Gartner for IT Leaders

Predicts 2022: Cybersecurity Leaders Are Losing Control in a Distributed Ecosystem

By Sam Olyaei, Claude Mandy, Christine Lee, Richard Addiscott, Tom Scholtz, Deepti Gopal

Predicts 2022: Cybersecurity Leaders Are Losing Control in a Distributed Ecosystem

Published 24 January 2022 - ID G00757928 - 20 min read

By Analyst(s): Sam Olyaei, Claude Mandy, Christine Lee, Richard Addiscott, Tom Scholtz, Deepti Gopal

Initiatives: Security and Risk Management Leaders

This research showcases Gartner's predictions on culture, evolution of the cybersecurity role, third-party exposure and the board's perception of cyber risk. A key theme for SRM leaders is the increasingly distributed ecosystem that has led to a loss of direct decision-making control.

Overview

Key Findings

- Cybersecurity is turning into a social phenomenon. Investor interest, public pressure, employee demands, and governmental regulations are strengthening the incentives for organizations to track and report cybersecurity goals and metrics within their environmental, social and governance (ESG) efforts as a business requirement.

- Customers are also increasingly expressing concern and interest in the cybersecurity posture of the organizations that they conduct business with.

- Gartner research shows that 88% of boards regard cybersecurity as a business risk rather than solely a technical IT problem. Thirteen percent of boards have responded to this by instituting cybersecurity-specific board committees overseen by a dedicated director.

- Traditional culture improvement efforts that focus exclusively on awareness are failing to facilitate secure behavior and have led to loss of control amid an increasingly distributed ecosystem.

- Executive performance evaluations are increasingly linked to an ability to appropriately manage cyber risk within their parts of the business.

Recommendations

As a security and risk management (SRM) leader, you should:

- Incentivize business executives to regard cybersecurity as one of their strategic business goals by ensuring that the board is reviewing outcome-driven cybersecurity performance reports.
- Reinforce desired executive cybersecurity risk behavior by working with the human resources (HR) team to insert cybersecurity performance goals in business executive employment agreements.
- Reduce your organization's potential for negative societal impact by developing environmental, social and governance goals (ESG) as part of your annual cybersecurity strategic planning.
- Define the scope and objectives of your third parties. For some, this might just be the critical IT vendors while for others it might include the entire ecosystem, such as individual customers/citizens or subsidiaries.
- Ensure cyber risk quantification is outcome driven. Clarify the specific business decision you want to influence and make quantification outputs directly actionable for decision-makers.

Strategic Planning Assumptions

By 2026, at least 50% of C-Level executives will have performance requirements related to cybersecurity risk built into their employment contracts.

By 2025, 60% of organizations will use cybersecurity risk as a significant determinant in conducting third-party transactions and business engagements.

By 2025, 50% of cybersecurity leaders will have tried, unsuccessfully, to use cyber risk quantification to drive enterprise decision-making.

By 2026, 30% of large organizations will have publicly shared environmental, social and governance (ESG) goals focused on cybersecurity, up from less than 2% in 2021.

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

Analysis

What You Need to Know

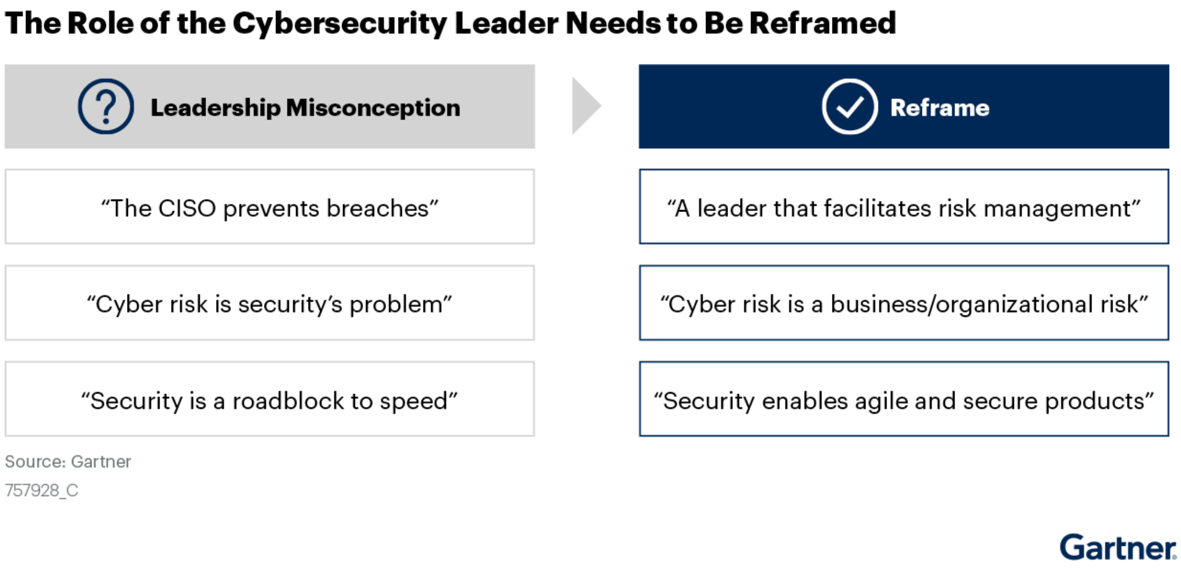
Every year, Gartner analysts offer their predictions on what they see as the key issues facing the business, IT practices and markets they cover. Gartner's security and risk management analysts have developed a set of representative predictions in this space for the next several years. This research highlights some of the top predictions for cybersecurity leadership.

Cybersecurity leader's today are burnt out, overworked and practice an "always-on" mode. This is a direct reflection of how elastic the role has been over the past decade due to the growing misalignment of expectations from stakeholders within their organizations. On a similar note, new concepts have emerged such as:

- Resilience and risk quantification
- Increased levels of digital connections forcing organization to put significantly higher levels of effort into controlling (evaluating, influencing) the cyberhealth of external parties
- Employees now making decisions with cyber risk implications without consulting security and risk management leaders
- Executive committees being established outside the scope/purview of the cybersecurity leader

These factors will lead to an environment where the cybersecurity leader will have less direct control over many of the decisions that typically would fall under their scope today. Therefore, Gartner recommends that leaders monitor these predictions and act on them as they see signs emerge in their respective environments. In addition, a growing number of cybersecurity leaders may need to reframe their roles in order to succeed (see Figure 1).

Figure 1. The Role of the Cybersecurity Leader Needs to Be Reframed



The Role of the Cybersecurity Leader Needs to Be Reframed

Leadership Misconception	Reframe
"The CISO prevents breaches"	"A leader that facilitates risk management"
"Cyber risk is security's problem"	"Cyber risk is a business/organizational risk"
"Security is a roadblock to speed"	"Security enables agile and secure products"

Source: Gartner
757928_C

Strategic Planning Assumptions

Strategic Planning Assumption: By 2026, at least 50% of C-Level executives will have performance requirements related to cybersecurity risk built into their employment contracts.

Analysis by: Richard Addiscott

Key Findings:

Gartner research shows that 88% of Boards now regard cybersecurity as a business risk rather than solely a technical IT problem. [1] Additionally, during the COVID-19 pandemic, SRM leaders increased their time focused on the following priorities:

- Educating the CIO/CEO and other senior stakeholders on the value of security and risk management.
- Measuring and articulating the value of the security and risk management function.
- Increasing their engagement and strengthening their relationships with the CEO and senior leadership team. [2]

This increased focus on educating business leaders on cybersecurity is partly attributable to increased board interest. Additionally, leading SRM leaders are responding proactively to a prevailing trend where they are seeing more non-IT or security people inside an organization making information risk decisions (see Cyber Judgment Benchmarking Report). However, it is still clear from hundreds of security governance-related interactions with Gartner clients that: [3]

- Accountability for treating cyber risks is usually not formally being allocated to the business.
- SRM leaders continue to struggle articulating why accountability for cybersecurity risk should reside with the business (and not IT or the security function).
- This impacts the timeliness and quality of information risk decisions which are increasingly being made by stakeholders outside of IT or security's line of sight.

However, Gartner does expect to see an inexorable shift in formal accountability for the treatment of cyber risks from the security leader to senior business leaders. Specifically, this accountability will increasingly, and ultimately, rest with business leaders who are:

- Responsible to the CEO for delivering strategic objectives (e.g., revenue, customer satisfaction).
- The owners of any associated business processes, applications and/or data that enable the achievement of those strategic objectives.
- Empowered (formally or informally) and willing to make independent technology acquisitions in pursuit of those objectives.
- Accountable for ensuring that any other operational risks to those objectives (and associated key performance indicators) are managed to acceptable levels.

Market Implications:

Increased recognition from boards that cybersecurity is a business risk is a welcome trend. As a result, Gartner expects it will become more common to see accountability for treating cybersecurity risks being articulated formally in business executive employment contracts. Accordingly, Gartner also expects to see executive performance evaluations, and potentially any at-risk remuneration (e.g., bonus payments), being linked to an executive's ability to manage cyber risks to acceptable levels inside their part of the business.

However, it is unfair and bordering on unethical to expect business executives to be accountable for something they're not equipped to handle, or have the knowledge to do. So, as formal accountability transfer for cybersecurity risk shifts to the business, the SRM leader's role also has to be redefined. The SRM leader's role will need to evolve from being the "de facto"' accountable person for treating cyber risks to being responsible for ensuring business leaders have the capabilities and knowledge required to make informed, high-quality independent information risk decisions.

Managed effectively, this serves as a win-win situation for the chief information security officer (CISO). Firstly, accountability for cybersecurity risk will increasingly rest on the "right" shoulders inside the organization. Secondly, the CISO now has the opportunity to shape and influence information risk decisions that may previously have been outside their line of sight, in turn helping to enhance the organization's cybersecurity risk posture. Forward thinking SRM leaders will also recognize that any perceived "loss of control" over information risk decisions will be outweighed by the opportunity to demonstrate the security team's value as an enabler of strategic business goals being achieved.

Recommendations:

- Incentivize business executives to regard cybersecurity as one of their strategic business goals by ensuring that the board is reviewing outcome-driven cybersecurity performance reports.
- Define clear accountability for cybersecurity risk with the business by creating an enterprise security charter that is signed by the board, CEO and business executives indicating their agreement that they will not take unilateral decisions exposing the organization to unacceptable levels of cyber risk.
- Establish access to a security advisory service that provides timely security and risk advice, and other self-service guidance material, enabling business leaders to make independent, high-quality information risk decisions.
- Reinforce desired executive cybersecurity risk behavior by working with the HR team to insert pragmatic and measurable cybersecurity performance goals in business executive employment agreements.

Related Research:

An Outcome-Driven Approach to Cybersecurity Improves Executive Decision Making

Select the Best Approach for Capturing and Communicating the Value of Cybersecurity

The Roadmap to CISO Effectiveness

Tool: Enterprise Security Charter Template

Strategic Planning Assumption: By 2025, 60% of organizations will use cybersecurity risk as a significant determinant in conducting third-party transactions and business engagements.

Analysis by: Sam Olyaei

Key Findings:

Cyberattacks related to third parties are increasing. However, most organizations do not have stringent measures in place to identify these risks. According to the latest data from Gartner's IT Score for Security and Risk Management (SRM), [4] only 23% of SRM leaders actually monitor their third parties in real time for cybersecurity exposure. Additionally, organizations typically limit their third-party coverage only to their immediate vendors and suppliers, without any regard for other ecosystem players such as customers, business partners, investors, regulators, etc.

Concern about cyber risk in the digital ecosystem is becoming critical. For example, 56% of customers (B2B and B2C) are now expressing frequent interest and concern in the cybersecurity posture of the organizations that they do business with. [5] Similarly, regulators (most notably the U.S. Securities and Exchange Commission) mandate that businesses disclose risk factors in their filings to the public to support investors in an attempt to increase transparency. As a result, Gartner believes that organizations will start to mandate and use cybersecurity risk as a significant determinant when conducting business with all third parties, across the digital ecosystem. These engagements may be as simple as monitoring a critical technology supplier, or more complicated such as investing in a new acquisition and/or assuring customer experience/satisfaction.

Market Implications:

Cybersecurity leaders now have to face this issue from two angles — the internal ramifications of third-party cyber risk exposure, as well as the continuous demand for transparency and cyber due diligence from the rest of the ecosystem players. This will lead to numerous market implications, most notably:

1. Demand for additional technology solutions that drive transparency into overall third-party risk management.

2. The introduction of new internal stakeholders — such as investor relations, marketing professionals and finance that may increase the requirements/expectations of the cybersecurity leadership team.

3. The shift to a customer-centric environment that focuses on balancing cybersecurity risk with user experience and customer experience. Overprotected organizations may suffer business disruptions the same way vulnerable organizations do today.

Recommendations:

- Define the scope and objectives of third-party cybersecurity management by engaging the business, procurement, supply chain, legal counsel and relevant stakeholders to set cybersecurity standards and expectations of third parties for various risk scenarios. For some, this might just be the critical IT vendors while for others might include the entire ecosystem such as individual customers or subsidiaries.
- Leverage risk-based evaluations (see Navigating the Vendor Risk Management Market) that highlight transparency and reward participants. Make sure to evaluate those engagements that present the most risk (risk triage), and develop predefined actionable outcomes to mitigate risk. Not all players require the same amount of monitoring or due diligence.
- Recognize that you will need to make decisions with incomplete data. Whether you are conducting due diligence on a merger/acquisition, monitoring your critical supply chain partner, or deciding whether to invest in a new company — you will not have the full picture.

Related Research:

Risk-Based Evaluations of Cloud Provider Security

Navigating the Vendor Risk Management Solution Market

Address the Increasing Cyber Risk Presented by Your Evolving Third-Party Network

Strategic Planning Assumption: By 2025, 50% of cybersecurity leaders will have tried, unsuccessfully, to use cyber risk quantification to drive enterprise decision-making.

Analysis by: Christine Lee and Khushbu Pratap

Key Findings:

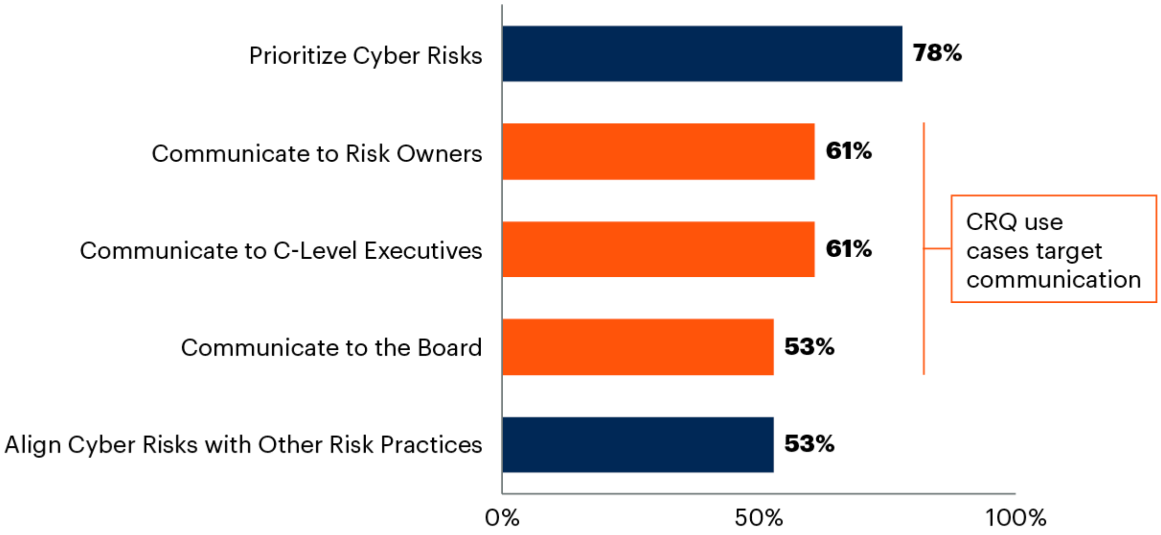
The 2021 Gartner Cyber Risk Quantification Survey shows that while 80% of respondents measure risk with ordinal scales, 20% use statistical modeling techniques (e.g., Monte Carlo simulations), and 43% plan to adopt statistics-based risk quantification within the next two years.

Popular use cases for cyber risk quantification (CRQ) include prioritizing cyber risks and improved communication with risk owners, executive management and boards. Notably, three of the top five use cases center on communication with enterprise partners. CRQ adopters believe that expressing risk in financial and business-relevant units will justify security investments, drive urgency around risk mitigation, and help business leaders make critical trade-off decisions — for example, between cyber and other enterprise risks or between cyber risk and value generation (see Figure 2).

Figure 2. SRM Leaders Primarily Leverage CRQ to Communicate Risk

SRM Leaders Primarily Leverage CRQ to Communicate Risk

Top Five Use Cases, Percentage of SRM Leaders



n = 51 Security and risk management leaders that have already adopted CRQ

Source: 2021 Gartner Cyber Risk Quantification Survey

757928_C

Market Implications:

Thus far, results are mixed. A majority (62%) of CRQ adopters cite soft gains in credibility and cyber risk awareness, but only 36% have achieved action-based results, including reducing risk, saving money or actual decision-influence.

Given where most experimenters are on the learning curve, it’s inevitable that inefficiencies and even outright failures will abound. Lack of quality data is unsurprisingly the top challenge faced by CRQ adopters, though 46% of Gartner’s survey respondents call out connecting CRQ to clear business decisions and outcomes as a serious obstacle.

As long as business leaders and boards continue demanding financial translations of cyber risk and data-backed justification for controls and security investments, cybersecurity leaders will feel compelled to invest in CRQ. In the vanguard are those in the financial, tech, or otherwise highly regulated industries, as well as organizations with robust cybersecurity risk management programs looking to take the next maturity leap. Organizations with less mature cybersecurity programs will be too focused on building and consolidating risk management processes to pursue CRQ meaningfully.

Organizations should be wary of jumping on the bandwagon given decidedly modest results. Over the next three to five years, the industry will be able to better discern the use cases that truly require increased precision and generate enough value to make the resource investment in CRQ worth it.

Recommendations:

- Focus your firepower on quantification decision makers ask for instead of producing self-directed analyses you then have to persuade the business to care about.
- Consider business assets rather than scenario-based CRQ to maximize use of existing enterprise data. Scenario-based CRQ requires subjective estimates of probability based on historical incidents or rare events. Modeling asset value and exposure to business disruption will allow you to use objective data from existing business impact analysis (BIAs) and monitoring capabilities.
- Be very skeptical about vendor promises. Effective CRQ requires deep understanding of your data, technology architecture and enterprise priorities, which vendors don’t have and which their solutions cannot provide without extensive tuning.

Related Research:

Infographic: Benchmarking Cyber-Risk Quantification: Models, Use Cases, and Outcomes

Case Study: Criteria to Determine When to Perform Cyber-Risk Quantification

Cyber Risk Quantification, Hype Cycle for Cyber and IT Risk Management, 2021

Strategic Planning Assumption: By 2026, 30% of large organizations will have publicly shared environmental, social and governance (ESG) goals focused on cybersecurity, up from less than 2% in 2021.

Analysis by: Claude Mandy, Deepti Gopal

Key Findings:

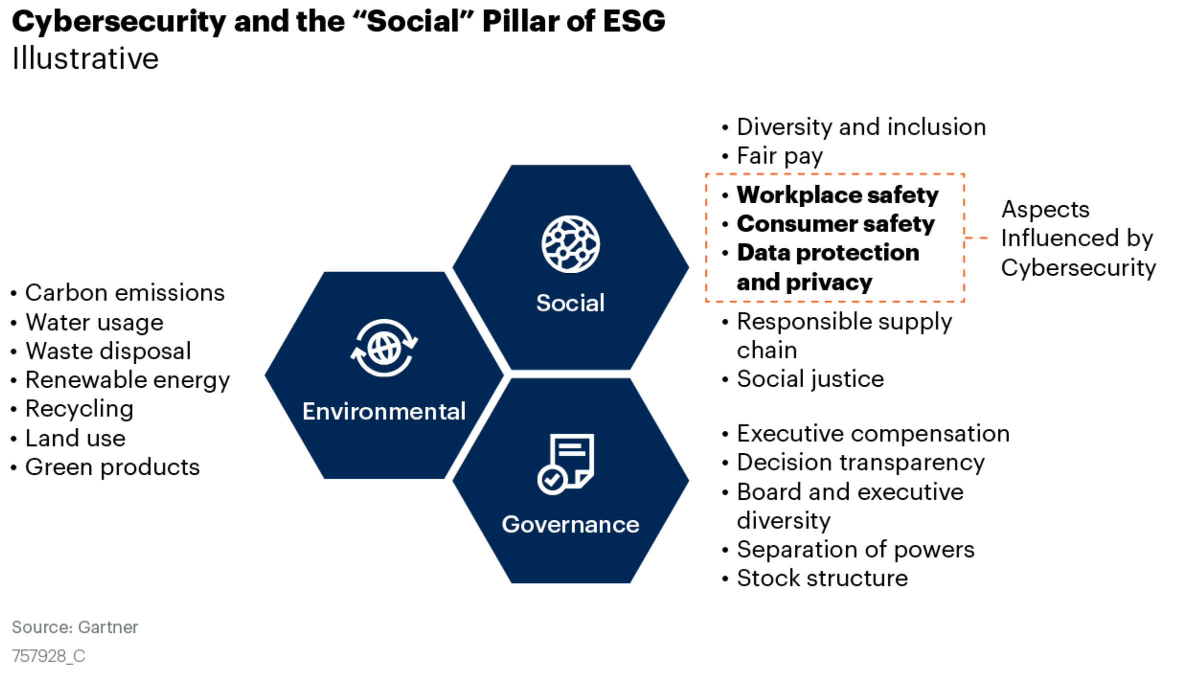
Expectations that organizations should be more transparent about their security risks have increased. This has resulted in public demand for greater transparency around environmental, social and governance goals (ESG) . ESG reporting is quickly moving from a discretionary activity to a business requirement. Investor interest, public pressure, employee demands, peer behavior and governmental regulations are strengthening the incentive for organizations to track and report their ESG efforts.

Organizations agree that cybersecurity is no longer solely a risk to the organization, but a societal risk. Although cybersecurity is rarely included in current ESG disclosures (see ESG Risk by the Numbers: Benchmarking ESG Disclosures), there are various indicators that it will become more widespread:

- A number of frameworks being developed by established third parties to benchmark ESG efforts (e.g., Global Reporting Initiative [GRI], Sustainability Accounting Standards Board) include data security or data breaches (as a subset of privacy) within their frameworks.
- Increased disclosure of cyber risks in pre-initial public offering disclosures and annual 10-K disclosures indicating greater demand from investors. [6]
- Increasing oversight from the board (see Note 1).
- Increasing social expectations of cybersecurity as a result of ongoing breaches.

As these frameworks and the inclusion of cybersecurity goals and metrics become industry norms, SRM leaders will increasingly have to demonstrate an organizational commitment to reducing the social issues that may arise from cybersecurity incidents (see Figure 3).

Figure 3. Cybersecurity and the “Social” Pillar of ESG



Market Implications:

SRM leaders already have a key role to play in supporting other ESG metrics; such as increasing equity and inclusion within the cybersecurity function, and ensuring security incidents are considered within executive compensation.

SRM leaders will be asked to develop goals and metrics to demonstrate their organizational commitment to reducing the social issues that may arise from cybersecurity incidents. This could include the organization’s strategy to reduce the social or societal impact of incidents such as, but not limited to:

- Data breaches of customer personal information.
- Potential safety concerns from use of cyber-physical systems.
- The potential for misuse and abuse within their products.
- Malicious cyberactivity (including ransomware) against critical infrastructure (CI).

As with other ESG metrics, in the absence of transparent insight and metrics, external stakeholders (particularly institutional investors) will rely on publicly available information and particularly security rating services (SRS) (see Hype Cycle for Cyber and IT Risk Management, 2021) to inform their assessment of an organization's cybersecurity posture. You can no longer expect to keep the failures and successes of your cybersecurity function a secret.

Recommendations:

- Work with enterprise risk and sustainability leaders to ensure that existing and emerging ESG reporting requirements and the short- and long-term implications for the cybersecurity strategy are proactively identified.
- Develop metrics to proactively assess the social or societal impact of cybersecurity incidents and increase transparency in the organization's current performance and strategies to reduce this impact. These metrics and strategies will form the basis of future cybersecurity ESG goals.
- Proactively monitor the potential data sources including security rating services that could be used by external stakeholders (particularly institutional investors) to inform their assessment of an organization's cybersecurity posture.
- Work closely with the board and senior executives to ensure that corporate communications, (including formal ESG disclosures) demonstrate commitment and progress to reducing the societal impact of cybersecurity incidents.

Related Research:

SRM Leaders Must Plan Immediately for Climate Change Risk or Become Outmoded

ESG Risk by the Numbers: Benchmarking ESG Disclosures

Anatomy of an ESG Program

Maverick* Research: Digital Growth Is Not Sustainable — Stop Digital Pollution and Lead EcoDigital Initiatives

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

Analysis by: Tom Scholtz

Key Findings:

Fostering a cyber risk-aware culture is a key enabler of an effective cybersecurity program. Changing the culture requires a combination of active leadership intervention and techniques based on an understanding of how people behave as individuals and in groups. SRM leaders will increasingly use knowledge from the social sciences of psychology, and sociology and behavioral economics for insights into influencing their security culture.

Technology users, and their leaders, are bombarded with information from all directions. Messages are often contradictory — for example, pressure to share information with clients or business partners versus demands for protecting data — resulting in dissonance and a lack of clarity around the right thing to do. Traditional awareness efforts are erroneously based on the flawed assumption that providing people with information about risk will change their risk behavior. Awareness and information do not automatically result in more secure behavior — awareness should not be conflated with actual risk management. The choices that people make as part of their behavior, while somewhat influenced by traditional awareness efforts, are much more influenced by the norms and cues inherent in the environment that they find themselves in.

Market Implications:

Successful providers of security awareness tools and services will increasingly provide functionality based on socio-behavioral principles. This will include materials to support techniques such as culture hacks and nudges, more granular target audience segmentation and analysis capabilities, gamification and security program branding.

Recommendations:

- Shift the primary objective of your security awareness program away from mere awareness toward establishing and nurturing a cyber risk-aware culture.
- Appoint someone with a background in social science to apply sociology or behavioral economics to improve your organization’s security culture.
- Look for tools that effectively leverage social science techniques to influence cybersecurity behavior.

Related Research:

Use Behavioral Economics to Influence Security Behavior and Individual Decisions

20 Culture Hacks CIOs Can Use to Make Their Organizations More Secure

Take 3 Steps to Prove That Your Security Awareness Program Is Actually Working

A Look Back

In response to your requests, we are taking a look back at some key predictions from previous years. We have intentionally selected predictions from opposite ends of the scale — one where we were wholly or largely on target, as well as one we missed.

This topic area is too new to have on-target or missed predictions.

Evidence

[1] 2022 Gartner View from the Board of Directors Survey, Q07: This study was conducted to understand how 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 board of directors. If respondents serve on multiple boards, they answered for the largest company, defined by its annual revenue, for which they are a board member.

The survey was developed collaboratively by Gartner analysts and the Research Data and Analytics team.

Disclaimer: Results of this study do not represent global findings or the market as a whole but reflect sentiments of the respondents and companies surveyed.

[2] Gartner 2021 Global Security and Risk Management Survey, Q02A.

[3] GEAR interactions data shows that since 2020, there have been 838 interactions with security and risk management programs that team analysts related to security governance, security metrics and security board reporting.

[4] The Gartner IT Score for Security and Risk Management is part of the Gartner Score Diagnostic Family, which is a set of diagnostics designed to help measure, prioritize and improve a function's performance on critical activities. Gartner IT Score for Security and Risk Management benchmark data was taken from 770 IT organizations between October 2020 and August 2021.

[5] Leadership Vision for Security and Risk Management 2022

[6] How Cybersecurity Risk Disclosures and Oversight Are Evolving in 2021, EY

Note 1: Cybersecurity-Related Risk Is Largely Viewed as a Business Risk

The View from the Board of Directors Survey 2022 [5] found that 88% of respondents viewed cybersecurity-related risk as a business risk, not just a technology risk. In addition, 51% of respondents had experienced a cyber-security risk incident in the past two years.

Recommended by the Authors

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

Predicts 2022: Consolidated Security Platforms Are the Future

Predicts 2022: APIs Demand Improved Security and Management

Predicts 2022: Cyber-Physical Systems Security — Critical Infrastructure in Focus Predicts 2022: Identity-First Security Demands Decentralized Enforcement and Centralized Control

Predicts 2022: Privacy Risk Expands

Actionable, objective insight

Position your organization for success. Explore these additional complimentary resources and tools for cybersecurity leaders:

Webinar

2022 Leadership Vision for Security and Risk Management Leaders

Plan for 2022 and stay ahead of evolving challenges.

Watch On Demand

Research

Top Trends in Cybersecurity for 2022

Address the new cybersecurity risks your organization may face.

Download Now

Article

What's Keeping Midsize Enterprise CIOs Up at Night

Uncover the unique challenges facing midsize enterprise CIOs.

Read Now

eBook

3 Must-Haves in Your Cybersecurity Incident Response Plan

Improve your organization's ability to prepare for an incident.

Download Now

Already a client?
Get access to even more resources in your client portal. Log In

Gartner®

Connect With Us

Get actionable, objective insight to deliver on your mission-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

Learn more about Gartner for IT Leaders
gartner.com/en/information-technology

Stay connected to the latest insights

Attend a Gartner conference
View Conferences

Gartner®