Top Trends in Cybersecurity 2023

Published 17 March 2023 - ID G00782545 - 44 min read

By Analyst(s): Richard Addiscott, Alex Michaels, Jeremy D'Hoinne, Lisa Neubauer, Henrique Teixeira, John Watts, William Candrick, Wam Voster

Initiatives: Cyber Risk

> The renewed focus on the human element continues to grow in this year's top cybersecurity trends. Security and risk management leaders must rethink their balance of investments across technology, structural and human-centric elements as they design and implement their cybersecurity programs.

Additional Perspectives

- Invest Implications: Top Trends in Cybersecurity 2023 (23 March 2023)

Overview

Opportunities

- Security leaders improve the security of their digital ecosystem when they implement controls that take a holistic view of their increasingly fragmented attack surfaces and brittle identity infrastructure.
- Simplifying supply chain dependencies through careful evaluation and consolidation of vendor portfolios provides opportunities for security and risk management (SRM) leaders to enhance their ability to effectively respond to threats across their digital ecosystem.
- Adopting a composable approach to security architectures helps security leaders attain "secure by design." In parallel, proactive alignment of security operating models to support distributed ways of working and information risk decision making helps security leaders support accelerated business outcomes, while limiting cyber-risk expansion.
- Human-centered approaches to control design and implementation will reduce security failures caused by employee activities. Similarly, leveraging human-centered business communications and cybersecurity talent management will help to improve business-risk decisions and cybersecurity staff retention.

Recommendations

Security and risk management (SRM) leaders should:

- Adopt an attacker's mindset to prioritize cyber-risk mitigation efforts by taking an end-to-end view of the attack surface and consolidate vendor portfolios, where appropriate.
- Optimize the alignment of cybersecurity capabilities to new, distributed ways of working by adopting new security operating models and architectural approaches that foster agility and embed security by design.
- Prioritize and optimize investments in employee behavior improvement to enhance and sustain the efficacy of enterprise security.

Strategic Planning Assumptions

- By 2026, organizations prioritizing their security investments via a continuous threat exposure management program will suffer two-thirds fewer breaches.
- By 2027, identity fabric immunity principles will prevent 85% of new attacks and thereby reduce the financial impact of breaches by 80%.
- Through 2026, more than 40% of organizations — including two-thirds of midsize enterprises — will rely on consolidated platforms to run cybersecurity validation assessments.
- By 2027, 75% of employees will acquire, modify or create technology outside IT's visibility — up from 41% in 2022.
- By 2027, more than 50% of core business applications will be built using composable architecture requiring a new security paradigm.
- By 2027, 50% of large enterprise CISOs will have adopted human-centric security design practices to minimize cybersecurity-induced friction and maximize control adoption.
- By 2026, 60% of organizations will shift from external hiring to "quiet hiring" from internal talent markets to address systemic cybersecurity recruitment challenges.
- By 2026, 70% of boards will include one member with cybersecurity experience.

What You Need to Know

This year's Gartner Top Trends in cybersecurity show increased recognition of the importance of employee engagement in the security program to address cybersecurity risks and sustain an effective cybersecurity function. The increasingly distributed nature of work amplifies the adoption of cloud. In turn, this increases dependency on end-to-end visibility of expanding digital ecosystems and having resilient supply chains. In addition, CIOs are changing their IT operating models to foster enhanced business agility. The regulatory environment continues to evolve, forcing boards to take a more active role in managing cybersecurity risks. While ransomware payments are falling, [1] large-scale ransomware attacks and attacks on identity systems continue. These global trends are seeing leading security and risk management (SRM) leaders focus their efforts by:

1. Driving focus on the essential role of people for security program success and sustainability.

2. Implementing technical security capabilities that provide far greater visibility and responsiveness across the organization's entire digital ecosystem.

3. Restructuring the way the security function operates to enable agility without compromising security.

Rebalancing Practices:

The historical imbalance between the three traditional focus areas of cybersecurity controls — people, process and technology — is finally getting attention. Technology has long been the dominant focus for security leaders, however, the evidence is clear that a singular focus on technology is limiting the efficacy of cybersecurity risk reduction efforts. There is growing recognition that people have a far greater influence on security and risk outcomes, and program sustainability than previously acknowledged. The board's interest in cybersecurity continues to grow due to regulatory changes and a demand for improved, audience-centric and relevant communications from security leaders. Human centricity is now a crucial foundation for effective cybersecurity programs.

Responsive Ecosystems:

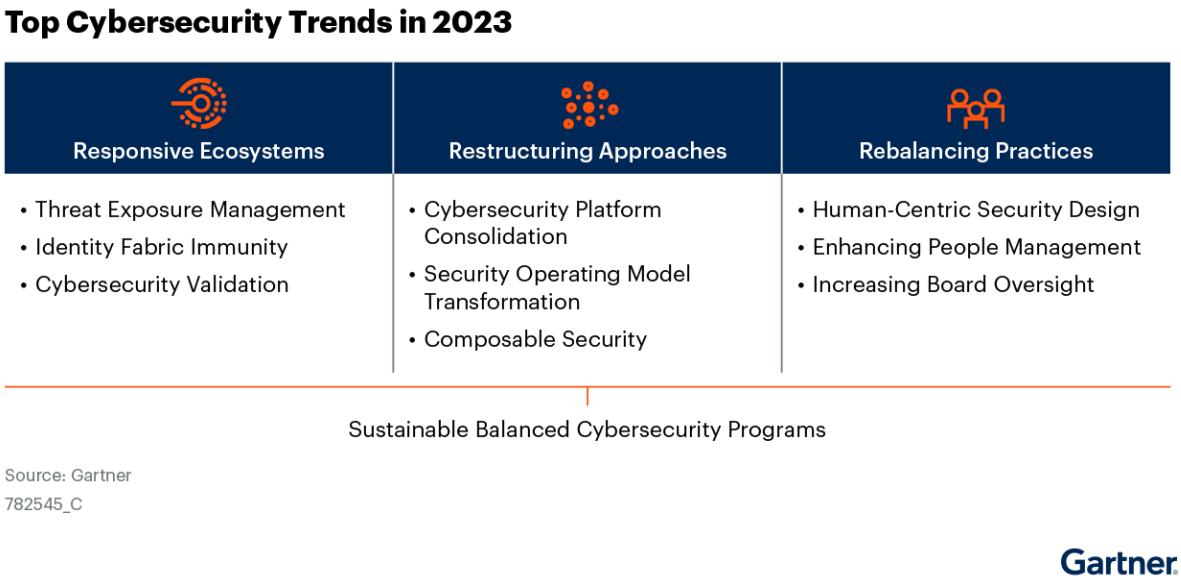
Expanding attack surfaces and threats against identity systems highlighted in Gartner's Top Trends in Cybersecurity 2022 continue into 2023. These persistent cybersecurity risks create challenges for SRM leaders' intent on keeping the security program in pace with the speed of business. There is a need to expand threat assessment horizons beyond the environment under the organization's direct control to include increasingly critical, and integrated, supply chains. As a result, it is no longer feasible to address every threat identified in an organization's digital ecosystem. Applying a continuous approach to threat management and cybersecurity validation is helping drive enhanced risk-centered remediation efforts. This approach enhances observability in brittle identity systems that, when coupled with elements of autoremediation, improve detection and response capabilities, and build more digitally immune identity ecosystems. This helps to improve organizational readiness and enable enhanced risk-prioritized remediation efforts.

Restructuring Approaches:

The increasing distribution of technology work (e.g., business technologists), hybrid work models becoming the norm, and accelerating digital transformation in response to shifting market conditions drive organizations to transform their security functions. Leaders are taking a strategic approach to consolidation of vendor portfolios to simplify operations and rationalize vendors in major domains of cybersecurity as their organizations face increasing challenges, both from the economy and threat landscape. Security platform consolidation within domains supported by more open integration with other platforms and point solutions enables a composable cybersecurity architecture. Security leaders can balance the need for operational simplicity with other platforms, and point solutions to cover more of their expanding attack surface.

SRM leaders seek to design and implement sustainable cybersecurity programs that provide an effective balance between people, process and technology. These 2023 trends should be considered holistically and not as a set of disparate phenomena that can be addressed in silos (see Figure 1).

Figure 1. Top Cybersecurity Trends in 2023



Trend Profiles: Click links to jump to profiles

Responsive Ecosystems	Restructuring Approaches	Rebalancing Practices
Threat Exposure Management	Cybersecurity Platform Consolidation	Human-Centric Security Design
Identity Fabric Immunity	Security Operating Model Transformation	Enhancing People Management
Cybersecurity Validation	Composable Security	Increasing Board Oversight

Threat Exposure Management

Back to top

Analysis by Jeremy D'Hoinne, Pete Shoard, Mitchell Schneider, Jonathan Nunez

SPA: By 2026, organizations prioritizing their security investments based on a continuous threat exposure management program will suffer two-thirds fewer breaches.

Description:

The attack surface of a modern enterprise is complex and fragmented, a symptom of evolving IT working practices (i.e., the use of SaaS). This creates diagnosis fatigue due to ever-growing and conflicting remediation priority lists. Enterprise CISOs sense the need to evolve their assessment practices to better understand their combined exposure to threats and address gaps in their posture. The use of continuous threat exposure management (CTEM) programs are emerging. CTEM is a pragmatic and effective systemic approach to continuously refine cybersecurity optimization priorities. CTEM programs expand traditional cybersecurity assessment to:

- Align the scopes of CTEM iterations with specific business risks and priorities.
- Address all vulnerabilities regardless if patches exist. This includes traditional, patchable vulnerabilities, but also more modern, unpatchable threat exposures that are relevant to these business risks and priorities.
- Validate the enterprise exposure and remediation priorities by weighing in the attacker's view.
- Shift expected outcomes from tactical and technical response to evidence-based security optimizations supported by improved cross-team mobilization.

Why Trending:

Zero-day vulnerabilities are rarely the primary cause of a breach. In other words, breaches could be prevented if organizations fix their exposure to a threat before an attacker exploits it. However, fixing every known vulnerability has always been operationally infeasible.

To solve this complex equation, CISOs must keep trying to continually evolve their assessment practices to keep up with their organization's digital velocity and evolving work practices. Recent attack trends highlight the need to evaluate appropriate risk-compensation methods, beyond traditional vulnerability remediation through patching, to adequately reduce enterprise threat exposure. CISOs must evaluate more than just technology vulnerability when trying to reduce the enterprise's exposure to threats. Security teams must also factor the risk-exposure of nonpatchable elements, such as human error, supply chain dependencies (SaaS platforms and third-party applications) and/or misconfigurations of their security controls. These factors have spurred the increased adoption of discovery tools and processes in an attempt to dynamically and continuously quantify the spread of their assets.

The proliferation of assessment tools, however, has amplified — rather than solved — the challenges of prioritizing the most relevant remediation actions.

To solve these challenges, security leaders must approach the problem differently, by changing how they scope exposure assessments, as well as how they approach remediation, which highlights the importance of appropriate compensations and interdepartmental team interactions. This gives no other choice to cybersecurity leaders other than changing how they scope exposure assessment and mobilize the required "remediation."

Implications:

Although many enterprises have some kind of vulnerability management program, it is often technology-centric and limited in its ability to mobilize resources beyond simple reporting, prioritization and semiautomated remediations. Building a CTEM program is a journey that should start with:

- Focusing on relevant scope before discovery: Multiple focused projects running simultaneously is more likely to succeed than attempting to address the entire attack surface at once.
- Validating exposure by taking the attacker's view.
- Better balancing strategic mobilization and tactical responses through cross-team relationship building.
- Combining patchable and nonpatchable issues for the same threat vectors and setting success metrics accordingly.

The outcome of the CTEM program will include different types of "treatments," such as technical mitigations, but "remediation" implies that the suggested course of action must also pass through the standard processes for risk acceptance, as well as operational viability. This requirement is the main reason why fully automated platforms are unlikely to emerge as the deus ex machina solution.

Actions:

- Select each CTEM cycle scope based on its alignment with business risks and required stakeholders for remediation and optimizations.

- Tackle threat exposure using emerging areas like attack surface management and security posture validation. When growing in maturity, start including assets that the organization has less control over, such as SaaS applications, data held by supply chain partners and suppliers' own dependencies.
- When expanding a vulnerability management program, get momentum with operational wins that frequently lie in improving the prioritization of findings through validation techniques.
- Integrate CTEM scopes with risk awareness and management programs to provide a relatable business-led focus to aspect.

Further Reading:

Implement a Continuous Threat Exposure Management (CTEM) Program

Predicts 2023: Enterprises Must Expand From Threat to Exposure Management

Identity Fabric Immunity

Back to top

Analysis by Henrique Teixeira, Michael Kelley, Erik Wahlstrom

SPA: By 2027, identity fabric immunity principles will prevent 85% of new attacks and thereby reduce the financial impact of breaches by 80%.

Description:

In 2022, Gartner introduced the importance of identity threat detection and response (ITDR) to fill gaps in infrastructure security and IAM controls when protecting the identity fabric against modern cyberattacks. ITDR assumes (and works best when) prevention steps were taken in the first place, before an attack.

The identity infrastructure in most organizations, however, is too brittle to survive a targeted attack. Over 80% of organizations have suffered an identity related breach in the last 12 months. [2] The fragility is in large part related to incomplete, misconfigured or vulnerable elements in the identity fabric. Because of this, most identity systems won't support a zero trust or identity-first security approach (see Identity-First Security Maximizes Cybersecurity Effectiveness).

Identity fabric immunity applies the concept of digital immune systems to identity systems (see Top Strategic Technology Trends for 2023: Digital Immune System). It not only protects the existing and new IAM components in the fabric with ITDR, but it also fortifies it by completing and properly configuring it.

Digital immunity concepts help to achieve this concerted and more balanced protection in two moments:

- Before an attack: With prevention mechanisms focused on hygiene and security posture management, as well as continuous threat exposure management (CTEM), of the identity fabric (see Implement a Continuous Threat Exposure Management (CTEM) Program). It includes discovery (through observability), configuration, attack surface and compliance management, and supply chain security.
- During an attack: With detection and response mechanisms, as described in Enhance Your Cyberattack Preparedness With Identity Threat Detection and Response, with elements of autoremediation and additional attention for site reliability engineering.

The main goal of adding digital immunity characteristics to the identity fabric is to minimize defects and failures, with balanced investments in prevention and in detection and response, for protection before and during attacks.

Why Trending:

The shift to identity-first security is driving a considerable investment in IAM infrastructure. [3] There is, however, an imbalance. Most organizations have failed to prepare identity systems to fulfill such a critical function:

- IAM systems are not properly configured (e.g., Microsoft reports that 78% of their Azure AD clients have not enabled MFA). [4]
- Excessive privileges is an ongoing problem (e.g., most IaaS users have far more entitlements than they will ever use). [5]
- There is no automated solution for disaster recovery in case of cloud identity provider failures. All existing strategies are expensive, complex and time-consuming (see Quick Answer: How Can We Reduce the Risks of SaaS-Based Identity and Access Management?).

- Supply chain attacks are on the rise. While 69% of organizations have invested in supplier risk management technologies for compliance and auditing, only 29% have deployed technologies for supply chain security (see Market Guide for Third-Party Risk Management Solutions).

Implications:

Organizations will build more resilient IAM systems if they make a concerted approach to:

- Plug holes (add missing pieces to the identity fabric)
- Avoid new holes (by properly configuring and cleaning it while it's built)
- Better detect and respond to attacks to the identity infrastructure

Without taking steps to protect the identity fabric, identity-first security initiatives will fail, as it requires consistency, context and continuity applied to identity. Likewise, Zero Trust initiatives cannot succeed with unreliable and fragile identity infrastructure.

Actions:

Organizations must take a cohesive, balanced approach to harden their IAM instructure, while making it less brittle and more resilient. For example:

- Tactical: Fix current holes by enforcing least privilege for high-risk access, removing dormant accounts and implementing phishing-resistant MFA.
- Strategic: Avoid new holes by implementing security posture management. Balance investment in prevention and in ITDR, and use what you have to its fullest potential by assessing IAM vendors' antifragile capabilities. Plan for failure and apply continuity management and CTEM.

Further Reading:

Top Strategic Technology Trends for 2023: Digital Immune System

Enhance Your Cyberattack Preparedness With Identity Threat Detection and Response

Identity-First Security Maximizes Cybersecurity Effectiveness

Cybersecurity Validation

Back to top

Analysis by Jeremy D'Hoinne, Mitchell Schneider, Jonathan Nunez and Pete Shoard

SPA: *Through 2026, more than 40% of organizations, including two-thirds of midsize enterprises will rely on consolidated platforms to run cybersecurity validation assessments.*

Description:

Cybersecurity validation is the convergence of techniques, processes and tools used to validate how potential attackers would actually exploit an identified threat exposure, and how protection systems and processes would react. Blue team and red team tools are converging toward high customization and flexible intrusiveness to test the enterprise's defenses — including the efficacy and configuration of security controls and monitoring tools — more effectively. The resulting insights enable easier cross-team decisions, including mobilizing decision makers to allocate relevant resources.

Why Trending:

Even security teams leading a clearly articulated security program still have to deal with a long list of prioritized treatments. Mature organizations continue to fail at triggering the required cross-team collaborative approach to remediate the highlighted issues. Cybersecurity validation assesses the likeliness of an attacker being successful, estimate the potential impact and identify if candidate responses would work as expected. Cybersecurity validation has commonly been limited to compliance-driven, infrequent and human-driven penetration testing engagement.

Cybersecurity validation tools are making quick progress to automate the highly repeatable and predictable aspects of assessments, enabling consistent and regular benchmarks of attack techniques, security controls and processes. The scope of cybersecurity validation includes:

- **Security effectiveness:** Red teaming activities to assess how much existing security controls can block and detect, leveraging attack simulation or semiautomated penetration testing.
- **Security consistency:** Automated and scheduled audits, such as analysis of security tool configurations or repeated attack scenario runs.

- **Incident response efficacy:** Evaluating the timeliness and effectiveness of response mechanisms by measuring time to investigate the tested attack scenarios.
- **User readiness:** Generally achieved through training, such as user awareness or tabletop and simulated exercises.

Cybersecurity validation platforms might embed or integrate into one of the capabilities mentioned below to gather additional insights, identify vulnerable attack paths or provide additional objectivity to overall risk posture:

- External attack surface management (EASM): EASM continues to be included as a feature, providing an outside-in view and enabling the simulation of the initial phases of an attack.
- Security Posture Management (SPM) tools: Shows the attack surface, often coming from insufficient hardening, of the assets to be tested.
- Digital risk prevention services (DRPS): Identifying leaked credentials, spoofing, domain sinkholing and other intelligence about digital risks to the organization.

The outcome of the process should then facilitate cross-team mobilization. To support that, converged cybersecurity validation tools output feasibility scores for various attack scenarios and/or attack paths, but also weighted scoring, based on feasibility and potential impacts.

Implications:

As more tools are available, organizations need to progressively expand their cybersecurity validation practices. They should start with narrower scope to gauge how much adding validating practices improves the ability to mobilize resources on remediation and optimization.

- Cybersecurity validation practices evolve quickly and platform consolidation is already happening.
- Breach and attack simulation (BAS) platforms are the preferred tools to carry out repeatable and consistent measurable assessments and refocus the scope of existing penetration testing engagements.

- Penetration testing and red teaming witnesses its own improvement, with PTaaS simplifying the administrative tasks and automated penetration testing tools augmenting existing pentesting/red team capabilities.

Actions:

- Embrace a cybersecurity validation approach to augment your existing workflows and enhance cybersecurity readiness.
- Go beyond security controls testing and evaluate the efficacy of procedures and processes.
- Scope validation to include the relevant threat vectors, but also the possibility of pivot and lateral movement.

Further Reading:

Quick Answer: What Are the Top and Niche Use Cases for Breach and Attack Simulation Technology?

Implement a Continuous Threat Exposure Management (CTEM) Program

Innovation Insight for Attack Surface Management

Cybersecurity Platform Consolidation

Back to top

Analysis by John Watts, Katell Thielemann, Henrique Teixeira, Frank Marsala

Description:

Organizations desire less complexity, simplify operations and make their staff more efficient. Vendors are consolidating into platforms around one or more major cybersecurity domains, such as Identity and Access Management, Network Security, Cloud Security, Data Security, Workspace Security, Cyber-Physical Systems and Security Operations. Many vendors are shifting their offerings to an as-a-service model, rather than a packaged product which leads to more single sourced infrastructure services. With fewer vendors, organizations benefit with improved staff efficiency, integration and more features from fewer products. However, as organizations reduce vendors, there comes concentration risk, higher pricing and operational impacts. It does not eliminate the need for integration between consolidated vendors. Organizations cite a growing concern for cyber resilience for security vendors as suppliers of key infrastructure services, such as identity and network security.

Why Trending:

This trend is driven by both demand and supply. Organizations want to reduce complexity and both suppliers and their customers face a potential "triple squeeze" of economic pressure, scarce expensive talent and supply chain challenges in 2023. [6]

On the demand side, Gartner observes interest by organizations who want to combine components where it makes sense, but support composable security through integration with other domains. For example, Security Service Edge combines formerly discrete point solutions for SWG and CASB. Some identity services now combine governance, privileged access and access management features in a common platform. CPS Protection Platforms now include asset discovery, inventory, topology mapping, with vulnerability management and network segmentation capabilities.

On the supply side, the availability of funding and growth in security markets led to an unprecedented proliferation of security vendors over the past few years. There are thousands of security vendors in the market today, but 2022 saw a reduction in funding and a rise in M&A transactions. [7] Small startups are facing increasing pressure and have seen staff reductions as demands for growth are replaced with the need to cut costs, generate cash flow and maximize profitability. [8,9]

The trend toward smaller companies being acquired and added to larger portfolio vendors is increasing as public offerings slow down and private equity firms continue acquiring vendors for restructuring. Further, larger vendors are rounding out their platforms by adding features to an integrated set of back-end and front-end services.

Implications:

Vendor consolidation yields benefits in better integration and more features available to deploy across the environment to address the organization's expanding attack surface. Staff may see improved efficiency in having to manage fewer integrations and benefit from improved analytics through back-end data sources, which are automatically ingested into the operational platform.

However, consolidation may lead to higher costs due to vendor lock-in, acquisition of more products than the organization can utilize an overlapping functionality. Fewer startups lead to potentially fewer innovations to emerging cybersecurity threats. Greater dependency on a single vendor for key operational security functions leads to a higher risk of operational downtime in the event of an outage.

Actions:

- Establish the ability to continuously inventory security controls to understand gaps and overlaps that exist to reduce the redundancy in consolidated platforms.
- Prefer platform vendors who commit to a broad ecosystem of partners to provide functions with out-of-the-box integrations in domains in which they may not meet requirements.
- Procure or retain smaller point solution vendors as requirements dictate, but create plans and contractual provisions for what to do if the vendor is acquired.
- Plan for increased costs in platform vendor portfolios as the cybersecurity industry faces the potential of a "triple squeeze" of high inflation, fewer vendors competing for the same opportunities and a shortage of engineering and other talent.

Further Reading:

9 Winning Actions to Navigate Inflation and Recession

Innovation Insight for Cyber-Physical Systems Protection Platforms

Top Trends in Cybersecurity — Survey Analysis: Cybersecurity Platform Consolidation

Transforming the Cybersecurity Operating Model to Support Value Creation

Back to top

Analysis by William Candrick, Christopher Mixter, Bernard Woo, Chiara Girardi

SPA: By 2027, 75% of employees will acquire, modify or create technology outside IT's visibility — up from 41% [10] in 2022

Description:

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. In fact, 41% [10] of employees now perform technology work in 2022 — a trend that will continue to grow exponentially over the next five years.

This trend directly impacts CISOs. For example, nearly three-fourths of cybersecurity leaders observed changes to risk decision rights and accountability in the past 12 months alone. Half of these leaders cite the need to facilitate business ownership of cybersecurity risk as a top driver for this change. [11]

Gartner is tracking a wide variety of changes to cybersecurity operating models, including:

- Changes to cybersecurity decision rights and accountability.
- New cybersecurity teams, functions and processes (e.g., DevSecOps, cloud security) to reflect evolving business environments.
- Policy changes to facilitate business ownership of risk decisions — such as coverage of new technologies, policy consolidation, increased policy flexibility, co-creation of policy with employees and policy automation.

Why Trending:

In 2022, business leaders have expressed their preference for more distributed technology work. Sixty-seven percent of CEOs want business functions to perform more technology work, and 73% of managers outside IT want more technologists on their teams. [12]

In fact, business leaders now widely accept that cybersecurity risk is a top business risk to manage — not a technology problem to solve. For example, 88% of board directors view cybersecurity risk as primarily a business risk, not a technology risk — up from just over half in 2016 compared to 2021. [13] Supporting and accelerating business outcomes is a core cybersecurity priority, yet remains a top challenge.

Distributed technology and analytical work exponentially expands the volume, variety and velocity of cybersecurity risk decision making. This expansion far exceeds what traditional cybersecurity operating models can support. For example, hands-on risk assessments, scheduled stop-gates and manual consultations cannot occur everywhere risk decisions are made.

To meet leadership expectations, cybersecurity operating models must transform to support and accelerate business outcomes — without creating undue cybersecurity risk or friction for the business and IT.

Implications:

CISOs must transform cybersecurity's operating model. Each component must fundamentally change to conveniently integrate into how work gets done at local levels. Consider the following implications:

- **Cybersecurity Is Becoming Human-Centric (Not Machine-Centric).** People — not technology — are the most significant factors in security outcomes. A significant portion of employees will become business technologists, meaning that cybersecurity risk decisions are increasingly made outside of cybersecurity's purview. Therefore, cybersecurity must think beyond technology and automation, and deeply engage with people to influence their decision making (see Quick Answer: Who Are Business Technologists?).
- **Your Attack Surface Will Only Expand.** The notion of "shrinking your attack surface" flies in the face of reality. The exponential expansion of business technologists means that your attack surface will expand as more people bring vulnerabilities into the business. Therefore, cybersecurity must support — rather than fight — distributed decision making, and adopt new mindsets, such as identity-first rather than perimeter-first security (see Identity-First Security Maximizes Cybersecurity Effectiveness).
- **Cybersecurity Theater No Longer Scales.** The size and complexity of the digital asset base has become so significant that the cybersecurity function can't keep up with the demand to pretend to protect everything, let alone actually do so (see Stop Performing Cybersecurity Theater: It Is No Longer Scaling).

- **The CISO's Role Must Fundamentally Change.** Only 16% of CISOs consider themselves control owners, down from 44% in 2021; and 37% of CISOs are now risk decision facilitators, up from 24%. [11] This has encouraged CISO's to experiment with a variety of different approaches to both centralized and independent security decisioning.

Actions:

- **Deliver Security as a Core Feature — Not a Requirement:** Cybersecurity risk is one of many risks employees must balance — including financial risk, reputational risk, competitive risk, legal risk, etc. Look for new ways to deliver security based on how and where work gets done.
- **Empower People to Make Independent Risk Decisions.** Go beyond traditional security awareness training to facilitate independent cyber judgment at scale. This requires building decision-making competence and providing tools and playbooks so that business technologists can independently make risk-informed decisions.
- **Establish Governance Structures to Support Cyber Judgment.** Risk decisions cannot be made in isolation. Implement a representative enterprise security steering committee supported by clearly defined risk acceptance, policy exemption and conflict resolution processes.
- **Connect Cybersecurity to Business Value.** Measure, assess and report cybersecurity's success against business outcomes and priorities — rather than operational activity.

Further Reading:

Cyber Judgment Presents a New Approach to Informed Risk Decision Making

Case Study: Framework to Enable Business Ownership of Cybersecurity Activities

Innovation Insight on Security Behavior and Culture Program Capabilities

Composable Businesses Need Composable Security

Back to top

Analysis by Wam Voster

SPA: By 2027, more than 50% of core business applications will be built using composable architecture requiring a new security paradigm.

Description:

Designed to protect composable business, composable security is an approach where cybersecurity controls are integrated into architectural patterns, and then applied at a modular level in composable technology implementations. Many organizations rely on traditional monolithic systems like ERP to deliver functionalities to the business, which have been designed to address the challenges from the past. To enable an organization to respond to the accelerating pace of business change, it needs to build modular capabilities in their applications.

This applies to all aspects of a business process, no matter whether it is products, assets, inventory orders or any other process. This means that the organization should be made from interchangeable building blocks. These blocks are often referred to as Packaged Business Capabilities (PBC) or elements. The key advantages of a composable organization are:

- Faster innovation.
- Greater agility through modularity.
- Business resilience.
- Platform ecosystem.

To support this, composable organizations need to rely on composable architecture and composable applications. Composable applications are applications built from these modular components. These modular components can interact with each other through well-defined and powerful APIs, and compose together to deliver business functionality. An authorization protocol like OAuth — currently used for services like Amazon, Google, Facebook, Microsoft and Twitter — will be used to facilitate access to these modular components resources on behalf of a resource owner without revealing passwords.

Why Trending:

Composable approaches to building digital capabilities continue to trend with the increasing deployment of composable business. Composability is an emerging strategy to increase business agility in response to dynamic market conditions. The roles involved in creating this composability are described in detail in the Quick Answer: How to Organize Roles for Governance of Composable Applications. In that note, the four C's are introduced as: Creators, Curators, Composers and Consumers. Creators create new components, Curators create a catalog of components and may create a marketplace (a "Component store" analog to an "App store"). Composers select a number of components and string those together to create a business application. The Consumers are the (internal and external) users of the composed applications.

CISOs should realize that the creation of applications with composable components will introduce undiscovered dependencies. More importantly, however, it will open up the door to allow unapproved external services to have access to whatever the users opening the door have access to. Traditional security methods will not be able to detect these issues, let alone be able to trace the root cause down to the composable component level. This is especially the case, since the blocks that comprise the application may, in fact, be cloud-native blocks.

Furthermore, while each component of the solution may be secure, the interaction between the composable components, and the data exchanged between them, can introduce new risks. Security efforts must therefore include API-centric approaches, as well while understanding the entire application context at the same time. This means that monitoring user behavior alone is not enough — detecting unexpected API behavior is just as critical. On top of that, the infrastructure substrate in which the composable apps operate needs to be included as well.

Implications:

The key benefit for CISOs is that this is a significant opportunity to embed privacy and security by design, and to create component based, reusable security control objects linked to security architecture reference patterns. Further, once the Component-Store Block store is populated with components that have been vetted by security, Composers and Consumers can deploy new applications or new business functionality much faster as security has been "moved left." New business functionality is delivered faster and more secure at the same time.

Actions:

- Identify whether any initiatives related to composable architecture are underway in your organization.
- Make sure that the CISO is included as the “Fifth C” in the process like the Creator, Curator, Composer and Consumer.
- Create a (internal) process to assess, test and vet building blocks and APIs to ensure that composable business applications are secure by design.
- Realize that, similar to Open Source libraries today, the use of external components and internal components exposed to the outside world create a new threat vector.

Further Reading:

Quick Answer: How to Organize Roles for Governance of Composable Applications

Top Strategic Technology Trends for 2023: Superapps

Human-Centric Security Design

Back to top

Analysis by Richard Addiscott, Christine Lee, Tom Scholtz

SPA: 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:

Human-centric security design (HCSD) prioritizes the role of employee experience — rather than technical considerations alone — across the controls management life cycle. Drawing upon the behavioral sciences, user-experience (UX) and related disciplines, HCSD specifically helps minimize one of the biggest causes of insecure employee behavior: cybersecurity-induced controls friction — real or perceived. Examples of HCSD include application of behavioral and UX principles (e.g., intuitiveness, ease of use) to control design, co-creating security controls with employees and providing risk-appropriate controls flexibility so individuals have multiple ways to achieve secure outcomes without compromising business objectives.

Why Trending:

Traditional security awareness programs have failed to reduce unsecure employee behavior. Gartner's 2022 Drivers of Secure Behavior Survey [14] found that 69% of employees intentionally bypassed their organization's cybersecurity guidance in the last 12 months. Further, over 90% of survey respondents who admitted behaving in an unsecure way acknowledged that they knew that their actions would increase cybersecurity risk levels for the organization and did it anyway.

If employees are aware of cybersecurity risk, why do they still behave unsecurely? Gartner research shows that 74% of employees would bypass a security control if it helps them, or their team, achieve a business objective. This should come as no surprise when employees are paid to deliver outcomes and any perceived or actual cybersecurity-induced friction impacts their ability to do so efficiently and/or effectively.

Implications:

Cybersecurity teams looking to leverage HCSD for the first time will need to brace themselves for new ways of thinking and operating by:

- **Shifting their mindsets.** Cybersecurity professionals are trained to think technically and/or operationally ("Is the control working as defined?"). It will take proactive engagement with UX practitioners and new metrics around employee experience to encourage a shift to human-centric security design thinking ("How are employees experiencing the control?").
- **Acquiring access to nontraditional capabilities.** HCSD may require an initial investment of UX expertise, which can often be sourced internally. UX departments — which source talent from human psychology, cognitive neuroscience, product design, journalism and related fields — are becoming commonplace across organizations.

Santander's (see Case Study: User-Experience-Focused Cybersecurity Design (Santander)) and SevenHills'* (see CISO Foundations: 4 Actions CISOs Must Take to Reduce Cybersecurity-Induced Friction) experience shows that effective implementation of HCSD techniques can increase adoption of desired behaviors, such as:

- Reporting suspicious incidents and emails
- Not installing unapproved third-party software
- Increased voluntary participation in cybersecurity initiatives

HCSD has also helped minimize resistance to change when new critical security capabilities are introduced that require modifications in employee behavior. For example, enterprisewide initiatives introducing new authentication methods often introduce friction. Organizations that leveraged HCSD techniques from the beginning have reported improved employee buy-in and control adoption.

The positive outcomes achieved above demonstrate the value and importance of inviting employees to contribute to the design and implementation of security controls that:

- Leverage empathy-based engagement where collaboration is intentional.
- Help facilitate a more flexible security experience.
- Consider ethical considerations to ensure security technology meets accessibility requirements and does not erode employee well-being or trust through manipulative techniques (e.g., nudge defaults when employees ought to be deliberating) or attention capture (e.g., unwarranted push notifications).

Actions:

- Review past cybersecurity incidents, control violations and exception requests to help identify major sources of cybersecurity-induced friction. Consider where you can ease the burden for employees through more human-centric controls redesign, or even retiring controls that add friction without meaningfully reducing risk.
- Evaluate the existing security roadmap. Identify an initiative likely to result in change to the user experience and leverage human-centric design practices with employees impacted by the initiative. Like SevenHills*, invite employees from across impacted user cohorts to co-design cybersecurity controls to ensure the employee experience is considered from the outset (see CISO Foundations: 4 Actions CISOs Must Take to Reduce Cybersecurity-Induced Friction).
- Upskill security staff in how to deliver more empathy-driven, outcomes-focused UX practices. Evaluate the success of these efforts by supplementing technical and operational cybersecurity control metrics with outcome-driven indicators that help measure the employee experience.

Further Reading:

CISO Foundations: Build a Culture of Security Consciousness: Introducing the Gartner PIPE Framework

Case Study: User-Experience-Focused Cybersecurity Design (Santander)

CISO Foundations: 4 Actions CISOs Must Take to Reduce Cybersecurity-Induced Friction

Enhancing People Management for Security Program Sustainability

Back to top

Analysis by Alex Michaels & Deepti Gopal

SPA:

- By 2026, 60% of organizations will shift from external hiring to “quiet hiring” from internal talent markets to address systemic cybersecurity recruitment challenges.

Description:

In light of the continuing global talent shortage, cybersecurity leaders are going beyond workforce architecture and shifting focus to human-centric talent management tactics to attract and retain talent. CISOs who prioritize these new and innovative tactics have seen improvements in their functional and technical maturity. Some of the most impactful cybersecurity talent management tactics include internal marketplaces, custom development paths and differentiating their employee value propositions by adding incentives that are tailored to employee preferences.

Why Trending:

Security Expert Marketplace and Attraction Drivers: Gartner research has revealed that the demand for security experts far exceeds the supply in almost every role. With this in mind, it is crucial to recognize the importance of retaining those that already are a part of your team. The current job market gives employees more power and knowledge to seek out opportunities that align with their personal preferences. Traditionally, cybersecurity leaders depended heavily on their workforce plans which were designed to satisfy their point in time objectives. It is essential for these leaders to layer this approach by considering team members' preferences, as well as the top drivers of attraction [1 5] where they may be lacking, such as compensation, development opportunity and future career opportunities. These glaring improvement areas emerged from a study on the market for technology workers including the cybersecurity function.

CISO Effectiveness: Cybersecurity leaders have traditionally focused heavily on improving the technology and processes that support their programs, with little to no focus on the people that drive these changes. To be effective, in addition to continuing to focus on technology and process improvements, cybersecurity leaders must also prioritize human-centric tactics that support strategic workforce planning. These tactics should not be confused with standard staff management practices. Rather, they are focused on tangible practices that have a proven track record of improving talent attraction and retention.

Cyber's Elevated Position: The Gartner View From the Board of Directors Survey for 2022 shows that 88% of boards of directors see cybersecurity as a business risk. Additionally, 54% regularly include cybersecurity on their meeting agendas. Security teams have become a vital part of most organizations. However, raising interest in redefining the cybersecurity employee journey seems to still be a challenge.

Implications:

Cybersecurity leaders who incorporate people management tactics into their strategic workforce plans must consider the following challenges and opportunities:

Challenges:

- Most human resources functions are not "cyber savvy" enough to provide meaningful support to cybersecurity leaders. HR often looks at IT and cybersecurity as the same thing, even though in terms of compensation, entry-level cybersecurity is midtier IT.

- Difficulty in creating an **employee value proposition** (EVP) that is differentiated from competitors, as well as actionable and measurable. While compensation is one of the leading drivers of attraction, it is not the only lever for impacting positive change.
- Resistance to changes to HR processes within rigid organizational cultures.

Opportunities:

- Increased engagement and effort from employees, including new hires.
- Showing employees that the company values them as individuals.
- Lowering annual employee turnover.
- Attracting top talent through a strong EVP.
- Supporting diversity, equity and inclusion initiatives.

Actions:

To retain and attract top experts and ensure the success of the cybersecurity function, it is crucial for CISOs to take the following actions:

- At a minimum**, conduct security workforce planning** to identify talent gaps and competencies that map to long-term organizational goals, as discussed in Ignition Guide to Creating a **Strategic Workforce** Plan for Cybersecurity. Create tailored training and professional development to help develop the necessary skills, competencies and knowledge for current and future leaders to excel in their roles and contribute to the success of the organization.
- Develop a **human-centric and inclusive cybersecurity program by leveraging the talent management life cycle.** Cybersecurity leaders should work closely with HR to redefine your cybersecurity EVP, as well as prioritize building strong relationships with their direct reports. This includes actively promoting recognition and appreciation for each employee's contributions within the organization. Starting by viewing employees as individuals and not just as a resource.

- **Prioritize cybersecurity talent strategy as a top five initiative to increase your effectiveness as a Cybersecurity leader.** This means reframing the way Cybersecurity leaders think about staff management. Effort should be made to pull levers that have a clear line of sight to measurable and proven retention, and attraction growth.

Further Reading:

Using a Digital Talent Management Framework to Future-Proof the IT Workforce

Ignition Guide to Developing and Communicating an EVP for Technology Talent

Renew Retention Strategies to Retain Technology Talent for Digital Business Success

Offer a 'Human Deal' to Attract and Retain IT Talent Amid the Great Resignation

Boards Expand Their Competency in Cybersecurity Oversight

Back to top

Analysis by Lisa Neubauer, Paul Furtado, Michael Kranawetter

SPA: By 2026, 70% of boards will include one member with cybersecurity experience.

Description:

The board's increased focus on cybersecurity (see Security Operating Model Transformation) is being driven by the trend toward explicit director-level accountability for cybersecurity to include enhanced responsibilities for board members in their governance and oversight activities. This trend will require additional cybersecurity expertise on boards going forward. Our 2022 Board of Directors Survey shows that only 50% of boards today have someone with cybersecurity knowledge or experience. [13]

Cybersecurity leaders need to provide boards with appropriate and meaningful reporting that demonstrates an understanding of the impact that the cybersecurity program has on an organization's ability to meet its goals and objectives.

The most effective cybersecurity leaders translate technically focused reporting into reporting conveyed in a risk management context. They ensure the continuous improvement of reporting processes and procedures to verify that information is relevant and accurate. They also ensure that visualizations and charts are used appropriately to make complex information easier to understand to drive informed decision making, and that it is clear where and when relevant decisions need to be made. Cybersecurity leaders must focus on providing cybersecurity reporting that is informative, actionable and aligned to business outcomes.

Why Trending:

Gartner reviews hundreds of cybersecurity board presentations annually. We find that what most organizations report to their boards does not provide the board with the appropriate information to conduct the proper level of oversight and/or drive decision making in today's environment.

For example, despite ever-increasing cybersecurity breaches and regulatory changes, nonexecutive board of directors surveyed report that they are willing to accept greater risk to generate additional growth through expanding product lines, or due to the long-term economic uncertainty that is affecting the business. [16]

For cybersecurity leaders to be recognized as business partners like their executive peers, cybersecurity leaders need to ensure that the board's enterprise risk appetite is defined. CISOs must also become adept at demonstrating how the cybersecurity program prevents unfavorable things from happening, and how cybersecurity improves the enterprise's ability to take risks effectively.

Implications:

Cybersecurity leaders must transition to a balanced reporting approach that demonstrates how the cybersecurity program supports the organization in achieving its goals and objectives. This can be accomplished through the creation of a cybersecurity strategy. Doing so will provide the cybersecurity leader with the ability to effectively communicate cybersecurity risk and the value of the cybersecurity program to their boards and:

- Rightsize investment in controls
- Influence and drive secure behaviors and culture
- Improve personal effectiveness

- Secure a defensible budget

For example, boards do not care about patch deployment rates. What they do care about is how long critical systems are exposed to a compromise of confidential information or potential disruption to operations, which all relate to the three areas they care about most: revenue, cost and risk. Communicate in the language of "we are uncomfortably exposed and another $1M will get us down to a comfortable level."

Actions:

Review current cybersecurity reporting for the board and assess whether it:

- Links cybersecurity strategy to the organization's business goals and objectives.
- Highlights the potential cybersecurity risks and opportunities to the organization in meeting its goals and objectives.
- Uses various mechanisms to monitor changes in cybersecurity risks against defined risk appetite and tolerance levels.
- Includes supporting documentation in an appendix for board members who would like more detailed information on items presented. This can include previously presented dashboards with Key Performance Indicators (KPIs) or more operationally focused metrics.
- Provides an opportunity to clarify common leadership misconceptions, two of which are:
  - "Cyber risk is cybersecurity's problem" to "Cybersecurity risk is a business risk"
  - "Security is a roadblock to speed" to "Security facilitates agile and secure projects"
- Encourages active board participation and engagement in cybersecurity decision making and provides recommendations for actions to be taken by the board, including allocation of budgets and resources.

Further Reading:

- CISO Foundations: Comprehensive Resource List for Presenting Cybersecurity to the Board of Directors

- Effective Metrics Practices for Cybersecurity Leaders
- Tool: Board Briefing - How to Communicate the Cyber-Risk Posture of your Organization
- 5 Corporate Governance Trends Affecting the Board's Oversight Role in 2023

Evidence

[1] Ransomware Revenue Down As More Victims Refuse to Pay, Chainalysis.

[2] 80% of Firms Suffered Identity-Related Breaches in Last 12 Months, Dark Reading.

[3] Access management is the second fastest growing segment in the entire cybersecurity industry, at 33.5%: Market Share Analysis: Security Software, Worldwide, 2021

[4] Microsoft Says MFA Adoption Remains Low, Only 22% Among Enterprise Customers, The Record.

[5] Cloud infrastructure entitlements are often overly permissive, with 95% of users in IaaS using less than 2% of their entitlements: Innovation Insight for Cloud Infrastructure Entitlement Management

[6] 2023 CIO and Technology Executive Agenda: Navigating the Triple Squeeze for CSPs

[7] SecurityWeek Analysis: Over 230 Cybersecurity M&A Deals Announced in First Half of 2022, SecurityWeek.

[8] Cybersecurity Startups, Once the VC Darling, Hammered by Layoffs, TechCrunch.

[9] Layoffs Mount as Cybersecurity Vendors Hunker Down, Dark Reading.

[10] 2020 Gartner Digital Friction Survey; 2021 Gartner Reimagining Technology Work Survey

The 2020 Digital Friction Survey was conducted via an online survey platform with a total of approximately 4,500 panel participants. The survey was developed collaboratively by a team of Gartner researchers and was reviewed, tested, and administered by Gartner's Quantitative Analytics and Data Science.

To determine the most impactful drivers of digital friction, we used regression-based maximum impact analysis to assess the impact of over 130 factors, ranging from organizational practices to leadership behaviors and mindsets. Maximum impact shows the most amount of improvement in reducing digital friction an organization can realize by improving each factor. **Note:** the results of this study are representative of the respondent base and not necessarily the market as a whole.

The 2021 Gartner Reimagining Technology Work Survey was conducted via an online platform in March 2021 among over 6,000 employees across functions, levels, industries and geographies. The survey examined the extent to which employees outside of IT were involved in customizing and building analytics or technology solutions, the types of activities they performed, the teams and structures they worked in, and the types of support they received, among others. To determine the key factors that help business technologists be more successful, we used logistic regression analysis to assess the impact of over 150 factors on successful achievement of business technologists' key objectives.

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

[12] **The 2021 Gartner Technology Skills Outside of IT Survey** was conducted via an online platform between November and December 2021 among over 3,000 employees across functions, levels, industries and geographies. The survey was designed to understand the role that CIOs should play to support employees who produced analytic or technology capabilities and reported to a business area outside of IT. Results do not represent "global" findings or the market as a whole but reflect sentiment of the respondents and companies surveyed.

[13] **The 2022 Gartner View From the Board of Directors Survey:** This survey was conducted to understand how boards of directors (BoDs) will address the risk from economic and political volatility and a multipolar world, and their intent to convert digital acceleration to digital momentum. The survey also helps understand the impact of the key societal issues that took center-stage during the pandemic on BoDs' strategy and investment approaches. The survey was conducted online from May through June 2021 among 273 respondents from the U.S., Europe and Asia/Pacific. Companies were screened to be midsize, large or global enterprises. Respondents were required to be a board director or a member of a corporate BoD. If respondents serve on multiple boards, they answered for the largest company, defined by its annual revenue, for which they are a board member. Disclaimer: Results of this survey do not represent global findings or the market as a whole, but reflect the sentiments of the respondents and companies surveyed.

[14] The 2022 Gartner Drivers of Secure Behavior Survey was conducted via an online platform from May through June 2022 among 1,310 employees across functions, levels, industries and geographies. The survey examined the extent to which employees behave securely in their day-to-day work, root causes of unsecure behavior, and the types of support and training that they received 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 ability to develop cyber judgment.

[15] **The Gartner 4Q22 Global Labor Market Survey** indicated that the attraction drivers for top talent among cybersecurity professionals — compensation, work-life harmonization, respect, technology level, future career opportunities, retirement benefits, vacation, location, health benefits.

The Gartner Global Labor Market Survey is a panel survey conducted by the Gartner HR practice on a monthly basis. Gartner collects 6,000 responses per month from employees across regions, industries, functions and seniority levels. IT employees usually make up ~10% of the sample.

The survey tracks key employee metrics overtime that include: discretionary effort, employee value proposition, confidence in economic situations and job prospects, job seeking behavior, and pay expectations. It is a rich dataset that can be used to inform CIOs about the latest IT labor market trends.

[16] **The 2023 Gartner Board of Directors Survey on Business Strategy in an Uncertain World:** This survey was conducted to understand the new approaches adopted by nonexecutive boards of directors (BoDs) to drive growth in a rapidly changing business environment. The survey also sought to understand the BoDs' focus on investments in digital acceleration; sustainability; and diversity, equity and inclusion. The survey was conducted online from June through July 2022 among 281 respondents from North America, Latin America, Europe and Asia/Pacific. Respondents came from all industries, except governments, nonprofits, charities and NGOs, and from organizations with $50 million or more in annual revenue. Respondents were required to be a board director or a member of a corporate board of directors. If respondents served on multiple boards, they answered for the largest company, defined by its annual revenue, for which they are a board member. Disclaimer: The results of this survey do not represent global findings or the market as a whole, but reflect the sentiments of the respondents and companies surveyed.

Recommended by the Authors

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

Case Study: Framework to Enable Business Ownership of Cybersecurity Activities

Improve IAM Architecture by Embracing 10 Identity Fabric Principles

Quick Answer: How Can We Reduce the Risks of SaaS-Based Identity and Access Management?

Responsive Ecosystems	Restructuring Approaches	Rebalancing Practices
Threat Exposure Management	Cybersecurity Platform Consolidation	Human-Centric Security Design
Identity Fabric Immunity	Security Operating Model Transformation	Enhancing People Management
Cybersecurity Validation	Composable Security	Increasing Board Oversight