VOL 6 | JUNE 2026

RSAC

CYBERSECURITY INSIGHTS & FUTURES

AI & ML Security Consumed RSAC 2026; Expect Emphasis on GRC and Incident Response to Surge for 2027

RSAC Authors:

Laura Koetzle
Head of Community Research

Chris Gates, PhD
Senior Director, Research

Athanasios Theocharis
Principal Researcher

Key Takeaways

- At RSAC™ 2026, "AI & ML Security" took top billing for the first time, but in 2027, GRC will reclaim its crown among Senior Leaders
- Senior Leaders prioritize vetting new startups, and they'll do so at least 10% more in 2027
- RSAC sees early signs of cyber insurance premium increases; negotiate now to avoid price hikes
- Tap Brazil for cybersecurity talent

Predictions from RSAC: What CISOs Should Expect for 2027 and Beyond

For 35 years and counting, RSAC has served as a window into the cybersecurity community's future. Here's a summary of our most important analyses of 2026 and predictions for 2027:

	2026 OBSERVATION	2027 PREDICTION
	"AI & ML Security" was the community's top priority at RSAC 2026 Conference…	…but in 2027, Senior Leaders will return to GRC, while Line Practitioners commit to incident response
	Senior Leaders' investment in workforce development didn't fall in 2026…	…thus, CISOs will prioritize workforce development and leadership in 2027
	At RSAC 2026, privacy interest rebounded modestly...	…and in 2027, RSAC expects that privacy's mindshare will hold steady
	The community showed a strong appetite for both startup and mainstream offerings at RSAC 2026…	… hence, we anticipate that Senior Leaders will invest at least 10% more in vetting startups at RSAC 2027
	RSAC sees early signs of the cyber insurance cost rises that we predicted...	…thus, CISOs should prepare for price increases in 2027
	At RSAC 2026, financial services Senior Leaders focused on the human side of cybersecurity…	…while in 2027, we predict that government Line Professionals will pursue critical infrastructure protection further
	Brazil's cybersecurity community deepened its engagement at RSAC 2026…	…and in 2027, more firms will tap Brazil's cybersecurity talent, and Israel will return to the top five source countries list for RSAC Conference

The Proof: Analyses of RSAC 2026 and Our Resulting 2027 Predictions

In this report, we synthesize several years of data from the RSAC™ Call for Submissions, Innovation Sandbox (ISB) competition, exhibitor descriptions, session attendance patterns, and session evaluations—including data gathered at the most recent RSAC 2026 Conference—to assess the state of the community in 2026. We use those insights to predict the course of 2027 for cybersecurity, and to recommend steps CISOs and other senior leaders should take now to prepare for that future.

RSAC 2026 took place before the advent of increased vulnerability discovery and exploitation capabilities from Anthropic's Mythos and OpenAI's GPT-5.5-Cyber models, and before the US government's imposition of export controls on Anthropic's Fable 5 and Mythos 5 models, so RSAC has adjusted our extrapolations from the data to account for the impact of those and other anticipated frontier model developments. Given the unusually high level of unknowns (even for a famously volatile field like cybersecurity), as of this writing, making high-confidence predictions is more difficult than usual.

RSAC 2026 • ATTENDEE PROFILES

One helpful frame for analyzing the cybersecurity community's behavior is to distinguish between the group we'll refer to as "Senior Leaders" (attendees with Director-level and above titles) and the population we'll refer to as "Line Professionals" (all other attendees). Here are the summary profiles for both groups:

Senior Leader — 44%

Director · Vice President · Senior Executive · C-Level Executive · Board of Directors · President

Experience in Cybersecurity	Startups Explored	Mainstream Exhibitors Visited
16+ Yrs / Attendee[1]	2.8 Avg / Attendee	8.5 Avg / Attendee

Top Learning Topics

AI & ML Security · GRC · Identity & Authentication

Top Industries[3]

Financial Services · Business Services & Consulting · Advertising

Line Professional — 56%

Manager · Supervisor · Team Lead · Individual Contributor

Experience in Cybersecurity	Startups Explored	Mainstream Exhibitors Visited
3 - 5 Yrs / Attendee[2]	2.6 Avg / Attendee	10.9 Avg / Attendee

Top Learning Topics

AI & ML Security · GRC · Identity & Authentication

Top Industries[3]

Financial Services · Government · Education

FIGURE 1

RSAC Top-Level Topics

RSAC assigns all Call for Submissions entries (including the subset selected for our in-person events) to one of the following top-level Topics, which we've used to analyze those entries since the Cybersecurity Insights & Futures Volume 1 report:[4]

TOPIC	DEFINITION
AI & ML Applications to Security	Use AI and ML to perform security functions
AI & ML Security	Secure the AI & ML models and applications themselves
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 cybercriminals 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
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)

AI & ML Security was the community's top priority at RSAC 2026...

- From CISOs to new recruits, the cybersecurity community devoted the largest share of its learning time at RSAC 2026 to sessions on "AI & ML Security" (See Figure 1).
- Senior Leaders and Line Professionals were unusually well-aligned in 2026; their top four priorities at the conference were identical (See Figures 2a and 2b).
- 2026 marks the first time since prior to 2022 that cloud security as a topic doesn't appear in the Top 10 for RSAC attendees overall, and it also fell out of the Top 10 Topics for Call for Submissions entries from the RSAC community's experts for the first time in 2026.

...but in 2027, Senior Leaders will return to GRC, while Line Practitioners commit to incident response

- In 2027, Senior Leaders will encourage their deep experts to continue to devote the largest slice of their learning time to "AI & ML Security"—hence, RSAC predicts that "AI & ML Security" sessions will remain the most popular for Line Professionals in 2027. Senior Leaders will rebalance their own engagement so that GRC claims their number one attendance spot at RSAC 2027 Conference.
- Line Professionals will invest more time in incident response in 2027, because they'll be streamlining remediation processes to handle the much larger volume of vulnerabilities discovered by and fixed with AI Agents. Further, Line Professionals will focus more on cloud security at RSAC 2027 (it'll return to their Top 10), because they'll be moving more stateless systems to the cloud to facilitate rebuilding from a clean image quickly.[5]

> **"Line Professionals will focus more on cloud security at RSAC 2027"**

FIGURE 2A • 2022-2027 SENIOR LEADERS' TOP FIVE SESSION TOPICS

GRC Will Return to the Top of Seniors Leaders' Agendas in 2027

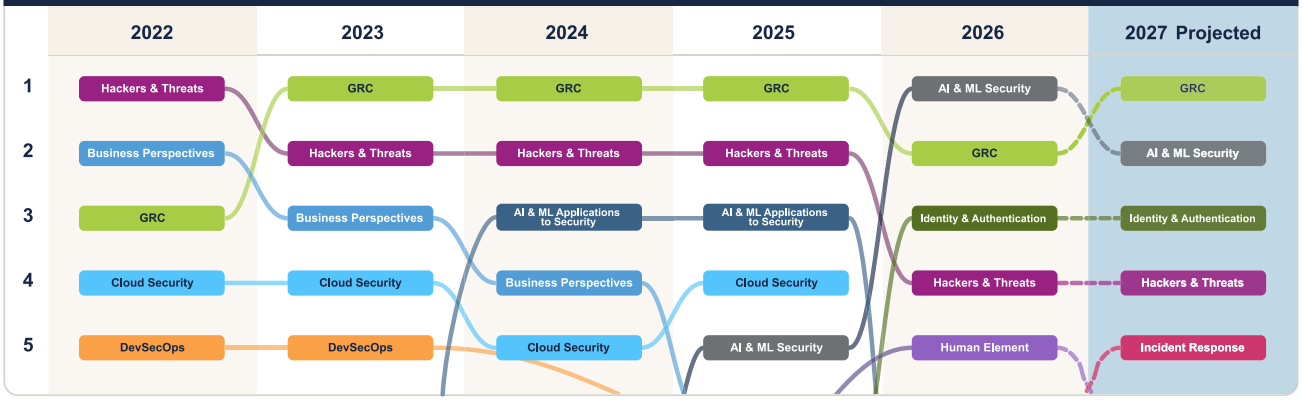


FIGURE 2B • 2022-2027 LINE PROFESSIONALS' TOP FIVE SESSION TOPICS

Line Professionals Will Continue to Dive Deepest into AI & ML Security in 2027

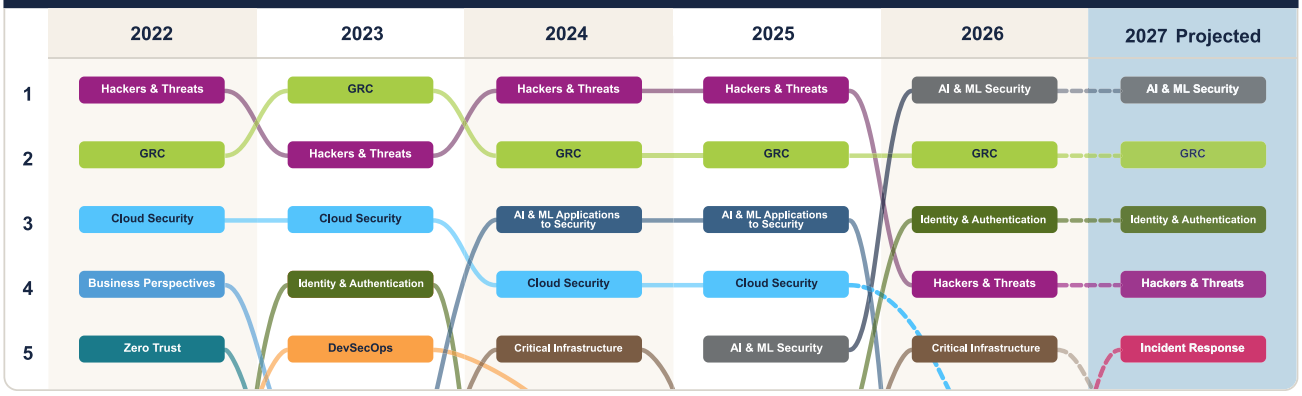


FIGURE 3 • CYBER WORKFORCE DEVELOPMENT

Interest in Cyber Workforce Development Remained Flat in 2026; It'll Rebound Slightly in 2027

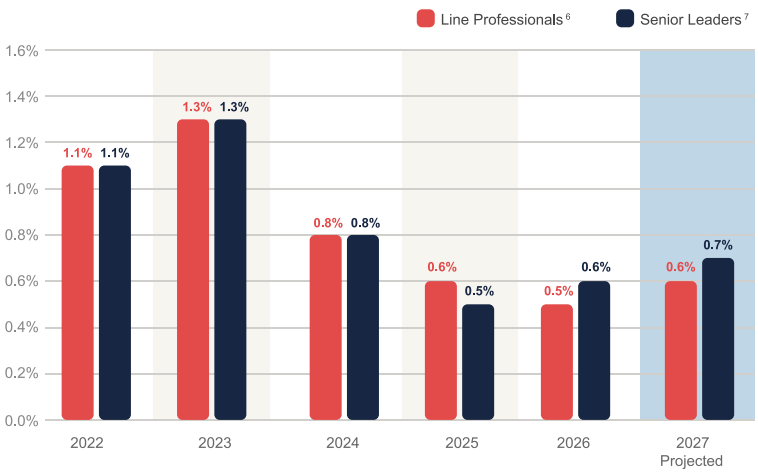
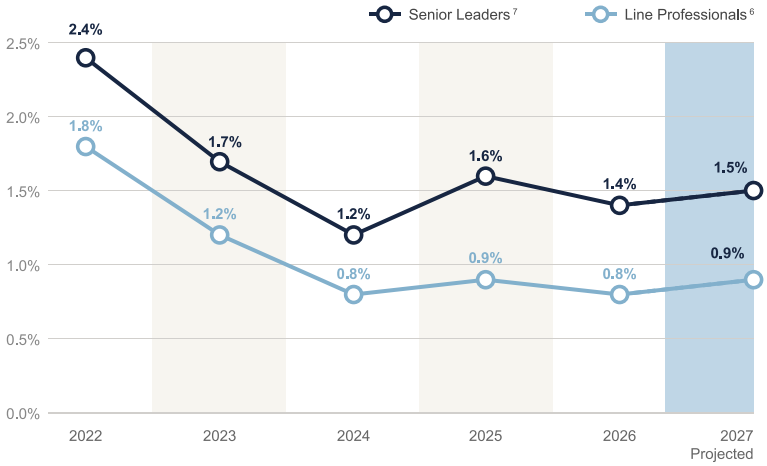


FIGURE 4 • LEADERSHIP INVESTMENT

Senior Leaders Invested Less in Leadership in 2026; RSAC Expects a Small Uptick in 2027



Senior Leaders' investment in workforce development didn't fall in 2026...

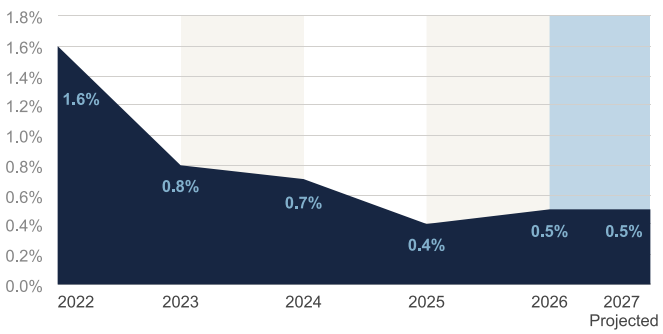
- RSAC pessimistically assumed that Senior Leaders would allow a softer job market,[8] efficiencies gained with AI, and low employee churn to lull them into spending even less of their learning time at RSAC 2026 in sessions assigned to our "Cyber Workforce Development" topic than they did at RSAC 2025.[9] But Senior Leaders didn't fall into that trap in 2026, likely in part because recruiting has already become more diffcult (See Figure 3).[10]
- Senior Leaders invested a slightly lower percentage of their time at RSAC 2026 in sessions on leadership sessions than they did in 2025, but they remain more likely than Line Professionals to invest in the development of their personal skills as leaders (See Figure 4).

...thus, CISOs will prioritize workforce development and leadership in 2027

- Senior Leaders will hire more over the next 12 months because the danger of burnout looms and their teams must develop new skills and processes to handle AI-discovered vulnerabilities and AI-created fixes.[11] Hence, in 2027, CISOs will commit slightly more time to cyber workforce development.
- In 2027, Senior Leaders will also refocus modestly on leadership topics, because they'll need to lead their teams through those process changes.

FIGURE 5 • PRIVACY SESSION ATTENDANCE

Time Invested in Privacy Sessions Rose Slightly in 2026, and Will Remain Unchanged in 2027 [12]



At RSAC 2026, privacy interest rebounded modestly...

- The community spent just 0.5% of its learning time on "Privacy and Privacy Enhancing Technologies" at RSAC 2026, which placed it at 17th of 23 total top-level topics (See Figure 5).

...and in 2027, RSAC expects that privacy's mindshare will hold steady

- Regulation drives interest in privacy, and RSAC believes that most of 2026-2027's regulatory energy will focus on AI, and US federal privacy legislation seems unlikely before 2029.[13] Hence, RSAC expects interest in privacy to remain about the same in 2027.

FIGURE 6 • STARTUP EXPLORATION

At RSAC 2026, Startups Garnered the Most Interest Since at Least 2022, and That Trend Will Continue in 2027*

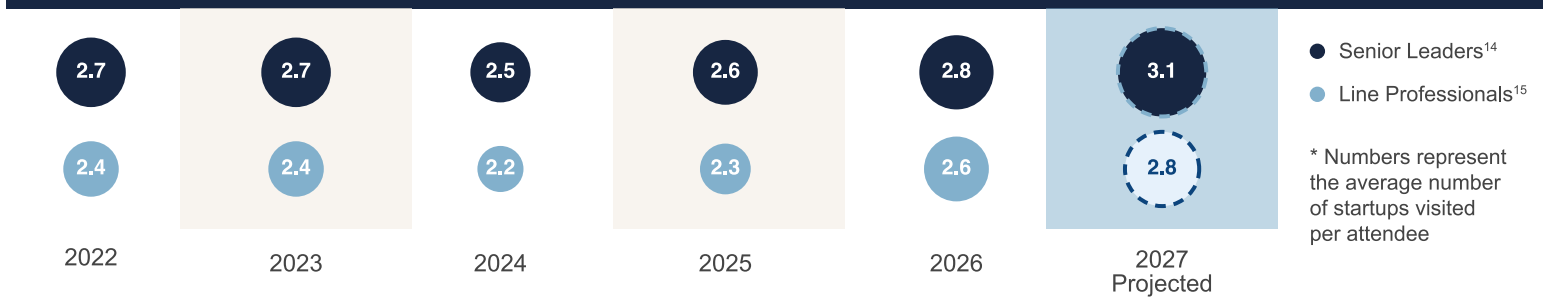
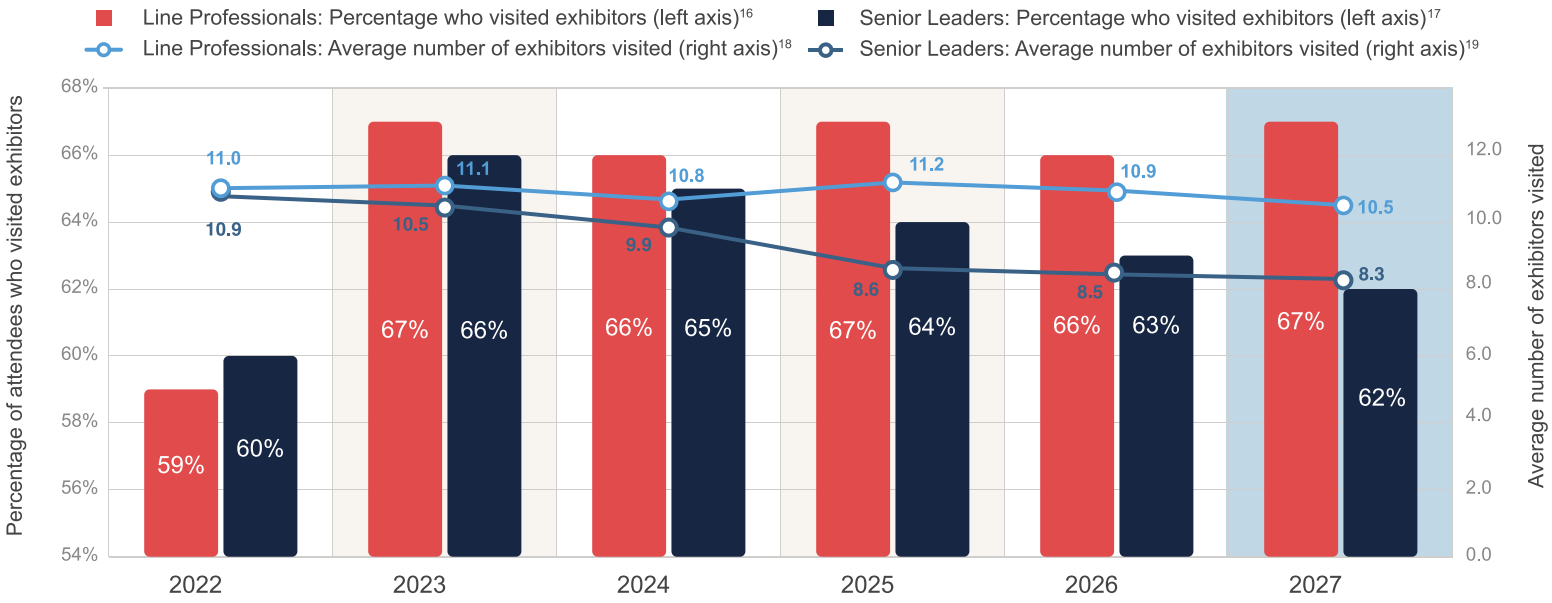


FIGURE 7 • MAINSTREAM EXHIBITORS VISITS

In 2026, More Than 60% of Attendees Checked Out Mainstream Exhibitors, and in 2027, They'll Average More Than Eight Exhbitor Visits Each



The community showed a strong appetite for both startup and mainstream offerings at RSAC 2026...

- Both Senior Leaders and Line Professionals who investigated startups committed more effort to it than at any previous edition of RSAC since at least 2022. The Senior Leader cohort vetted an average of 2.8 startups, while the Line Professionals spent time with an average of 2.6 startups (See Figure 6).
- Attendees' actions speak louder than their complaints about the noise and crowding of the RSAC Expo. At RSAC 2026, 63% of Senior Leaders and 66% of Line Professionals visited at least one mainstream exhibitor at the Expo (See Figure 7).

...hence, we anticipate that Senior Leaders will invest at least 10% more in vetting startups in 2027

- Senior Leaders comprised 44% of RSAC 2026 attendees, and they accounted for more than 47% of visitors to RSAC™ Early Stage Expo and Innovation Sandbox Finalist startups. In 2027, RSAC anticipates that both Senior Leaders and Line Professionals will increase their average numbers of startups vetted.
- In 2027, we expect the cybersecurity community to devote about the same amount of effort to examining cybersecurity products from mainstream exhibitors as they did in 2026, given that there's a constant inflow of newly-mature suppliers; today's ISB offerings grow into tomorrow's mainstream products.

RSAC sees early signs of the cyber insurance cost rises that we predicted...

- RSAC 2026 attendees may regret not spending much time on “Cyber Insurance & Risk Transfer” sessions at RSAC 2026 Conference, because they’re liable to be participating in more fraught policy renewals in H2 2026 and beyond.
- Cyber insurers in many markets are contending with rising claims, increased competition, and deteriorating profitability.[20] “Loss plus defense and cost-containment (DCC)” ratios rose to 49% in the US market in 2024 (See Figure 8).[21] Although full-year audited “loss + DCC” ratio averages are not yet available for 2025,[22] preliminary results give us an estimate of 52% for the “loss + DCC” ratio, which drives it above the 50% ceiling of the zone of stable profitability for insurers.[23]

...thus, CISOs should prepare for price increases in 2027

- Conventional wisdom maintained that cyber insurance was hard to price profitably because underwriters lacked robust historical data, but that a maturing market would grow more predictable (and the reductions in average premiums of 2023-2025 seemed to bear that out).
- However, the combination of attackers’ ability to shift strategies and incorporate new tools with the long tail of regulatory- and litigation-related costs is weighing on insurers.[24] Given the looming impact of Mythos-class frontier LLMs, RSAC expects the underwriters’ jobs to get harder, not easier through 2027 and beyond. Hence, RSAC believes that CISOs and their companies will have to contend with cyber insurance premium increases of 4% in 2027.

FIGURE 8 • CYBER INSURANCE PREMIUMS

Rising Loss + DCC Ratios Will Cause Cyber Insurance Premiums to Rise in H2 2026 and 2027

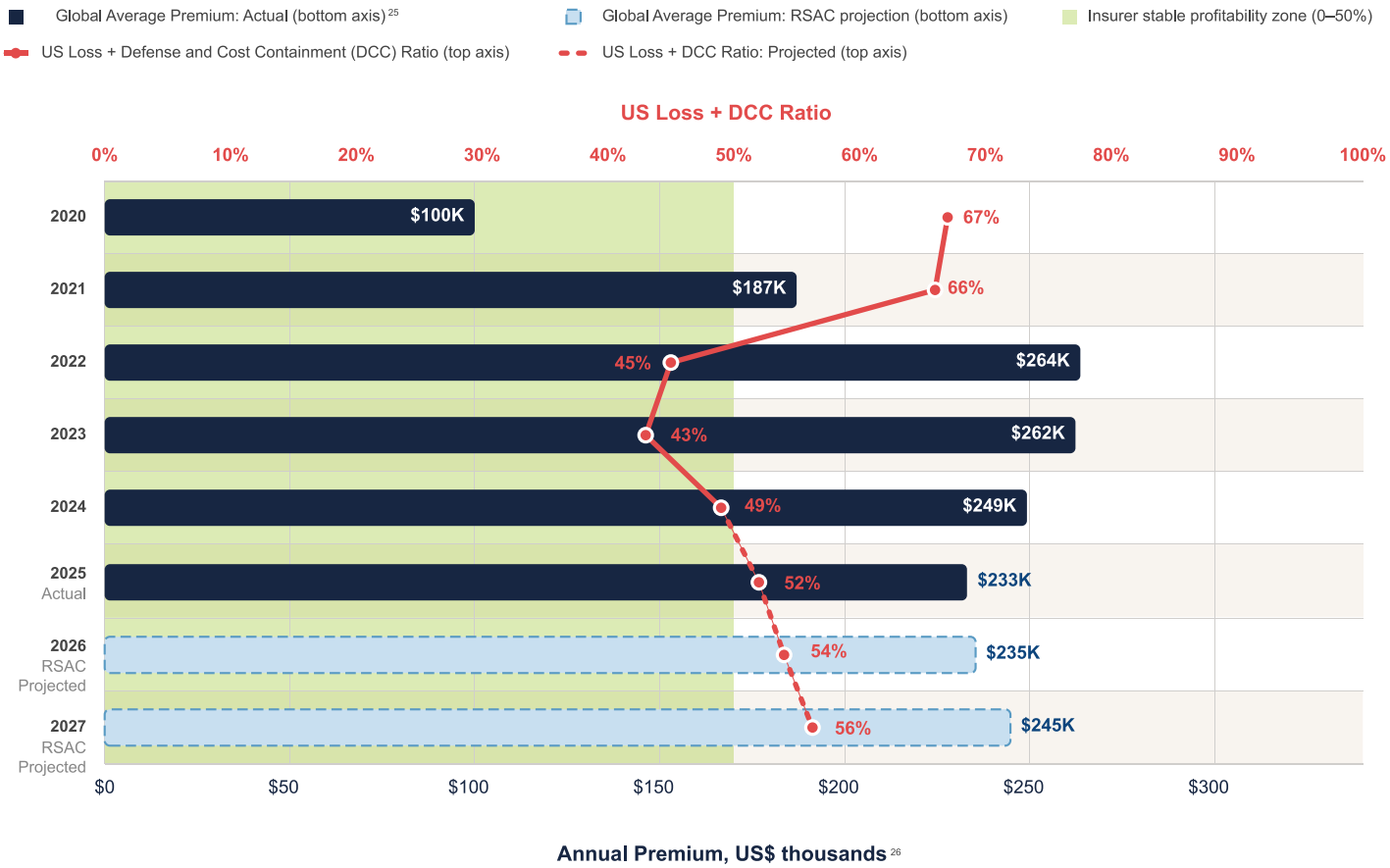


FIGURE 9

Industry Breakdowns for RSAC 2026 Attendance[27]

SENIOR LEADERS	LINE PROFESSIONALS
1. Cybersecurity / Information Technology / Operational Technology	1. Cybersecurity / Information Technology / Operational Technology
2. Software / Hardware	2. Software / Hardware
3. Financial Services / Accounting / Banking / Insurance	3. Financial Services / Accounting / Banking / Insurance
4. Business Services / Consulting	4. Government
5. Advertising / Marketing / PR / Media	5. Education

At RSAC 2026, financial services Senior Leaders focused on the human side of cybersecurity…

- It will surprise no-one to learn that the three largest groups of attendees at RSAC 2026 come from cybersecurity vendors, other software and hardware vendors, and financial services firms (See Figure 9). Thereafter, a differentiated picture emerges: the next-largest cohort of Senior Leaders works in business services, whereas the next-largest cohort of Line Professionals hails from government.
- In 2026, Senior Leaders in the Financial Services industry prioritized sessions devoted to the "Human Element" ahead of "Hackers & Threats" for the first time since at least 2022 (See Figure 10a).

…while in 2027, we predict that government Line Professionals will pursue critical infrastructure protection further

- Critical infrastructure always ranks higher in priority for government cybersecurity professionals than for the community as a whole—indeed, it was priority number five for Government attendees at RSAC 2026 (See Figure 10b). RSAC anticipates that will continue to be true in 2027.
- RSAC expects that financial services firms will prioritize sessions related to the "Human Element" of cybersecurity slightly less in 2027 in favor of incident response given the accelerated pace of AI vulnerability discovery.

FIGURE 10A • SENIOR LEADERS IN FINANCIAL SERVICES

Top Five Topics for 2022-2027: GRC Will Edge Out AI & ML Security to Return to Number One in 2027

	2022	2023	2024	2025	2026	2027 Projected
1	Hackers & Threats	GRC	GRC	GRC	AI & ML Security	GRC
2	Business Perspectives	Cloud Security	Hackers & Threats	AI & ML Applications to Security	GRC	AI & ML Security
3	GRC	Business Perspectives	Business Perspectives	Identity & Authentication	Identity & Authentication	Identity & Authentication
4	Human Element	Hackers & Threats	AI & ML Applications to Security	Hackers & Threats	Human Element	Hackers & Threats
5	DevSecOps	Identity & Authentication	Cloud Security	Cloud Security	Hackers & Threats	Incident Response

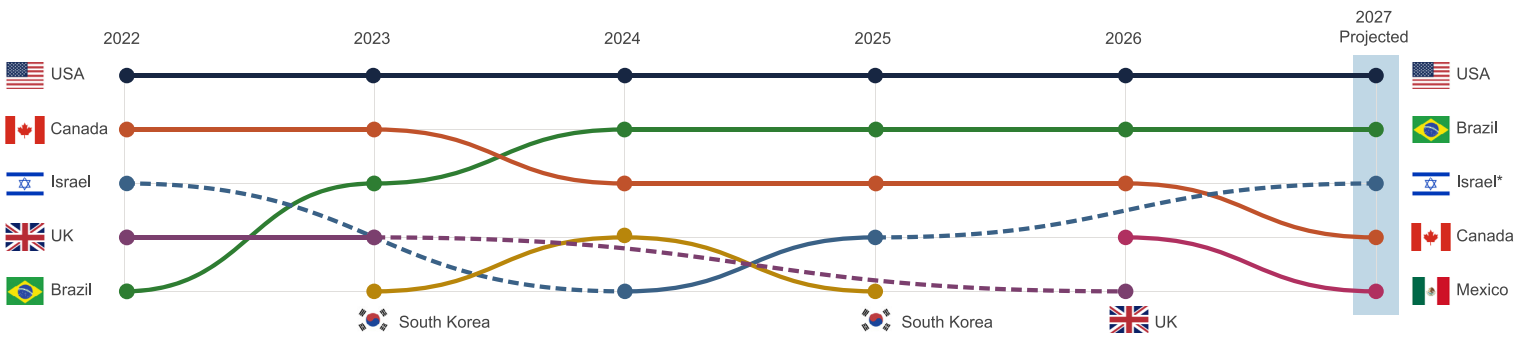
FIGURE 10B • LINE PROFESSIONALS IN GOVERNMENT

Top Five Topics for 2022-2027: Hackers & Threats Will Reclaim the Number Two Spot in 2027

	2022	2023	2024	2025	2026	2027 Projected
1	Hackers & Threats	Hackers & Threats	Hackers & Threats	Hackers & Threats	GRC	GRC
2	GRC	GRC	GRC	GRC	AI & ML Security	Hackers & Threats
3	Cloud Security	Critical Infrastructure	Critical Infrastructure	AI & ML Applications to Security	Hackers & Threats	AI & ML Security
4	Business Perspectives	Cloud Security	AI & ML Applications to Security	AI & ML Security	Identity & Authentication	Identity & Authentication
5	Supply Chain Security	Business Perspectives	Cloud Security	Cloud Security	Critical Infrastructure	Critical Infrastructure

FIGURE 11 • RSAC ATTENDANCE BY COUNTRY

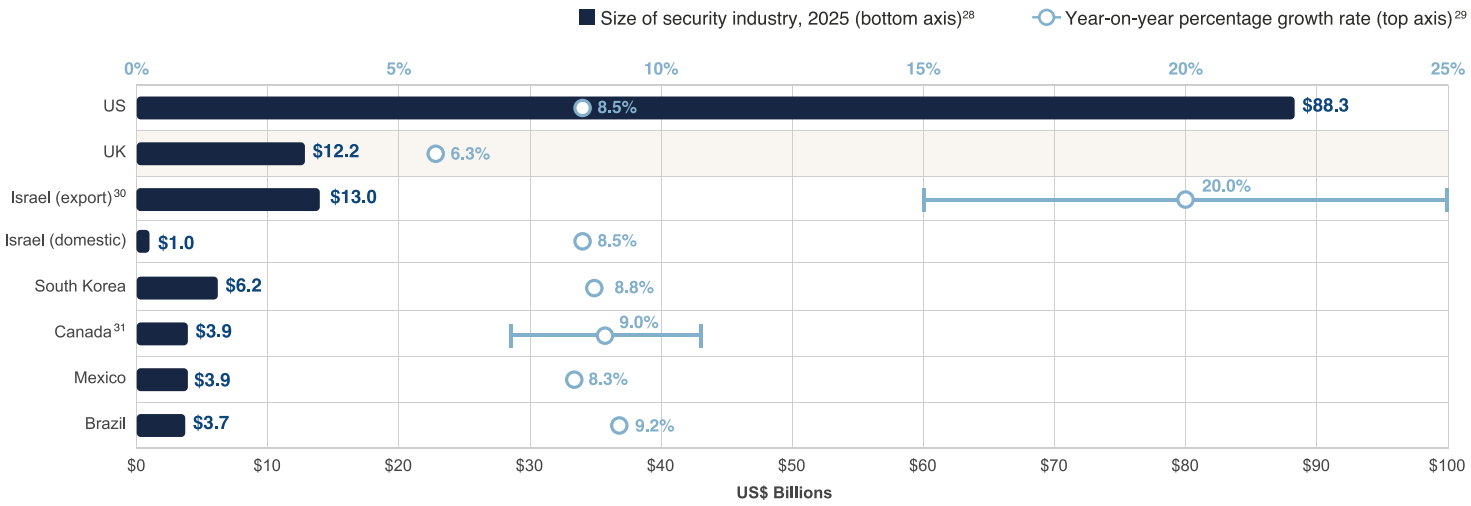
RSAC 2026 Attracted the Largest-Ever Number of Attendees from Brazil; RSAC Expects Israeli Attendance to Rebound in 2027



* Note: Israel's share of attendance fell to number eight in 2026 because of the wars in the Middle East.

FIGURE 12 • TOP RSAC SOURCE COUNTRY DATA

The Cybersecurity Markets in All of the Top Source Countries for RSAC Attendees Grew by 6.3% or More Year-on-Year in 2025



Brazil's cybersecurity community deepened its engagement at RSAC 2026...

- Since 2023, despite the average of 32-plus hours of roundtrip air travel required between São Paulo and San Francisco, Brazil has been the second-most-common source country for RSAC attendees (See Figure 11).
- Brazil's cybersecurity industry reached an estimated US $3.7B in 2025 (See Figure 12). Further, Brazil's GDP grew at a faster rate than that of any of the other top RSAC source countries save Israel's in 2025.[32]
- Israel's contingent was only the eighth largest at RSAC 2026—but that's because it was very difficult to travel to or from Israel during the conference due to the US-Israel-Iran War.

...and in 2027, more firms will tap Brazil's cybersecurity talent, and Israel will return to the top five source countries list for RSAC Conference

- Brazil's companies are making big investments in their cyber workforce by sending them to RSAC, which argues for increased consideration of Brazil as a source of cybersecurity talent.
- Brazil's market for cybersecurity products and services is expanding—it grew by an estimated 9.2% in 2025. However, the World Bank expects Brazil's GDP to grow by just 1.6% in 2026 and 1.8% in 2027 due to higher interest rates, which will exert a drag on the cybersecurity market.
- Assuming that at least a ceasefire will be in place in the Middle East as of April 2027, RSAC expects that: 1) Israel will narrowly outstrip Canada as a source of RSAC 2027 attendees to land at number three behind Brazil; and 2) Israel's cybersecurity industry will continue on its current high growth trajectory.

Endnotes

1. For Senior Leaders, "16+ years" was by far the most common number of years of experience, with 39% of the total. The next most common value was "10-12 years," with just 14%. Base: 22,788.
2. For Line Professionals, "3-5 years" was narrowly the most common number of years of experience, with 19% of the total. The next most common values were "Less than 1 year" (16%), and "6-9 years" (15%). Base: 28,935.
3. RSAC registrants select their organization's industry from a list. RSAC attracts a large number of attendees from cybersecurity firms and other software/hardware companies; we've excluded those attendees from this "top-industries" summary to focus on the attendees from companies who are purchasing and implementing those solutions.
4. For further detail on how RSAC created the Topic and Subtopic taxonomy we use to classify Call for Submissions entries, see endnote 2 of the Volume 4 report.
5. For stateless systems, the preferred pattern is to: 1) add the fix to a known clean image; 2) rebuild (or rehydrate) a new instance for that updated image; and 3) delete the existing running instance. This both accelerates remediation and reduces the risk that a compromise persists after conventional patching. Stateful systems still require a more traditional isolate-and-patch strategy.
6. Base: Line Professionals total session attendances—2022: 34,126 | 2023: 47,878 | 2024: 56,879 | 2025: 49,832 | 2026: 45,942.
7. Base: Senior Leaders total session attendances—2022: 19,381 | 2023: 26,173 | 2024: 28,573 | 2025: 32,650 | 2026: 31,118.
8. We noted the easier hiring environment in mid-2025 in the Volume 2 report, where an ISC2 survey reported that nearly half of employers reported successfully recruiting senior-level cybersecurity hires in six months or fewer.
9. For example, 69% of RSAC™ Cyber Leaders' Forum (CLF) CISOs reported turnover of less than 5% in the six months to March 2026. The CLF community consists of CISOs of organizations with 500 or more employees (that are not Fortune 1000 or equivalently sized).
10. As of March 2026, just 33% of respondents managed to hire for senior roles in six months or less. Note that senior roles require 10-15 years of experience. Source: SANS
11. For example, just 15% of RSAC™ CISO Boot Camp (CBC) members that we surveyed in March 2026 reported that the stress of being a cybersecurity leader was not taking a toll on any aspect of their lives. CBC members are aspiring CISOs poised to assume leadership roles within the next 12-18 months at organizations with 500 or more employees.
12. Base: Total session attendances—2022: 53,507 | 2023: 74,051 | 2024: 85,452 | 2025: 82,482 | 2026: 77,060.
13. The SECURE Data Act proposal that went before the US House Committee on Energy and Commerce Subcommittee on Commerce, Manufacturing, and Trade on 3 June 2026 contains the same previsions for pre-empting US State privacy laws that caused previous proposed legislation (like the proposed American Privacy Rights Act (APRA) of 2025) to fail. Sources: IAPP, Wiley
14. Base: Number of Senior Leaders who visited at least one startup—2022: 521 | 2023: 884 | 2024: 1,052 | 2025: 1,293 | 2026: 1,077.
15. Base: Number of Line Professionals who visited at least one startup—2022: 818 | 2023: 1,462 | 2024: 1,696 | 2025: 1,659 | 2026: 1,210.
16. Base: Number of Line Professionals—2022: 23,791 | 2023: 30,792 | 2024: 33,330 | 2025: 28,637 | 2026: 28,934.
17. Base: Number of Senior Leaders—2022: 12,356 | 2023: 15,104 | 2024: 16,169 | 2025: 22,084 | 2026: 22,782.
18. Base: Number of Line Professionals who visited at least one mainstream exhibitor—2022: 13,999 | 2023: 20,669 | 2024: 21,838 | 2025: 19,141 | 2026: 18,960.
19. Base: Number of Senior Leaders who visited at least one mainstream exhibitor—2022: 7,373 | 2023: 9,990 | 2024: 10,435 | 2025: 14,073 | 2026: 14,341.
20. For example, insurer Beazley specified in its December 2025 earnings report that it would resist the downward pressure on prices in the US cyber insurance market. Source: Beazley
21. "Loss + defense and cost containment (DCC)" is calculated as: (incurred losses + (legal, forensic, and breach coach expenses, ransom negotiator fees, and court costs)), divided by direct earned premium. This is the standard cyber insurance reporting basis for the US National Association of Insurance Commissioners (NAIC). Source: NAIC
22. The NAIC will publish the official loss + DCC ratio averages for 2025 in November 2026.
23. RSAC estimates based on a variety of sources that cyber insurance is profitable for insurers when loss + DCC ratios are <= 50%, that profits compress with loss + DCC ratios between 50-60%, and that the coverage starts to become unprofitable when those loss + DCC ratios exceed 60%. Sources: Actuary.org; The Record; Aon Cyber
24. Sources: Tokio Marine HCC, Aon Cyber
25. RSAC started with an estimate of US $100K for US $68M in coverage in 2020 and applied the industry average premium percentage change to calculate the average premium for equivalent coverage in each subsequent year. See the Volume 2 report endnotes 2 and 3, and the Volume 4 report endnotes 22-24 for further details.
26. Data labels rounded to nearest US$ thousand.
27. RSAC excluded blank responses and "Other" from these rankings. Bases: Senior Leaders: 22,146 | Line Professionals: 25,489.
28. We've charted the domestic cybersecurity market for all countries except Israel, where we've charted both the domestic and export cybersecurity markets. All country cybersecurity market sizes are for 2025 except the one listed for Israel (export), which is for 2024. Sources: Brazil: US Department of Commerce; Canada: Statista (Canada); Israel (domestic) Mordor Intelligence (Israel); Israel (export, 2024): The Marker; Mexico: IMARC (Mexico); South Korea: IMARC (South Korea); UK, US: Statista (Forecast, Dec 2025).
29. See endnote 30 for details on the range we've given for the year-on-year growth of Israel's cyber exports, and see endnote 31 for details on the range we've given for the year-on-year growth of Canada's cybersecurity market. All other countries' year-on-year growth rates are 2024-2025. Sources: Brazil: Databridge (Brazil), US Department of Commerce; Israel (domestic): Mordor Intelligence (Israel); South Korea: IMARC (South Korea), IMARC (press, 2025); Mexico: Cyberpeace, IMARC (Mexico); UK, US: Statista (Forecast, Dec 2025).
30. Israel's export cyber industry dwarfs its domestic cyber industry, so we've charted them separately. We've given a range for the year-on-year growth for 2024-2025 of Israel's cybersecurity export market from 15-25% because we're extrapolating from sources whose prior-year baselines vary considerably; the official numbers from the Israel Export Institute should be available by Q4 2026. Ordinarily, in this case, we'd use the prior-year growth numbers, but the 2023-2024 year-on-year growth numbers for cybersecurity exports for Israel were unusually nearly flat, likely in part because of the Israel-Gaza war that began in October 2023. Sources: The Marker; Israel Innovation Authority; Jerusalem Post; Times of Israel.
31. We've given a range for the year-on-year growth of Canada's cybersecurity market for 2024-2025 of 7-11% because the sources vary. Sources: Databridge (Canada); Expert Market Research; Statista (Canada); Verified Market Research
32. In 2025, Brazil's GDP grew by 2.3%, and Israel's by 2.9%. Source: IMF.
33. Source: Cybersecurity Insiders
34. Coinsurance requirements mean that you have to pay for a percentage of a certain type of loss yourself. Source: CoverLink Insurance
35. Deductibles are often referred to as "retentions" in cyber insurance, but they work the same way as other insurance deductibles—you're responsible for the first $X thousand in costs, and your insurance company pays thereafter. Source: SeedPod Cyber
36. Source: SANS
37. Source: Programs.com
38. Sources: StartBrazil, HiveDesk

CISO Checklist

Here's what RSAC recommends that CISOs and other senior cybersecurity leaders do to prepare for the impact of these predictions:

NEXT WEEK

- [ ] **If your firm hasn't renewed its cyber insurance policy in 2026 yet, advocate for initiating that process now.** And look for tightening of underwriting standards that may reduce your coverage in less obvious ways, including: 1) sub-limits on coverage for particular types of events;[33] 2) coinsurance requirements;[34] and 3) higher deductibles.[35]

- [ ] **Upgrade incident response and recovery and cloud security practices.** To summarize the core suggestions from our recent paper on preparing for the impact of substantial improvements in frontier model vulnerability discovery: a) Compress patch windows and SLAs; b) "Rehydrate" all stateless systems to reduce the number of systems requiring traditional patching; c) Practice continuous attack surface management; and d) Create a vulnerability surge mode.

- [ ] **Invest in your staff's skill development.** As of early 2026, more than half of cybersecurity professionals surveyed report that their firms suffer from at least a moderate skills gap, and more than 50% also say that lack of skills is a bigger problem than an inability to hire more staff.[36] Hence, CISOs should identify the most pressing skill gaps and devote budget to addressing them.

WITHIN THE NEXT 3 MONTHS

- [ ] **Allocate more resources to leadership development for your people leaders.** In Volume 2, we encouraged CISOs to invest in their own leadership acumen, and that advice stands. Because the old saw that "people join companies, but they leave managers," remains true, CISOs should also upgrade their direct reports' leadership skills to equip those managers to retain key staff.

WITHIN THE NEXT YEAR

- [ ] **Add Brazil to your list of cybersecurity staff search locations.** Brazil is one of the few markets whose cybersecurity talent supply has improved in the last five years.[37] If your firm already operates in Brazil, or if something like an employer-of-record arrangement proves cost-effective for you, look for new recruits in cities like Belo Horizonte, Florianópolis, Recife, and São Paulo.[38]

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.

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. 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.

Additionally, RSAC Conference has become a launchpad for groundbreaking cybersecurity startups through initiatives like the RSAC Innovation Sandbox 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 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 Conference 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

CYBERSECURITY INSIGHTS & FUTURES
VOL 6 | JUNE 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