios in 2020 and 2021 across the cyber insurance industry averaged around 70%, and insurers need to keep loss ratios below 60-65% to offer the coverage profitably. Source: Alliant. Ransomware payouts totaled an estimated US $765M in 2020 and US $766M in 2021. Source: Statista

5 Note that the RSAC Call for Submissions deadline for the 2023 event was in October 2022.

6 Note that the consensus industry estimate is -6% for 2025, but RSAC estimates a more pessimistic -2.5% because we believe ransomware-related payouts and damages will be larger in 2025 than the industry was anticipating at the beginning of 2025, and that contracts signed in the second half of 2025 will start to reflect those payouts and damages. And then RSAC expects that in 2026, the average company will pay a 1% rise in premiums. 2025 consensus source: Marsh

7 S&P estimates the 2022 loss ratio to be 43.1%, which indicates that the insurer profited by offering the coverage. Source: S&P Global

8 Sources: 2023: Marsh (2023); 2024: Marsh (2024)

9 This enforcement action timeline may sound slow given that the EU's GDPR became applicable in May 2018 and the Portuguese data protection authority issued its first fine just two months later. Source: Covington & Burling. We expect the first DORA action announcements to take longer because each country's national supervisor first had to gather data and submit it to the appropriate EU-level supervising authority; the deadlines for this were in April 2025, and enforcement processes began thereafter. Source: ESMA

10 Like the GDPR, EU DORA applies to all firms who meet the criteria regardless of where they're located or headquartered. The European Commission clarified that ICT services must be provided on an ongoing basis to be covered by DORA. Source: EIOPA. But unlike the GDPR, the DORA regulation doesn't specify absolute numbers or percentages for monetary fines, and no fines have yet been announced, so estimates vary. See for example: IFSC

11 See EU DORA article 28:1:a. Source: European Union

12 By "topic," we mean one of the top-level topics we use to categorize our Call for Submissions data in our RSAC Cybersecurity Atlas: Map of Topics toolset.

13 There have been many public reports of North Korean attackers successfully getting hired by large multinational companies, including KnowBe4 and Google Cloud. Sources: KnowBe4, Google Cloud

14 We used the Canadian, US, and European data because accurate data on remote working is too scarce for other regions to include them. For example, of the major Asian economies, only Japan and Australia publish figures, and in Latin America, only Brazil publishes reliable data. Sources: 1) Europe 2020-2024: Eurostat; 2) US 2019-2021: US Bureau of Labor Statistics (BLS) (Vol 13, Oct 2024); 3) US 2022: US BLS (2024); 4) US 2023: US BLS (2023); 5) US 2024: US BLS (Vol 14, 2024); 6) Canada 2020-2023: Statistics Canada (11-631-X2024001); 7) Canada 2023-2025: Statistics Canada (33-10-0836-01), Robert Half International (Canada)

15 US projections based on: US BLS (April 2025), US BLS (Vol 14), and Robert Half International (US). Canadian projections based on: Statistics Canada, Robert Half International (Canada). Our average percentages of the workforce working remotely for the US and Canada are weighted for population (as of 2025, the US has roughly 8.2 times as many people as Canada). We have not labelled this as "North America" because we were unable to include Mexico due to the lack of published official data on remote working rates in Mexico. European projections based on: 1) France: Insee; 2) UK: Statista; 3) Germany: Ifo Institute; 4) Europe 2020-2024: Eurostat

16 Source: CyberSN

17 Source (dates): Germany, Federal Office for Information Security (BSI)

18 For financial services firms with training for customer service or fraud prevention teams on how to spot attackers trying to fool remote know-your-customer procedures, the tools that attackers masquerading as potential remote employees use are similar, so recruiters could use that training to learn how to spot malicious applicants.

19 Sources: RSAC 2025 Conference: "DPRK Remote IT Workers – Have You Hired One and Are You at Risk?", and RSAC 2025 Conference: "Hacking Exposed: Next-Generation Tactics, Techniques & Procedures"

20 Source: Stack Overflow

21 Source: RSAC 2025 Conference, "DevSecOps Revolution: Unleashing Generative AI for Automated Excellence"

22 By AI Code Assistants, we mean tools like GitHub Copilot, Amazon Q Developer, or Google Gemini Code Assist.

**RSAC Cybersecurity Insights & Futures, Volume 2 | July 29, 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**