Gartner Research

Top Trends in Cybersecurity 2022

By Peter Firstbrook, Sam Olyaei, Pete Shoard, Katell Thielemann, Mary Ruddy, Felix Gaehtgens, Richard Addiscott, William Candrick

18 February 2022

Gartner®

Top Trends in Cybersecurity 2022

Published 18 February 2022 - ID G00760806 - 26 min read

By Analyst(s): Peter Firstbrook, Sam Olyaei, Pete Shoard, Katell Thielemann, Mary Ruddy, Felix Gaehtgens, Richard Addiscott, William Candrick

Initiatives: Cybersecurity and IT Risk; Infrastructure Security

> The endlessly expanding digital footprint of modern organizations is driving this year's top cybersecurity trends. Security and risk management leaders who understand these trends will be better able to address new risks and elevate their standing in their organizations.

Additional Perspectives

- Invest Implications: Top Trends in Cybersecurity 2022 (23 February 2022)

Overview

Opportunities

- Security leaders who redefine the cybersecurity function and technology architecture are positioning the business to maintain and increase value in an increasingly agile, distributed and decentralized environment.
- Organizations that push cybersecurity decision making out to the business units are improving their security posture, even as digital scale and complexity increase.
- Security education that emphasizes organizational cultural change and fosters better cyber judgment is the most effective way to avoid social engineering incidents and poor decisions about business technology.
- Security product consolidation and the cybersecurity mesh enable leaders to build a more efficient and integrated security infrastructure for the expanding attack surface.

Recommendations

Security and risk management leaders who wish to better address new risks should:

- Decentralize decision making to empower business leaders, other cybersecurity leaders and employees to make informed risk decisions.
- Prioritize tools that are able to interoperate and provide more complete implementations of standards.
- Anticipate the continuous expansion of the enterprise attack surface, and increase investment in processes and tools for identity threat detection and remediation and digital supply chain integrity.

What You Need to Know

Gartner's Top Trends for Cybersecurity in 2022 emerged from the challenges inherent in protecting the ever-expanding digital footprint of modern organizations. The pandemic response has accelerated hybrid work and the digitalization of business processes in the cloud, both of which introduce new security challenges. Concurrently, last year experienced sustained big game ransomware attacks, multiple attacks on the digital supply chain, deeply embedded vulnerabilities, and increasing attacks on identity systems. These accumulated security challenges are compounded by a shortage of skilled security staff. These events are impacting cybersecurity practice in three primary ways (see Figure 1):

1. The evolution and reframing of the security practice
2. Rethinking technology
3. New responses to sophisticated new threats

Reframing the Security Practice

The dramatic changes in scope, scale and complexity of the modern digital organization has obsoleted the centralized approach to cybersecurity control. New cybersecurity leaders are being placed in different parts of the organization to decentralize security decisions.

Business technologists are making significant IT decisions, and social engineering continues to grow as a source of successful attack. For these and other reasons, traditional approaches to security awareness training are becoming embarrassingly ineffective. Distributing security responsibility requires a reconsideration and refocus of security awareness programs to enable more sophisticated security thinking. Progressive security and risk management (SRM) leaders are investing heavily in security behavior and culture programs fostering new ways of thinking and embedding new behaviors to help secure the organization.

Rethinking Technology

Gartner clients increasingly express frustration with the operational complexity of the modern security stack. Given the human capital constraints, efficient cybersecurity remains out of reach for the majority of organizations. As such, there is an increased desire to consolidate security products into multifunction solutions addressing a broad set of related challenges, such as securing “hybrid work” or “cloud workloads.” Across a range of security domains, integration capabilities such as secure access service edge (SASE) and extended detection and response (XDR) are leading to enhanced product integration. The security market will never be completely consolidated, however. As a result, we see the cybersecurity mesh architectural conceptualization illustrate how heterogeneous solutions can integrate through emerging standards.

Responding to New Threats

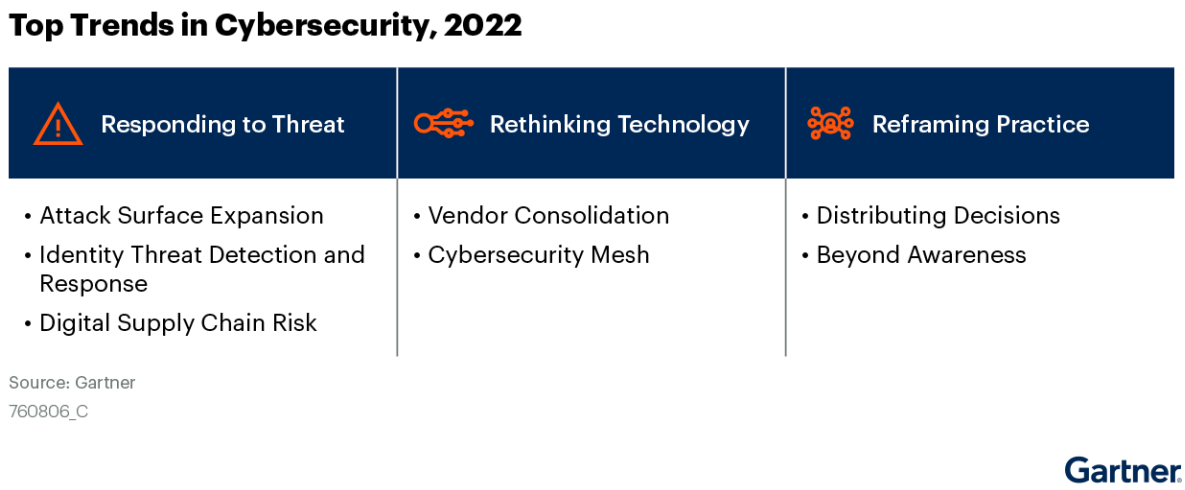
The expanding digital footprint introduces gaps in inventory and data collection, which inevitably weakens preventative controls, business continuity plans, data protection, monitoring and incident response capabilities. The lack of visibility across the expanding environment of an organization leads to more enterprise blind spots, some of which are exploited by attackers. During the last year, two alarming changes in the attack landscape became more obvious. The first significant attack domain involves the exploitation of identity. Unsurprisingly, acceleration of credential misuse continues, leading to a tragic increase in security incidents. Even more disturbing, advanced attackers are increasingly attacking and attempting to exploit the identity system. This can provide a successful attacker with unprecedented levels of access while making detection and response significantly more difficult. The second noteworthy attack domain is the digital supply chain. Vulnerabilities that are deeply embedded in the digital supply chain are often extremely difficult to detect, and thousands of applications or devices may be simultaneously impacted. As a result, Gartner recommends that cybersecurity teams pay increasing attention to two emerging security domains:

- Identity threat detection and response

- Digital supply chain integrity

These trends don't exist in isolation; they build on and reinforce one another. We selected our trends for 2022 in part based on the combined effects of these trends. Taken together, attention to our top cybersecurity trends will help security and risk management leaders evolve their roles to meet future challenges and elevate their standing in their organizations.

Figure 1. Top 2022 Trends in Cybersecurity.



Attack Surface Expansion

Analysis by Pete Shoard

Description:

Organizations needs to look beyond vulnerability patching to manage a wider set of security "exposures." A dramatic increase in attack surface is emerging from changes in the use of digital systems, including new hybrid work, accelerating use of public cloud, more tightly interconnected supply chains, expansion of public-facing digital assets and greater use of operational technology (Cyber Physical Systems [CPS]).

Why Trending:

As enterprises update their IT and security programs for more modern work practices, organizations must acknowledge that hybrid working is the future. Currently, 60% of knowledge workers are remote, [1] and at least 18% of users will not return to the office. These changes in the way we work have created new and challenging attack surfaces. Concurrently, rapidly increasing digital processes have expanded the diversity and complexity of mission-critical systems. Risks associated with open-source code, IoT physical systems, cloud workloads, SaaS applications, social media and more have exponentially increased the exposed surface of an organization beyond the traditional set of controllable assets. These changes introduce gaps in coverage for log data collection, preventative controls, business continuity plans, data protection, monitoring and incident response capabilities. The lack of visibility across the expanding digital environment leads to an increase in exploitable blind spots.

Implications:

Traditional approaches to security monitoring, detection and response need to shift significantly to address the risks posed by new technologies and business initiatives. Enterprises should begin to look at the value placed on areas that may currently seem inconsequential, like the increases to the attack surface brought about by users connecting to new applications and services outside the corporate perview. Digital risk protection services (DRPS), external attack surface management (EASM) technologies and cyber asset attack surface management (CAASM) can help visualize the external and internal parts of the business that enable systems and thus automate the discovery of some of the gaps in coverage.

Organizations must begin to think about security strategies beyond the traditional “castle-keep” scenarios and take action to increase security visibility and risk mitigation of critical business functions.

Actions:

- Perform an enterprise attack surface gap analysis to detect potential blind spots in monitoring, products and processes in the security operations center (SOC) and incident response processes.
- Evaluate attack surface management (ASM) technologies to visualize the external and internal parts of the business that enable systems and thus automate the discovery of some of the gaps in coverage.

- Consider simulation technologies that provide an attacker perspective, such as breach and attack simulation (BAS), to provide regular assessment of uncontrollable security configuration change and emerging threats.
- Test response planning more frequently and iteratively to keep up with the pace of change of both architecture and the threat landscape.

Further Reading:

- Competitive Landscape: Digital Risk Protection Services
- Hype Cycle for Security Operations, 2021
- Emerging Technologies: Critical Insights for External Attack Surface
- Management Quick Answer: What Are the Top Use Cases for Breach and Attack Simulation Technology?

Identity Threat Detection and Response

Analysis by Mary Ruddy

Description:

In 2021, Gartner identified the urgency of treating “Identity as the new perimeter” as a top trend. This trend was reinforced during the year by multiple events that illustrated the extent to which the identity system itself is coming under sustained attacks. A primary objective of all advanced attacks is to gain privileged credentials to achieve their goals.

This year, we are introducing a new term, “identity threat detection and response” (ITDR) to describe the collection of tools and best practices to successfully defend identity systems from endemic levels of attacks. Much like network and endpoint detection and response tools, ITDR tools support discovery and inspection, provide analysis capabilities, enable policy evaluation, and provide incident management and remediation suggestions to restore affected systems.

Why Trending:

The more-sophisticated attackers are now actively targeting the IAM infrastructure itself. For instance, the SolarWinds breach used administrative permissions to gain access to the organization's global administrator account or trusted SAML token signing certificate to forge SAML tokens for lateral movement. [2] More recently, this threat actor has used a custom backdoor malware to compromise Active Directory Federation Servers. [3] Credential misuse [4] is now a primary attack vector.

Implications:

Although organizations have spent considerable effort improving IAM capabilities, much of it has been spent on technology to improve user authentication. Although this represents an important security advance, somewhat ironically, it has also increased the attack surface for a foundational part of the cybersecurity infrastructure. Consequently, more needs to be done to protect identity systems, detect when they are compromised, and enable rapid investigations and efficient remediation. Although the need for better prevention and detection is clear, ensuring the highest levels of IAM fabric resilience also requires the ability to quickly revert to a known good state.

Many organizations' IAM teams spend too much of their time protecting other group's digital assets, and not enough time protecting their own IAM infrastructure.

ITDR is not yet a consolidated product offering. Instead, a number of tools can assist organizations in building a defensive IAM capability. These tools include:

- A single authoritative user directory that is protected by active management, threat detection and response tools
- Identity proofing mechanisms, such as remote document-centric identity proofing
- A single sign-on access management (AM) tool that continuously assesses user context attributes
- Deception identity breadcrumbs to confuse and expose attackers
- A privileged access management (PAM) tool to restrict access to sensitive accounts
- Multifactor authentications tools
- Account takeover (ATO) fraud detection tools

- Identity governance and administration (IGA) and a cloud infrastructure entitlement management (CIEM) capability to identify anomalies in entitlement configurations and ensure that people and machines have least privilege
- User and entity behavior analytics (UEBA) tools

Many IAM tools are operating in silos that are not visible to incident responders. Organizations must reevaluate their IAM infrastructure with a goal of identifying opportunities for detecting compromise and immediately investigating and responding. Currently, best practice is to use a layered approach (defense-in-depth strategy) that leverages complementary IAM and security controls. However, the vendor consolidation trend is also impacting this category, and in the longer term, Gartner anticipates more consolidated solutions enabled by emerging standards and more comprehensive ITDR solutions.

Actions:

- Prioritize the security of identity infrastructure with tools to monitor identity attack techniques, protect identity and access controls, detect when inclusions are occurring, and enable fast remediation.
- Use the MITRE ATT&CK framework to correlate ITDR techniques with common attack scenarios.
- Invest in foundational IAM infrastructure hygiene security best practices for your AD, including credential management and privileged access management.
- Modernize IAM infrastructure using current and emerging standards (i.e., OAuth 2.0).

Further Reading:

- The Future of Security Architecture: Cybersecurity Mesh Architecture (CSMA)
- Predicts 2022: Identity-First Security Demands Decentralized Enforcement and Centralized Control
- 2022 Planning Guide for Identity and Access Management
- Managing Machine Identities, Secrets, Keys and Certificates

Digital Supply Chain Risk

Analysis by Katell Thielemann

Description:

Digital supply chain risks generally fall into four main categories:

1. The potential disclosure of sensitive information shared with supply chain partners

2. Compromise of infrastructure shared with supply chain partners such as networks, software, cloud service and managed services providers

3. Attacks through common commercial and open-source software used in business and IT operations

4. The exploitation of security flaws in the digital products sold to customers

These risks are becoming significant enough to demand new mitigation approaches that involve more deliberate risk-based vendor/partner segmentation and scoring, more requests for evidence of security controls and secure best practices, a shift to resilience-based thinking, and efforts to get ahead of coming regulations.

Why Trending:

Advanced attackers have made it clear that attacking the digital supply chain can provide a high return on investment. Recent examples include:

- SolarWinds Orion code was modified in the build process to compromise SolarWinds clients.
- The REvil ransomware gang exploited a zero day vulnerability in Kaseya remote access software commonly used by managed security services providers (MSSPs)

As widespread vulnerabilities such as URGENT/11 and Log4j spread through the supply chain via reuse across all types of technology stacks (see What to Do About Log4j?), more attacks will emerge. The U.S. Federal government is putting significant efforts into exploring effective practices for information and communications technology (ICT) supply chain risk management. The Telecommunications Industry Association (TIA) just released the first-ever supply chain security standard (SCS 9001), which was developed specifically to aid the information and communications technology (ICT) industry.[5] Associated mandates are increasingly being applied to software providers (see U.S. Federal Government Market Implications of Executive Order on Cybersecurity) and suppliers holding Controlled Unclassified Information (see CMMC and DFARS 101 — What Your Peers Are Saying and Doing).

Implications:

As a result, security and risk management teams need to partner with other departments to prioritize and manage digital supply chain risks. Although the overall level of risk transparency remains disappointingly low, pressure should increasingly be put on vendors and suppliers to provide:

- Evidence of industry-standard and best-practice internal security controls if you share data, infrastructure or services
- Evidence of secure design and engineering practices
- Bill of materials (BOMs) for products, services and components, which includes all logic-bearing (e.g., readable/writable/programmable) hardware, firmware and software
- Evidence of vulnerability disclosure and management programs
- Evidence of anti-tamper/anti-counterfeit controls and provenance efforts such as only buying from original equipment manufacturers (OEMs) or licensed resellers and not buying from prohibited vendors

Regulatory frameworks are emerging for organizations that support public-sector- and critical-infrastructure-related markets, and adherence will increasingly become mandatory. These efforts can provide a blueprint for new approaches to managing supply chain risks in nonregulated entities. Although it is certainly desirable to ascertain a critical partner's susceptibility to attack, current approaches are only partially successful in identifying and remediating supply chain attacks Today's organization can never hope to entirely avoid security failure, and effective leaders focus on the organizational resilience of mission-critical systems with the goal of quickly recovering from both anticipated and unexpected attack scenarios.

Actions:

- Create partnerships with your key IT, procurement, supply chain, operations, systems owners, and product development stakeholders, and develop a joint governance model.
- Inventory major ICT supply chain partners in the four categories listed above, and classify them as high/medium/low risk based on business or mission criticality.
- For those rated high-risk or regulated, SRM leaders should require these vendors/partners to provide evidence to demonstrate security best practices.
- Establish detection and resilience capabilities for any mission-critical supply chain partners. This should include a cyber incident response plan, downtime procedures (workarounds and manual procedures) and a continuity of operations plan so that critical functions and operations can continue if critical supplier systems are disrupted or need to be shut down.

Further Reading:

- ICT Supply Chain Risk Management Is Mission-Critical, but Best Practices Are Just Emerging
- Creating a Supply Chain Resilience Framework
- 5-Step Roadmap to Achieving Organizational Resilience
- Identifying High-Risk Third Parties
- Managing Third-Party Risks

- How to Prepare a Third-Party Risk Management Framework

Vendor Consolidation

Analysis by Peter Firstbrook

SPA: By 2024, 30% of enterprises will adopt cloud-delivered secure web gateway (SWG), cloud access security broker (CASB), zero trust network access (ZTNA) and branch office firewall as a service (FWaaS) capabilities from the same vendor.

By 2025, 50% of midmarket security buyers will leverage extended detection and response (XDR) to drive consolidation of workspace security technologies such as endpoint and cloud application security, and identity.

By 2025, 70% of new access management, governance, administration and privileged access deployments will be converged identity and access management platforms.

Description:

Across multiple security domains, security technology convergence is accelerating driven by the need to reduce complexity, leverage commonalities, reduce administration overhead and provide more effective security. New platform approaches such as XDR, security service edge (SSE) and cloud native application protection platforms (CNAPP) are accelerating the benefits of converged solutions. Functional convergence in identity and access management is also ramping up, delivering a combination of access management, identity governance and administration, and privileged access management capabilities. At the same time, pricing and licensing options from multiproduct companies are making packaged solution buying significantly more attractive than point product buying. Undeniably, the security market is emulating other mature IT markets, which experienced this type of consolidation in the past.

Why Trending:

The security product consolidation trend is driven by changes in both demand and supply. On the demand side, the technical security staff necessary to effectively integrate a best-of-breed portfolio of security products is simply not available to most organizations. As a result, 80% of SRM leaders are now looking to consolidate their security spending with fewer vendors. [6] These leaders are anticipating that consolidation will result in improvements to the enterprise risk posture and security staff efficiency.

On the supply side, security solution providers are integrating product portfolios with common services such as data and alert management, common agents, intel sharing, workflow and automation. Concurrently, cloud development has opened up new integration opportunities using services-oriented architectures and the scalability of cloud infrastructure.

Implications:

Consolation of security functions into broader security systems is a welcome trend and should lower total cost of ownership and improve operational efficiency in the long term. This should lead to better overall security. Products that are acquired to solve related security problems are good candidates for consolidation.

Solution buying may introduce new challenges. It can potentially reduce negotiations power with vendors, limit the diversity of security intelligence and methods, increase new near-term costs such as license overlaps and migration costs, and create potential single points of failure. Buyers must differentiate integrated “solutions” from packages that simply offer multiple independent products. Migrating to security solutions buying typically takes from one to three years and often requires professional services. Despite these concerns, astute SRM leaders are scrutinizing isolated security product buying and increasingly relying on incumbent providers to deliver more.

Actions:

- Inventory the security product portfolio and group products by the security problems they help solve.
- Evaluate products that could be enhanced by shared data management, common policies enforcement and integrated workflows.
- Highly scrutinize isolated security product buying, and ensure that incumbent providers are on the shortlist of prospective solutions wherever possible.
- Keep candidate stand-alone product licenses short (one year) to enable rapid replacement.
- Budget for and acquire professional services assistance for consolidation projects to augment staff.

Further Reading:

- Market Guide for Extended Detection and Response
- Predicts 2022: Identity-First Security Demands Decentralized Enforcement and Centralized Control
- Predicts 2022: Consolidated Security Platforms Are the Future
- Magic Quadrant for Secure Services Edge

Cybersecurity Mesh

Analysis by Felix Gaehtgens

SPA: By 2024, organizations adopting a cybersecurity mesh architecture will reduce the financial impact of individual security incidents by an average of 90%.

Description:

The cybersecurity mesh architecture concept is evolving and gaining popularity as a technical approach, driven by bundled vendor offerings and new emerging standards. Although not exclusively offered on an “as a service” basis, the transition to the cybersecurity mesh approach has also contributed to making cloud delivery the preferred approach for most cybersecurity technologies.

Existing approaches to security and identity architectures are siloed and work in isolation from each other. This makes a zero-trust architecture — where context and (near) real-time events drive an adaptive security posture — challenging. A cybersecurity mesh architecture (CSMA) helps provide a common, integrated security structure and posture to secure all assets, whether they’re on-premises, in data centers or in the cloud.

CSMA creates and leverages interoperable connections between stand-alone security tools to promote composability and a consistent security posture. This allows these tools to share and leverage security intelligence and apply a dynamic policy model that is based on the current state of assets. CSMA achieves this integration of security tools through a common security intelligence and analytics layer, a distributed identity fabric, centralized policy and dashboarding.

Why Trending:

The security product consolidation trend is driving functional integration of related components of security architecture. However, despite this trend line, security consolidation will never result in single-sourced security architecture. Moreover, single-vendor approaches introduce new challenges. As a result, there is still a need to manage security policy, enable workflows, and exchange data between consolidated solutions.

Recent events that support composable interoperability along new dimensions include:

- The Shared Signals and Events Working Group is attempting to enable the sharing of security events, state changes and other signals between dynamic security systems.
- The OpenID Continuous Access Evaluation Profile (CAEP) was established for more consistent sharing of event signals.
- Identity Query Language (IDQL) for policy orchestration has been proposed to establish a standard policy syntax for identity and access policy sharing.
- Open policy agent (OPA) uptake is increasing to provide a unified framework for stating and sharing policy that is decoupled from code.
- Industry collaborations like the emerging XDR alliances also illustrate emerging opportunities for more interoperability between security solutions

Implications:

- Most organizations already have many pieces of the puzzle to build interconnections between security tools that would foster better integration and thus a more adaptive security stance across those tools. Using a CSMA to integrate them will render those benefits.
- Additionally, many organizations have acquired integrated security product suites that have characteristics of a CSMA, but are still struggling to extend this toward deeper integrations with third-party security tools.
- Some more advanced organizations are building supportive layers for a vendor-neutral CSMA that allow for full integration toward a dynamic, adaptive security posture.

Actions:

As part of the ongoing evolution of their security and identity planning and operations, organizations should:

- Focus security modernization efforts on composable security tools that will provide the most strategic benefit in a cloud-application-centric and hybrid worker future.
- Evaluate and choose security products that are able to interoperate through established and emerging standards.
- Leverage CSMA best practices to evolve your IAM infrastructure to operate as an identity fabric (composable, secure, resilient system of systems) rather than a set of isolated, unprotected components.

Further Reading:

- The Future of Security Architecture: Cybersecurity Mesh Architecture (CSMA)
- Top Strategic Technology Trends for 2022: Cybersecurity Mesh
- Client Question Video: How Can We Architect Our IAM to Be More Adaptive?
- Guide to Cloud Security Concepts

Distributing Decisions

Analysis by Sam Olyaei and William Candrick

SPA: By 2025, a single, centralized cybersecurity function will not be agile enough to meet the needs of a digital organization.

Description:

Enterprise needs and expectations of cybersecurity are maturing. Business stakeholders — from the board and c-suite to managers and project owners — demand more security flexibility and coverage. Business technologists need advice and assurance, and they want it immediately. This increased demand for cybersecurity is driven by new attack vectors (e.g., supply chain attacks), growing threats (e.g., ransomware), expanding requirements (e.g., privacy laws and regulatory compliance) and new ways of working (e.g., DevSecOps and development work within business lines). The CISO and the centralized function will continue to set policy, and it will be consulted and informed by the business technologists. However, the scope, scale, complexity and time expectations of digital business make it increasingly necessary to shift cybersecurity decisions, responsibility and accountability to business units.

Why Trending:

Executive leaders require fast and agile workflows to support digital business priorities. As executives and boards become more familiar with cyber risk, they also have a more abstract and strategic set of expectations from CISOs. These trends have led to new cybersecurity leaders placed in different parts of the organization to perform baseline security operations and risk management practices. These include product lines (product security officers), service lines (business security officers), risk functions (cyber risk officer) and others. Many of these leaders operate outside the direct purview of the traditional CISO.

Implications:

Business leaders often view cybersecurity as a specialized IT role because of the overlap in skills and tools. However, Cybersecurity is really a specialization within the umbrella of business risk management. Cybersecurity no longer exists just to secure things. It exists to help the business thrive in a hostile environment. This can only happen when higher levels of cybersecurity responsibility and accountability are integrated into business technology and risk management roles.

The CISO role has shifted from that of a technical subject matter expert to an executive risk management role. Moving forward, CISOs must reconceptualize their organization's responsibility matrix based on specific enterprise needs. For example, CISOs that work in highly regulated organizations (e.g., financial services and healthcare) should plan for multiple layers of cybersecurity leadership — such as a CISO, cyber risk Officer, cyber resilience manager and so on.

Security leaders may adopt new titles or work with security stakeholders with new titles. Alternatively, some security and risk management leaders may evolve into board members accountable for cybersecurity, digital risk officers or other emerging roles. In last year's top trends, we noted Gartner observations that some boards have started to recruit former cybersecurity leaders to chair risk committees and oversee cyber risk management (see Top Security and Risk Management Trends 2021).

These new security roles and profiles reflect a splintering of the general CISO role into various roles, much closer to the business functions, and more specific to individual enterprise needs. This shift is also an opportunity for security and risk management leaders to craft new roles and new career opportunities.

Actions:

- Make fewer risk decisions. Empower and enable business leaders, other cybersecurity leaders and others to make their own informed risk decisions.
- Identify specific activities that no longer fit the CISO's elevated leadership role, and define and build the team that will meet these activities in an "office of the CISO."
- Foster cyber judgment throughout the enterprise and reduce dependency on hands-on risk decision facilitation by investing in self-serve tools that teach decision makers better cyber judgment through experiential learning.
- Redeploy information risk governance by empowering local governing bodies with decision rights instead of defaulting to top-down, centralized governance.

Further Reading:

- The Roadmap to CISO Effectiveness
- Client Question Video: What Are the Top 5 Relationships That CISOs Need to Establish?
- Case Study: Actionable CISO Succession Planning
- Expert Insights Video: Cyber Judgment: Navigating the Era of Distributed Decision Making
- Leadership Vision for 2022: Security and Risk Management

Beyond Awareness

Analysis by Richard Addiscott and Alex Michaels

SPA: By 2025, 40% of cybersecurity programs will deploy socio-behavioral principles (such as nudge techniques) to influence security culture across the organization, up from less than 5% in 2021.

Description:

The human element continues to feature in the majority of data breaches, [7] a clear signal that traditional approaches to security awareness training are no longer effective. Progressive security and risk management (SRM) leaders are moving beyond legacy security awareness programs by investing heavily in holistic security behavior and culture change programs more akin to a classical marketing campaign than an old-school, compliance-centric security awareness campaign.

Why Trending:

As employee generational demographics shift, digital aptitude and cyber literacy levels will continue to increase across the organization, as will overall awareness of the omnipresence of cyberthreats. Training focused merely on how to spot cyberthreats, or on expected anti-phishing behaviors, can become stale. Even worse, it fails to prepare technologists, both in IT and in the business, to make effective cybersecurity decisions. These problems are especially critical if the security awareness training content:

- Remains static
- Is not relevant or in some way contextualized to the individual learner
- Is delivered via a nonpreferred medium
- Can't be consumed at a time, at a location, via an application, or on a device of the employee's choice

When employee engagement in the program diminishes, the potential for cybersecurity failure increases. As business technologists make increasingly significant decisions about digital activity, they need to be empowered to make better decisions about security — a skill that Gartner refers to as cyber judgment.

Phishing remains the threat actor's favorite attack vector. However, several other human activities contribute to over half of all data breaches, [7] including system misconfiguration, data misuse/misdelivery and weak credentials. These are all eminently avoidable behaviors that must also be addressed via a security behavior and culture program (SBCP).

Executing an SBCP to reduce human-born cyber risk levels requires a paradigm shift where the objective extends beyond merely raising awareness of cyberthreats. An SBCP focuses on fostering new ways of thinking and embedding new behavior with the intent to provoke new, more secure ways of working across the organization.

Implications:

Establishing and executing an SBCP requires an approach analogous to a multichannel, user-centric, marketing, and organizational change management program. SRM leaders will therefore need access to new skills and competencies that traditionally aren't a feature of the cybersecurity practitioner's knowledge domain, including:

- Marketing and public relations
- Human-centric design techniques such as design thinking
- Organizational change management frameworks and practices
- Knowledge of psychology (individual human behavior) and sociology (human behavior in groups)

A holistic SBCP will also help reduce human-born vulnerabilities in the organization's digital supply chain by focusing on "shifting left" security awareness and embedding secure engineering capabilities and practices into infrastructure and operations teams. Executing an SBCP may also result in technology and architectural implications because it will require a more platform-centric, integration-enabled solution stack that leverages multiple vendors to deliver the capabilities and data required.

Actions:

- Develop and promulgate a cybersecurity culture change that equips all users of digital systems not just with cybersecurity awareness, but with cyber judgment skills and a passion for applying them.

- Investigate the use of organizational change management best practices and social science principles such as culture hacks.
- Collaborate with business leaders to ensure that everyone functioning as a business technologist is regularly involved with culture-changing activities and has access to training.
- Adopt a platform-centric approach with cybersecurity training vendors that can provide innovative features such as contextualized training material, in-the-moment nudges, gamification, real-world phishing simulations and outcome-driven metrics.

Further Reading:

- Take 3 Steps to Prove That Your Security Awareness Program Is Actually Working
- Client Question Video: How Do I Benchmark My Phishing Simulation Program
- Use Behavioral Economics to Influence Security Behavior and Individual Decisions
- How to Design a Security Champion Program
- To Improve Employee Experience, Manage Memory

Evidence

[1] The Rise of Working From Home, The Economist.

[2] Customer Guidance on Recent Nation-State Cyber Attacks, MSRC.

[3] FoggyWeb: Targeted NOBELIUM Malware Leads to Persistent Backdoor, Microsoft Security Blog.

[4] Detecting Abuse of Authentication Mechanisms, National Security Agency, Cybersecurity Advisory.

[5] About SCS 9001: Supply Chain Security Standard, TIA.

[6] Gartner's 2020 Security and IAM Solution Adoption Trend Survey was conducted online during March and Apri 2020 among 405 respondents from North America, Western Europe and the Asia/Pacific region. Companies from different industries were screened for having annual revenue of less than $500 million. Respondents were required to be at manager level or above (excluding the C-suite) and to have a primary involvement and responsibility in risk management roles for their organization.

[7] 2021 Data Breach Investigations Report, Verizon.

Acronym Key and Glossary Terms

CPS	Engineered systems that orchestrate sensing, computation, control, networking and analytics to interact with the physical world (including humans) and enable safe, real-time, secure, reliable, resilient and adaptable performance.

Document Revision History

Top Security and Risk Management Trends 2021 - 30 March 2021

Top Security and Risk Management Trends - 27 February 2020

Top Security and Risk Management Trends - 31 January 2019

Top Security and Risk Management Trends - 26 April 2018

Connect With Us

Get actionable, objective insight to deliver on your most critical priorities. Our expert guidance and tools enable faster, smarter decisions and stronger performance. Contact us to become a client:

U.S.: 1 855 811 7593

International: +44 (0) 3330 607 044

Become a Client

Stay connected to the latest insights

Attend a Gartner webinar

View Webinars

Gartner®