Gartner

2026 Executive Summary

From the Conference Chair

As the demands of your role continue to evolve, embrace guidance to strengthen your organization's resilience amid tariffs, global instability, and emerging AI threats.

We hope to see you at Gartner Security & Risk Management Summit 2027.

Sincerely,
Khushbu Pratap,
Conference Chair and VP, Team Manager, Gartner

Top Takeaways

1 Transform work to unlock AI's full potential

Leverage enterprise AI investments to modernize identity and future-proof your security foundation. Reframe the normalization of cyberattacks as a catalyst to strengthen resilience in your goals and practices. Then monetize ongoing innovation by embedding a continuous learning cycle—enabling you to reinvest in advanced solutions and extend your capacity to adapt, secure new frontiers, and empower AI adoption for lasting business value.

"By strategically assessing emerging trends, CISOs can determine whether to embrace, monitor, or deprioritize developments."

Wam Voster,
VP Analyst,
Gartner

2 Refine your cybersecurity vision to address key imperatives

Align your vision with your cybersecurity program by emphasizing performance, resilience, and agility. As a CISO, your influence grows when you leverage power bases, build political capital, and apply advanced persuasion techniques. An operating model helps evaluate the impact of change, enabling risk-informed prioritization and improved data security governance. Launching a postquantum security initiative, integrating supply chain risk, and prioritizing threat-informed cyber resilience will further strengthen your security posture.

"Resilience is not just about technology responding automatically, it's about people making decisions under pressure."

Ganesh Ramamoorthy,
Managing Vice President,
Gartner

3 Close cyber resilience gaps and strengthen security

To develop a cyber resilience strategy, begin by addressing stakeholders' and regulators' focus on system and data availability. Evaluate the depth and accuracy of your current Business Impact Analyses (BIAs) to leverage existing insights. Enhance cyber resilience by collaborating across teams with a focus on business impact. With strong security hygiene and integrated advanced capabilities like automated threat detection and response, you can effectively embed resilience into your program.

"Cyber resilience isn't just a strategic advantage; it's a critical necessity for survival."

Franz Hinner,
Sr Director Analyst,
Gartner

4 Focus on security trends and strategic choices

Strategize your cybersecurity plans by addressing trends like geopolitics, post-quantum cryptography, and tactical AI, while aligning zero trust initiatives with strategic goals. Combat cybersecurity burnout by balancing workloads and promoting mental health through HR support and wellness programs. Use a platform consolidation framework to streamline efforts but be cautious of improper scope and vendor influence leading to cost overruns. Embrace a cultural shift by fostering adaptability and openness to change, which can help overcome resistance and adapt to zero trust's complexity.

"We need to shift from awareness and training, to managing fundamental employee behavior change."

Ganesh Ramamoorthy
Managing Vice President,
Gartner

5 Scale your third-party cyber risk management

With frequent third-party disruptions and increased scrutiny, Gartner predicts TPCRM performance will be a key board agenda item by 2026. Use the Gartner TPCRM life cycle to assess program completeness and transparency in labor division. Facilitate sponsor involvement in cyber risk management by clarifying roles and focusing on critical activities. Shift from compliance to risk appetite-driven TPCRM by tracking outcome-driven metrics and using comparative advantage for tech investments. Keep your board updated on TPCRM performance, ensuring reporting and budgeting align with ODMs and PLAs.

"Use the expanding and prescriptive regulatory mandates to transform TPCRM risk into clear business requirements that drive the investment roadmap."

Rahul Balakrishnan,
Sr Director, Research,
Gartner

6 Leverage the *Executive Faststart Framework* to maximize impact

Whether you're new to an organization or newly promoted, it's crucial to hit the ground running. In your first year, focus on understanding your environment, role, and stakeholders' core objectives to establish initial priorities. Quickly build key relationships and manage stakeholders for both short- and long-term success. Deliver on your priorities to show progress and demonstrate value, while also focusing on building your personal brand—own it by actively shaping how you're perceived through your actions and communication.

"You get one chance to make a great first impression as a new CISO: your credibility is hard to build, easy to lose."

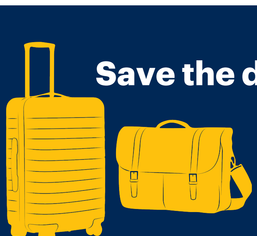
Niyati Daftary,
Principal Analyst,
Gartner

7 Prioritize the human factor

It's essential to recognize that while most cybersecurity investments focus on technical solutions, human error is often the root cause of incidents. Embrace a human resilience mindset from day one, shifting focus from prevention to resilience, and change the language used in cybersecurity to avoid us versus them narratives. First, develop metrics to measure human resilience and move away from failure-focused metrics. Then transition from traditional compliance training to dynamic nudges that encourage safer habits and pivot your cybersecurity strategy towards broader cyber resilience.

"Humans are the biggest overlooked opportunity for cybersecurity. This is an exciting opportunity — and perhaps even a new frontier for cybersecurity."

Apoorva Chhabra,
Sr Principal Analyst,
Gartner



Save the date!

Join us 8 - 9 March 2027 in Mumbai, India for Gartner Security & Risk Management Summit!

#GartnerSEC

Gartner