Gartner

Top Trends in Cybersecurity for 2025

12 December 2024 - ID G00822766 - 49 min read

By: Richard Addiscott, Anson Chen, Joerg Fritsch, Tom Scholtz, Will Candrick, Jeremy D'Hoinne, John Watts, Chiara Girardi, Manuel Acosta, Felix Gaehtgens, Oscar Isaka, Alex Michaels

Initiatives:Cyber Risk; Build and Optimize Cybersecurity Programs; Demonstrate Value and Collaborate With Business Partners; Meet Daily Cybersecurity Needs

> Relentless technological and business disruption test the limits of security programs and team performance. Security and risk management leaders must enable business value and double down on embedding organizational, personal and team resilience to prove security program effectiveness in 2025.

Overview

Opportunities

- Delivering business value in the face of ever-changing technologies and the business’ desire to exploit them for strategic gain is a constant challenge for security and risk management (SRM) leaders. Collaborating with data and business leaders and extending enterprise IAM strategies helps ensure enterprise data and systems are AI-ready. Concurrently, collaboration fosters more independent and effective cybersecurity risk decision making that enables secure business transformation.

- Supporting business demand for stable continuity of operations and absorbing pressure from the ever-shifting threat landscape is a constant for SRM leaders. These challenges provide opportunity for a more proactive and comprehensive approach that embeds resilience into technological and human-driven capabilities.

- Grassroots initiatives focused on enhancing secure behavior and culture, managing third-party risk associated with generative AI (GenAI), and improving the business’ perception of cybersecurity presents SRM leaders with a unique opportunity. By collaborating with IT and business leaders to address these areas, SRM leaders can derive dual benefit from driving secure business transformation and embedding resilience within the organization.

Recommendations

As an SRM leader seeking to optimize your organization's cybersecurity program and investment, you should:

- Build trusted foundations for secure, AI-enabled business transformation by formalizing cybersecurity risk accountability, fostering cyber judgment, reinvigorating data security management programs and extending enterprise IAM strategies to include machine identities.
- Embed resilience by engaging in planning and regular review of both technological and human-driven capabilities. This involves optimizing technology investment and use, integrating AI into existing workflows, and monitoring for and reacting to signs of burnout within security teams.
- Strengthen the foundation for secure business transformation by developing clear, actionable third- party risk policies and fostering targeted collaborative engagements with IT and the business. This approach will reinforce security decision making and enhance the perception that a strong cybersecurity culture is anchored in resilience, agility and defensibility.

Strategic Planning Assumptions

- By 2027, CISOs investing in cybersecurity-specific personal resilience programming will see 50% less burnout-related attrition than peers who don't.
- By 2026, enterprises combining GenAI with an integrated platforms-based architecture in security behavior and culture programs will experience 40% fewer employee-driven cybersecurity incidents.

What You Need to Know

Unsurprisingly, GenAI, and AI more broadly, has been a common element in the core focus areas for SRM leaders in 2024. Gartner expects it will continue to impact their strategic objectives in multiple ways in 2025:

- Setting heightened expectations for creating efficiency and consistency in the deliverables from cyber teams and making them more understandable for nonsecurity leaders
- Triggering changes to existing security processes to ensure relevance, to suggest effective change in and enable business agility

- Expanding the scope of existing enterprise security initiatives, thus strengthening the foundations for exploiting AI use cases
- Amplifying pressure on already stretched resources

Coupled with the enduring challenges of an ever-evolving threat landscape, widening talent gaps and increasing regulatory oversight, SRM leaders are predominantly concentrating their efforts into two areas:

- Enabling transformation
- Embedding resilience

Enabling Transformation

Business leaders are leveraging the latest AI innovations and other progressive, and increasingly accessible, technologies at the organization's edge to drive strategic value This results in a corresponding decentralization of cybersecurity decision rights and accountability.

Leading SRM leaders proactively adapt to these shifts by implementing collaborative risk management practices. This enhances opportunities to codify business ownership of cyber risk and instill improved cyber judgment across the enterprise. This helps enable increased business technology autonomy and agility without introducing unacceptable levels of cybersecurity risk.

Having ready access to healthy and secure data is a key prerequisite for even the smallest AI initiatives. SRM leaders are working alongside their data and analytics and privacy colleagues to ensure any structured and unstructured data proposed for use in approved GenAI use cases is both AI-ready and secure.

Forward-looking SRM leaders have also recognized that, with GenAI capabilities gaining footholds inside organizations, there is a corresponding increase in cloud services and automation pilots. In response, they extend the scope of ongoing efforts to strengthen identity and access management strategies to include machine identities (see Note 1).

Embedding Resilience

In 2024, SRM leaders were focused on optimizing their security programs to deliver organizational and cyberresilience. This work will continue into 2025.

We are seeing increasing recognition that a “zero-tolerance for failure” mindset has reached its peak in achieving sustainable risk buy-down and only increases the risk of security team burnout. SRM leaders are focusing on moving to embed resilience into the corporate culture’s lexicon, exploring cyber deterrence as a differentiator and cyberstorage capabilities to enable transformation and foster increased resilience.

There are more than 3,000 cybersecurity vendors to choose from. [1] Consequently, SRM leaders are finding it more challenging to manage the inherent tension between trying to enhance their capabilities to address new technologies and emergent risks and concurrently reducing operational overhead and complexity. SRM leaders who align their available resources and in-house technical capabilities can balance the adoption of platforms with pursuit of cybersecurity mesh architectures to settle on the right mix of tools and vendors to achieve their desired outcomes.

The ever-shifting threat and technology landscape, increasing business demand, and regulatory requirements, coupled with the endemic talent shortage, is generating a perfect storm. As a result, the security industry is experiencing a mental health crisis as SRM leaders and their teams experience increasing levels of burnout. Effective SRM leaders are acknowledging and responding to this issue as one of their highest priorities to ensure they deliver a resilient and sustainable cybersecurity program.

Dual Focus Delivering Dual Outcomes

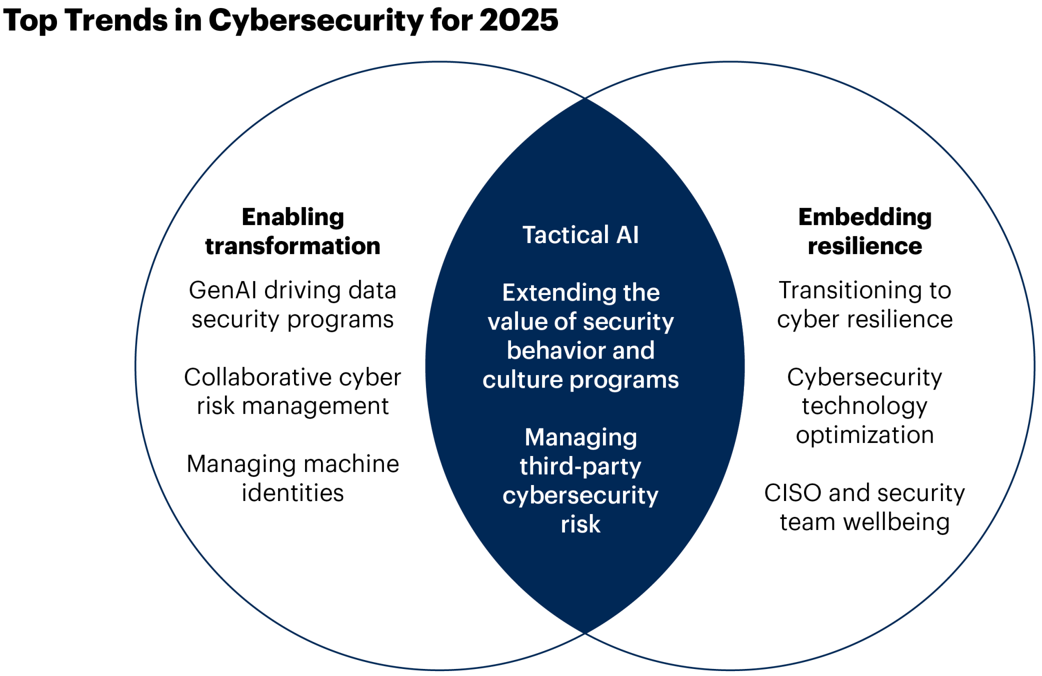
Several of this year’s trends provide SRM leaders the opportunity to enable transformation and further embed cyber resilience.

SRM leaders are learning from AI transformation pilots and refining their processes based on initial success in taking a more tactical approach to AI integration. This scaled-back approach is also serving to reduce risks to security program outcomes and maintain the function’s credibility by focusing on, and delivering more, incremental security benefits than myopically striving for hype-driven seismic change.

A continued focus on third-party cybersecurity risk management and maturing security behavior and culture programs (SBCPs) from 2024 is delivering value in two ways. First, they provide protection from cybersecurity incidents occurring inside and outside the organization. Second, they offer guidance and guardrails for increasingly autonomous business areas undertaking more and more technology work that expands the organization’s digital ecosystem and associated attack surface.

Figure 1 depicts the Top Trends in Cybersecurity for 2025.

Figure 1: Top Trends in Cybersecurity for 2025


Top Trends in Cybersecurity for 2025
Enabling transformation
GenAI driving data security programs
Collaborative cyber risk management
Managing machine identities
Tactical AI
Extending the value of security behavior and culture programs
Managing third-party cybersecurity risk
Embedding resilience
Transitioning to cyber resilience
Cybersecurity technology optimization
CISO and security team wellbeing

Source: Gartner
822766_C

Table 1: Top Trends in Cybersecurity for 2025

Enabling transformation	Embedding resilience
GenAI driving data security programs	Transitioning to cyber resilience
Collaborative cyber-risk management	Cybersecurity technology optimization
Managing machine identities	CISO and security team well-being
Tactical AI	
Extending the value of security behavior and culture programs	
Managing third-party cybersecurity risks	

Source: Gartner

Enabling Transformation

GenAI Driving Data Security Programs

Analysis by Joerg Fritsch, Anson Chen, Brian Lowans

Description:

The rise of GenAI is transforming data security programs, notably in three dimensions:

Preference for Synthetic Over Obfuscated Data in GenAI Training

Synthetic data is increasingly favored over traditional anonymization methods for training AI models. Gartner observes that mature end customers who need to mask sensitive information are frequently using products that generate vertical-specific or custom-made synthetic data. Synthetic data ensures privacy preservation and addresses the challenges of insufficient data in the adoption of GenAI technologies by generating artificial training data instead of relying on real-world observations. This process involves different models where the synthetic data AI is trained once and can produce synthetic data multiple times for various use cases, edge cases or rare scenarios. The real data is used sparingly to re-check model alignment and monitor for model drift, making synthetic data invaluable in sectors like healthcare and finance. Additionally, the AIs that generate synthetic data are supervised to prevent reinforcing biases or errors, or to intentionally introduce bias and errors to assist with capabilities such as fraud prevention.

Shift From Structured to Unstructured Data Security

This shift is necessary because unstructured data is becoming more prevalent and more valuable in the age of GenAI. Previously, data security technologies focused on structured data like databases. However, GenAI's ability to process unstructured data — text, images, videos — has shifted attention as GenAI makes end customers increasingly aware of the value of their unstructured data.

Increased Need to Assess the Data Security Posture of GenAI

GenAI's ability to be trained on an organization's data creates risks that data is unknowingly accessed or shared with vendors or cloud service providers. This training also creates internal access risks through prompting. This establishes the need for data security posture management (DSPM) solutions that can discover, assess and monitor GenAI access to data and could also detect data pipelines that connect outside the organizational infrastructure. DSPM vendors are rapidly enhancing their tools to support organizations on their journeys to securely use third-party GenAI services and secure access to data via custom GenAI architectures.

Why Trending:

The demand for leveraging GenAI either through third-party services, as part of existing business applications or via custom-made GenAI architectures continues to grow as organizations push to identify where AI can create the most value. However, unease over data accuracy, privacy and/or compliance is a major barrier impeding GenAI adoption. [2,3]

Senior business leaders have started recognizing the opportunities and increasing pressure on IT leaders involved with data security. They are urging IT leaders to investigate GenAI data security requirements and make them part of their security programs. This involves allocating a budget to implement a mix of mature controls and accessible early-stage innovations frequently offered by DSPM.

Implications:

In various use cases, synthetic data enables innovation without the delays associated with deidentification, risk management or approval processes required for using production data or masked/deidentified production data. This approach not only accelerates development but also reduces costs, privacy risks and data bias.

Other technologies, such as DSPM, have transitioned from immature niche offerings to mature commercial data security solutions. They are now used for governing, cataloging and monitoring data leveraged for GenAI. DSPM adoption is increasing and implementations to securely use GenAI have been observed across various industries.

Finally the shift of attention and dedicated budgets from the security of structured data to the security of unstructured data eventually enabled organizations to leverage diverse types of data that previously were not protected adequately.

Actions:

- Evaluate and invest in synthetic data generation tools to replace traditional anonymization methods. This will help mitigate privacy risks and facilitate compliance, especially in highly regulated industries such as healthcare and finance.
- Leverage technologies (e.g., DSPM) to catalog, monitor and govern both structured and unstructured data. Ensure these tools are capable of supporting GenAI use cases and can integrate effectively with existing security frameworks.

- Reallocate resources and budgets to support both structured and unstructured data security. Invest in technologies and practices that protect text, images, videos and other forms of unstructured data, which are increasingly valuable in GenAI applications.

Further Reading:

Market Guide for Data Masking and Synthetic Data

Innovation Insight: Data Security Posture Management

2024 Strategic Roadmap for World-Class Security of Unstructured Data

Collaborative Cyber-Risk Management Enables Digital Transformation

Analysis by Tom Scholtz, Michael Kranawetter, Oscar Isaka

Description:

As technology investment decisions are increasingly being made independently by business technologists in the lines of business, traditional centralized cyber-risk management processes fail to scale, introduce friction and inhibit agility. Business adoption of transformative technology such as GenAI results in a rapidly evolving cyber-risk environment.

Historically, centralization of risk decisions meant that all decisions had to go through a single decision-making body. Now, cyber-risk management requires a scalable approach with risk decisions made by informed business technologists. This approach emphasizes the centralization of flexible oversight while supporting local decisions through a collaborative and agile cyber-risk management process.

Why Trending:

57% of respondents to a Gartner survey indicate that they are making resource owners directly accountable for the cyber risk associated with their resources. [4] However, in other somewhat counterintuitive responses, a majority claim to be centralizing cyber-risk decision making. This apparent contradiction is explained by 55% of respondents stating that they are centralizing the cyber-risk decisions in an enterprise security steering committee in order to facilitate business ownership of cybersecurity risk. [4]

The reason many CISO's are "centralizing to decentralize" risk management is due to the reality that cyber-risk decisions cannot be made in isolation, regardless of the level of autonomy enjoyed by the risk owners. Resource owners (i.e., the risk owners) should be enabled to make autonomous cyber-risk decisions, but when making decisions, they have to consider wider risks to the enterprise, (e.g., the reputational and financial risks) inherent in their cyber-risk decisions.

Implications:

- CISO's must reassess and adapt their organizations and cyber-risk management processes to deal with this new reality.
- Cyber judgment, while part of the answer, is not the solution to this dilemma. Although cyber-risk decisions can be made autonomously "at the edge," they can never be made in isolation. Every autonomous cyber-risk decision must, at a minimum, take into consideration the reputational and financial risk to the enterprise.
- This broader impact of risk decisions necessitates some level of centralized validation, as well as common risk acceptance, escalation procedures and conflict resolution forums.

Actions:

- Formalize and socialize the notion of owner accountability for cybersecurity risks. Document the principle of owner accountability in an enterprise security charter (see Tool: Enterprise Information Security Charter Template), which must be signed and clearly supported by the CEO and the board. The ESC must clearly state that the ultimate accountability for protecting the enterprise's information resources and, by implication, its business processes and outcomes, rests with the business owners of the information resources.
- Implement cyber judgment, which is the ability of decision makers and risk owners throughout the organization to independently make *informed* cyber-risk decisions. This is the key element of the decentralized element of collaborative risk management.
- Create centralized validation and conflict resolution processes, which will help organizations make sure that cyber-risk decisions made by business technologists are consistent, well-informed and aligned with the company's broader goals.

Further Reading:

CISO Effectiveness: Security Operating Models Are Evolving

2025 Strategic Roadmap for Cyber GRC

The Cyber-Risk Management Cookbook for Security Leaders

Enterprisewide IAM Strategies to Address the Rise of Machine Identities

Analysis by Felix Gaehtgens, Oscar Isaka, Zachary Smith

Description:

The importance of managing (nonhuman) identities and access for machines (devices and workloads) is growing. Cloud services, the rise of automation and DevOps practices, and the emergence of AI, among other organizational trends, have led to the prolific use of machine accounts and credentials for physical devices and software workloads. But machine accounts and credentials are frequently created and used by different teams within organizations. As a result, they are often uncontrolled and unmanaged, making them an enticing target for cyber adversaries to gain unauthorized access to IT systems. As the importance of managing identities and access for machines surges, SRM leaders are under pressure to build a strategy to implement robust machine identity and access management across the enterprise to protect against such attacks.

Why Trending:

Gartner's 2024 IAM Leadership Survey found that 54% organizations have seen an increase in the number of identity-related breaches, with one in three organizations experiencing increased business interruptions, financial loss or regulatory penalties from such incidents. [5] As many as 85% of identity-related breaches can be attributed to hacked machine identities such as service and automation accounts. [6]

It's no surprise that cybersecurity is increasingly focusing on managing identities — and machine identities specifically. Nearly three in four organizations say that "effectively managing and securing identities" is a top 3 cybersecurity priority (vs. 61% in 2024; IDSA 2024), [7] A 2023 Study by Venafi found that nearly nine in 10 security and IT leaders believe handling machine identities is essential for successfully implementing zero-trust models. [8] , [9] But SRM leaders (including IAM leaders) can't handle machine identities without a coordinated enterprisewide effort. Gartner found that IAM teams are only responsible for 44% of an organization's machine identities. [5] Thus, managing all machine identities will require a concerted effort and coordination among multifaceted teams.

Implications:

- **Centralized/decentralized IAM execution:** Machine identities are managed outside the core IAM team in nearly half of organizations. But core IAM teams are themselves becoming increasingly dispersed in 62% of organizations, [5] necessitating a division of responsibilities between core and satellite IAM functions for both planning/sponsorship and execution of machine identity management. This concept of centralized guidance and decentralized execution is aligned with the Collaborative Cyber-Risk Management Enables Digital Transformation trend discussed in this research.
- **Policy and accountability:** Organizations must establish governance over machine identities, including clear policies and ensuring compliance across all teams performing IAM functions, with defined responsibilities and accountability.
- **Enhanced security posture:** Effective IAM management, including both human and machine identities, is crucial for future-proofing security and mitigating sophisticated cyberthreats. SRM leaders need to form a machine identity working group and collaborate with all stakeholders to ensure machine identities are part of the overall cybersecurity strategy for the organization.
- **Effective machine identity strategy:** Organizations should develop a central strategy to diminish or remove the need for workloads to handle secrets (machine credentials) themselves. Instead, work toward a strategy where a distinct trust infrastructure secures interactions between workloads without requiring workloads to handle secrets. That would shrink the attack surface that needs to be managed, since workload secrets are very sensitive and at risk of being discovered and stolen.

Actions:

- Ensure that machine accounts and credentials are properly scoped in terms of permissions, cataloged, managed, monitored and protected against accidental disclosure in the short term. Build a strategy to prevent credentials from being exposed to workloads, and consider using infrastructure-managed service accounts to minimize credential exposure.

- Establish comprehensive IAM policies that outline the responsibilities and accountabilities of both core IAM and other security and business teams with shared machine IAM responsibilities. These policies should drive toward the strategy mentioned above.
- Establish regular communication channels, joint training sessions and periodic check-ins between core IAM teams and other teams responsible for machine identities to ensure alignment and knowledge sharing.

Further Reading:

Managing Machine Identities, Secrets, Keys and Certificates

CISO Foundations: 5 Questions CISOs Should Ask About IAM

Prioritize IAM Hygiene for Robust Identity-First Security

Embedding Resilience

Transitioning to Cyber Resilience

Analysis by Will Candrick, Wayne Hankins, Preeti Bhave

Description:

SRM leaders are pivoting cybersecurity from a prevention mindset to a resilience focus. Cyber resilience embraces a "when, not if" mentality, and seeks to minimize the impact of cyber incidents on the enterprise and enhance adaptability, rather than engage in misguided notions of outright prevention.

Why Trending:

Board directors and C-suite leaders now widely view cyber risk as a core business risk to manage — not a technology problem to solve. In the 2024 Gartner Board of Directors Survey, 84% of board directors view cyber risk as a business risk, up from just over half in 2016. [10] This shifting perspective leads to more frequent and intense CISO interactions with board directors and C-suite leaders.

In fact, 82% of CISOs present to the board two or more times a year, and nearly 60% do so quarterly or more. Seventy-five percent of CISOs also present to the C-suite quarterly or more. [11] In addition, the SEC's cybersecurity reporting and disclosure rules increase cybersecurity transparency with the public, and reinforce the concept of business materiality to cyber incidents. As a result, SRM leaders face pressure to pivot cybersecurity to a resilience focus and communicate these efforts to nontechnical stakeholders.

Implications:

SRM leaders must prepare for the following implications as they transition to cyber resilience:

- The SRM leader's remit is expanding. Cyber resilience requires coordination across adjacent risk areas. This includes business continuity management, disaster recovery (including data backups), cyber-physical system (operational technology [OT], Internet of Things [IoT], Industrial IoT [IIoT]) security, procurement, privacy, data governance and AI adoption. In many cases, SRM leaders are tasked with leading and managing across these risk domains.
- SRM leaders must prepare for personal liability. Material business impacts from cyber incidents — such as operational outages, data leaks or ransom payments — and new laws and regulations may expose SRM leaders to personal civil and criminal liability risk. Even though such liability risk may vary by jurisdiction, all SRM leaders should monitor the regulatory landscape and prepare for changes to liability exposure in the future.
- Cyber resilience extends well beyond technical controls. Pursuing resilience expands the risk mitigations SRM leaders must consider. For example, third-party risk management extends to supply chain redundancies, CPS security expands into physical and life-safety risks, cyber deterrence exploits attacker motivations and human decision making, and GenAI threats exploit human behavior with more convincing social engineering.

Actions:

- Drive a new culture of resilience across the cybersecurity team and senior leadership. Pivot away from a "hero culture" based on a zero-tolerance-for-failure mindset. Because incidents cannot be outright prevented, cybersecurity's success should be measured by sustained achievement of business outcomes, not cyber incident prevention.

- Adopt cyber deterrence measures to address anticipated attacks. Expand cybersecurity beyond reactive controls, and embrace tactics that exploit attacker motivations and discourage attackers from targeting your organization. Cyber deterrence explores novel methods to manage cyber risk — and improve resilience — beyond traditional investments that react to current and realized threats.
- Build cyberstorage capabilities. Identify I&O leaders responsible for storage and backup systems, and work with them to evaluate cyberstorage capabilities that actively defend storage systems and data from cyber attack. SRM leaders may even take full ownership or co-ownership of cyberstorage as part of a holistic resilience strategy in the face of ransomware.

Further Reading:

Succeed as an SRM Leader by Infusing Resilience Into Your Program

CISO Edge: Use Cyber Deterrence to Stop Attacks Before They Start

Innovation Insight: Cyberstorage Mitigates the Impact of Cyberattacks

Cybersecurity Technology Optimization

Analysis by John Watts, Dionisio Zumerle, Michael Kelley

Description:

The choice of cybersecurity technology providers for SRM leaders continues to expand while, paradoxically, large cybersecurity vendors are incentivizing customers to consolidate into broader platform offerings. This has created tension for SRM leaders who want to reduce complexity and overhead through platforms when, increasingly, large vendor platforms overlap and compete with point solutions. Expanding platforms address more threats through broader product capabilities, but may force shelfware conversations and require point solutions to fill in gaps not addressed by platforms.

SRM leaders depend on optimization of their technology stacks to reduce inefficiencies. Those predispositioned to consolidation for financial and optimization benefits run the risk of failing to meet cybersecurity requirements. Consolidation must be balanced. There are diminishing returns the further along the consolidation path organizations go. Organizations are seeking to strike the right balance between consolidation of commodity capabilities and purchase of separate, differentiated products to address niche requirements.

Why Trending:

SRM leaders face a paradox of choice in today's cybersecurity industry. They need to master the art of knowing when to experiment with startups and small vendors to address unique challenges and when economies of scale through large vendors outweigh vendor lock-in risk. There are an estimated 3,000 or more vendors in the cybersecurity space [1, 12] generating over $200 billion in revenue. [13] Some large vendors report growth in their strategic platforms. [14, 15] This complexity often leads to cybersecurity incidents as many are a result of single vector control failures rather than a mix of complex techniques. [16]

The average organization has 43 tools in its cybersecurity product portfolio, and 5% of organizations have more than 100 tools. Sixty-nine percent of surveyed organizations indicated an increase in cybersecurity tools from 2022 through 2023. [17]

In the long term, organizations that optimize tools must update their resilience strategy and response plans to operational risk. The CrowdStrike incident in July 2024 [18] highlighted the long-term need for updated resilience strategy and response plans in the wake of the outage, based on Gartner's post incident survey. [19] The U.S. Cyber Safety Review Board (CSRB) Microsoft incident report [20] showed that over-reliance on a single vendor increases impact to a large number of organizations if that vendor experiences a compromise.

Operational resilience is an increasing focus for Gartner clients as more consolidated cybersecurity platforms such as extended detection and response (XDR) and secure access service edge (SASE) are being rolled out worldwide.

Implications:

SRM leaders are shifting focus to tool optimization rather than vendor consolidation. The move toward tool optimization allows organizations to find the right mix of platform and point solutions and creates a balance between reducing complexity and providing flexibility in deploying tools to meet cybersecurity objectives.

The emergence of standards such as Open Cybersecurity Schema Framework (OCSF), data fabric for security vendors, and accessibility of cybersecurity vendor product APIs creates opportunities to establish a framework to consolidate in some domains and integrate point solutions as needed. Establishing a cybersecurity mesh architecture prioritizes integration flexibility over proprietary platforms for those positioned to take advantage of it.

A further risk of consolidation is mistaking bundling for a platform. By using bundled products, there is an increased risk of adding to technical debt. In many cases, shelfware can not be avoided when purchasing bundled security products.

Actions:

- Mitigate the risks of vendor lock-in and overconsolidation by using cybersecurity mesh architecture as a guide to optimize the mix of platforms and point solutions. Evaluate startup vendors to address unique threats or efficacy issues in platforms and align technology acquisition strategy with partners in procurement and IT.
- Focus on architecture that enhances portability of data between systems and invest in operational efficiency to deliver better outcomes from existing tools.
- Evaluate your organization’s capacity to build and maintain integrations between point security solutions, and err on the side of more consolidation of tools when preintegrated components reduce the burden on staff.
- Implement core security controls and secure configurations fully to prevent the most common threats. Use threat modeling to determine when advanced features, point solutions and additional controls are required.

Further Reading:

Innovation Insight for Security Platforms

Simplify Cybersecurity With a Platform Consolidation Framework

The Future of Security Architecture: Cybersecurity Mesh Architecture (CSMA)

Addressing Cybersecurity Burnout to Ensure Cybersecurity Program Effectiveness

Analysis by Richard Addiscott, Deepti Gopal, Christine Lee

SPA:

- By 2027, CISOs investing in cybersecurity-specific personal resilience programming will see 50% less burnout-related attrition than peers who don't.

Description:

SRM leader and security team burnout is a key concern for an industry already impacted by a systemic skills shortage. Forward-looking SRM leaders are increasingly speaking up about the importance of mental health and wellness.[21, 22, 23, 24] The most effective SRM leaders are not only prioritizing their own stress management; they are also investing in teamwide well-being initiatives, which demonstrably improve personal resilience. Gartner's conversations with CISOs indicate they are also deepening their partnership with HR to optimize team workload management, such as by monitoring excess work, rotating staff between active incident response and support roles, and encouraging employees to take PTO after stressful periods.

Why Trending:

There are clear signs the cybersecurity community is experiencing a mental health crisis. Sixty-two percent of cybersecurity leaders in Gartner's Peer Community Survey state they have experienced burnout.[25] A separate study reports that "90% of CISOs are concerned about stress, fatigue, or burnout affecting their team's well-being."[26]

This pervasive stress stems from the relentless demands associated with securing highly complex organizations in constantly changing threat, regulatory and business environments with limited authority, executive support and resources.

Evidence that unmanaged stress has adverse effects on enterprise security posture and program sustainability is also emerging:

- "65% of CISOs say their ability to protect their organization is compromised due to workload and stress."[27]
- 83% of IT security professionals acknowledge they, or someone in their department, "made an error due to burnout that resulted in a security breach."[28]
- 46% of respondents state that high stress is the reason why cybersecurity professionals left their roles in 2024.[29]

Implications:

Challenges:

- Other executive leaders are likely unaware of cybersecurity-specific burnout. As such, they may be reluctant to commit resources to fixing root causes around cybersecurity skills shortages or lack of business support for cybersecurity.
- Lack of cybersecurity-specific resilience training may be a deterrent to cybersecurity leaders and teams who feel generic well-being and mental health offerings are insufficient to address the unique stressors of working in cybersecurity. Cyber-focused nonprofits, such as Cybermindz and Mind Over Cyber, dedicated to supporting the mental well-being of cybersecurity professionals are emerging, and Gartner anticipates that for-profit vendors will follow suit.

Opportunities:

Analysis of benchmarking data from Gartner's 2024 CISO Effectiveness Diagnostic shows that improving competency in three stress- or wellness-specific activities can increase leadership effectiveness by up to 25%:

- Keeping a clear distinction between work and nonwork
- Treating job stressors as directly within one's direct control
- Effectively managing stress at work

Cybersecurity leaders who embrace burnout prevention and remediation head on have the opportunity to:

- Boost their team's and program's effectiveness
- Improve workforce resilience
- Better balance investments between people, process optimization and technology

Actions:

- Acknowledge and socialize the reality of cybersecurity burnout and its potential organizational impact. Ensure executive leaders understand the connection between burnout and increased cybersecurity risk. Remain vigilant and continuously monitor for signals of individual and team burnout such as increasing levels of cynicism and/or loss of interest in work. Be prepared to act and pull in HR when these indicators manifest themselves.

- Evaluate current and foreseeable workloads. Determine what can be either delegated, shared and/or deprioritized. This is especially important for small teams. Distributing a mix of meaningful and administrative work across the team helps allocate workload and associated pressures evenly and provides opportunities for skills development for emerging leaders. Over time, scale cybersecurity across the organization by investing in collaborative risk management and driving employee cyber judgment.

- Establish a security team wellness initiative. To ensure individual and team effectiveness, as well as program sustainability, SRM leaders should execute an ongoing initiative promoting and safeguarding the mental health of their teams by:

  - Partnering with HR on workforce management and process improvements

  - Prioritizing human connections over digital connections

  - Conducting meditation and mindfulness sessions

  - Embedding wellness activities directly into employee work practices where practicable to make it easy for staff to access the support they need

  - Promoting the use of the organization’s wellness programs where they exist

Further Reading:

Augmented Cybersecurity: Act Now to Thrive Amid Chaos and Complexity

CISO Effectiveness: Start Practicing 3 Burnout-Avoiding Behaviors Now

Predicts 2024: Augmented Cybersecurity Leadership Is Needed to Navigate Turbulent Times

Dual Focus Delivering Dual Outcomes

Tactical AI

Analysis by Jeremy D'Hoinne, Andrew Walls, Avivah Litan

Description:

SRM leaders are facing mixed results with their implementations of the latest AI features and products. Initial disappointment due to inflated expectations based on GenAI hype led SRM leaders to reprioritize their initiatives and focus on narrower use cases with direct measurable impacts. These more tactical implementations of AI align AI practices and tools with existing metrics, fitting them into existing initiatives, and enhancing visibility of the real value of AI investments. They also give SRM leaders a sustainable approach to preparing for the massive hype around AI agents that Gartner expects to peak in 2025.

As they update their 12-month and three-year strategies, SRM leaders have moved past the fascination state of 2023, conducted their first GenAI pilots and gathered feedback from their teams and key stakeholders. SRM leaders have clear responsibilities to:

1. Secure third-party AI consumption

2. Protect enterprise AI applications

3. Improve cybersecurity with AI

By focusing on more tactical, demonstrably beneficial improvements, SRM leaders minimize the risks for their cybersecurity programs and can more easily demonstrate progress.

Why Trending:

SRM leaders and their teams are actively evaluating, piloting or implementing GenAI. Less than 10% of security leaders say they have no plan to adopt GenAI for cybersecurity use cases, according to a recent Gartner survey on data security and GenAI. [30]

SRM leaders feel compelled to at least experiment with the newest AI technologies, but want to think longer term. The most frequent question Gartner hears from SRM leaders on GenAI is a variation of "How do I integrate it into my existing cybersecurity program?"

Fast, radical adoption — as suggested by aggressive claims from providers — is tempting but imprudent for a variety of reasons:

- Most of the recent AI announcements are based on GenAI, which is still immature and evolving. The majority of the disruptive use cases are still experimental.
- Larger-scale implementations require upskilling in the security teams, and could face change resistance.
- The absence of credible benchmarks based on sufficiently long pilots and large-scale deployment turns everyone into an early adopter.

When asked about outcomes of GenAI in cybersecurity, only 12% of CISOs answered that they have already achieved measurable results [TA2]. [31]

Although some organizations might report transformational results, most security teams mention specific tasks when asked about successful recent AI progress. Frequent examples include document or report generation or translating human questions into tool queries. But, as they gain experience, SRM leaders also report frequent inaccuracies. The general sentiment is that newer GenAI tools require human supervision and reviews of outputs.

When it comes to securing AI initiatives and third-party AI application consumption, most security teams lack enough AI knowledge or mature practices and technologies to influence secure design or implementation of AI or even AI controls. For the foreseeable future, security teams must focus on tactical — yet important — actions they are familiar with: AI discovery and inventory (including third-party uses), infrastructure security and runtime monitoring.

Implications:

- Tactical and incremental additions of AI in the SRM leader’s strategy help balance their roadmap and better manage expectations while preparing teams to better evaluate the future waves of technological improvements, with AI agents being next in line.
- SRM leaders need to remain open to experiments, balancing the more tactical implementations with proofs of concepts for more ambitious objectives with strategic implications.
- The more tactical approach also helps SRM leaders secure AI applications by focusing on technical reality rather than force fitting a strategy onto a dynamic technology.

Actions:

- Focus cybersecurity AI usage on technologies that integrate with existing workflows rather than aiming to replace those workflows. Measure outcomes with existing cybersecurity metrics, not ad hoc new ones. Ensure broad collaboration with key IT, HR, legal and business leaders to implement longer-term data security, governance and AI approval workflows. Leverage existing governance structures and policies as much as possible.
- Treat AI applications as normal applications first, starting with discovery and runtime enforcements. Then apply existing application security best practices to AI applications, such as API security, credential protections and extending infrastructure security and security operations to AI applications.
- Extend your AI security program by integrating AI trust, risk and security management (AI TRiSM) components progressively.

Further Reading:

How to Evaluate Cybersecurity AI Assistants

Use TRiSM to Manage AI Governance, Trust, Risk and Security

Use ODMs to Guide Defensible Cybersecurity Investment in GenAI Risk Reduction

AI Technology Sandwich: A Conceptual Framework for Executing AI

Extending the Value of Security Behavior and Culture Programs

Analysis by Alex Michaels, Richard Addiscott, Victoria Cason

SPA:

- By 2026, enterprises combining GenAI with an integrated platforms-based architecture in security behavior and culture programs will experience 40% fewer employee-driven cybersecurity incidents.

Description:

Security behavior and culture programs (SBCPs) have reached a point of inflection for most organizations. Effective SRM leaders recognize the value these programs bring to improve the posture of their cybersecurity initiatives. As a result, cultural and behavior-focused activities have become a prominent approach to address cyber-risk comprehension and ownership at the human level, reflecting a strategic shift toward embedding security into the organizational culture.

Why Trending:

This trend is gaining traction due to the increasing recognition that human behavior, both good and bad, is a critical component of cybersecurity. According to the 2024 Verizon Data Breach Investigations Report, 68% of cybersecurity breaches are primarily caused by human action. [32] This statistic underscores the importance of fostering a security-conscious culture within organizations. By investing in SBCPs, SRM leaders aim to leverage nonconventional tactics, like behavioral psychology, nudge theory and user experience, to improve their ability to influence change across the organization.

One of the largest drivers of this change is GenAI. GenAI is also making it far easier for workers from across the organization to undertake technology work. This two-edged sword can enhance SBCP’s by enabling hyperpersonalization of content, but also introduces new threat vectors for realizing operational cybersecurity risks.

Moreover, some organizations are beginning to move past traditional security awareness programs to integrate existing practices into an evolved and formalized SBCP. These organizations are leading the way and now are being asked: what’s next beyond phishing? These programs are expanding to cover a broader range of security behaviors, such as secure coding practices, system misconfiguration and unauthorized software install. This evolution is driven by the understanding that a comprehensive approach to security behavior can address a wider array of threats and vulnerabilities.

The increasing regulatory landscape also plays a significant role in this trend. Global regulations such as the General Data Protection Regulation (GDPR), Digital Operational Resilience Act (DORA), Network and Information Security Directive 2 (NIS2) mandate stringent data and privacy protection measures, including employee training and awareness programs. Organizations are recognizing that investing in SBCPs not only helps them comply with these regulations but also builds a resilient security culture that can adapt to future regulatory changes.

Implications:

- **Enhanced security posture:** By embedding increased security consciousness into the cultural fabric of an organization, employees become more vigilant and active in identifying and mitigating potential threats.
- **Reduced incident response time:** Employees educated in cybersecurity best practices can identify and report incidents more quickly, reducing the time to respond and contain breaches effectively.

Challenges:

- **Lack of time and staff:** Allocating sufficient budget and resources to these programs can be challenging, especially for smaller organizations. You cannot simply purchase a tool to secure people and drive culture change.
- **Measuring effectiveness:** Quantifying the impact of cultural and behavioral programs on security outcomes can be difficult. True impact can only be effectively measured with a mature incident management process, which can help you identify data-driven incident patterns stemming from employee actions.

Opportunities:

- **Cross-functional collaboration:** These programs can foster collaboration between IT, marketing, communications and other functions, leading to a more cohesive security strategy.
- **Employee engagement**: Well-designed programs can increase overall employee engagement and satisfaction because employees feel more involved in the organization's security efforts. This gives them more agency in how the controls they need to work with are designed for their specific context, and, in turn, helps with reducing control friction and increasing control adoption.

Actions:

- Build an SBCP strategic plan that intersects with the organization's strategic plan and shows executive leadership why an SBCP is needed. Ensure SBCP outcome-driven metrics (ODMs) are embedded into executive cybersecurity and board reporting.

- Focus SBCP efforts on the riskiest employee behaviors by regularly reviewing a defensible sample of past cybersecurity incidents to determine the volume and type of cybersecurity incidents associated with unsecured employee behavior.
- Refine SBCP policy statements that create clear expectations for the workforce throughout the organization.

Further Reading:

Tool: Security Behavior and Culture Program Dashboard

5 Communications Tactics to Get People to Take Cyber Risk More Seriously

The Impact of Generative AI on Security Behavior and Culture Programs

Increased Emphasis on Response and Recovery Addresses GenAI Third-Party Risks

Analysis by Manuel Acosta, Chiara Girardi, Oscar Isaka, Craig Porter

Description:

The increased reliance on third parties using GenAI tools and features reinforces the importance of strengthening the organization's approach to response and recovery. Progressive SRM leaders prioritize establishing policies for pausing and exiting third-party relationships to build resilience against unexpected events. Simultaneously, they collaborate with business sponsors to co-manage risks emanating from third parties using GenAI and, consequently, inform control implementation.

Why Trending:

Organizations today heavily rely on vendors to expand their GenAI capabilities. Half of the respondents to the Gartner Generative AI 2024 Planning Survey report are buying GenAI capabilities from a new third party, while 26% are waiting for an existing vendor to offer GenAI tools. [33] Often, GenAI capabilities are incorporated into existing third parties' services suddenly or without notice.

As reliance on third parties using GenAI grows, savvy SRM leaders are investing just as much in response and recovery as in preventative controls. The 2024 Gartner Data Security in the Age of GenAI Advancements [34] survey reveals that third-party risk, response and recovery are areas where SRM leaders have the greatest influence on GenAI-related decisions. 89% of respondents report being able to exert influence over how the organization responds to security incidents involving GenAI tools, articulating policies to stop or pause a GenAI tool/feature (85%), and establishing plans for testing and validating third-party GenAI tools (81%).

Implications:

- GenAI third-party risk must inform the data security strategy. Third parties using GenAI introduce data security risks (e.g.; privacy, integrity, poisoning and data leaks). To effectively manage these risks, SRM leaders must partner with data governance teams to address data ownership, classification and quality considerations for the data leveraged by third parties using GenAI.
- Increased reliance on third parties using GenAI expands business continuity risk. The Gartner 2023 Evolution of the Cybersecurity Leader [35] survey found that the number of SRM leaders expected to own and lead business continuity management efforts is rising. 66% of Cybersecurity leaders are now responsible for BCM, a 12% increase from the previous year. Within BCM, SRM leaders prioritize conducting a business impact analysis (83%), crisis management (80%) and activation procedures (72%)
- GenAI holds potential to increase precontractual due diligence efficiency. Progressive SRM leaders know traditional due diligence alone is a resource-intensive activity. They are looking for ways to leverage GenAI to identify risk faster and shift resources to resilience-driven activities (e.g., identification of controls, incident response and business continuity planning). To quickly identify risk factors, SRM leaders have started using internal GenAI tools to scan vendors' artifacts against a set of nonnegotiable controls mapped to security frameworks (e.g., ISO27001, NIST AI RMF).

Actions:

- Partner with business leaders for early visibility into third-party GenAI decisions. Prioritize engagements with risk functions involved in third-party cybersecurity risk management (TPCRM; e.g., ERM, compliance, procurement). When SRM leaders are included from the planning stage in adopting GenAI features and third-party GenAI tools, they are 1.35 times more likely to prevent attempts to exfiltrate data and block external unauthorized access. [33]

- Make it easy for the business to co-manage the risk presented by third parties using GenAI. Set expectations for co-managing risk by spelling out how responsibilities are divided between the business and cybersecurity. Further, work with business owners to assess the potential impact of third parties using GenAI. Business sponsors know what each supplier does, what access rights they have and what data they use. By tapping into the business owners' insights, cybersecurity is better-positioned to prioritize high-risk GenAI third parties.

- Define GenAI-specific contingency plans in conjunction with internal functions (e.g.; D&A, procurement, vendor management, supply chain, BCM) to prepare for GenAI third-party disruptions. Develop incident response playbooks, conduct tabletop exercises and establish policies for exiting or pausing relationships with third parties using GenAI.

Further Reading:

CISOs: 3 Steps to Business Accountability for Third-Party Cybersecurity Risks

Take a Life Cycle Approach to Managing Third-Party Cyber Risk

Use ODMs to Guide Defensible Cybersecurity Investment in GenAI Risk Reduction

Evidence

[1] How Many Cybersecurity Products Are There?, The Security Industry.

[2] **Gartner Generative AI 2024 Planning Survey.** This survey was conducted to examine generative AI's use-case implementation and impact by business function. The survey was conducted from September through November 2023. In total, 822 business executives who lead corporate functions outside IT and who indicated their organizations would begin or continue to implement generative AI across the next 12 months qualified and participated. The research was collected via online surveys in English. The sample was equally split across the following eight corporate functions: finance; HR; marketing; sales; customer service; supply chain; procurement; and legal, risk and compliance. The sample mix by location was North America (n = 536), Europe (n = 176) and Asia/Pacific (n = 110). The sample mix by size was $50 million to less than $500 million (n = 119), $500 million to less than $1 billion (n = 129), $1 billion to less than $10 billion (n = 374) and $10 billion or more (n = 200). Disclaimer: The results of this survey do not represent global findings or the market as a whole, but reflect the sentiments of the respondents and companies surveyed.

[3] **2024 Gartner General Manager Survey.** This survey sought to understand how economic turbulence poses challenges to general managers, how confident they are in their ability to achieve their plans and the measures planned to tackle the uncertainty. The survey also sought general managers' outlook on customer profiles and the competitive environment. Results will be used to help technology and service providers (T&SPs) understand how their peers see the future and how they are organizing product organizations for success. The survey was conducted online from August through December 2023 among 200 general managers from North America (136; the U.S. and Canada) and Western Europe (64; the U.K., Germany and France). Selected general managers were from organizations with $250 million or more in annual revenue from T&SP industries with the majority (139) from organizations with $1 billion or more in annual revenue. General managers were responsible for overall portfolio management or distribution of revenue targets for the portfolio or representation of the portfolio in business reviews with executive leadership. Disclaimer: The results of this survey do not represent global findings or the market as a whole, but reflect the sentiments of the respondents and companies surveyed.

[4] **2022 Gartner Shifting Cyber-security Operating Model Survey.** This study was conducted to determine the impact of the changing technology governance environment on the security operating model at the macro level. The survey was conducted online from October through November 2022 among 462 respondents from North America (n = 148), Europe (n = 216), Latin America (n = 33) and Asia/Pacific (n = 61). Respondents were required to be cybersecurity or information security leaders. The study was developed collaboratively by Gartner security analysts and Gartner's Primary Research Team. Disclaimer: Results of this survey do not represent global findings or the market as a whole, but reflect the sentiments of the respondents and companies surveyed.

[5] **2024 Gartner IAM Leadership Survey.** This 15-minute survey assesses identity and access management (IAM) leaders' approach to building IAM strategy, aligning with business and cybersecurity goals, and collaborating with cybersecurity functions. The combined data represents responses from 335 IAM leaders globally across industries, geographies and revenue bands, and was collected from August 2024 through October 2024. Gartner created measures to determine an IAM leader's ability to deliver against key outcomes. Gartner then used regression analysis to identify approaches that are less prevalent among IAM leaders but have the strongest impact on their ability to deliver key outcomes. Disclaimer: The results of this study do not represent global findings or the market as a whole but reflect the sentiments of the respondents and companies surveyed.

[6] How Poorly Secured Service Accounts Lead to Breaches, Reliaquest.

[7] 2024 Trends in Securing Digital Identities, Identity Defined Security Alliance.

[8] Research: The Impact of Machine Identities on Cloud-Native Security in 2023. Venafi.

[9] Social media analytics methodology: Gartner conducts social listening analysis leveraging third-party data tools to complement or supplement the other fact bases presented in this document. Due to its qualitative and organic nature, the results should not be used separately from the rest of this research. No conclusions should be drawn from this data alone. Social Media Data in reference is from 1 June 2023 through 30 June 2024 in all geographies (except China) and recognized languages.

[10] **2024 Gartner Board of Directors Survey on Driving Business Success in an Uncertain World.** This survey was conducted to understand the new approaches adopted by nonexecutive boards of directors (BoDs) to drive growth in a rapidly changing business environment. The survey also sought to understand the BoDs' focus on investments in digital acceleration; sustainability; and diversity, equity and inclusion. The survey was conducted online from June through August 2023 among 285 respondents from North America, Latin America, Europe and Asia/Pacific. Respondents came from organizations with $50 million or more in annual revenue in industries except governments, nonprofits, charities and nongovernmental organizations (NGOs). Respondents were required to be nonexecutive members of corporate boards of directors. If respondents served on multiple boards, they answered questions about the largest company, defined by its annual revenue, for which they are a board member. Disclaimer: The results of this survey do not represent global findings or the market as a whole, but reflect the sentiments of the respondents and companies surveyed.

[11] **2023 Gartner Evolution of the Cybersecurity Leader and Their Function Survey.** This survey was conducted to understand the evolution of the role and responsibilities of cybersecurity leaders or CISOs. The survey was conducted online from 31 July through 13 September 2023 among 318 respondents (n = 211 from a vendor panel and n = 107 from a list of conferences). The geographical representation came from North America (n = 112 in the U.S. and Canada), Latin America (n = 42 in Brazil, Argentina, Honduras, Mexico, Chile and Ecuador), Asia/Pacific (n = 62 in India, Australia, Singapore, Taiwan, Japan, Thailand, China, South Korea, Malaysia and Tajikistan) and EMEA (n = 102 in Germany, France, U.K., Portugal, Netherlands, Norway, Switzerland, Italy, Denmark, Spain, Belgium, Sweden, Austria, Israel, U.A.E., Kuwait, Serbia, Saudi Arabia and South Africa). Respondents' organizations had $50 million or more in 2022 enterprisewide annual revenue and 100 or more employees. Respondents were required to be team members and have some responsibility for their organization's cybersecurity/risk function and were required to be up to two layers away from their CISO/head of cybersecurity. Disclaimer: The results of this survey do not represent global findings or the market as a whole, but reflect the sentiments of the respondents and companies surveyed.

[12] Cyber Database, CyberDB.

[13] Gartner Forecasts Global Security and Risk Management Spending to Grow 14% in 2024

[14] Palo Alto Networks (PANW) Q4 2024 Earnings Call Transcript, The Motley Fool.

[15] Microsoft Security Reaches Another Milestone — Comprehensive, Customer-Centric Solutions Drive Results, Microsoft

[16] White House Report Dishes Deets on All 11 Major Government Breaches From 2023, The Regiser.

[17] **2023 Gartner Technology Adoption Roadmap for Large Enterprises Survey.** This survey harnesses the collective wisdom of IT leaders to understand deployment plans, adoption timelines, value and risks posed by 205 technologies across infrastructure and operations; data and analytics; software engineering; cybersecurity; and strategic portfolio management. The survey was conducted through an online panel from August through October 2023 among 598 respondents from North America, EMEA and Asia/Pacific across industries and enterprises with annual revenue of more than $1 billion. Qualified respondents were CxOs, senior IT leaders, their peers and their direct reports. The results will allow leaders in infrastructure and operations, data and analytics, software engineering, cybersecurity, and strategic portfolio management to cut through vendor hype to determine which technologies to invest in, and when, to remain competitive among peers.

[18] Minimize Disruption From the CrowdStrike Windows Outage

[19] **2024 Gartner CrowdStrike Survey.** This survey was conducted online from 31 July through 12 August 2024 to explore how organizations create effective business continuity plans for addressing disruptive events such as the 2024 CrowdStrike incident. A total of 110 security risk management leaders and CIOs participated. All participants were members of Gartner's Research Circle, a Gartner-managed panel. Participants were from North America (n = 48), EMEA (n = 42), Asia/Pacific (n = 11) and Latin America (n = 9). Disclaimer: The results of this survey do not represent global findings or the market as a whole, but reflect the sentiments of the respondents and companies surveyed.

[20] Quick Answer: How to Respond to the Cyber Safety Review Board's Criticism of Microsoft?

[21] The Scourge of Ransomware: Victim Insights on Harms to Individuals, Organisations and Society, Royal United Services Institute for Defense and Security Studies.

[22] Don Gibson: How Security Incidents Affect the Individual, Trident Talks (YouTube).

[23] Let's Talk About Stress and Burnout in Cyber, Joe Lewis (LinkedIn).

[24] I Believe, I Belong, I Matter — Avoiding CISO Burnout, Malcolm Harkins.

[25] Cybersecurity Leaders are Burned Out. Here's Why

[26] Building a Firewall Against Cybersecurity Burnout, Hack The Box.

[27] Implications for Stress on CISOs, Cynet.

[28] Devo Cybersecurity Burnout Survey: Quick Read Report, Conducted by Wakefield Research

[29] State of Cybersecurity 2024: Global Update on Workforce Efforts, Resources and Cyberoperations, ISACA.

[30] **2024 Gartner Data Security in the Age of AI Advancements Survey.** This survey sought to understand the practices that cybersecurity leaders should follow to better manage risks associated with data. The survey was conducted from June through August 2024. In total, 318 senior executives participated, who were involved in data security across organizations of different industries, geographies and sizes. This research was further substantiated and informed by in-depth practitioner interviews with more than 40 chief information security officers (CISOs) to understand cybersecurity goals and challenges associated with data security, given the rapid rise in adoption of GenAI tools and technologies. Gartner used statistical analysis to measure and identify the most impactful data security practices for improving key cybersecurity outcomes. Disclaimer: The results of this survey do not represent global findings or the market as a whole, but reflect the sentiments of the respondents and companies surveyed.

[31] 3 Themes From CISOs on Their Outlook for AI, Evanta.

[32] 2024 Data Breach Investigations Report, Verizon Business.

[33] **Gartner Generative AI 2024 Planning Survey.** This survey was conducted to examine generative AI's use-case implementation and impact by business function. The survey was conducted from September through November 2023. In total, 822 business executives who lead corporate functions outside IT and who indicated they will begin or continue to implement generative AI across the next 12 months qualified and participated. The research was collected via online surveys in English. The sample was equally split across the following eight corporate functions: finance; HR; marketing; sales; customer service; supply chain; procurement; and legal, risk and compliance. The sample mix by location was North America (n = 536), Europe (n = 176) and Asia/Pacific (n = 110). The sample mix by size was $50 million to less than $500 million (n = 119), $500 million to less than $1 billion (n = 129), $1 billion to less than $10 billion (n = 374) and $10 billion or more (n = 200). Disclaimer: The results of this survey do not represent global findings or the market as a whole, but reflect the sentiments of the respondents and companies surveyed.

[34] **2024 Gartner Data Security in the Age of AI Advancements Survey.** This survey sought to understand the practices that cybersecurity leaders should follow to better manage risks associated with data. The survey was conducted from June through August 2024. In total, 318 senior executives participated, who were involved in data security across organizations of different industries, geographies and sizes. This research was further substantiated and informed by in-depth practitioner interviews with over 40 chief information security officers (CISOs) to understand cybersecurity goals and challenges associated with data security, given the rapid rise in adoption of GenAI tools and technologies. Gartner used statistical analysis to measure and identify the most impactful data security practices for improving key cybersecurity outcomes. Disclaimer: The results of this survey do not represent global findings or the market as a whole, but reflect the sentiments of the respondents and companies surveyed.

[35] **2023 Gartner Evolution of the Cybersecurity Leader and their Function Survey.** This survey was conducted to understand the evolution of the role and responsibilities of cybersecurity leaders or CISOs. The survey was conducted online from 31 July through 13 September 2023 among 318 respondents (n = 211 from a vendor panel and n = 107 from a list of conferences). The geographical representation came from North America (n = 112 in the U.S. and Canada), Latin America (n = 42 in Brazil, Argentina, Honduras, Mexico, Chile and Ecuador), Asia/Pacific (n = 62 in India, Australia, Singapore, Taiwan, Japan, Thailand, China, South Korea, Malaysia and Tajikistan) and EMEA (n = 102 in Germany, France, U.K., Portugal, Netherlands, Norway, Switzerland, Italy, Denmark, Spain, Belgium, Sweden, Austria, Israel, U.A.E., Kuwait, Serbia, Saudi Arabia and South Africa). Respondents' organizations had $50 million or more in 2022 enterprisewide annual revenue, and 100 or more employees. Respondents were required to be team members and have some responsibility for their organization's cybersecurity/risk function and were required to be up to two layers away from their CISO/head of cybersecurity. Disclaimer: The results of this survey do not represent global findings or the market as a whole, but reflect the sentiments of the respondents and companies surveyed.

Note 1

For a secure AI-enabled environment, machine identities should be applied to anything (not human) that is part of a secure, authenticated interaction between and including systems. This includes AI agents, APIs, bots (helping with automation) and other software programs — all of which could be on-premises or cloud-delivered. The trend related to machine identities being referred to here acts as an enabler for the business seeking to leverage AI as part of transformation efforts.

Recommended by the Authors

Some documents may not be available as part of your current Gartner subscription.

2024 Strategic Roadmap for World-Class Security of Unstructured Data

Innovation Insight: Data Security Posture Management

Market Guide for Data Masking and Synthetic Data

The Cyber-Risk Management Cookbook for Security Leaders

2025 Strategic Roadmap for Cyber GRC

CISO Effectiveness: Security Operating Models Are Evolving

Prioritize IAM Hygiene for Robust Identity-First Security

CISO Foundations: 5 Questions CISOs Should Ask About IAM

Managing Machine Identities, Secrets, Keys and Certificates

Innovation Insight: Cyberstorage Mitigates the Impact of Cyberattacks

CISO Edge: Use Cyber Deterrence to Stop Attacks Before They Start

Succeed as an SRM Leader by Infusing Resilience Into Your Program

The Future of Security Architecture: Cybersecurity Mesh Architecture (CSMA)

Simplify Cybersecurity With a Platform Consolidation Framework

Innovation Insight for Security Platforms

Predicts 2024: Augmented Cybersecurity Leadership Is Needed to Navigate Turbulent Times

CISO Effectiveness: Start Practicing 3 Burnout-Avoiding Behaviors Now

Augmented Cybersecurity: Act Now to Thrive Amid Chaos and Complexity

Use ODMs to Guide Defensible Cybersecurity Investment in GenAI Risk Reduction

Use TRiSM to Manage AI Governance, Trust, Risk and Security

How to Evaluate Cybersecurity AI Assistants

Take a Life Cycle Approach to Managing Third-Party Cyber Risk

Table 1: Top Trends in Cybersecurity for 2025

Enabling transformation	Embedding resilience
GenAI driving data security programs	Transitioning to cyber resilience
Collaborative cyber-risk management	Cybersecurity technology optimization
Managing machine identities	CISO and security team well-being
Tactical AI	
Extending the value of security behavior and culture programs	
Managing third-party cybersecurity risks	

Source: Gartner