Gartner Security & Risk Management Summit
23 - 25 September 2024

Gartner

2024 Executive Summary

We hope to see you at Gartner Security & Risk Management Summit 2025.

Sincerely,
Pete Shoard
Conference Chair, and Vice President Analyst, Gartner

Top takeaways

1 Adopt an *Augmented Cybersecurity* approach

Instead of merely surviving amid permanent complexity, you can thrive by increasing cybersecurity's resilience in a sustainable way. Abandon the zero-tolerance-for-failure mindset, and elevate response and recovery to equal status with prevention. Develop a fault-tolerant organization, adopt new tactics to increase your team's resilience, and embrace a minimum effective toolset approach.

> **"This is an essential rebalancing for a world where complexity increases...and your resources don't!"**
>
> Christopher Mixter,
> VP Analyst,
> Gartner

2 Revisit your cybersecurity vision and mission

Address these three common, key imperatives and make sure they're reflected in your cybersecurity vision and mission: the impact of increasing business unit autonomy in the adoption of new digital technology; the rapid adoption of AI in the business; and the importance of the role of individuals, especially the need to change behaviors and establish a security consciousness within the corporate culture.

> **"CISOs face a bewildering array of rapidly evolving priorities, threats, demands, regulatory pressures, and technology changes."**
>
> Tom Scholtz,
> Distinguished VP Analyst,
> Gartner

3 Strategically design your security strategies

Factor in Gartner's top predictions as you design and execute your security strategies in this volatile, uncertain, complex, and ambiguous world. As you look out over the next decade and strategize the cybersecurity plan for your organization, seriously consider the scenarios outlined alongside the top predictions. The CISO's increasing legal exposure, GenAI, misinformation, identity response, the skill gap, insider risk, and more must be on your radar.

> **"One thing is certain — a different future awaits!"**
>
> Craig Porter,
> Director Analyst,
> Gartner

4 Increase effectiveness with the right behaviors and mindsets

The drivers of CISO effectiveness are primarily behaviors and mindsets, putting CISO effectiveness within your control. Use the Gartner CISO Effectiveness Diagnostic to evaluate your current performance, create the space to execute on your professional development by mastering your time, and build your professional development plan around the 11 controllable drivers of CISO effectiveness.

> **"It is the fundamentals, not excellence at *whack-a-threat*, that will enable you to thrive in today's highly complex environment."**
>
> Victoria Cason,
> Principal Analyst,
> Gartner

5 Understand what drives human behavior around security

To ensure you know what actually drives human behavior around security, start to embrace concepts such as prospect theory, desire paths, and inclusive design. This will help to shape security controls that optimize resilience and mitigate weaknesses in the cybersecurity chain that may have been created or exacerbated by cybersecurity practitioners placing unreasonable expectations on users.

> **"Engage with people to design cybersecurity controls with minimum effective friction."**
>
> Ant Allan,
> VP Analyst,
> Gartner

6 Embrace the *Cyber Resilience Framework*

Adopt the *Cyber Resilience Framework* to ensure you build resilient processes, enhance the resilience of your team (with effective hiring practices, operations, and culture), and focus on resilient partners that play a critical role in your organization. Remember, cyber resilience goes beyond just controls and metrics.

> **"Cyber resilience cannot be achieved by the CISO alone. Functions need to work together, not in siloes."**
>
> Arthur Sivanathan,
> Sr Director Analyst,
> Gartner

7 Augment cybersecurity with AI

Build foundations to augment cybersecurity with AI. Start by crafting a strategic cybersecurity roadmap to support AI, defining acceptable policies, and reducing risk to a commonly agreed residual level. Help to build foundational knowledge about GenAI in your organization, continually manage change, and focus on the new skills you'll need (not on removing the need for skills).

> **"We too often see Generative AI as a battle between attackers and defenders, whereas we should really evaluate outcomes against expectations."**
>
> Jeremy D'Hoinne,
> VP Analyst,
> Gartner

8 Harness creative conflict

As attackers become more innovative in their approaches, you must continuously get creative and welcome different perspectives. Improve cybersecurity transformation by understanding the connection between conflict and creativity, fostering creativity with diverse mindsets, moderating emotional friction, paving the way, and harnessing the power of creative conflict.

> **"Cybersecurity excellence depends on creative conflict."**
>
> Cynthia Phillips,
> Sr Director Analyst,
> Gartner

9 Rethink cloud security skills

Cloud is the new normal and you must adapt your skills to support cloud security. Instead of assuming this is simple and your team can pick it up quickly, be open-minded to new ways of implementing security by transferring, readapting, and rethinking existing skills to support cloud security architecture. Remember, cloud security (while having novel and interesting technologies and approaches), is still security.

> **"Many of the risks we experience in the cloud are similar, if not the same as on-prem, but they are magnified in the cloud."**
>
> Richard Bartley,
> VP Analyst,
> Gartner

Save the date!

Join us 22 - 24 September 2025 in London for Gartner Security & Risk Management Summit.

#GartnerSEC

Gartner