TECHNOLOGY BRIEFING

# Cybersecurity Leaders are Losing Control in a Distributed Education Ecosystem

BY STEVE KING

CyberEd.io

# Rethinking the Traditional Approach

The data points contained in this research report are strong co-indicators of trends in cybersecurity that argue for increased, enterprise-wide education and training.

But, they don’t argue for traditional approaches to education and training as these trends developed in spite of programs that tried to create a culture of security consciousness throughout the enterprise and didn’t just fail to accomplish their goals, they worked in opposition to those goals by creating an environment where these negative trends flourished.

# Emerging Trends

Cybersecurity leaders today are burned out, overworked and practice in 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**

**Employees now making decisions with cyber-risk implications without consulting security and risk management leaders**

**Increased levels of digital connections forcing organizations to put significantly higher levels of effort into controlling (evaluating, influencing) the cyber health of external parties**

**Executive committees being established outside the scope or purview of cybersecurity leaders**

# Top Predictions for Cybersecurity Leadership

These factors have led to an environment where the cybersecurity leader now has less direct control over many of the decisions that historically would fall under their scope. 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.

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.

Among them:

2025

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 as an indicator of cybersecurity danger.

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.

2026

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

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.

# Focusing in on Business Risk

Gartner research shows that 88% of Boards of Directors (BOD) now regard cybersecurity as a business risk rather than solely a technical IT problem.

Additionally, during the COVID-19 pandemic, Security and Risk Management (SRM) leaders increased the time they 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.**

# Educating Business Leaders

This increased focus on educating business leaders on cybersecurity is partly attributable to increased board interest. Additionally, SRM leaders were responding proactively to a prevailing trend where they were seeing more non-IT or security people inside an organization making information risk decisions.

However, it is still clear from hundreds of security governance-related interactions with Gartner clients that:

**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.**

# Shifting Accountability

At the same time, 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).**

**Empowered (formally or informally) and willing to make independent technology acquisitions in pursuit of those objectives.**

**The owners of any associated business processes, applications and/or data that enable the achievement of those strategic objectives.**

**Accountable for ensuring that any other operational risks to those objectives (and associated key performance indicators) are managed to acceptable levels.**

# Evolution of the SRM Leader's Role

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 neither equipped nor have the knowledge to handle. 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.

# Opportunities for Influence

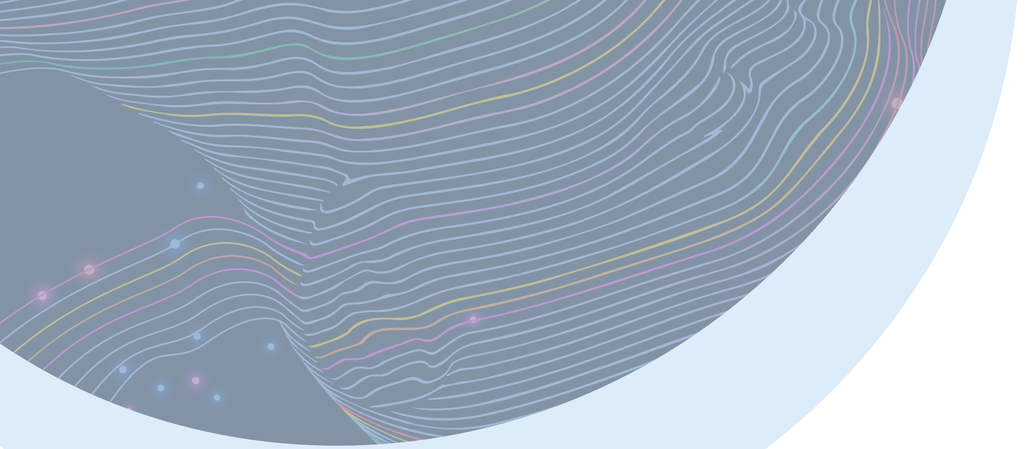
Managed effectively, this serves as a win-win situation for the chief information security officer (CISO). First, accountability for cybersecurity risk will increasingly rest on the “right” shoulders inside the organization. Second, the CISO now has the opportunity to shape and influence information 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.

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, 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.



# Changing Risk Behavior

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. Yet all security awareness programs begin with that assumption. 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 in which they find themselves.

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.

# Gartner 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 results.

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.

Strive to create and measure a culture of consciousness around cybersecurity that everyone in the enterprise can endorse and find paths toward active participation.

Look for tools that effectively leverage social science techniques to influence cybersecurity behavior.

# Conclusion

We would argue that because cybersecurity leaders today are burned out and overworked, and that HR and L&D teams are similarly over-burdened, the administration and management of enterprise-wide cybersecurity training and education programs should be outsourced and managed by professional third parties to assure cost-efficient and measurable, outcome-driven delivery goals.

These third parties are also already skilled in leveraging social science techniques to influence cybersecurity behavior, as their security awareness programs are engineered on the premises inherent in socio-behavioral principles.

Otherwise, historical evidence suggests that traditional approaches to education and training will fail to create a culture of security consciousness throughout the enterprise and continue to foster an environment where unilateral decisions exposing the organization to unacceptable levels of cyber risk will continue to flourish.

*Research Methodology:*

*2022 Gartner View from the Board of Directors Survey: 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.*

# CyberEd.io

CyberEd.io is on a mission to Close the Gap and provide comprehensive cybersecurity education to the industry. Millions of cybersecurity jobs go unfilled today globally due to the essential skills shortage. From basic cybersecurity skills to jobs/role specific skills — the shortage of qualified resources is overwhelming. And this gap continues to expand with every new attack, every new technology innovation introduced at an organization, every new compliance requirement, and every new business initiative that extends an organization beyond its physical boundaries and geographical reach. CyberEd.io provides the cybersecurity training and education needed to close this gap. Taught by a faculty of industry-renowned practitioners, the courseware on CyberEd.io is focused on building resiliency and improving the capability maturity for cybersecurity programs at organizations of every size.


CONTACT INFORMATION

cybered.io • 609.356.1499 • info@cybered.io • 902 Carnegie Center, Suite 430 Princeton, NJ 08540