Gartner

Leadership Vision for 2023

Top 3 Strategic Priorities for Security and Risk Management Leaders

From Tom Scholtz, Distinguished VP Analyst

Today's organizations are facing uncertainty brought about by persistent inflation; scarce, expensive talent; and global supply constraints caused by the Russian invasion of Ukraine, COVID-19 lockdowns and energy shortages. This triple squeeze is impacting business globally and directly impacting the cybersecurity threat landscape for 2023.

The decisions you make as a cybersecurity leader in difficult times will determine if your company takes unnecessary cybersecurity risks or is able to leverage technology innovation in order to thrive. Your teams must be capable of agile pivots.

Despite economic uncertainty and perceived headwinds leading into 2023, chief information security officers (CISOs) indicate their current plans call for continued investment in cybersecurity. Cybersecurity risks also increase as technology decisions become more democratized.

Top-performing CISOs have the courage to experiment with new ideas. They should focus on improving their own personal effectiveness and driving cultural change in their enterprises, and champion the adoption of cyber judgment.

As organizations continue to invest in technologies to innovate and differentiate themselves from competitors, security and risk management (SRM) leaders must ensure risk is measured and managed, while executing new ways to educate and guide the organization on security best practices.

Gartner Leadership Vision provides top-level guidance to leaders and their teams on where to focus — based on our data-driven research. We're providing detailed insights to our clients across dozens of roles, and we're now excited to share excerpts with the business community beyond our clients. We hope this will help you to focus discussions with your teams, peers and other leaders so you can more quickly and effectively diagnose priorities and actions, especially as you solidify your strategic plans for 2023.

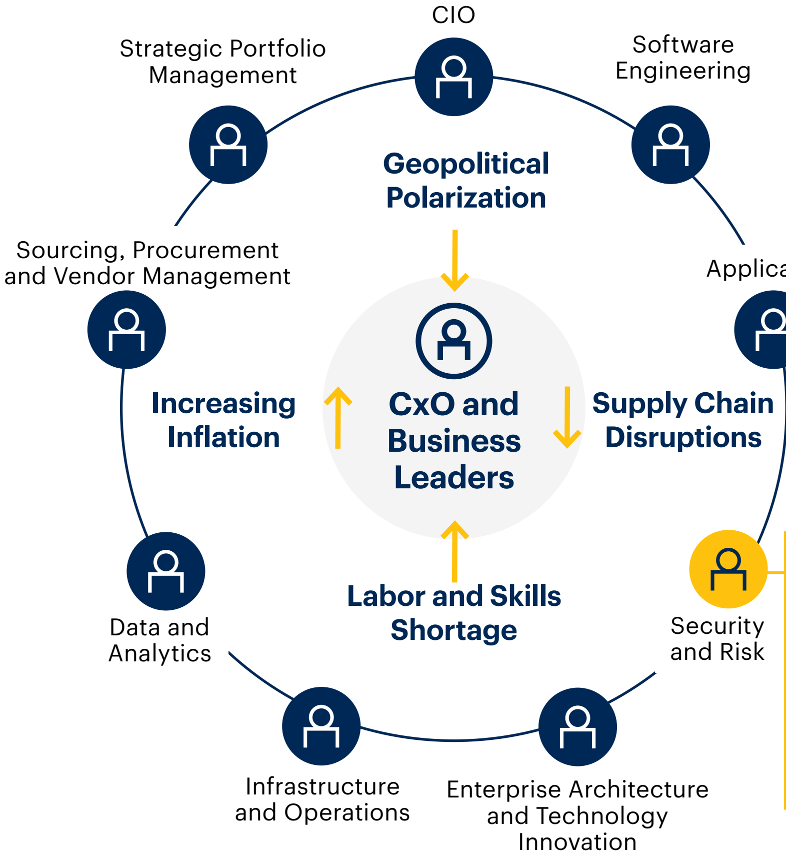
Tom Scholtz
Distinguished VP Analyst

Unique business environments require a team effort

SRM leaders work to enable security digitalization in an increasingly complex and dangerous world.

As organizations deal with unpredictable operating environments while seeking out innovative technologies to provide competitive differentiation, they are willing to increase their risk appetites and invest robustly in security for the foreseeable future.

To understand and respond to both internal and external challenges, it’s more critical than ever for SRM leaders to partner with stakeholders across the organization, ensuring business leaders have the knowledge and capabilities to make informed, high-quality security risk decisions.


CIO
Strategic Portfolio Management
Software Engineering
Geopolitical Polarization
Sourcing, Procurement and Vendor Management
Applications
Increasing Inflation
CxO and Business Leaders
Supply Chain Disruptions
Data and Analytics
Labor and Skills Shortage
Security and Risk
Infrastructure and Operations
Enterprise Architecture and Technology Innovation

Security and Risk Managers’ Role on the Team:

- Enable secure digitalization
- Drive cyber judgment
- Establish a cyber-risk-aware culture

Source: Gartner

Three key trends impacting SRM leaders

More technologists working outside of IT

To best achieve digital acceleration, 67% of CEOs want more technology work done within business functions. This trend means more “business technologists” — employees outside of the IT organization who can not only use tech, but produce it — on teams outside the direct control of the SRM leader.

Increased focus on third-party security risks

Recent cybersecurity incidents have highlighted weaknesses in supply chains. By 2025, 60% of organizations will use cybersecurity risk as a significant factor in conducting third-party transactions to prevent the compromise of information, systems and infrastructure.

The cybersecurity mesh evolves

If endpoints, digital citizens and IT assets can be located anywhere, cybersecurity controls need to follow suit. The cybersecurity mesh approach is a highly flexible and collaborative ecosystem of composable, distributed tools and controls that is being successfully applied to protect assets across the organization and the world.

Challenges and actions for the SRM leader

1 Dealing with the human factor

The majority of data breaches continue to involve a human element. A recent Gartner survey found that employees still engage — sometimes knowingly — in recognized risky security practices like using the same password for multiple accounts or opening emails from unknown sources on work devices.

2 Driving SRM effectiveness

Currently only 12% of SRM leaders exceed stakeholder expectations. Leaders must improve effectiveness across all their areas of responsibility to demonstrate their ability to deliver on cybersecurity priorities.

3 Accelerating the cyber judgment journey

SRM leaders must support the ability of decisionmakers throughout the organization to independently make informed risk decisions — also known as cyber judgment — rather than relying on the SRM team or automation.

Actions for the SRM leader

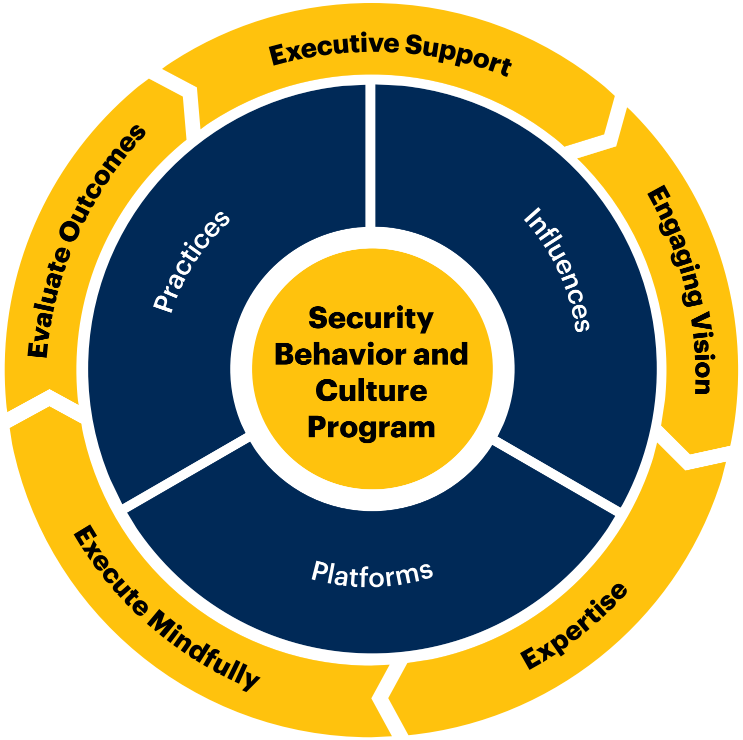
Employ the Gartner PIPE framework — which focuses on practices, influences, platforms and enablers — to guide the successful execution of a security behavior and culture program.

Focus on improving effectiveness across identified categories to better align with the business priorities and protect the security of the organization.

Drive cyber judgment across the enterprise by supporting autonomy through strategies like self-certification and group trust scoring.

Reduce the human factor on security risks

To reduce the negative impact of human behaviors on cybersecurity risk levels, SRM leaders must take a radically different approach to their security training programs. The Gartner PIPE framework can guide that execution. Leaders must also mitigate digital supply chain risks by developing best practices around third-party interactions.



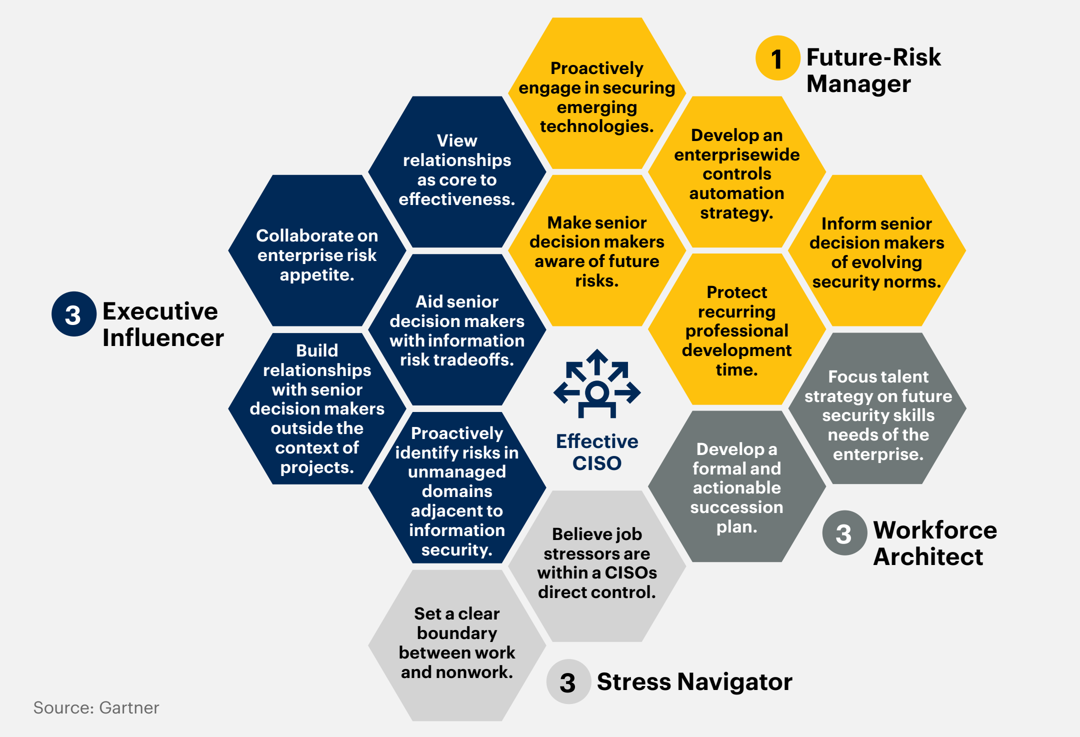
Source: Gartner

Recommended Next Steps

1. Consider the user experience when designing controls.
2. Design role-relevant cybersecurity learning experiences.
3. Focus on outcome-driven metrics to determine how well the organization is protected.
4. When engaging with supply chain vendors:
   - Identify potential security risks across shared data and infrastructure.
   - Ensure you’re meeting new regulatory mandates.
   - Create key partnerships across stakeholders to develop joint governance.
   - Evaluate and implement emerging best practices.

Improve leadership effectiveness

As the role of the SRM leader continues to evolve and expand, it's critical to continually assess and improve leadership effectiveness across categories. SRM leaders must align their priorities with those of the business to better drive value and protect the enterprise.



1 Future-Risk Manager
Proactively engage in securing emerging technologies.
Develop an enterprisewide controls automation strategy.
Make senior decision makers aware of future risks.
Inform senior decision makers of evolving security norms.
Protect recurring professional development time.
3 Executive Influencer
View relationships as core to effectiveness.
Collaborate on enterprise risk appetite.
Aid senior decision makers with information risk tradeoffs.
Build relationships with senior decision makers outside the context of projects.
Proactively identify risks in unmanaged domains adjacent to information security.
Effective CISO
3 Workforce Architect
Focus talent strategy on future security skills needs of the enterprise.
Develop a formal and actionable succession plan.
3 Stress Navigator
Believe job stressors are within a CISOs direct control.
Set a clear boundary between work and nonwork.

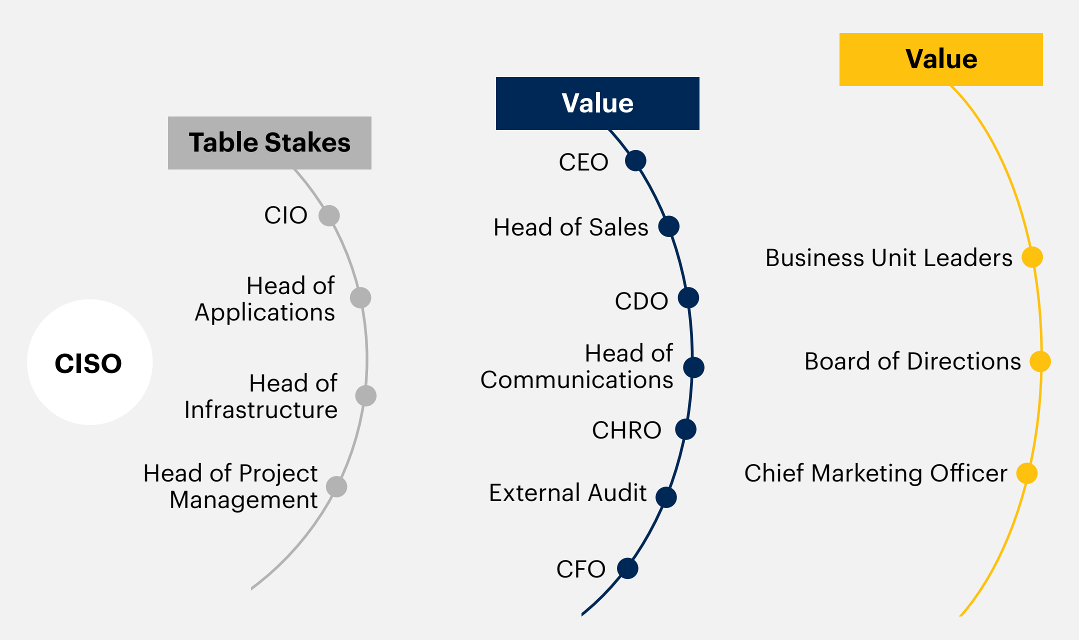
Source: Gartner

Recommended Next Steps

1. Build relationships with senior leadership outside of IT.
2. Prevent future risks by updating decision makers on new security norms.
3. Proactively secure business use of AI.
4. Track workforce performance and address skills gaps creatively.
5. Manage stress by maintaining boundaries between work and private life.

Drive security capabilities across the enterprise

Supporting groups outside the direct influence of the SRM leader to perform cybersecurity activities independently builds competence across the organization and allows SRM teams to focus on higher-value activities. Initiating a cybersecurity mesh strategy will help strengthen the security of integrated systems and protect access, configuration and data — no matter where assets are located.



Source: Gartner

Recommended Next Steps

1. Empower delivery teams to self-certify applications for release through the QP Express program.
2. Use group trust scoring to identify teams that are capable of executing cybersecurity activities.
3. Initiate your cybersecurity mesh strategy:
   - Assess maturity of currently deployed tools.
   - Survey your team's ability to integrate.
   - Determine a reasonable level of investment.
   - Decide how to build — with a mix of proprietary integrations and open standards, a consolidated platform, layered composable products or a combined approach.

Actionable, objective insight

Explore these additional complimentary resources and tools for security leaders:

Tool

IT Score for Security and Risk Management

Gain perspective on your highest-priority activities.

Learn More

Roadmap

The IT Roadmap for Cybersecurity

Create a resilient, scalable and agile cybersecurity strategy.

Download Roadmap

eBook

3 Must-Haves in Your Cybersecurity Incident Response Plan

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

Download Now

eBook

Four Facets of Effective CISO Leadership

Discover how best-in-class leaders tackle their expanding remit.

Download Now

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

Gartner

Advance your 2023 IT strategy by attending a Gartner destination conference!

In 2022, Gartner hosted 34 conferences with more than 46,000 business and technology professionals in attendance. Join forward-thinking leaders this year at conferences that accelerate learning, guide decision making and identify important trends.

Don’t miss out.

View the 2023 Conference Calendar today and find the conference that’s right for you.

→ Explore the Calendar

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.: 1 866 263 8917

International: +44 (0) 03301 628 476

Become a Client

Learn more about Gartner for Cybersecurity Leaders
gartner.com/en/cybersecurity

Stay connected to the latest insights

Gartner®