Gartner. Autorisé à distribuer

Principales tendances en matière de cybersécurité pour 2025

12 décembre 2024 - ID G00822766 - 49 min de lecture

Par **Richard** Addiscott , Anson Chen et **10 autres**

Les bouleversements technologiques et commerciaux incessants mettent à l'épreuve les limites des programmes de sécurité et la performance des équipes. Les responsables de la sécurité et de la gestion des risques doivent créer de la valeur pour l'entreprise et redoubler d'efforts pour renforcer la résilience organisationnelle, personnelle et collective afin de démontrer l'efficacité des programmes de sécurité en 2025.

Aperçu

Opportunités

- Créer de la valeur ajoutée face à l'évolution constante des technologies et à la volonté des entreprises de les exploiter à des fins stratégiques est un défi constant pour les responsables de la sécurité et de la gestion des risques (SRM). Collaborer avec les responsables des données et de l'entreprise, et étendre les stratégies IAM de l'entreprise, permet de garantir que les données et les systèmes de l'entreprise sont compatibles avec l'IA. Parallèlement , cette collaboration favorise une prise de décision plus indépendante et plus efficace en matière de risques de cybersécurité, permettant ainsi une transformation sécurisée de l'entreprise.
- Soutenir la demande des entreprises en matière de continuité d'exploitation stable et absorber la pression d'un paysage de menaces en constante évolution est une constante

pour les responsables SRM. Ces défis offrent l'opportunité d'adopter une approche plus proactive et globale, intégrant la résilience aux capacités technologiques et humaines.

- Les initiatives locales axées sur l'amélioration des comportements et de la culture de sécurité, la gestion des risques liés aux tiers associés à l'IA générative (GenAI) et l'amélioration de la perception de la cybersécurité par l'entreprise offrent aux responsables SRM une opportunité unique. En collaborant avec les responsables informatiques et métiers pour aborder ces sujets, les responsables SRM peuvent tirer un double avantage : favoriser la transformation sécurisée de l'entreprise et ancrer la résilience au sein de l'organisation.

Recommandations

En tant que responsable SRM cherchant à optimiser le programme et l'investissement en cybersécurité de votre organisation, vous devez :

- Créez des bases fiables pour une transformation commerciale sécurisée et basée sur l'IA en formalisant la responsabilité des risques de cybersécurité, en encourageant le jugement cybernétique, en redynamisant les programmes de gestion de la sécurité des données et en étendant les stratégies IAM d'entreprise pour inclure les identités des machines.

- Intégrer la résilience en planifiant et en évaluant régulièrement les capacités technologiques et humaines. Cela implique d'optimiser l'investissement et l'utilisation des technologies, d'intégrer l'IA aux flux de travail existants et de surveiller et de réagir aux signes d'épuisement professionnel au sein des équipes de sécurité.

- Renforcez les bases d'une transformation sécurisée de votre entreprise en élaborant des politiques claires et concrètes de gestion des risques liés aux tiers et en favorisant des collaborations ciblées avec l'IT et l'entreprise. Cette approche renforcera la prise de décision en matière de sécurité et renforcera l'idée qu'une culture de cybersécurité solide repose sur la résilience, l'agilité et la capacité de défense.

Hypothèses de planification stratégique

- D'ici 2027, les RSSI qui investissent dans des programmes de résilience personnelle spécifiques à la cybersécurité constateront 50 % de moins d'attrition liée à l'épuisement

professionnel que leurs pairs qui ne le font pas.

- D'ici 2026, les entreprises combinant GenAI avec une architecture intégrée basée sur des plates-formes dans des programmes de comportement et de culture de sécurité connaîtront 40 % d'incidents de cybersécurité liés aux employés en moins.

Ce que vous devez savoir

Sans surprise, GenAI, et l'IA plus largement, ont été un élément commun dans les principaux domaines d'intérêt des dirigeants SRM en 2024. Gartner s'attend à ce que cela continue d'impacter leurs objectifs stratégiques de multiples façons en 2025 :

- Établir des attentes plus élevées pour créer de l'efficacité et de la cohérence dans les livrables des équipes cybernétiques et les rendre plus compréhensibles pour les responsables non liés à la sécurité
- Déclencher des changements dans les processus de sécurité existants pour garantir la pertinence, suggérer des changements efficaces et permettre l'agilité de l'entreprise
- Élargir la portée des initiatives de sécurité d'entreprise existantes, renforçant ainsi les bases de l'exploitation des cas d'utilisation de l'IA
- Amplifier la pression sur des ressources déjà limitées

Confrontés aux défis persistants d'un paysage de menaces en constante évolution , à l'élargissement des écarts de talents et à une surveillance réglementaire croissante, les dirigeants de SRM concentrent principalement leurs efforts dans deux domaines :

- Permettre la transformation
- Intégrer la résilience

Permettre la transformation

Les dirigeants d'entreprise exploitent les dernières innovations en matière d'IA et d'autres technologies progressives et de plus en plus accessibles à la périphérie de l'organisation pour générer de la valeur stratégique. Cela se traduit par une décentralisation correspondante des droits de décision et de responsabilité en matière de cybersécurité.

Les responsables SRM s'adaptent proactivement à ces changements en mettant en œuvre des pratiques collaboratives de gestion des risques. Cela permet de codifier la prise en charge des cyberrisques par l'entreprise et d'instaurer un meilleur jugement en matière de cybersécurité dans l'ensemble de l'entreprise. Cela permet d'accroître l'autonomie et l'agilité technologiques de l'entreprise sans introduire de niveaux inacceptables de risques de cybersécurité.

Un accès facile à des données saines et sécurisées est une condition essentielle, même pour les plus petites initiatives d'IA . Les responsables SRM collaborent avec leurs collègues des données , de l'analyse et de la confidentialité pour garantir que toutes les données, structurées et non structurées, proposées pour les cas d'utilisation GenAI approuvés, soient à la fois compatibles avec l'IA et sécurisées.

Les leaders de la gestion des identités et des accès (SRM) tournés vers l'avenir ont également reconnu que l' adoption croissante des capacités GenAI au sein des organisations s'accompagnait d'une augmentation correspondante des services cloud et des projets pilotes d'automatisation . En réponse, ils étendent la portée de leurs efforts actuels visant à renforcer les stratégies de gestion des identités et des accès aux identités machine (voir note 1).

Intégrer la résilience

En 2024, les responsables de la gestion des risques de sécurité se sont concentrés sur l'optimisation de leurs programmes de sécurité afin d'assurer la résilience organisationnelle et cybernétique. Ces efforts se poursuivront en 2025 .

Nous constatons une reconnaissance croissante du fait que la mentalité de « tolérance zéro à l'échec » a atteint son apogée en matière de réduction durable des risques et ne fait qu'accroître le risque d' épuisement des équipes de sécurité . Les responsables SRM s'attachent à intégrer la résilience dans la culture d'entreprise, en explorant la cyberdissuasion comme facteur de différenciation et les capacités de cyberstockage pour favoriser la transformation et renforcer la résilience.

Il existe plus de 3 000 fournisseurs de cybersécurité parmi lesquels choisir.1 Par conséquent, les responsables SRM ont de plus en plus de mal à gérer la tension inhérente entre l'amélioration de leurs capacités à faire face aux nouvelles technologies et aux risques émergents et la réduction simultanée des frais généraux et de la complexité opérationnelle. Les responsables SRM qui alignent leurs ressources disponibles et leurs capacités

techniques internes peuvent équilibrer l'adoption de plateformes et la recherche d' architectures maillées de cybersécurité afin de choisir la bonne combinaison d'outils et de fournisseurs pour atteindre les résultats souhaités.

L'évolution constante des menaces et du paysage technologique, la demande croissante des entreprises et les exigences réglementaires, conjuguées à la pénurie endémique de talents, créent une situation critique. Par conséquent , le secteur de la sécurité traverse une crise psychologique, les responsables SRM et leurs équipes étant confrontés à un burn-out croissant. Les responsables SRM efficaces reconnaissent ce problème et y répondent comme l'une de leurs principales priorités afin de garantir la mise en place d'un programme de cybersécurité résilient et durable.

Double objectif pour des résultats doubles

Plusieurs tendances de cette année offrent aux dirigeants du SRM l’opportunité de permettre la transformation et d’intégrer davantage la cyber-résilience.

Les responsables SRM tirent les leçons des projets pilotes de transformation de l'IA et affinent leurs processus en s'appuyant sur les premiers succès obtenus grâce à une approche plus tactique de l'intégration de l'IA. Cette approche allégée permet également de réduire les risques pesant sur les résultats du programme de sécurité et de préserver la crédibilité de la fonction en se concentrant sur des avantages de sécurité progressifs et en les générant davantage, plutôt que de rechercher à courte vue des changements radicaux motivés par le battage médiatique.

L'accent mis en permanence sur la gestion des risques de cybersécurité liés aux tiers et la maturation des programmes de comportement et de culture de sécurité (PCCS) à partir de 2024 génèrent de la valeur à deux niveaux. Premièrement, ils offrent une protection contre les incidents de cybersécurité survenant à l'intérieur et à l'extérieur de l'organisation. Deuxièmement , ils offrent des conseils et des garde-fous aux services métier de plus en plus autonomes qui entreprennent de plus en plus de travaux technologiques élargissant l'écosystème numérique de l'organisation et la surface d'attaque associée.

La figure 1 illustre les principales tendances en matière de cybersécurité pour 2025.

Figure 1 : Principales tendances en matière de cybersécurité pour 2025

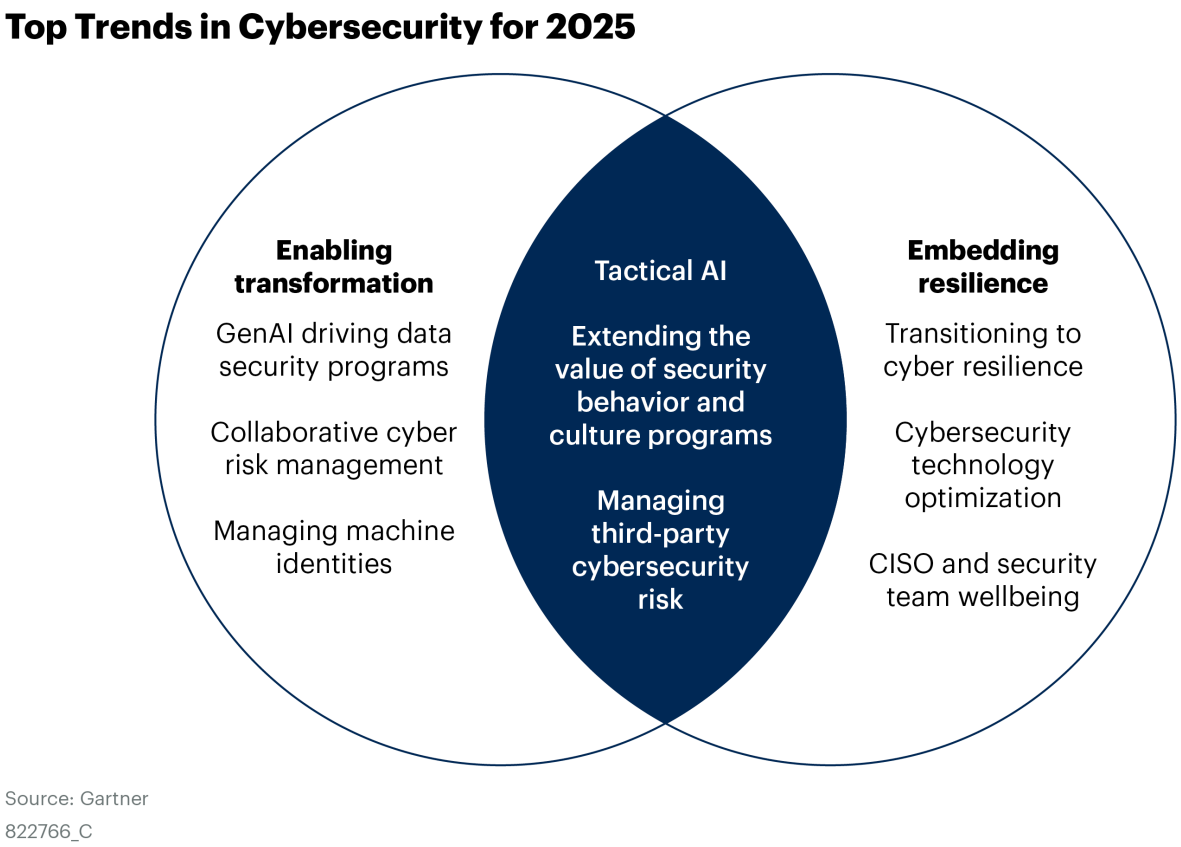

Tableau 1 : Principales tendances en matière de cybersécurité pour 2025

Permettre la transformation	Intégrer la résilience
GenAI pilote les programmes de sécurité des données	Transition vers la cyber-résilience
Gestion collaborative des cyber-risques	Optimisation des technologies de cybersécurité
Gestion des identités des machines	Bien-être du RSSI et de l'équipe de sécurité
IA tactique	
Étendre la valeur des programmes de comportement et de culture de sécurité	

Gestion des risques de cybersécurité des tiers

Source : Gartner

Permettre la transformation

GenAI pilote les programmes de sécurité des données

Analyse de Joerg Fritsch, Anson Chen, Brian Lowans

Description:

L'essor de GenAI transforme les programmes de sécurité des données, notamment dans trois dimensions :

Préférence pour les données synthétiques plutôt que pour les données obscurcies dan formation GenAI

Les données synthétiques sont de plus en plus privilégiées par rapport aux méthodes d'anonymisation traditionnelles pour l'entraînement des modèles d'IA. Gartner observe c les clients finaux matures, qui doivent masquer des informations sensibles, utilisent fréquemment des produits générant des données synthétiques spécifiques à un secteur sur mesure. Les données synthétiques garantissent la confidentialité et répondent aux défis liés au manque de données lors de l'adoption des technologies GenAI en générant des données d'entraînement artificielles plutôt que de s'appuyer sur des observations du monde réel. Ce processus implique différents modèles où l'IA de données synthétiques est entraînée une fois et peut produire des données synthétiques plusieurs fois pour divers cas d'utilisation, cas limites ou scénarios rares. Les données réelles sont utilisées avec parcimonie pour revérifier l'alignement du modèle et surveiller ses dérives, ce qui rend les données synthétiques précieuses dans des secteurs comme la santé et la finance. De plus, les IA qui génèrent des données synthétiques sont supervisées afin d'éviter les biais ou les erreurs de renforcement, ou d'introduire intentionnellement des biais et des erreurs pour renforcer des fonctionnalités telles que la prévention de la fraude.

Passer de la sécurité des données structurées à la sécurité des données non structurées

Cette évolution est nécessaire car les données non structurées gagnent en importance et en valeur à l'ère de la GenAI. Auparavant, les technologies de sécurité des données se

concentraient sur les données structurées comme les bases de données. Cependant, la capacité de la GenAI à traiter des données non structurées (texte, images, vidéos) a suscité un intérêt croissant, car elle sensibilise de plus en plus les clients finaux à la valeur de leurs données non structurées.

Besoin accru d'évaluer la posture de sécurité des données de GenAI

La capacité de GenAI à s'entraîner sur les données d'une organisation crée des risques d'accès ou de partage involontaire des données avec des fournisseurs ou des prestataires de services cloud. Cet entraînement engendre également des risques d'accès interne par sollicitation. D'où la nécessité de solutions de gestion de la posture de sécurité des données (DSPM) capables de détecter, d'évaluer et de surveiller l'accès de GenAI aux données, et de détecter les pipelines de données connectés en dehors de l'infrastructure organisationnelle. Les fournisseurs de DSPM améliorent rapidement leurs outils pour accompagner les organisations dans leur démarche d'utilisation sécurisée des services GenAI tiers et de sécurisation de l'accès aux données via des architectures GenAI personnalisées.

Pourquoi tendance :

La demande d' exploitation de GenAI, que ce soit par le biais de services tiers , d'applications métier existantes ou d'architectures GenAI sur mesure, ne cesse de croître, les organisations cherchant à identifier les domaines où l'IA peut créer le plus de valeur . Cependant, les inquiétudes concernant l'exactitude, la confidentialité et/ou la conformité des données constituent un obstacle majeur à l'adoption de GenAI .

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

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.

© 2025 Gartner, Inc. et/ou ses filiales. Tous droits réservés. Gartner est une marque déposée de Gartner, Inc. et de ses filiales. Cette publication ne peut être reproduite ou distribuée sous quelque forme que ce soit sans l'autorisation écrite préalable de Gartner. Elle présente les opinions de l'organisme de recherche Gartner, qui ne doivent pas être interprétées comme des déclarations de faits. Bien que les informations contenues dans cette publication proviennent de sources considérées comme fiables, Gartner décline toute garantie quant à l'exactitude, l'exhaustivité ou la pertinence de ces informations. Bien que les recherches de Gartner puissent aborder des questions juridiques et financières, Gartner ne fournit pas de conseils juridiques ou d'investissement et ses recherches ne doivent pas être interprétées ou utilisées comme telles. Votre accès et votre utilisation de cette publication sont régis par la politique d'utilisation de Gartner . Gartner est fier de sa réputation d'indépendance et d'objectivité. Ses recherches sont produites de manière indépendante par son organisme de recherche, sans apport ni influence de tiers. Pour plus d'informations, consultez les « Principes directeurs sur l'indépendance et l'objectivité ». Les recherches de Gartner ne peuvent pas être utilisées comme contribution à la formation ou au développement de l'intelligence artificielle générative, de l'apprentissage automatique, des algorithmes, des logiciels ou des technologies connexes.

© 2025 Gartner, Inc. et/ou ses filiales. Tous droits réservés.