

Top Trends in Cybersecurity for 2024

2 January 2024 - ID G00802944 - 49 min read

By Richard Addiscott, Jeremy D'Hoinne, [and 7 more](#)

Security and risk management leaders face disruptions on multiple fronts: technological, organizational and human. Preparation and pragmatic execution are vital to address these disruptions and deliver an effective cybersecurity program.

Overview

Opportunities

- Security and risk management (SRM) leaders can improve the security function's reputation and performance by using generative artificial intelligence (GenAI) in proactive collaboration with business stakeholders. This will help lay the foundations for ethical, safe and secure use of this disruptive technology.
- Investment in effective risk management of third-party services and software, enhanced security for the identity fabric, and continuous monitoring of hybrid digital environments can harden an organization's attack surface and strengthen its resilience.
- Aligning security governance efforts with the use of business-aligned cybersecurity reporting can improve the security function's performance and reputation as a trusted partner and key enabler of an organization's strategic objectives.
- Increased focus on the human elements of security programs continues to show significant promise in the mission to minimize the impact of employees' unsecure behavior. It can also provide greater assurance when experimenting with emerging technologies in democratized digital environments.

Recommendations

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

- Improve organizational resilience by implementing continuous, pragmatic, business-aligned risk management efforts across your organization's digital and third-party ecosystems. Extend the role that identity and access management (IAM) plays in reducing cybersecurity risk.
- Support decentralized technology projects by coordinating cybersecurity decision making. Measure the security function's performance using business-aligned, outcome-driven metrics (ODMs) aligned with protection-level agreements (PLAs).
- Enable resilient operations in the face of localization rules by embracing a composable application architecture that incorporates a data-decoupling strategy.
- Take a strategic, human-centric approach to improving the security function's performance by reskilling existing security talent, using GenAI to augment – not replace – human efforts, and implementing a contextually appropriate security behavior and culture program.

Strategic Planning Assumptions

- By 2026, organizations prioritizing their security investments based on a continuous threat exposure management program will realize a two-thirds reduction in breaches.
- By 2025, 10% of global businesses will operate more than one discrete business unit bound to and by a specific sovereign data strategy, doubling or more its business costs for the same business value.
- Through 2025, generative AI will cause a spike in the cybersecurity resources required to secure it, causing more than a 15% incremental spend on application and data security.
- By 2025, 40% of cybersecurity programs will deploy socio-behavioral principles (such as nudge techniques) to influence security culture across the organization, up from less than 5% in 2021.
- By 2027, 50% of large enterprise chief information security officers (CISOs) will have adopted human-centric security design practices to minimize cybersecurity-induced friction and maximize control adoption.
- Fifty percent of large enterprises will use agile learning as their primary upskilling/reskilling method by 2026.

What You Need to Know

Generative AI's (GenAI's) appearance as a mainstream capability in late 2022 caused one of the largest disruptions in digital and business sectors in decades. It is a powerful force that SRM leaders cannot ignore.

However, while GenAI has been inescapable as a force to be reckoned with, there are other external forces outside the SRM leader's control that they must continue to contend with. They also face:

- The quest to bridge the divide between the supply and demand for security talent.
- Relentless growth in cloud adoption, which is expanding, and altering the composition of, digital ecosystems.
- Increasing regulatory obligations and government oversight of cybersecurity, privacy, and data localization across the public and private sectors.
- Continued decentralization of digital capabilities across enterprises.
- The eternal challenge of managing security exposures in a constantly evolving threat environment.

SRM leaders are responding to the combined impact of these forces by adopting a range of practices, technical capabilities, and structural reforms within their security programs with a view to improving organizational resilience and the cybersecurity function's performance.

Optimizing for Resilience

Improving organizational resilience has become a primary driver of security investments for several interconnected reasons: ¹

- Digital ecosystems continue to sprawl, due to increasing cloud adoption.
- Organizations are entrenching hybrid work arrangements.
- The threat environment continues to evolve as emerging capabilities also embolden attackers.

SRM leaders increasingly recognize the folly of trying to remediate the exploding number of vulnerabilities in their organizations' expanding digital environments. As such, momentum continues to build for programs that enable continuous threat exposure management (CTEM) and deliver more robust, security-enabling identity and access management (IAM) capabilities (both continuing trends from 2023).

Additionally, SRM leaders who have embraced resilience-focused third-party cybersecurity risk management approaches are reaping rewards in terms of risk reduction and the speed at which they can enable the launch of new digitization initiatives.

Multinational organizations using cloud services are adopting modular application and data architectures to help them comply with a global patchwork of privacy and data sovereignty requirements. This is seen as key to addressing the increase in data localization requirements and reducing the risk of business disruption.

Optimizing for Performance

GenAI is occupying significant amounts of the SRM leader’s headspace as another challenge to manage. But proactive SRM leaders also see an opportunity to harness GenAI’s capabilities to augment the security function at an operational level.

The need to use GenAI securely is further impacting security skills planning and development. It is also a key reason why security behavior and culture programs designed to minimize the impact of unsecure employee behavior are gaining traction.

Strengthened regulatory frameworks are making improved cybersecurity board reporting imperative, not just desirable. Consequently, outcome-driven metrics are increasingly being adopted to facilitate more effective cybersecurity risk and investment decision making.



As organizations continue to distribute and democratize digital decision making, the trend for reforming security operating models reform persists.

Figure 1 summarizes the main cybersecurity trends for 2024.

Figure 1: Top Cybersecurity Trends for 2024



Top Cybersecurity Trends for 2024

 Optimizing for Resilience	 Optimizing for Performance
<ul style="list-style-type: none"> • Continuous Threat Exposure Management • Extending IAM’s Cybersecurity Value • Third-Party Cybersecurity Risk Management • Privacy-Driven Application and Data Decoupling 	<ul style="list-style-type: none"> • Generative AI • Security Behavior and Culture Programs • Cybersecurity Outcome-Driven Metrics • Evolving Cybersecurity Operating Models • Cybersecurity Reskilling

Optimized Cybersecurity Programs

Source: Gartner
802944_C



Trend Profiles: Click links to jump to profiles

Optimizing for Resilience	Optimizing for Performance
Continuous Threat Exposure Management	Generative AI

Extending IAM's Cybersecurity Value	Security Behavior and Culture Programs
Third-Party Cybersecurity Risk Management	Cybersecurity Outcome-Driven Metrics
Privacy-Driven Application and Data Decoupling	Evolving Cybersecurity Operating Models
	Cybersecurity Reskilling

Continuous Threat Exposure Management Programs Gain Momentum

[Back to top](#)

Analysis by Pete Shoard, Angela Zhao, Jeremy D'Hoinne, Jonathan Nunez

Strategic Planning Assumption: By 2026, organizations prioritizing their security investments based on a continuous threat exposure management program will realize a two-thirds reduction in breaches.

Description:

Organizational attack surfaces have expanded enormously in recent years. This growth has been driven notably by accelerated adoption of SaaS, expanding digital supply chains, increased corporate presence on social media, custom application development, remote working, and internet-based customer interaction.

This increased attack surface has left organizations with potential blindspots, as well as huge numbers of potential exposures to address.

To cope, SRM leaders have introduced pilot processes that govern the volume and importance of threat exposures and the impact of dealing with them with continuous threat exposure management (CTEM) programs. They are now expanding these pilots beyond cybersecurity validation activities. The more mature organizations are starting to offer ranges of security optimizations to better mobilize business leaders, not just short-term remediations.

Why Trending:

Most organizations' efforts to manage threat exposure focus too single-mindedly on finding and correcting technology-based vulnerabilities. This focus is encouraged by SecOps compliance initiatives, but often does not consider significant shifts in the operational practices of modern

organizations, such as the move to cloud-driven applications and containers. It is essential that security teams enhance their current model, in which patching and securing physical and self-managed software-based systems is the primary objective, and move beyond it. SRM leaders have realized that existing practices are not broad enough, and at the same time, that staffing constraints limit the volume of work that can be completed.

Specific reasons for the growing adoption of CTEM programs include:

- **Lack of visibility into the huge volume of potential issues.** The sheer number of ways in which an organization may be exposed to threats is daunting; for example; at least one open-source vulnerability was found in 84% of codebases in 2023. ² New ways to scope and categorize potential issues are needed to provide direction and offer a chance to remediate issues of potentially high business impact.
- **Siloed acquisition of technology across the business.** With more technology available and accessible than ever before, its acquisition by multiple departments is hard to track and its ownership difficult to identify. SRM leaders require modern approaches to respond to, and to mobilize about, discovered exposures that put the organization at risk.
- **Increased dependency on third parties.** Ownership of cyber risk is not something a business can outsource alongside the other operational capabilities that it can acquire from a variety of business partners and vendors of software as a service (SaaS), infrastructure as a service (IaaS) and platform as a service (PaaS). The number of SaaS applications used by typical organizations has grown rapidly over the last decade – to approximately 130 SaaS, according to recent reporting. ³

Implications:

The focus of concern with exposure-related problems has shifted away from simply managing software vulnerabilities in commercial products. The realization of increased technology risk on such a large scale is overwhelming to security operations teams. Lack of alignment with business objectives will lead to poor decisions about which issues to tackle first, which will result in unquantifiable exposure gaps and the potential for security budget to be wasted remedying issues that will not matter. SRM leaders must use broader processes for threat exposure management, while balancing already-stretched operations teams, and creating effective and preagreed remediation mobilization channels to respond to discovered issues.

Actions:

- **Focus on relevant issues by aligning CTEM scope with business objectives.** SRM leaders must aim for visibility into exposures and attract the interest of other senior leaders by highlighting the issues with the most potential impact on an organization's critical operations. They should define a

narrower scope for CTEM, aligned with business objectives, using familiar language and explaining the impact on the business, not technology.

- **Reduce the number of prioritized issues through validation.** Introduce validation steps and supporting technologies such as breach and attack simulation (BAS) and automated penetration testing tools. Such tools reduce the burden imposed by the outputs of exposure assessment tools such as vulnerability assessment (VA) solutions by highlighting discovered issues that may result from genuine compromises using real-world techniques.
- **Carry out prework to engage responding business departments.** SRM leaders must expand communication channels between themselves and the heads of departments, asset owners and third parties with the aim of having clear paths to mobilize responses and remediations. Get traction with business departments and asset owners by clearly articulating and discussing the residual risk associated with postponement of remediation efforts. Offer short- and long-term options with a view to reducing or eliminating exposure.

Further Reading:

- [Top Strategic Technology Trends for 2024](#)
- [Implement a Continuous Threat Exposure Management \(CTEM\) Program](#)
- [2024 Strategic Roadmap for Managing Threat Exposure](#)

Evolving IAM to Support Its Increasing Role in Improving Cybersecurity Outcomes

[Back to top](#)

Analysis by Felix Gaehtgens, Paul Rabinovich

Description:

An identity-first approach to security shifts the focus from network security and other traditional controls to IAM. It makes IAM a key contributor to organizations' cybersecurity outcomes and therefore to business outcomes. Organizations adopting this approach have to pay closer attention to fundamental IAM hygiene and the hardening of IAM systems to improve resilience. This includes closing long-standing gaps in prevention capabilities by, for example, expanding control over cloud entitlements and machine identities, and introducing new advanced capabilities for identity threat detection and response (ITDR). IAM architecture is evolving toward an identity fabric and taking on new functions to enable real-time identity controls in a composable manner.

Why Trending:

- IAM's role in cybersecurity has been increasing steadily. As of 2023, IAM is the second-most-popular topic of discussion by SRM leaders who use Gartner's client inquiry service.
- Attacks against identity infrastructure are common, and defenders are using strategies such as ITDR to counter them.
- IAM and data security are customer responsibilities in the cloud-shared responsibility model for every type of service, from IaaS to SaaS.
- Almost two-thirds of the respondents to a Gartner survey expect their organization to increase its investment in IAM capabilities, including fraud detection, authentication, customer identity, workforce identity governance and administration, and privilege access management, over the next 12 months. ⁴
- Identity-first security is becoming a key control surface for security (see [Identity-First Security Maximizes Cybersecurity Effectiveness](#)).
- Conversations with Gartner clients indicate that they increasingly use outcome-driven metrics (ODMs) for IAM to encourage better security (see [Use Outcome-Driven Metrics to Drive Value for Identity and Access Management](#)). These metrics focus on enhancing resilience and security by affecting identity-specific variables, such as the accuracy of identity data, and bringing organizations closer to the principle of least privilege.

Based on these points, Gartner sees an increased role for IAM in organizations' security programs. Organizations' IAM practices therefore need to evolve.

Implications:

- Organizations must redouble their efforts to implement better identity hygiene. This is critical, because poor identity hygiene undermines many of the potential gains of ITDR. Misset permissions provide entry points for bad actors, create opportunities for lateral movement, and can exacerbate the collateral damage caused by simple mistakes. Given the vast number of entitlements, accounts and even local account repositories, implementing hygiene holistically is a major undertaking. ODMs can help define directional guidance for implementing better hygiene, but automation is also required.
- ITDR requires additional effort and skills. It works effectively only with a focus on hygiene. Organizations that use other security detection and response processes, and perhaps even have their own security operations center (SOC), can profit from ITDR, but this requires IAM training for SOC teams.
- IAM infrastructure must change to deepen its support for security functions. Much of the traditional IAM infrastructure in use today is overly complex and has significant gaps. IAM

technical debt, a technical accumulation of suboptimal or inefficient IAM technology decisions, is a widespread problem.

- IAM infrastructure must evolve into an identity fabric (see [Definition: Identity Fabric](#)) architected to enable identity-first security. It must use, and broker, context to provide and support adaptive, continuous, risk-aware and resilient access controls in a consistent manner for any applicable human or machine.

Actions:

- Redouble efforts to implement proper identity hygiene. Define this as a priority for the security program and use ODMs to provide directional guidance and set the bar for improvement.
- Expand ITDR as a practice by training security operations staff in IAM. Implement security posture assessments and threat detection and response capabilities for key enterprise identity systems such as Microsoft Active Directory and cloud-delivered access management services.
- Refactor identity infrastructure to support identity-first security principles by evolving toward an identity fabric. Start by improving integration between IAM tools by using a composable tool strategy.

Further Reading:

- [Enhance Your Cyberattack Preparedness With Identity Threat Detection and Response](#)
- [Identity-First Security Maximizes Cybersecurity Effectiveness](#)
- [Use Outcome-Driven Metrics to Drive Value for Identity and Access Management](#)

Resilience-Driven, Resource-Efficient Third-Party Cybersecurity Risk Management

[Back to top](#)

Analysis by Chiara Girardi, Rahul Balakrishnan, Luke Ellery, Christopher Mixer

Description:

The inevitability of third parties experiencing cybersecurity incidents is pressuring SRM leaders to focus more on resilience-oriented investments and move away from front-loaded due-diligence activities. Progressive SRM leaders are prioritizing resilience-driven activities such as implementing compensating controls and strengthening incident response planning. In parallel, they are providing targeted support for business partners to inform third-party contracting and influence control decisions.

Why Trending:

SRM leaders have increasingly been pouring resources into precontractual due-diligence activities. Almost two-thirds (65%) of those who responded to the 2023 Gartner Reimagine Third-Party Cybersecurity Risk Survey reported increasing budgets, and 76% spend more time on third-party cybersecurity risk management initiatives, compared with 2021. ⁵

While well-intentioned, this growing investment is not yielding the desired results. In the same survey, 45% of the respondents said the volume of business disruptions due to third-party cybersecurity-related incidents had increased, compared with two years earlier. ⁵ Disillusioned with how ineffective traditional TPCRM practices are at safeguarding enterprises against third-party cyber risks, SRM leaders are looking for alternatives to deliver a better return on investment.

Implications:

Organizations that adopt a resilience-driven, resource-efficient approach to TPCRM have already seen tangible successes. They are more than twice as likely to exceed executive leaders' expectations for minimizing the impact of third-party incidents. ⁵ They have also achieved better business outcomes: Nearly 80% of the respondents' organizations that have adopted this approach to TPCRM are ahead of their peers in terms of the speed at which they launch new digitization initiatives. ⁵

SRM leaders who want to adopt this approach must recognize that:

- **Business priorities influence TPCRM efforts and vice versa.** Business leaders are central to the success of TPCRM. Engaging with them in order to understand their priorities enables SRM leaders to articulate the value at stake and to align plans. Concurrently, this engagement empowers the business to make better risk-based decisions and facilitates implementation of the security controls that deliver resilience.
- **TPCRM needs to be a collaborative endeavor.** With an eye on resource efficiency for the security team, effective SRM leaders recognize that TPCRM requires partnerships with all risk functions that have a role to play in third-party risk management (namely procurement, legal and enterprise risk management). Policies, procedures and practices must be jointly established to ensure consistency across functions and minimize friction in terms of workflows. For example, initial cybersecurity risk triage needs to be built into procurement processes. This approach helps ensure the cybersecurity team's expertise is applied to initiatives that have the greatest impact on cybersecurity risk outcomes.
- **Critical third parties are your allies.** SRM leaders must shift their engagement strategy from policing to partnering with third parties. This will help ensure that all of their enterprise's most valuable assets (such as material data, networks and business processes) that critical third parties come in contact with are continuously safeguarded. Building mutually beneficial

relationships promotes greater transparency, facilitates the implementation of controls by third parties and improves collaboration in the event of cybersecurity incidents.

Actions:

- **Strengthen contingency plans for third-party engagements that pose the highest cybersecurity risk.** Create third-party-specific incident playbooks, conduct tabletop exercises and define a clear offboarding strategy involving, for example, timely revocation of access and destruction of data.
- **Reallocate resources to resilience-driven activities by making due diligence more efficient.** Instead of extensively customizing risk questionnaires, use industry-standard risk questionnaires (such as the Standardized Information Gathering [SIG] Questionnaire and the Consensus Assessments Initiative Questionnaire [CAIQ]). Invest in automation technologies to help cybersecurity teams analyze questionnaire responses at scale.
- **Build mutually beneficial relationships with critical third parties.** In a hyperconnected environment, your suppliers' risk is also your risk. It is in SRM leaders' interest to help them mature, so they can safeguard the enterprise better. First, develop a baseline of security requirements to assess vendors' maturity in terms of risk management practices. Second, work with the less mature vendors that have access to your critical assets (such as systems, datasets, networks and business processes) – share with them best practices for incident management and recommend controls for managing risks.

Further Reading:

- [Infographic: Minimize Disruption from Third-party Cybersecurity Risks](#)
- [Data Interactive: Services/Capabilities Used to Manage Third-Party Cybersecurity Risk](#)
- [Data Interactive: Which Functions Are Involved in Managing Third-Party Cybersecurity Risk?](#)

Privacy-Driven Application and Data Decoupling for Enhanced Operations in a Fragmented World

[Back to top](#)

Analysis by Anson Chen, Bernard Woo

Strategic Planning Assumption: By 2025, 10% of global businesses will operate more than one discrete business unit bound to and by a specific sovereign data strategy, doubling or more its business costs for the same business value.

Description:

Multinational companies (MNCs) that have relied on single-tenant applications for decades face rising compliance demands and business disruption risks. This is due to increasing nationalistic privacy and data protection and localization requirements that result in enforced fragmentation of enterprise application architectures and data localization practices. Forward-thinking organizations are responding by planning and implementing various levels of application and data decoupling strategies. These include reducing IT resource dependencies, adopting modular and composable architectures (including industry cloud platforms), and isolating applications, data repositories and infrastructure for highly regulated markets. This helps reduce compliance risks and create a competitive advantage. ^{6,7}

Why Trending:

Operating multinationally has become more challenging, due to increasing complex geopolitical risks and compliance obligations that prevent globally consistent enterprise architectures. “Sovereignty” considerations related to personal data have evolved into localization requirements for both personal and critical business information. The expansion in the number and the scope of requirements causes MNCs to adapt their cloud adoption strategies. MNCs have pivoted to either a modular application architecture design or a decoupling of their centralized applications (such as ERP, CRM, and data and analytics platforms) in their global headquarters for high-risk markets in which they have substantial business operations. The 2022 Gartner CIO and Technology Executive Survey found that 7% of respondents had already invested in creating a composable enterprise and that another 61% expected to do so by 2024. ⁸

Implications:

The cybersecurity and data security implications of decoupling efforts relate to:

- **Regulatory compliance.** Compliance efforts and audits have greatly increased in complexity, due to new, and often conflicting, requirements arising from new regulations in targeted regions.
- **Data migration and integration practices.** Decoupling of applications and data storage can lead to isolation and interoperability challenges, which diminishes information fidelity and hinders business continuity and innovation. MNCs can incorporate edge operations and composable architecture to mitigate some of these challenges (see [Mitigate Geopolitical Risks With Architectural Composability](#)).
- **Data architectures and storage.** Data localization requirements are causing rapid evolution in the hosting of applications and data (see [Top Trends in Privacy Driving Your Business Through 2024](#)), which is adding to the expansion of the attack surface. Meanwhile, data access and threat management orchestration need to be reimagined, as the same requirements about data localization make it difficult, if not impossible, to conduct such activities from one central location.

- **Secure development practices.** As applications are revamped, an opportunity emerges for security requirements to be “baked into” development practices,⁹ rather than “bolted on” later. If applications need to be decoupled, the security standards among the different jurisdictions may differ. Accordingly, where such differences exist, they need to be harmonized as applications are developed.

Actions:

- Collaborate with business, IT and legal teams persistently to map out data localization requirements for countries in which your organization already operates and those it plans to expand into. Any instances of noncompliance and of conflicting laws must be identified by the legal department and a jointly developed mitigation strategy put in place that includes a cost-benefit analysis.
- Maintain a data inventory and map to identify information assets that are subject to localization requirements. Prioritize investment in tools that continuously discover sensitive and personal data in the cloud. This will inform the data security strategy and serve as input to a data or information governance setup to maximize knowledge and buy-in from business stakeholders.
- Incorporate secure development practices, such as those found in the Secure Software Development Framework (SSDF) and the LINDDUN privacy-focused threat modeling framework,^{10,11} into the software development life cycle. Apply security architecture controls by adopting a modular approach to accompany the overall shift to composable applications, microservices architectures, cloud/container deployments and so on.

Further Reading:

- [Top Trends in Privacy Driving Your Business Through 2024](#)
- [Trends 2023: Rise and Risks From EU, U.S., China and Other Sovereign Data Strategies and Policies](#)
- [Geopolitics Is Shaping Generative AI \(and Vice Versa\)](#)

Generative AI Prompts Short-Term Skepticism but Inspires Long-Term Hope

[Back to top](#)

Analysis by Jeremy D’Hoinne, Avivah Litan, Angela Zhao and Mark Horvath

Strategic Planning Assumption: Through 2025, generative AI will cause a spike in the cybersecurity resources required to secure it, causing more than a 15% incremental spend on application and data security.

Description:

Large language model (LLM) applications, such as ChatGPT, have put generative AI (GenAI) on the agenda for inclusion in many business, IT and cybersecurity roadmaps. The term GenAI describes techniques that learn from representations of data and model artifacts in order to generate new artifacts.

GenAI introduces new attack surfaces, which need protecting. This requires changes to application and data security practices and to user monitoring. GenAI will also change the cybersecurity market's dynamics.

GenAI already impacts SRM leaders in multiple ways that are:

- **Direct and urgent:** To start with, unmanaged and uncontrolled uses of ChatGPT needed tackling to minimize risks. The most notable issues were the use of confidential data in third-party GenAI applications and the copyright infringement and brand damage that could result from the use of unvetted generated content. Very quickly, business initiatives drove requirements to secure GenAI applications that added new attack surfaces to those defended by traditional application security.
- **Direct and hyped as urgent:** Cybersecurity providers made a wave of hyperbolic AI announcements designed to spark interest in what GenAI might be able to do. These early announcements mostly involved interactive prompts. These raised expectations, mostly from leaders outside the security field, about the benefits for security teams' productivity, although most of these announcements were only early previews, sometimes verging on "AI washing." We already see GenAI features used in security operations and application security, but have yet to observe cybersecurity products use GenAI techniques directly to detect or prevent threats.
- **Indirect and scary:** As SRM leaders plan for 2024, they are raising legitimate questions about new risks and threats, due to privacy issues and threat actors getting access to LLM technologies. They need to ignore the "fear, uncertainty and doubt," and navigate the unpredictable changes in the threat landscape that GenAI could cause by monitoring detection performance drifts in existing security controls, and doubling down on resilience and exposure management initiatives.
- **Indirect and latent:** As more teams – potentially almost every team – within organizations seize the opportunity to integrate GenAI capabilities into their systems, cybersecurity teams will have to keep adapting to changes in processes. For example, the HR team might incorporate GenAI into recruitment processes, and the procurement team might use GenAI when selecting or renewing contracts for products. Upcoming regulations and compliance requirements will also impact security teams.

Why Trending:

Increased use of GenAI is inevitable. In the 2024 Gartner CIO and Technology Executive Survey, only 3% of the respondents stated they are not interested in GenAI. ¹² SRM leaders holding off embracing new security practices for GenAI applications or ignoring GenAI for security use cases (even based on today's basic implementations and examples) risk losing their organization's competitive edge as other companies proceed with them. The same survey found that one-third (34%) of organizations planned to deploy GenAI in the next 12 months.

SRM leaders also need to prepare for swift evolution, as LLM applications like ChatGPT are only the start in terms of GenAI disruption. Already, multimodal GenAI – which involves training models on different types of data – is expanding the scope of GenAI use cases beyond text. “Large action models” – foundation models that can perform actions automatically – are also on the horizon.

Implications:

Security teams regularly prove their ability to adapt to paradigm changes. However, the immaturity of emerging security tools intended to secure GenAI applications (their models and prompts, for example), together with the dynamics of GenAI application architecture, makes it difficult to develop best practices and make recommendations.

According to the 2024 Gartner Technology Adoption Roadmap for Large Enterprises Survey, the top three risk-related concerns about the usage of GenAI are: ¹³

1. Access to sensitive data by third parties (a concern of nearly half the cybersecurity leaders who responded).
2. GenAI application and data breaches (two-fifths of the responding cybersecurity leaders).
3. Erroneous decision making (more than one-third of the responding cybersecurity leaders).

GenAI hype shrinks security leaders' time horizons. They are stuck in the situation of having to make emergency reactions to the many GenAI initiatives occurring across their organization – a similar situation to when enterprises started moving to the cloud. SRM leaders cannot wait until everything stabilizes to prepare and plan, because:

- Although organizations with existing AI projects can tune their existing governance policies, those pivoting to GenAI will need to build policies from scratch. Among other things, determining responsibility for data confidentiality, output biases and drifts, copyright infringement, trustworthiness and explainability of GenAI applications requires new or updated governance principles.
- Application security practices must quickly evolve to:
 - Integrate new development tools, such as GenAI code assistants.

- Secure new attack surfaces at runtime (prompts, for example) and during the entire development cycle (to manage training data, for instance) (see [Innovation Guide for Generative AI in Trust, Risk and Security Management](#)).
- Meet privacy and data security requirements, notably by evaluating and implementing privacy-enhancing technologies (see [Three Critical Use Cases for Privacy-Enhancing Computation Techniques](#)).
- Evaluate and use new GenAI techniques in application security tools – for example, to reduce the false-positive rate, provide developer-friendly explainability and enable semiautomated remediation.
- Skill requirements will evolve, as new tools will augment the existing workflow and reduce the learning curve within the security team. As the skills required to perform some key jobs evolve, the level of risk will change too.
- Technology markets will see new GenAI-centric tools emerge, and possibly shifts in their competitive dynamics. This will change the vendor landscape, but will first require new evaluation requirements to assess the value of, and the risks posed by, new GenAI features.

Within the cybersecurity practice, security operations and application security are the two primary areas where providers add capabilities by using GenAI. Early implementations take the form of an assistant, essentially an interactive prompt aimed at answering questions. Too many of these implementations might soon create “prompt fatigue,” so interactions with GenAI will need to progress. We also expect new use cases to appear soon, using specially trained models.

Actions:

- **AI consumption:** Industrialize efforts to inventory, monitor and manage new use cases for third-party GenAI applications and GenAI features embedded in existing applications. Include IT and software supply chain dependencies in risk assessments.
- **Provider and technology selection requirements:** Update these to address privacy, copyright, traceability and explainability challenges. Establish policy for, and oversight of, GenAI-based products entering the organization, so that an agreed set of harmonized policies can be understood by internal teams wanting to use this technology.
- **Security of AI applications:** Update application and data security practices to integrate new attack surfaces, such as the prompts or the orchestration layers used to instrument AI models. Evaluate technologies that support the AI trust, risk and security management (TRiSM) framework.
- **Generative cybersecurity AI:** Run proof of concepts before integrating GenAI into cybersecurity programs, starting with application security and security operations. Aim to augment the work of

humans, rather than replace them, and ensure that the new tools, while improvements in themselves, also increase the team's knowledge.

- **Changes in the threat landscape:** Monitor decline in the detection accuracy and general performance of your existing security controls. Ensure you have access to the right intelligence on the changing threat landscape. Acknowledge, and communicate, that scenario planning for future GenAI attacks is tricky and might not be the most profitable use of resources.

Further Reading:

- [4 Ways Generative AI Will Impact CISOs and Their Teams](#)
- [Predicts 2024: AI & Cybersecurity – Turning Disruption Into an Opportunity](#)
- [Innovation Guide for Generative AI in Trust, Risk and Security Management](#)

Security Behavior and Culture Programs Gain Increasing Traction to Reduce Human-Born Cybersecurity Risks

[Back to top](#)

Analysis by Richard Addiscott, Andrew Walls, Christine Lee, Victoria Cason

Strategic Planning Assumptions:

- By 2025, 40% of cybersecurity programs will deploy socio-behavioral principles (such as nudge techniques) to influence security culture across the organization, up from less than 5% in 2021.
- By 2027, 50% of large enterprise CISOs will have adopted human-centric security design practices to minimize cybersecurity-induced friction and maximize control adoption.

Description:

Security behavior and culture programs (SBCPs) encapsulate an enterprisewide approach to minimizing cybersecurity incidents associated with employee behavior, whether inadvertent or deliberate.

An SBCP's primary objective is to change behavior. It encompasses traditional practices, such as awareness training and phishing simulation, and a spectrum of behavior-influencing disciplines, including:

- Organizational change management.
- Human-centered user experience (UX) design.

- DevSecOps.

SBCPs also consider a range of factors that influence program design, and encourage a platform-based architecture, to help:

- Reduce employees' susceptibility to social engineering and improve their responses when attacked.
- Improve adoption of security controls.
- Minimize vulnerabilities introduced through system acquisition processes.
- Institute agile, business-led digital decision making without increasing security risk.

Why Trending:

Clients and vendors have recognized that the prevailing singular focus on raising employees' cybersecurity awareness is largely ineffective at reducing the number of security incidents resulting from employees' behavior. The 2022 Gartner Drivers of Secure Behavior Survey found that: ¹⁴

- 69% of the employees surveyed admitted deliberately bypassing security controls in the previous 12 months.
- 93% of the employees knew their actions would increase risk to their organization but undertook them anyway.

The democratization of GenAI amplifies this challenge, as it gives employees potentially unfettered access to powerful technical capabilities that, if used without due care, could result in data breaches.

Since Gartner's introduction of the SBCP concept and the associated PIPE (Practices, Influences, Platforms, Enablers) Framework in 2022, calls to Gartner's client inquiry service on this topic have more than quadrupled. SRM leaders recognize that shifting focus from increasing awareness to fostering behavioral change will help reduce cybersecurity risks. Additionally, this shift enables SRM leaders to tackle the challenges of "security fatigue," control friction, and organizational cultures that prioritize speed and profit regardless of risk. Leading vendors are responding and rapidly transforming solutions to support behavioral change and enhance the security consciousness of their clients' corporate cultures.

Implications:

Organizations such as Santander and "SevenHills" (see [Case Study: Framework to Enable Business Ownership of Cybersecurity Activities](#) [SevenHills is a pseudonym]) that have adopted SBCP-related practices have seen:

- Improved employee adoption of security controls.
- Reductions in unsecure behavior.
- Increases in speed and agility.
- More effective use of cybersecurity resources as employees become competent at making independent cyber-risk decisions.

However, current investment is often insufficient to achieve the outcomes listed above. The 2022 Gartner Cybersecurity Awareness Survey found that, while 84% of the responding organizations indicated that the primary objective of their awareness program was to change behavior, 80% of the organizations had less than one full-time equivalent (FTE), and 50% had less than 0.6 of an FTE, associated with their awareness program. ¹⁵

To execute effective SBCPs, SRM leaders need more FTE capacity and capability, a more platform-centric technology architecture, and increased sophistication in program design. Given the requirement for a whole-of-enterprise approach, an SBCP also demands greater senior executive support and more time commitment across the organization than does a traditional awareness campaign. It is therefore unsurprising that 68% of cybersecurity leaders who responded to another Gartner survey indicated that they were finding it more challenging to obtain executive support for their SBCP than for previous security awareness campaigns. ¹⁶ Nonetheless, visible and sustained advocacy from the organization's senior executives will be critical to optimize the program's chances of delivering measurably improved secure behaviors and to ingrain a more security-conscious corporate culture.

Actions:

- 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 unsecure employee behavior.
- Guide effective and efficient implementation of your SBCP by adopting the Gartner PIPE Framework using a scalable approach appropriate to the funding and resources available.
- Foster higher levels of sustained and visible executive support by using outcome-driven, behavior-centered metrics to help demonstrate the business value of the SBCP to executive stakeholders and the board of directors.

Further Reading:

- [CISO Foundations: Build a Culture of Security Consciousness: Introducing the Gartner PIPE Framework](#)

- [CISO Foundations: 4 Actions CISOs Must Take to Reduce Cybersecurity-Induced Friction](#)
- [Innovation Insight on Security Behavior and Culture Program Capabilities](#)

Cybersecurity Outcome-Driven Metrics Bridging the Communications Gap in the Boardroom

[Back to top](#)

Analysis by Paul Furtado, Christopher Mixter, Paul Proctor

Description:

Cybersecurity outcome-driven metrics (ODMs) are operational metrics with special properties – they enable cybersecurity’s stakeholders to draw a straight line between cybersecurity investment and the delivered protection levels that investment generates. ODMs are central to creating a defensible cybersecurity investment strategy. They reflect agreed protection levels with powerful properties, in simple language, so as to:

- Provide a credible and defensible expression of risk appetite that supports direct investment.
- Be explainable to non-IT executives who have no technical background.
- Act as value levers that support direct investment to change protection levels.

ODMs assist with many tasks that have been problematic for decades. For example, they help:

- Address business decision making to accept third-party risk without accountability.
- Support SRM leaders with multiple, semiautonomous operating units to manage security protection levels while maintaining autonomy.
- Support cybersecurity due diligence for the “buy” side in mergers and acquisitions.
- Explain material cyberincidents to executives and guide specific investments to remediate them.
- Support transparency to educate executives, lines of business and corporate functions about inappropriate or cavalier risk acceptance.
- Expose matrixed management problems, such as the role the IT team plays in patching problems for which the security organization is typically held accountable.

Why Trending:

The 2023 Gartner Evolution of Cybersecurity Leader Survey asked chief information security officers (CISOs) the following question: “What has been the impact of changing business objectives on your cybersecurity strategy?”¹⁷ In response, 60% said there had been some impact or a major impact. When the business pivots we need to be able to articulate the change in residual risk in a measurable and defensible way. Despite significant investments in cybersecurity people, processes and technologies, the frequency and negative impact of cybersecurity incidents on organizations across sectors continues to rise. This undermines the confidence of board members and C-level leaders in their cybersecurity organization’s strategies. New regulation from the U.S. Securities and Exchange Commission (SEC), the second version of the EU’s Network and Information Systems Directive (NIS2), and recent signals from the Australian Securities and Investments Commission (ASIC) highlight continued governmental pressure on executives to meet this need.

SRM leaders continue to struggle to convey the value of cybersecurity investment beyond the importance of regulatory compliance and “closing gaps in functional and technological maturity,” neither of which have a meaningful correlation to protection. Traditional approaches to connecting cybersecurity investment with business value are equally limited. Spending does not equal protection. Cyber-risk quantification is still in its infancy, is expensive, and supports only broad strategic decisions. Heat maps are highly subjective.

Organizations are seeking an approach to measuring cybersecurity value that resonates with executives and supports practical investment decisions that align with business needs. ODMs are increasingly being adopted as one of the most promising candidates.

Implications:

- ODMs change cybersecurity governance to support direct negotiations with non-IT executives for funding and desired protection levels through protection-level agreements (PLAs) (see [Six Steps to Manage Cybersecurity Risk Appetite Through Protection-Level Agreements](#)).
- Managing outcomes replaces any need to discuss tools and technology with executives while preserving complete flexibility in terms of delivery methods.
- ODMs offer an alternative definition of “risk appetite,” one that is less about willingness to accept loss and more about desire for achieving agreed protection levels and for demonstrating whether they are being achieved.
- ODMs enable SRM leaders to reset their accountability, so that it is less about preventing breaches and more about “keeping risk owners within their risk appetite.”
- SRM leaders must encourage non-IT leaders to take less interest in threat scenarios and likelihood-based investment justifications and more in protection levels for ongoing exposures.

- Investment is required to prepare systems and processes to gather new data continuously for ODMs.

Actions:

- Use Gartner's [Tool: Catalog of Business-Aligned Outcome-Driven Metrics for Risk and Security](#) to select the ODMs that represent a holistic view of current performance against your enterprise's biggest risks.
- Negotiate protection levels (desired performance) for each ODM with lines of business and corporate function leaders. PLAs may vary between operating groups and departments.
- Use Gartner's [Cybersecurity Business Value Benchmark](#) to provide stakeholders with an external perspective on ODM performance.
- Begin reporting ODM performance at board level to support the board's role in overseeing risk appetite management and decision making.

Further Reading:

- [Quick Answer: What Is a Cybersecurity Outcome-Driven Metric?](#)
- [Tool: Cybersecurity Assessment Template Using Outcome-Driven Metrics](#)
- [Four Steps to Develop Outcome-Driven Metrics for Cybersecurity](#)

Shifting Sands: Evolving Cybersecurity Operating Models

[Back to top](#)

Analysis by Tom Scholtz, Oscar Isaka, William Candrick, Michael Kranawetter

Description:

The acquisition, creation and delivery of technology continues to move from central IT functions to lines of business. This transformation breaks traditional cybersecurity operating models. SRM leaders are adapting cybersecurity operating models to meet business needs for autonomy, innovation and agility. Decision rights are becoming dispersed, policy details are now owned at the edge, some governance is being centralized and formalized to better support risk owners at the edge, and the SRM leader role is evolving into a value enabler role.

Why Trending:

The way enterprises use technology is transforming: Two-thirds (67%) of the CEOs and senior business executives who responded to a Gartner survey expressed a desire to have more technology work done directly within business functions.¹⁸ In addition, many enterprises are undergoing digital transformation and cloud migrations, dispersing work within remote or hybrid models, and facing regulatory pressure to build privacy, compliance and cybersecurity into business operations. As a result, responsibility for the acquisition, creation and delivery of technology is moving from central IT functions to lines of business, corporate functions, fusion teams and even individual employees.

Traditional cybersecurity operating models do not scale within this new reality. Cybersecurity needs tighter connections with the business to maintain visibility over data assets and to support controls implementation. Top-down governance or controls will not scale, because the heterogeneity of workflows and the fragmentation of technology ownership means the security function cannot oversee every decision with cybersecurity risk implications. SRM leaders need to improve the cyber literacy and cyber judgment of business decision makers, so that employees can integrate cybersecurity considerations into their day-to-day work, and implement collaborative risk management processes.

Implications:

Gartner's research indicates that SRM leaders are adopting a variety of strategies to evolve their cybersecurity operating models:

- **They are “centralizing to decentralize.”** This means centralizing and streamlining cybersecurity oversight and collaborative decision making while driving local autonomy and accountability across decentralized resource owners. Progressive SRM leaders recognize that localized cyber judgment at the edge reduces risk and supports creation of business value.
- **They are centralizing policy governance,** while making policy implementation (of standards and guidelines, for example) more flexible and locally managed to accommodate control ownership at the edge. In fact, 45% of the CISOs surveyed by Gartner are consolidating or reducing policy, not expanding policy.^{18,19} To make policies more user-friendly, SRM leaders and their teams are now co-creating policies with end users, and giving risk and data owners more control over specific standards and implementations.
- **They are creating new processes and adding new capabilities** to support new operating models. For example, 64% of the CISOs who responded to a Gartner survey had created new cybersecurity processes and 60% had created new teams or functions over the prior 24 months.¹⁹

SRM leaders take a leading role in evolving their roles and transforming cybersecurity's operating model. At least 85% of the CISOs who responded to a Gartner survey led or co-led changes to their operating models, rather than receiving changes from other leaders such as the CIO, CTO or chief risk officer.¹⁹

Actions:

- Promote collaborative, centrally enabled decision making and cyber judgment (that is, employees' ability to make risk-informed decisions autonomously) by establishing a representative steering committee with stakeholders from risk and business functions, and ensure collaborative risk-decision-making processes.
- Implement streamlined and standardized cybersecurity processes – including risk assessment, risk acceptance, exception management and conflict resolution – to enhance collaboration and risk-decision-making efficiency.
- Develop a flexible policy framework that allows resource owners to tailor cybersecurity procedures and controls to their specific needs. This promotes a sense of ownership and responsibility for risk management, while maintaining policy compliance.
- Embrace the SRM leader's evolving role as a facilitator of cybersecurity risk decisions by engaging with business stakeholders, promoting cyber judgment and aligning security measures with the dynamic needs of the organization.

Further Reading:

- [CISO Effectiveness: Security Operating Models Are Evolving](#)
- [CISO Foundations: Build a Defensible and Agile Security Program](#)
- [Infographic: Building Cyber Judgment to Improve Risk Decision Making](#)

Cybersecurity Reskilling to Future-Proof the Organization

[Back to top](#)

Analysis by William Candrick, John Watts, Jeremy D'Hoinne, Alex Michaels, Craig Porter

Strategic Planning Assumption: Fifty percent of large enterprises will use agile learning as their primary upskilling/reskilling method by 2026.

Description:

The global cybersecurity talent shortage is a perennial issue. In the U.S. alone, there are only enough qualified cybersecurity professionals to meet 70% of current demand – an all-time low over the past decade.²⁰ Unfortunately, labor market supply-and-demand issues cannot be solved by individual SRM leaders.

What can be solved is an emerging skills gap. The skills that cybersecurity teams need are changing drastically, yet cybersecurity leaders continue to hire for legacy roles and skills. SRM leaders must reskill their teams by retraining existing talent and hiring new talent with new profiles.

Why Trending:

SRM leaders face a convergence of megatrends, all of which impact the skills cybersecurity teams need to thrive. These trends include:

- **Cloud adoption.** Most organizations are now cloud-first (or cloud-preferred) entities. Their migration to the cloud drives further abstraction away from securing underlying infrastructure.
- **GenAI.** The rapid rise and general availability of GenAI tools transform both the technologies that must be secured and the tools that cybersecurity teams will use.
- **Operating model transformation.** Cybersecurity professionals increasingly need to work with and through business partners, rather than individually managing cybersecurity implementation.
- **Vendor consolidation.** This means cybersecurity teams must manage fewer security solution suites and vendor relationships.
- **Expansion of the threat landscape.** The threat landscape now encompasses cyber-physical systems, remote work, GenAI technology and employees' use of low/no-code solutions.
- **An augmented connected workforce.** To enable GenAI pioneers inside organizations, strategies are being developed and implemented to optimize the value derived from human workers (see [Top Strategic Technology Trends for 2024: Augmented Connected Workforce](#)).

Collectively, these trends are transforming the skills cybersecurity teams need. Demand for new skills will grow faster than the widespread creation of new roles, new certifications, new job descriptions, new titles and so on. Therefore, learning and development solutions, hiring platforms and HR practices will lag behind the needs of cybersecurity.

Implications:

Cybersecurity teams need new skills, many of which are not yet defined or standardized. SRM leaders should consider the following implications:

- **“Adjacent skills” will address some skills gaps.** Demand for new, emerging skills will grow before HR practices, job description templates and certification and training services can catch up. SRM leaders will need to hire for “adjacent skills” – both internally and externally – that approximately address emerging skills needs, in order to navigate the megatrends outlined above (see [Innovation](#)

Insight for AI-Enabled Skills Management and Tool: Identifying Adjacent Talent for Key Cybersecurity Roles).

- **“Soft” skills will trump technical prowess.** Risk decisions and policy details are increasingly owned at the edge – outside cybersecurity’s direct purview. Cybersecurity teams need more soft skills, such as business acumen, verbal communication ability and empathy, to work with others. These skills help cybersecurity professionals understand how cyber risk impacts business outcomes, how controls create friction for the business, and how to negotiate for outcomes that balance cyber risk with other considerations.
- **New skills will be needed for new challenges.** Cybersecurity teams will need new skills, many of which did not exist in years past. These skills may be part of entirely new cybersecurity roles or new skills that augment existing roles. For example, data scientists may need skills in AI ethics, and security awareness managers may need skills in human psychology.

Actions:

- **Develop a cybersecurity workforce plan.** Document emerging skill needs, and map these to current or new-in-kind cybersecurity roles. Socialize your roadmap with cybersecurity staff, so they understand how their roles will evolve and how leadership will support their continued development and career advancement (see [Tool: A CISO’s Guide for Conversations With the CHRO](#)).
- **Hire for the future, not the past.** Update job descriptions and outsourcing RFPs to reflect anticipated future, rather than past, skills needs. Be careful to remove legacy skills, so as not to develop job descriptions that describe “unicorns” – ideal applicants that do not exist or are nearly impossible to find, hire and retain.
- **Foster an agile learning culture.** Revamp cybersecurity’s learning and development program around agile learning. Agile learning prioritizes hands-on skills development via iterative, short bursts, as opposed to waterfall-based training and certification programs (see [Future of Work Trends: The Agile Learning Imperative](#)).

Further Reading:

- [CISO Effectiveness: How to Attract, Retain and Release Cybersecurity Talent](#)
- [CISO Foundations: Cybersecurity Talent Strategies for CISOs](#)
- [Future of Work Trends: The Agile Learning Imperative](#)

Changes Since Last Year

Continuous threat exposure management (CTEM). In alignment with the expansion of the attack surface, SRM leaders have realized they need new processes to make effective decisions. Initially,

vulnerability assessment and risk-based vulnerability management practices did not work as well as needed for this purpose and added unpatchable exposures to the already overwhelming abundance of discovered vulnerabilities. But initial efforts to better align the scopes of assessments with the ability to remediate issues showed promising results. Among other things, these efforts significantly standardized practices for managing threat exposure and connected the management of security posture governed by new processes such as CTEM.

Evidence

¹ CISO Leadership Perspectives Survey Priorities & Spending Data, June 2023, Evanta.

² [2023 Open Source Security and Risk Analysis Report](#), Synopsys.

³ M. Chertoff, [Cyber Risk Is Growing. Here's How Companies Can Keep Up](#), *Harvard Business Review*, 13 April 2023.

⁴ [2023 Gartner IAM Modernization Preventing Identity-First Security Survey](#). This survey was conducted to determine how far the market has moved toward identity-first security. It was conducted online from 9 June through 24 July 2023 among 303 respondents from North America (n = 104 in the U.S. and Canada), Latin America (n = 41 in Brazil), Asia/Pacific (n = 59 in India, Australia and Singapore) and EMEA (n = 99 in Germany, France and the U.K.). Respondents' organizations generated \$100 million or more in enterprisewide revenue in 2022 and had at least 250 employees. Respondents were required to have some involvement in their organizations' IAM and to be planning at least one workforce, consumer or machine/nonhuman IAM initiative in their organization within the next two years. *Disclaimer: The results of this survey do not represent global findings or the market as a whole. They reflect the sentiments of the respondents and companies surveyed.*

⁵ [2023 Gartner Reimagining Third-Party Cybersecurity Risk Management Survey](#). This was a survey of 376 senior executives involved in third-party cybersecurity risk management across organizations of different sizes in different industries and geographies. It was further substantiated and informed by in-depth practitioner interviews with over 60 chief information security officers (CISOs) to understand cybersecurity goals and challenges associated with third-party cybersecurity risk management. The aim of the survey, which was conducted from July through August 2023, was to understand the practices that cybersecurity leaders should follow to better manage cybersecurity risks emanating from third-party relationships. Gartner used descriptive statistics to ensure all normal distribution of data and created a measure of effectiveness that determines how effective an organization is at achieving key cybersecurity outcomes. We then used a regression-based maximum impact analysis to determine which of the hypothesized practices in third-party cybersecurity risk management were most impactful in improving those outcomes. Maximum impact analysis reveals the largest amount of improvement in outcomes that an organization can realize by improving each factor when managing third-party cybersecurity risk. *Disclaimer: The results of this survey do not represent global findings or the market as a whole. They reflect the sentiments of the respondents and companies surveyed.*

⁶ R. McMorrow and others, [Multinationals in China Accelerate Push to Decouple Data](#), *Financial Times*, 16 July 2023.

⁷ S. Parekh and others, [Localization of Data Privacy Regulations Creates Competitive Opportunities](#), McKinsey & Company.

⁸ **2022 Gartner CIO and Technology Executive Survey**. This survey was conducted to help CIOs and technology executives adopt business composability as a means to thrive during periods of volatility and uncertainty. It was conducted online from 3 May through 19 July 2021 with Gartner Executive Programs members and other technology executives. Qualified respondents were the most senior IT leader (CIO) for their overall organization or a part of their organization (for example, a business unit or region). The total sample was 2,387, with representation from all geographies and industry sectors (public and private). *Disclaimer: The results of this survey do not represent global findings or the market as a whole. They reflect the sentiments of the respondents and companies surveyed.*

⁹ [Shifting the Balance of Cybersecurity Risk: Principles and Approaches for Security-by-Design and -Default](#), Cybersecurity and Infrastructure Security Agency, 13 April 2023.

¹⁰ [Secure Software Development Framework](#), National Institute of Standards and Technology (NIST).

¹¹ [LINDDUN Privacy Threat Modeling](#), DistriNet, KU Leuven.

¹² **2024 Gartner CIO and Technology Executive Survey**. This survey was conducted online from 2 May through 27 June 2023 to help CIOs determine how to distribute digital leadership across the enterprise and to identify technology adoption and functional performance trends. Ninety-seven percent of the respondents led an information technology function. In total, 2,457 CIOs and technology executives participated, with representation from all geographies, revenue bands and industry sectors (public and private). *Disclaimer: The results of this survey do not represent global findings or the market as a whole. They reflect the sentiments of the respondents and companies surveyed.*

¹³ **2024 Gartner Technology Adoption Roadmap for Large Enterprises Survey**. This online survey had more than 600 respondents from North America, EMEA and Asia/Pacific. They represented enterprises, from various industries, with annual revenue of more than \$1 billion. This research summarizes findings from more than 120 respondents who were identified as cybersecurity leaders.

¹⁴ **2022 Gartner Drivers of Secure Behavior Survey**. This online survey, conducted from May through June 2022, covered 1,310 employees across functions, levels, industries and geographies. It examined the extent to which they behave securely in their day-to-day work, the root causes of unsecure behavior, and the types of support and training they receive from their organizations to drive desirable secure behaviors. We used descriptive statistics and regression analysis to determine

the key factors that drive or impede employees' secure behaviors and the development of cyber judgment.

¹⁵ **2022 Gartner Cybersecurity Awareness Survey.** The online survey ran from February through April 2022. The respondents included heads of cybersecurity functions. It was conducted to get a better understanding of the size, scope and objectives of cybersecurity awareness campaigns in organizations. *Disclaimer: The results of this survey do not represent global findings or the market as a whole. They reflect the sentiments of the respondents and companies surveyed.*

¹⁶ **Gartner Peer Community, Security Behavior and Culture Programs: Adoption Strategies Survey.**

¹⁷ **2023 Gartner Evolution of Cybersecurity Leader Survey.** This online survey was conducted to understand the evolution of the role and responsibilities of cybersecurity leaders or CISOs. It ran from 31 July through 13 September 2023. There were 318 respondents (211 conducted through a vendor panel and 107 via a list of conferences). They came from different regions: North America (n = 112; U.S. and Canada), Latin America (n = 42; Brazil, Argentina, Honduras, Mexico, Chile and Ecuador), Asia/Pacific (n = 62; India, Australia, Singapore, Taiwan, Japan, Thailand, China, South Korea, Malaysia and Tajikistan) and EMEA (n = 102; Germany, France, U.K., Portugal, Netherlands, Norway, Switzerland, Italy, Denmark, Spain, Belgium, Sweden, Austria, Israel, United Arab Emirates, Kuwait, Serbia, Saudi Arabia and South Africa). Respondents' organizations had \$50 million or more in enterprisewide annual revenue for 2022 and at least 100 employees. Respondents were required to be team members and have some responsibility for their organization's cybersecurity/risk function; they were also required to be up to two layers away from their CISO/head of cybersecurity. *Disclaimer: The results of this study do not represent global findings or the market as a whole. They reflect the sentiments of the respondents and companies surveyed.*

¹⁸ **2022 Gartner CEO and Senior Business Executive Survey.** This survey was conducted to examine the views of CEOs and senior business executives on current business issues, as well as some areas of technology agenda impact. It ran from July 2021 through December 2021, with questions about the period from 2021 through 2023. One-quarter of the survey sample was collected in July and August 2021, and three-quarters in October through December 2021. In total, 410 actively employed CEOs and other senior business leaders qualified and participated. The research was collected via 382 online surveys and 28 telephone interviews. The sample mix by role was CEO (n = 253); CFO (n = 88); COO or other C-level executive (n = 19); and chair, president or board director (n = 50). The sample mix by location was North America (n = 176), Europe (n = 97), Asia/Pacific (n = 86), Latin America (n = 40), the Middle East (n = 4) and South Africa (n = 7). The sample mix by organization revenue was \$50 million to less than \$250 million (n = 58), \$250 million to less than \$1 billion (n = 81), \$1 billion to less than \$10 billion (n = 212) and \$10 billion or more (n = 59). *Disclaimer: The results of this survey do not represent global findings or the market as a whole. They reflect the sentiments of the respondents and companies surveyed.*

¹⁹ **2022 Gartner Shifting Cybersecurity Operating Model Survey**. This online survey was conducted to determine the impact of the changing technology governance environment on the security operating model at the macro level. It ran from October through November 2022, covering 462 respondents from North America, Europe, Latin America and Asia/Pacific. Respondents were required to be cybersecurity or information security leaders. *Disclaimer: The results of this survey do not represent global findings or the market as a whole. They reflect the sentiments of the respondents and companies surveyed.*

²⁰ **Cybersecurity Supply/Demand Heat Map**, Cyberseek US, 2023.

**Learn how Gartner
can help you succeed**

Become a Client

© 2024 Gartner, Inc. and/or its affiliates. All rights reserved. Gartner is a registered trademark of Gartner, Inc. and its affiliates. This publication may not be reproduced or distributed in any form without Gartner's prior written permission. It consists of the opinions of Gartner's research organization, which should not be construed as statements of fact. While the information contained in this publication has been obtained from sources believed to be reliable, Gartner disclaims all warranties as to the accuracy, completeness or adequacy of such information. Although Gartner research may address legal and financial issues, Gartner does not provide legal or investment advice and its research should not be construed or used as such. Your access and use of this publication are governed by [Gartner's Usage Policy](#). Gartner prides itself on its reputation for independence and objectivity. Its research is produced independently by its research organization without input or influence from any third party. For further information, see "[Guiding Principles on Independence and Objectivity](#)." Gartner research may not be used as input into or for the training or development of generative artificial intelligence, machine learning, algorithms, software, or related technologies.