RSAC Cybersecurity Insights & Futures, Volume 4

79% of Our Predictions Made the Grade, and CISOs Should Invest in Secure Vibe-Coding and Agentic AI Skills in 2026

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

Athanasios Theocharis
Principal Researcher
RSAC

JANUARY 21, 2026

For 35 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 fourth edition of RSAC™ Cybersecurity Insights & Futures include:

- Half of our predictions were right on target
- US CISOs can worry less about personal liability for breaches in 2026
- Post-quantum startup activity will hold steady in 2027
- Supply chain security will climb the ranks in 2027
- All security staffers should experiment with vibe-coding
- AppSec experts must build Agentic AI security skills
- Identity proofing and anti-fraud vendors should target the mid-market

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 35 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. Through our Call for Submissions process, RSAC received **nearly 3,000 proposals** from the global cybersecurity community for RSAC 2026 Conference.

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. For ISB 2026, which will be 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 Conference is expecting **650 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 firms.

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

Evaluating RSAC's 2025 and 2026 Predictions: Seven Top Scores and an Overall Pass Rate of 79%

In RSAC Cybersecurity Insights & Futures Volume 1 and Volume 2, we published predictions for the global cybersecurity community in 2025-2026. To arrive at those predictions, we extrapolated from several years of data that the cybersecurity community shares with us and with each other. Now that RSAC has analyzed the community's 2026 Call for Submissions (CFS) entries, Innovation Sandbox (ISB) competition entries, and Exhibitor descriptions, we can determine how close many of those predictions came to being correct. Thus far, we have sufficient data and adequate space in this report to present detailed evaluations of 14 of our predictions, and we've assigned each of them one of three letter grades.[1] Just three of our 14 predictions received failing grades, which earns RSAC a pass rate of 79%. While RSAC's inner straight-A student wouldn't normally crow about a score of 79%, in a volatile field like cybersecurity, any score above 55% means that our predictions are worth paying attention to.

Prediction Scoring Key

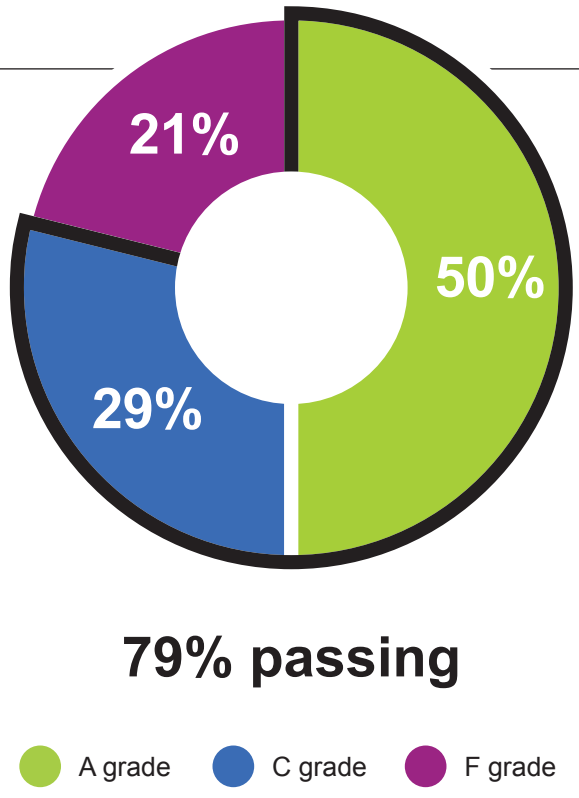
Grade	Pass/ Fail	Explanation
A	Pass	1) Actual value close to estimated value; OR 2) Prediction directionally correct (positive or negative change) AND estimated percentage change close to actual percentage change.[a]
C	Pass	1) Prediction directionally correct and within reasonable distance of actual value; OR 2) Projected percentage increase/decrease close to actual value; OR 3) Prediction velocity correct but actual and predicted values diverge.
F	Fail	Any other condition.[b]

Summary

GRADE: A — 7 total

GRADE: C — 4 total

GRADE: F — 3 total



Detailed Report

Prediction*	Grade
Growth in RSAC™ Call for Submissions (CFS) entries on “AI & ML Security" will outpace growth in "AI & ML Applications to Security" proposals.	A
Nearly 20% of RSAC Innovation Sandbox (ISB) competitors will be “AI & ML Security” startups.[c]	C
“AI & ML Applications to Security” startups will account for almost 19% of ISB competitors.[c]	C
The share of CFS entries on “AI Agents and Autonomous System Security” will at least double.	A
Entries on ransomware will snap back to 2.1%.[d]	F
4.6% of ISB startups will focus on post-quantum security.[d]	F
The share of CFS entries focused on the CISO’s personal liability for security breaches will be just 0.5%.	A
Privacy’s share of Call for Submissions proposals will rise modestly to 2.1%.	A
Focus on securing the remote workforce will rebound to its highest level since 2021.[d]	F
Cyber insurance premiums will decrease by an average of 2.5% in 2025 compared with 2024.[e]	A
The CFS share of proposals on cyber insurance will return to just above its 2024 level.	C
We expect cloud security's share of startups to fall slightly further.	A
AI will drive more than half of all application security startups.	A
Supply chain security will re-emerge as a Top 10 priority for the community.	C

*All predictions in this table are for 2026 unless otherwise specified.

Detailed Evaluations: How Our Predictions Went Right (and Wrong!), and RSAC Gazes into Our Crystal Ball for 2027

In this section, RSAC provides the detailed evidence to support the letter grades that we’ve assigned each of our previous predictions, and we also use the full set of 2021-2026 Call for Submissions and Innovation Sandbox data and our RSAC™ Cybersecurity Atlas toolset to extrapolate new predictions for 2027.[2]

GRADE:

A

2026 Prediction: Growth in CFS entries on "AI & ML Security" will outpace growth in "AI & ML Applications to Security" proposals.

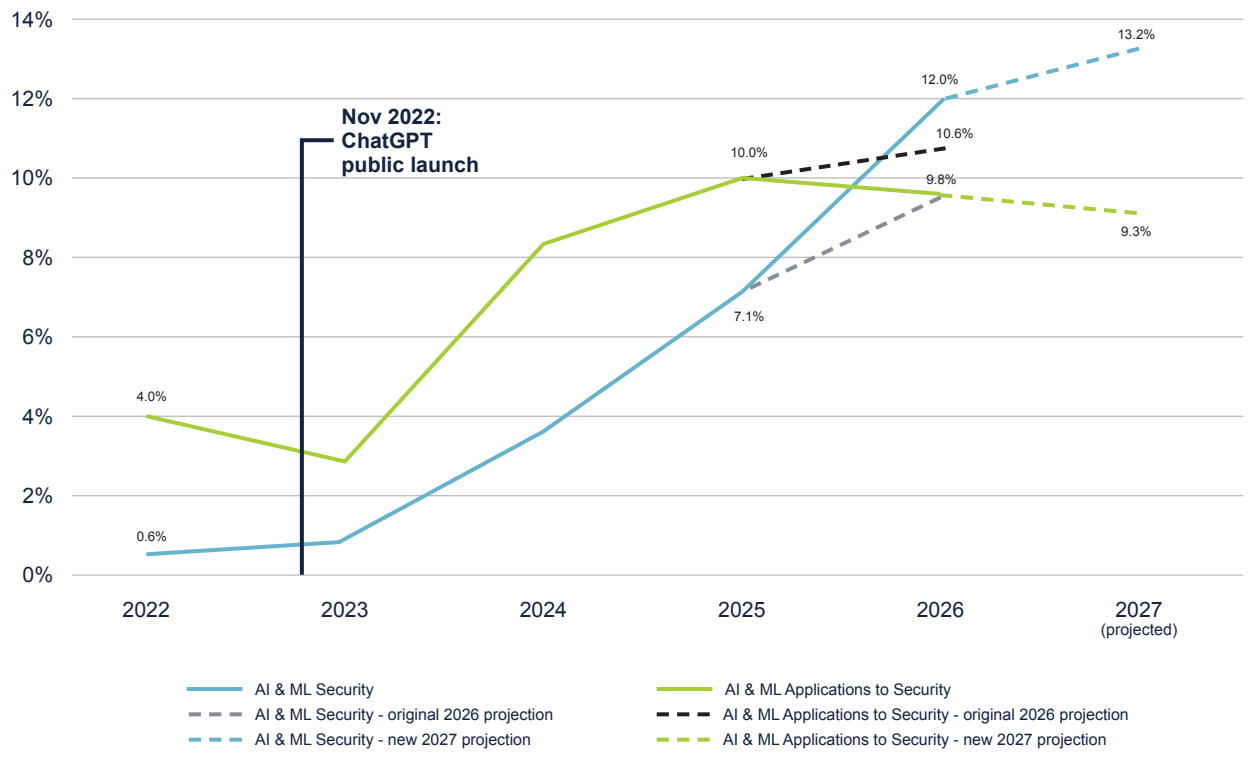
Evidence: Between 2025 and 2026, the "AI & ML Security" share of Call for Submissions entries increased even faster than RSAC predicted, rocketing from 7.1% to 12.0%, while we'd originally posited that it would rise by nearly 35% (See Figure 1). But the percentage of "AI & ML Applications to Security" proposals remained nearly unchanged over that period (it declined very slightly from 10.0% to 9.8%). Hence, growth in the cybersecurity community's CFS proposals on "AI & ML Security" did indeed outpace growth in "AI & ML Applications to Security" entries.

RSAC expects "AI & ML Security" submissions to grow more slowly through 2027, while the "AI & ML Applications to Security" share of proposals will decline slightly. "AI & ML Security" proposals already represent the second-largest share of CFS entries overall for 2026, and RSAC is skeptical that they will keep growing at the previous meteoric rate. Applying AI & ML to solve security problems is already mainstream—indeed, CISOs will find few suppliers in the RSAC 2026 Conference Expo who *aren't* using AI & ML—and thus RSAC predicts that "AI & ML Applications to Security" will capture a slightly smaller slice of cybersecurity expert interest in 2027.

Definitions:

- **"AI & ML Applications to Security": Using AI and ML to perform security functions**
- **"AI & ML Security" or "Security for AI": Securing the AI & ML applications themselves**[3]

Figure 1: "AI & ML Security" Call for Submissions Entries Overtook "AI & ML Applications to Security" Proposals at RSAC 2026 as Predicted



GRADE:

C

2026 Prediction: Nearly 20% of ISB competitors will be "AI & ML Security" startups.

Evidence: RSAC estimated that "AI & ML Security" startups' share of the ISB contest total would jump by 176% to 19.7% in 2026. Instead, that share grew by a still-impressive 113% to 15.1%.[4]

GRADE:

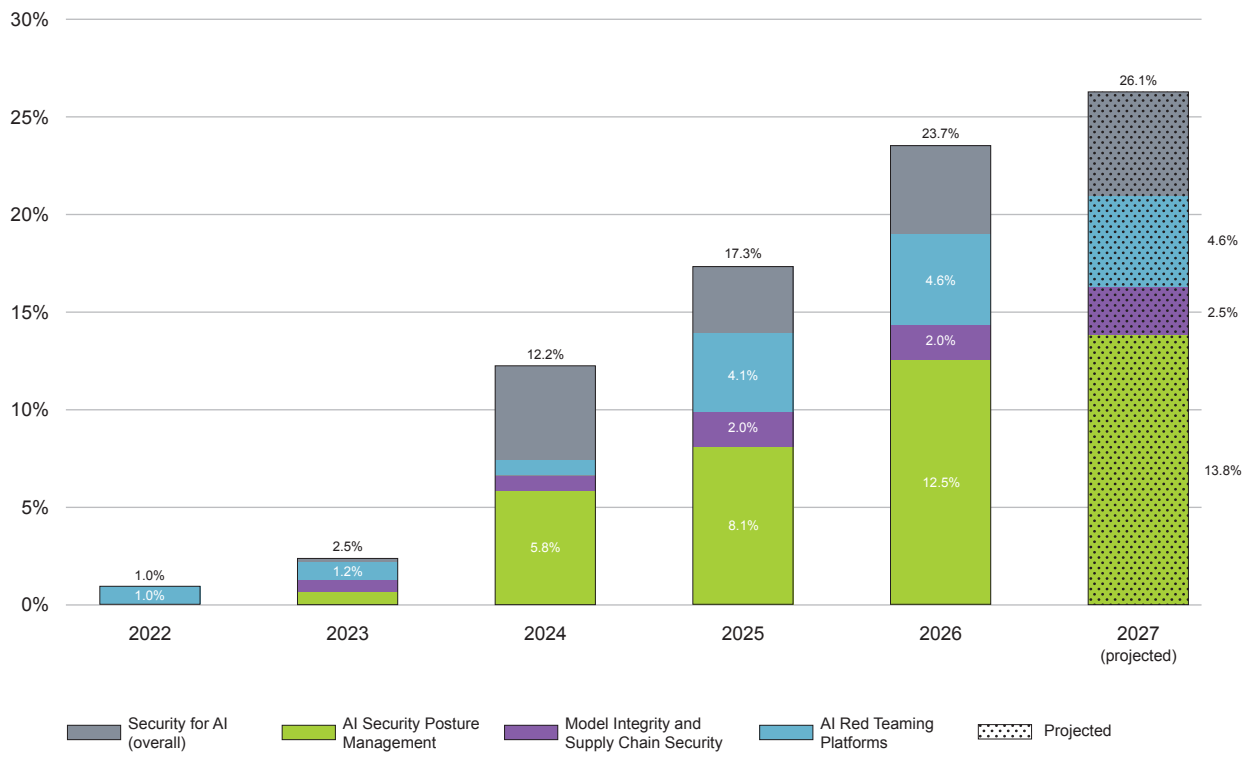
C

2026 Prediction: "AI & ML Applications to Security" startups will account for almost 19% of Innovation Sandbox competitors.

Evidence: RSAC projected that the "AI & ML Applications to Security" portion of the 2026 ISB contest would bounce back to 18.9%, but it rose even higher than we'd anticipated, growing by 127% to reach 23% of the total.

"Security for AI" startups' share of the ISB 2027 contest will rise by at least 10%. The "AI Security Posture Management" (AISPM)[5] Subcategory of the "Security for AI" Category in Innovation Sandbox shot up by 54% between 2025 and 2026, and RSAC anticipates it'll grow further in 2027 (See Figure 2).[6] The "Model Integrity and Supply Chain Security" Subcategory held steady in 2026, but we expect it to grow faster than the rest of the "Security for AI" Category from 2026-2027 because we'll start to see more practical attacks using vectors like: 1) targeted training data poisoning;[7] and 2) the introduction of malicious code hidden in the (previously) non-existent software package dependencies commonly hallucinated by AI code assistants.[8]

Figure 2: In 2027, "Security for AI" Startups' Share of Innovation Sandbox Entries Will Rise, and the AISPM Subcategory Will Remain Its Largest



GRADE:

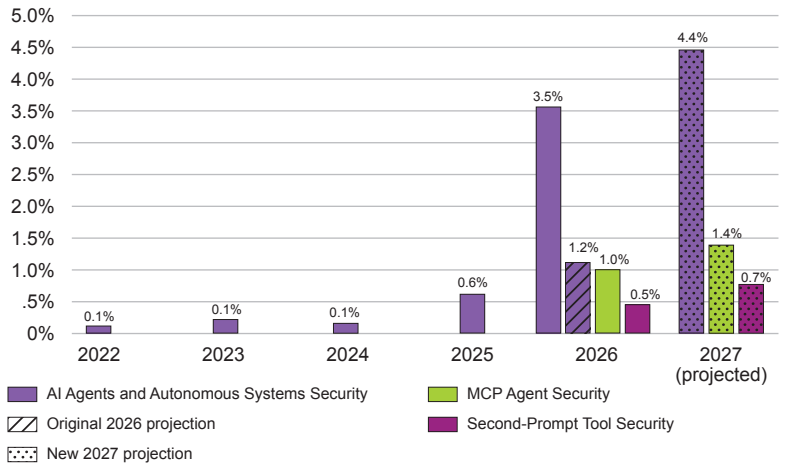
A

2026 Prediction: The share of Call for Submissions entries on "AI Agents and Autonomous Systems Security" will at least double.[9]

Evidence: This prediction turned out to be conservative; the percentage of CFS proposals on "AI Agents and Autonomous Systems Security" more than quintupled from 2025 to 2026 (See Figure 3). Further, RSAC's analysis of the 2026 entries revealed two new Agentic AI-related Subtopics: "Model Context Protocol (MCP) Agent Security" and "Second-Prompt Tool Security,"[10] which accounted for 1.0% and 0.5% of 2026 CFS entries respectively.[11]

For 2027, RSAC anticipates that the proportion of proposals related to Agentic AI Security will grow by more than 30%. As developers' AI agents increase in capability, they'll reveal new security challenges. Hence, RSAC expects the sum of the "AI Agents and Autonomous Systems Security," "MCP Agent Security," and "Second-Prompt Tool Security" Subtopics to increase again as a share of CFS entries through 2027, albeit more slowly than it did from 2025 to 2026.

Figure 3: Agentic AI Security's Share of Proposals Will Rise Again in 2027, but at a Less Meteoric Rate



GRADE:

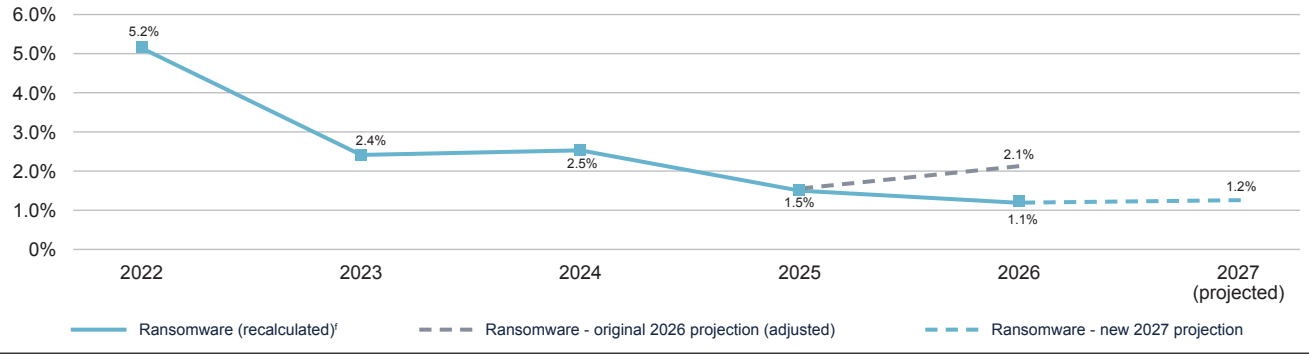
F

2026 Prediction: Entries on ransomware will snap back to 2.1%.[12]

Evidence: The percentage of entries on ransomware declined to 1.1% (See Figure 4). Ransomware's prevalence among community proposals fell by 27% between 2025 and 2026 rather than growing by 38% as RSAC had anticipated.[13]

We're standing firm—RSAC believes that in the final accounting, 2025 will have proven a profitable year for ransomware gangs, which will help drive an increase of at least 10% in ransomware-related submissions for RSAC 2027. In H1 2025, the number of ransomware attacks rose dramatically and ransomware incidents accounted for a majority of declared losses.[14] Ransomware gangs are using AI to scale both attacks and negotiations.[15] Rising payouts and new attacker techniques typically drive more community research into ransomware and the threat actors behind it, and thus we expect more CFS entries for 2027.

Figure 4: Submissions on Ransomware Slumped in 2026, but RSAC Still Expects a Slight Uptick in 2027



GRADE:

F

2026 Prediction: 4.6% of Innovation Sandbox startups will focus on post-quantum security.[16]

Evidence: RSAC misjudged this segment; we had anticipated a 50% increase in the percentage of post-quantum security startups for ISB 2026, but we instead observed a 14% decrease in their share to 2.6% (See Figure 5).

We're curbing our enthusiasm; RSAC predicts that post-quantum security's share of ISB entries will remain flat in 2027. Because it's smaller, the ISB data set is noisier than the CFS data set, so it's harder to accurately predict. Many national and regional authorities require (or at least recommend) a transition to post-quantum encryption by 2030 or 2035, with interim milestones for cryptographic inventory, planning, and starting the transition in 2026-2028.[17] Further, industry standards bodies like the Payment Card Industry's Security Standards Council (PCI-SSC) concentrate on cryptographic inventory, risk assessment, and agility rather than imposing specific deadlines. Hence, we won't see a flood of startups in 2027.

Figure 5: RSAC Expects Post-Quantum Startups' Share of Innovation Sandbox to Hold Steady in 2027

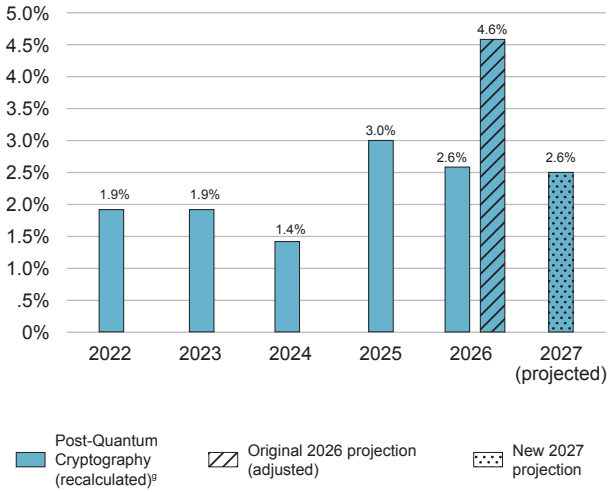
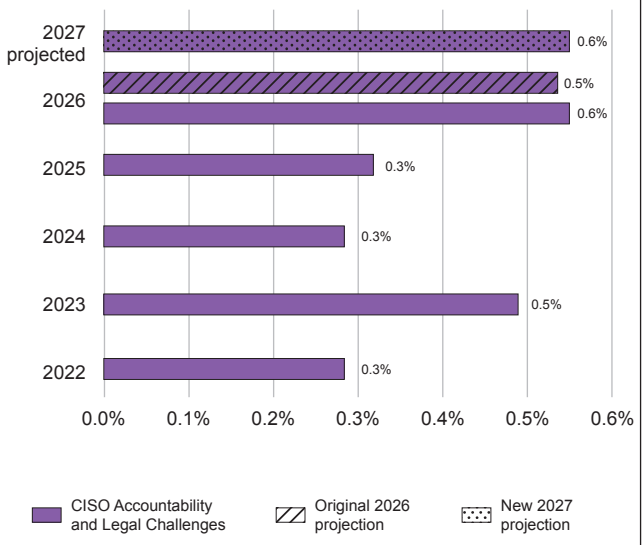


Figure 6: 2027's Share of Proposals on CISO Personal Liability Will Remain Unchanged



GRADE:

A

2026 Prediction: The share of CFS entries focused on the CISO's personal liability for security breaches will be just 0.5%.

Evidence: This extrapolation of the share of Call for Submissions proposals devoted to the "CISO Accountability and Legal Challenges" Subtopic in 2026 proved nearly exactly correct—the 2026 percentage was 0.55% (See Figure 6).[18]

RSAC stands by our reasoning from the Volume 1 report and projects it into 2027; the share of 2027 CFS proposals on CISO personal accountability will remain at around 2026 levels. This reflects less US regulatory focus on the CISO's potential personal liability for security breaches balanced against the beginnings of increased scrutiny from EU regulators. For example, in late November 2025, the US SEC announced it was dropping its lawsuit against SolarWinds and its CISO Timothy K. Brown. However, the Dutch Data Protection Authority's investigation into Clearview's directors continues.[19]

GRADE:

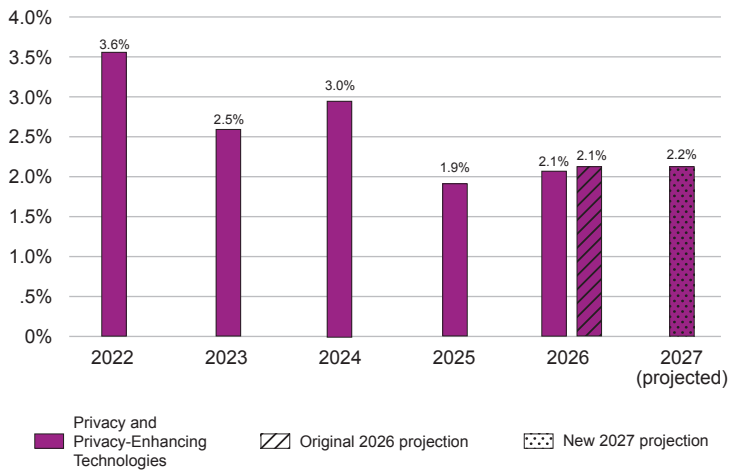
A

2026 Prediction: Privacy's share of Call for Submissions proposals will rise modestly to 2.1%.

Evidence: Our projection of the "Privacy and Privacy-Enhancing Technologies" Subtopic's portion of CFS entries was almost exactly on target—it rose by 7% to reach 2.05% (See Figure 7).[20]

We anticipate further slight growth in cybersecurity expert interest in privacy, raising its share of 2027 submissions by at least 5%. Vendors will continue to release new and more-performant applications of privacy-enhancing technologies like homomorphic encryption and differential privacy throughout 2026, which will drive more community effort in this area.

Figure 7: In 2027, RSAC Predicts a Further Small Increase in Expert Interest in Privacy



GRADE:

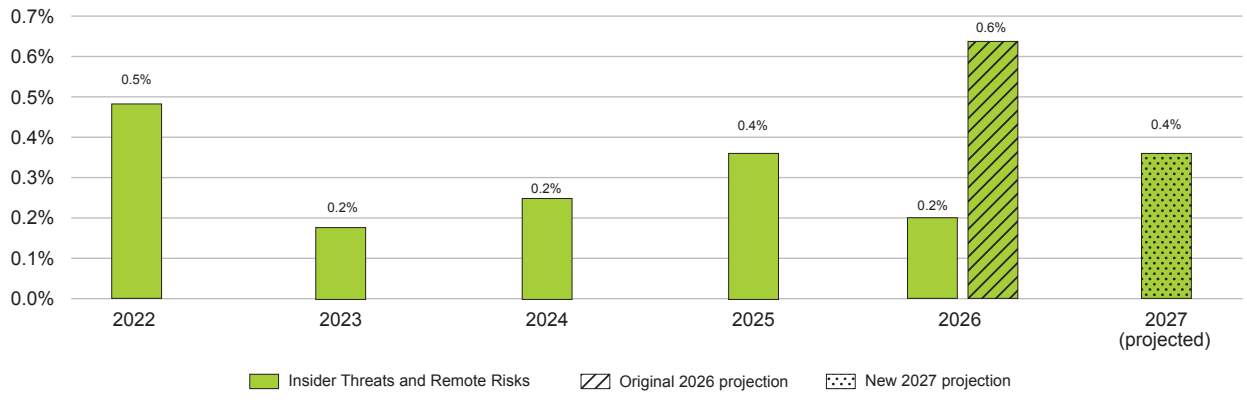
F

2026 Prediction: Focus on securing the remote workforce will rebound to its highest level since 2021.

Evidence: We expected a rise of 74% in the share of CFS entries devoted to the "Insider Threats and Remote Work Risks" Subtopic in 2026, but it instead fell by 44% (See Figure 8).[21] Despite high-profile companies like Amazon continuing to report foiling North Koreans using false identities to attempt to secure remote jobs, community interest in securing remote work and remote identity proofing dropped below even 2024's levels.

2027 will see yet more hackers try to fill remote roles under false pretenses, pushing cybersecurity experts' interest in new techniques for securing remote workforces back up to at least 2025 levels. For all the noise about bosses ordering their workforces back to the office at least part-time, remote work isn't going away. Thus, security, HR, and finance teams must continue combatting remote work fraud together.

Figure 8: Contrary to Expectations, Cybersecurity Community Interest in Securing the Remote Workforce Waned Between 2025 and 2026, but RSAC Expects It to Rise in 2027



GRADE:

A

2025 Prediction: Cyber insurance premiums will decrease by an average of 2.5% in 2025 compared with 2024.

Evidence: Premiums fell by an average of 6.3% year-over-year for Q1 through Q3 2025 versus Q1 through Q3 2024 (See Figure 9).[22]

RSAC stands by our previous prediction that after three years of modest declines, cyber insurance premiums will increase by an average of 1% year-on-year by the end of 2026. In part because RSAC estimates that the final tally of ransomware payouts will be higher in 2025 than in 2024, we foresee that by the end of 2026, the average company will pay 136% more than they did in 2020 for comparable coverage.[23]

GRADE:

C

2026 Prediction: The Call for Submissions share of proposals on cyber insurance will return to just above its 2024 level.

Evidence: We expected the share of CFS entries focused on "Cyber Insurance and Risk Transfer" to rise by 35% from 2025 to 2026, but it actually remained flat (See Figure 9).

We anticipate that the portion of community submissions on cyber insurance topics will grow by at least 10% through 2027. The cumulative increase in cyber insurance premiums for 2026 that we discuss above, plus an increase in claim refusals by insurers that are applying contract terms more narrowly, will induce more experts to dive into the cyber insurance details.[24]

Figure 9: RSAC Still Expects a Slight Rise in Cyber Insurance Premiums in 2026, and a Small Increase in Call for Submissions Interest in Cyberinsurance In 2027

GRADE:

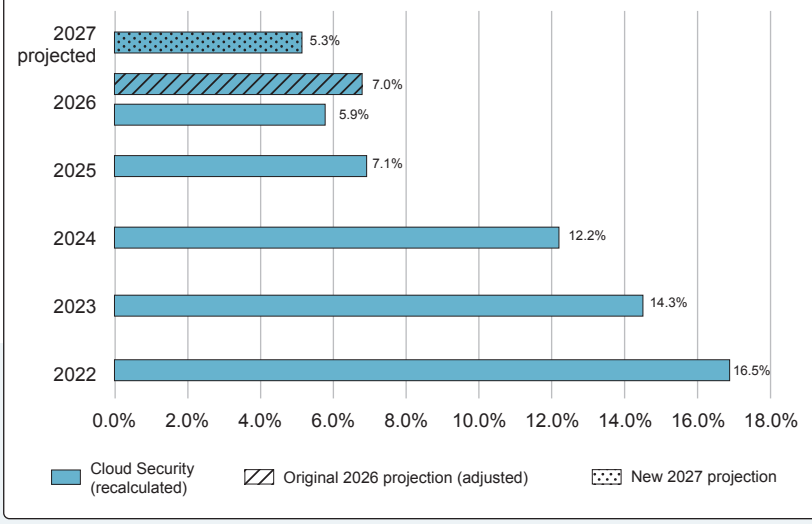
A

2026 Prediction: We expect cloud security's share of startups to fall slightly further.

Evidence: RSAC estimated that cloud security's share of Innovation Sandbox entries would decrease by 2% between 2025 and 2026, and it fell by 16% (See Figure 10).[25]

Because cloud deployments are ubiquitous, the portion of startups that focus on cloud security as a distinct function will decline again for ISB 2027. Hence, RSAC reaffirms our recommendation from Volume 2 of investing in training in cloud security skills for all security team members rather than hiring more cloud security specialists.

Figure 10: Cloud Security Startups' Share of Innovation Sandbox Will Continue to Slide in 2027



GRADE:

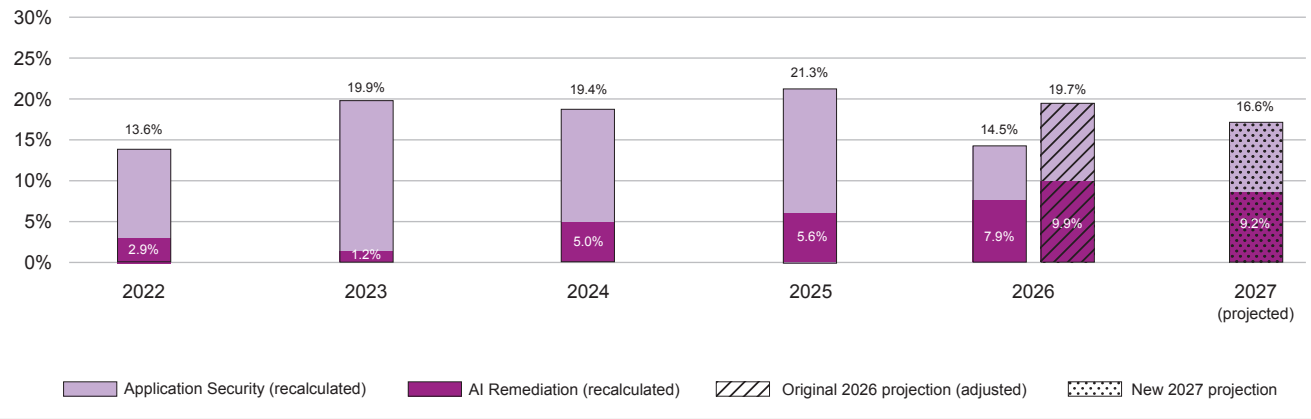
A

2026 Prediction: AI will drive more than half of all application security startups.

Evidence: The "AI Remediation" Subcategory accounted for 55% of application security startups for Innovation Sandbox 2026.[26]

RSAC anticipates that this relationship will continue in 2027; "AI Remediation" startups will once again constitute at least 55% of application security startups for ISB 2027. As developers and non-developers alike harness vibe-coding to build more software faster, security teams will need to implement more capable "AI Remediation" solutions to keep up—and more new Innovation Sandbox startups will attempt to capture that demand.[27]

Figure 11: AI Drove More Than 50% of ISB's Application Security Startups in 2026, and RSAC Expects That Ratio to Hold in 2027



GRADE:

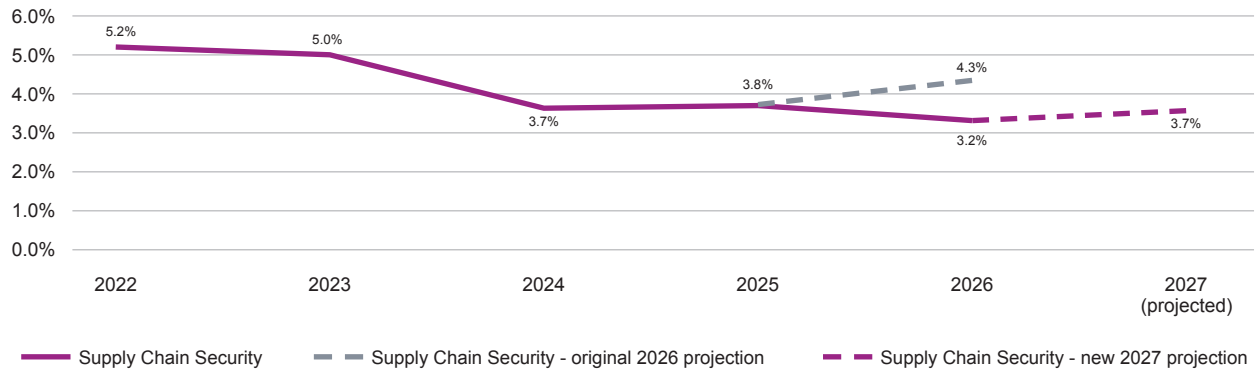
C

2026 Prediction: Supply chain security will re-emerge as a Top 10 priority for the community.

Evidence: We predicted that supply chain security would rise from the #12 top-level Topic for 2025 to the #10 Topic in 2026, but it instead fell to #13 in the rankings with 3.2% of total CFS entries (See Figure 12). Meaning that instead of supply chain security's rank among top-level Topics rising by 9% (two places of 23), it fell by 4% (one place of 23). Given the closeness of those values, RSAC ekes out a "C" for this prediction.

This prediction was one year too early; RSAC anticipates that supply chain security will increase its share of RSAC 2027 CFS entries by at least 15%. Why? Because more attackers will exploit LLM fine-tuning methods like Low-Rank Adaptation (LoRA) to poison models.[28] Futher, technology suppliers must begin their EU Cyber Resilience Act (CRA) reporting in September 2026.

Figure 12: Supply Chain Security Will Join the RSAC Top 10 in 2027, One Year Later Than Predicted



RSAC's Recommendations: 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 these evaluations and our new predictions:

CISOs and Senior Cybersecurity Leaders

- **Encourage all your security team members to experiment with vibe-coding.** Between 2025 and 2026, the percentage of RSAC Call for Submissions entries on "Securing Vibe-Coding" nearly tripled—which is no surprise given the ubiquity of vibe-coding tools like Cursor, Lovable, and Windsurf. To understand the incoming avalanche of security vulnerabilities and remediation challenges they face, your whole security team (not just the application security experts!) needs to see firsthand just how much capable software non-developers can build quickly and easily with these tools.

- **Build Agentic AI Security capacity.** Non-developers can use tools like Gumloop, Microsoft's CoPilot Studio, and Zapier to build and deploy AI agents, too, which means that your application security teams must provide secure options to all those new part-time automation engineers.

- **Keep investing in cryptographic agility and monitor quantum developments.** Don't neglect those interim post-quantum migration milestones in 2026-2028, not least because quantum breakthroughs could arrive faster than experts currently expect—if your groundwork and planning are already complete, you'll find it a lot easier to accelerate your rollout if needed. And remember: the 2030 (Australia, the EU) migration deadlines are now less than five years away.

- **Invest in asset inventory tools and supply chain security now to avoid EU CRA-related surprises in 2027.** Start working with your key technology suppliers now to understand their plans for EU CRA compliance; that'll give you time to plan for the products that you'll need to upgrade or replace. Focus on your operational technology (OT) environment, where you'll likely see suppliers changing support and upgrade timelines to limit their EU CRA compliance obligations.

- **In Volume 2, RSAC advised locking in your cyber insurance premium before rates start to rise; the good news is those rises likely won't filter through until July 2026.** It's still worth checking if your insurer will offer you concessions to renew early, given that as of this writing, the current average premium is still lower than it has been since 2021. And look for new exclusions in your policy renewal; the recent declines in cyber insurance premiums reflect not just increased competition among insurers and more mature security programs at their clients, but also tighter underwriting standards.[29]

Technology Suppliers

- **Get your EU CRA house in order.** Yes, the regulators sometime accede to industry's pleas for deadline extensions, but don't bank on delays in CRA enforcement. Further, your forward-looking CISO customers will expect answers on your plans for your product portfolio starting now, because they'll want as much lead time as they can get to upgrade or replace specific key hardware and software (especially in OT environments).

- **Remote identity proofing and anti-fraud vendors: exploit the mid-market opportunity.** Mid-market firms want to take advantage of remote talent but worry they lack the expertise to avoid being victimized by hackers seeking to steal data and earn hard currency under false pretenses. If you can provide user-friendly solutions at a price these buyers can afford, you'll reap the financial rewards.

Endnotes to Text

1 The eight total predictions from the RSAC Cybersecurity Insights & Futures Volume 1 and Volume 2 reports that we cannot evaluate here either: a) require full-year 2025 or 2026 data that's not yet available (four predictions); b) use a previous classification methodology that RSAC has deprecated (three predictions); or c) represent an alternate version of a projection that we did evaluate (one prediction). There are five further predictions that we are able to assess, but have excluded from this report to keep it to a manageable length. Those five predictions received the following scores: three "C"s and two "F"s. If we include those five, the percentage of RSAC's predictions receiving passing grades falls to 68%, and our grades would be seven "A"s, six "C"s, and six "F"s.

2 Some of the values for the RSAC Call for Submissions (CFS) data from 2021-2025 in this report will differ from the values in Volume 1 and Volume 2. This is because RSAC updated the data classification process when incorporating the 2026 data. To produce the data for this report, we: 1) used GPT-5 to do the classification (previously, we used GPT-4o); 2) extracted new Subtopics as they arose in the 2026 data; 3) reprocessed the data from 2021-2025 to apply new Subtopics from 2026 to earlier years of data as appropriate; 4) forced reclassification of sessions assigned to the least-frequently-used 15% of Subtopics to keep the number of Subtopics manageable; and 5) maintained our previous practice of assigning submissions to one Subtopic only. The disadvantage of this approach is that one cannot use the current RSAC Cybersecurity Atlas: Map of Topics tool to faithfully reproduce old results. We selected this option because LLM-driven Subtopic assignment isn't deterministic, so we prioritized improvement in classification over reproducibility. In the case where the only changes to the 2021-2025 values previously published in Volume 1 and Volume 2 resulted from the updates to the data classification process that we describe above, we've kept our percentage predictions for 2026 from those reports the same so that we can evaluate them. Readers should assume that there are minor differences throughout due to the classification process updates. Finally, for certain predictions, we have adjusted the original percentages proportionally to apply an improved calculation methodology retroactively, and we evaluate those adjusted values when grading those predictions.

3 For Innovation Sandbox (ISB), we'll use the term "Security for AI" instead of "AI & ML Security" in our forward-looking predictions from this report onward so that we can use the new vendor/product classification system we've developed to apply to both ISB startups and mainstream RSAC Conference Exhibitors. RSAC developed this new vendor/product classification system (which uses Category/Subcategory instead of Topic/Subtopic) because we determined that the CFS "choose only one" Topic/Subtopic scheme didn't fit vendors well (especially the larger Exhibitors, most of whom have products in multiple Subcategories). We've switched methodologies to enable more consistent calculations and better predictions in the future. "Security for AI" applies to a broader set of startups than the "AI & ML Security" CFS Topic, so they aren't exactly identical, but they're reasonably close.

4 RSAC also re-ran the classification process on the full 2021-2026 ISB dataset using the new Subtopics extracted from the 2026 CFS dataset and GPT-5 as described above in endnote 2. Hence, here, we've followed the same process for "AI & ML Security" and "AI & ML Applications to Security" ISB entries that we specify for CFS proposals in endnote 2 above—we've kept our percentage predictions for 2026 from Volume 1 and Volume 2 the same so that we can evaluate them.

5 AI Security Posture Management (AISPM) products address the challenge of continuously monitoring, assessing, and improving the overall security readiness of AI systems. AISPM is sometimes also referred to as LLM posture management, AI risk posture analytics, or AI security governance.

6 As described in endnote 3 above, RSAC created a new vendor/product classification system for ISB startups and Exhibitors. ISB startups could in principle have more than one product and thus be assigned to more than one Subcategory, but in practice all ISB entrants to date have featured a single product, so they've each only been assigned to a single Subcategory.

7 Recent research by Anthropic, the UK AI Security Institute, and the Alan Turing Institute has demonstrated that as few as 250 malicious training documents can produce a vulnerability in an LLM of any size, contrary to previous assumptions that attackers would need to control a percentage of training data (which would make poisoning a larger model harder given the much larger size of its training data set).

8 Research conducted at the University of Texas at San Antonio using 16 different LLMs to generate code demonstrated that the LLMs' rate of "package hallucination" (meaning that the LLMs recommend or generate references to software packages that don't exist) ranged from 5.2% for commercial models to 21.7% for open source models. Attackers could thus introduce malicious code by publishing packages to open source repositories using those hallucinated package names.

9 For our analysis in Volume 1, we shortened the "AI Agents and Autonomous Systems Security" Subtopic's name to "Agentic AI Security" to conserve space; as of the initial analysis of CFS entries for 2021-2025, it was the only Agentic AI-related Subtopic.

10 By "MCP Agent Security," we mean: "security risks and defenses specific to the Model Context Protocol (MCP) and agent toolchains, including rogue MCP middleware, toolchain hijacking, context poisoning, sentinel services, and policy enforcement for safe-by-design integrations," and by "Second-Prompt Tool Security," we mean: "the security of model-generated actions and tool invocations—"second prompts"—including ReAct threat models, tool abuse pathways, application-specific prompt patching, and controls at the action layer where models instruct tools, APIs, and systems."

11 The phrasing of the original prediction—"will *at least* double"—allows RSAC to earn an "A" grade despite our substantial underestimation of the absolute increase in interest in this topic.

12 This is one of the predictions that we've proportionally adjusted from its Volume 1 value to reflect RSAC's improved calculation of the total share of CFS proposals devoted to ransomware. The new calculation is the sum of the "Ransomware Evolution," "Ransomware Response Strategies," and "Cloud Ransomware Threats" Subtopics, and we applied it to the full 2021-2026 CFS data set. Note that the original prediction we published was 4% of the total.

13 Note that in Volume 1 we also predicted that 2025's ransomware payout total would rise to more than US $1.3B. We cannot yet evaluate that projection's accuracy, because as of this writing, full year ransomware payout totals for 2025 are not yet available, and the evidence related to those payouts to date is contradictory. For example, in October 2025, ExtraHop published a report claiming that ransomware payouts had hit record highs due to a growth in average payment size. Six days later, Security Week published a report claiming that ransomware payouts had dropped in Q3 2025 due to lower percentages of firms agreeing to pay.

14 There were 4,310 publicly disclosed ransomware attacks in H1 2025. Estimates for the percentage of of declared losses attributable to ransomware in 2025 range from 60% to 76%. Sources: Resilience Cyber Insurance Solutions, S&P Global

15 Ransomware gangs are using LLM-driven chatbots to offload "customer" communications (in their case, to negotiate with victims) just as legitimate businesses do. Source: Axios

16 RSAC recalculated post-quantum security startups' share of the ISB contest using the "Post-Quantum Cryptography" Subcategory from our new vendor/product classification system discussed in mutiple endnotes above for the full 2021-2026 CFS data set. Hence, this prediction has been proportionally adjusted from its Volume 1 value to reflect this improved calculation of the total share of ISB contest applicants devoted to post-quantum security (the original prediction was 10.1% of the total).

17 For example, Australia has established 2026 and 2028 interim milestones and requires post-quantum migrations to be complete by 2030. The EU has a 2026 interim milestone and expects compliance for high- and medium-risk use cases by 2030. The US specifies that all new national security systems (NSS) acquired after Jan. 1, 2027 must use Commercial National Security Algorithm (CNSA) Suite 2.0 algorithms (where the asymmetric encryption options are quantum-resistant), and requires all NSS to be compliant by 2033, but doesn't expect compliance across a broad swath of general infrastructure and systems until 2035. Sources: Australian Signals Directorate (ASD); European Commission (EC); US National Security Agency (NSA), US National Institute of Standards and Technology (NIST).

18 Note that this percentage has been rounded to 0.6% in the associated figure.

19 See RSAC Cybersecurity Insights and Futures Volume 3 for our discussion of the history and recent developments in CISO personal accountability in the EU.

20 Note that this percentage has been rounded to 2.1% in the associated figure.

21 In the Volume 2 report, RSAC grouped the sessions classified into the "Insider Threats and Remote Work Risks" and "Fraud in Remote Work Environments" Subtopics together when charting 2021-2025's CFS data (in Figure 6). As part of the improvements to data processing that RSAC implemented when incorporating the 2026 CFS data (as described in endnote 2 above), "Fraud in Remote Work Environments" was one of the low-frequency Subtopics that we eliminated, and those sessions were reclassified into other Subtopics. Hence, here we've used just the "Insider Threats and Remote Work Risks" Subtopic and our original 2026 projection for that Subtopic to grade this prediction, rather than the aggregation of the two Subtopics that we used in the Volume 2 report.

22 Source: Marsh

23 For more details on how RSAC calculated these average cyber insurance premiums, see the Volume 2 report.

24 Source: S&P Global

25 RSAC recalculated the cloud security ISB totals for 2021-2025 using our new company/product classification scheme mentioned above. These values are different than those that appear in Volume 2, but they follow the same trajectory (the new classification system also has a top-level Category for "Cloud Security"). RSAC adjusted the original 2026 projection for cloud security using the 2025-2026 percentage decrease that we'd originally predicted in Volume 2 (-2%) so that we could assess the accuracy of the prediction.

26 RSAC recalculated the application security ISB totals for 2021-2025 using our new company/product classification scheme mentioned above. These values are different than the ones that appear in Volume 2, but they follow the same trajectory (the new classification system has a top-level Category for "Application Security," which is quite close to the "DevOps and Application Security" top-level Topic that we used in our original analysis). Here, "AI Remediation" means "using AI to detect and remediate software vulnerabilities." RSAC adjusted the original 2026 projection for application security using the 2025-2026 percentage decrease that we'd originally predicted in Volume 2 (-7.4%) and then calculated the 2026 projection for "AI Remediation" using the original 50.4% of the overall "DevOps and Application Security" Topic that we'd estimated the "AI-Driven Application Security" Subtopic would account for. The absolute predictions for 2026 were only close enough to warrant a "C" rating (19.7% projected vs. 14.5% actual for application security, and 9.9% projected vs 7.9% actual for "AI Remediation"), but the published predction was a relational one, and "AI Remediation" constituted 54.5% percent of application security, which is indeed "more than half." So this prediction earns an "A" rating.

27 By "vibe-coding," we mean "AI-assisted and agentic software development."

28 See for example: OWASP

29 Sources: Infosecurity Magazine, S&P Global

Endnotes to Figures

a Relational predictions (for example: "X will grow faster than Y") will be scored "A" if the statement correctly predicted the future relationship, regardless of how closely the projected values match the actual values.

b Relational predictions will be scored "F" if the statement got the relationship wrong, regardless of how closely the projected values match the actual values.

c In the Volume 1 report "Summary of Predictions," these two projections were combined into a single item. We've separated them here to make them easier to evaluate, because the original version didn't express a relationship between the two; we'd merely consolidated them to conserve space.

d The percentages in these predictions have been adjusted from their Volume 1 and Volume 2 values to reflect updated categorization and calculation methodologies for certain subsets of CFS proposals and for all ISB startups. See the graphs and accompanying text for each prediction in the next segment of this report for the details of why and how.

e This "A" grade is provisional, because we don't yet have data on cyberinsurance rates for Q4 2025.

f Note that the 2022-2025 values are different than those in Volume 1, but they follow the same trajectory, for the reasons explained in endnote 12 in the above "Endnotes to Text" section.

g The 2022-2025 values differ from the values that appear in the Volume 1 report, and they follow a somewhat different trajectory because we're using the new vendor/product classification system discussed in the "Endnotes to Text" section above.

h The data labels in the chart have been rounded to the nearest thousand.

RSAC Cybersecurity Insights & Futures, Volume 4 | January 21, 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.

RSAC
Cybersecurity, Together™

OneRSAC.com