Gartner Research

2025 Strategic Roadmap for Cybersecurity Leadership

Pedro Pablo Perea de Duenas, Tom Scholtz
Tisha Bhambry

23 August 2024

Gartner®

2025 Strategic Roadmap for Cybersecurity Leadership

23 August 2024 - ID G00811077 - 24 min read

By: Pedro Pablo Perea de Duenas, Tom Scholtz, Tisha Bhambry

Initiatives: Cybersecurity Leadership; Build and Optimize Cybersecurity Programs

The increasingly complex threat landscape requires cybersecurity leaders to balance comprehensiveness with agility. This roadmap offers actionable steps and resources to establish and refine cybersecurity programs by combining cyber risk management activities, capabilities, people and technology.

Overview

Key Findings

- The acquisition, creation and delivery of technology is moving from central IT functions to lines of business. As a result, top-down cybersecurity operating models fail to align to business needs or effectively manage risk.
- Strategic planning processes that follow strict stage-gates and static assessments fail to adapt to shifting business needs, evolving threats and emerging technology. In short, waterfall planning fails to support agile businesses.
- Employees often adopt new technology, such as GenAI, before understanding the cybersecurity implications of their decisions. While these actions are typically well-intentioned (e.g., innovation, efficiency), they rarely consider the associated risks.
- Human behavior significantly impacts cyber risk — yet traditional, compliance-based approaches to security awareness fail to change employees' behavior as desired.
- Cybersecurity leaders face an overwhelming supply of cybersecurity vendors and services. As cybersecurity programs grow, they often add solutions with overlapping and redundant capabilities; this leads to more complexity and less effectiveness.

Recommendations

Cybersecurity leaders must develop strategic roadmaps that:

- Assess and evolve their security operating model to meet business needs and drive collaborative strategic decisions.
- Shift to a dynamic approach for enhancing the cybersecurity program and continuously adapting it to organizational and environmental changes through collaborative risk management, regular security assessments, environmental scanning and scenario planning.
- Enable secure AI initiatives — such as generative AI (GenAI) — to enhance business operations by establishing security requirements, guiding the use of AI and communicating its potential risks to support informed decision making.
- Develop a security behavior and culture program that considers practices, influences and platforms to foster and embed more secure employee behavior to reduce cybersecurity risk. Continuously monitor and assess the program's effectiveness for ongoing improvement.
- Optimize security tool adoption by evaluating new features in existing technologies before procuring new solutions. Regularly evaluate platform rationalization opportunities to enhance organization risk posture and efficiency.

Introduction

Historically, cybersecurity has been treated in isolation, focusing primarily on technical safeguards and often positioning cybersecurity leaders as obstacles to innovation.

However, with security now recognized as a business risk, a strategic and risk-based approach is essential. The digital shift and technologies like GenAI demand adaptive security leadership and evolving models.

This context forces security teams to play a critical role in strategic decision making and achieving organizational goals, moving from a background function to a cornerstone of business success.

Cybersecurity leaders are also challenged to foster a culture of security that promotes safer behaviors and practices. This involves getting rid of the old label of obstruction to become champions of innovation.

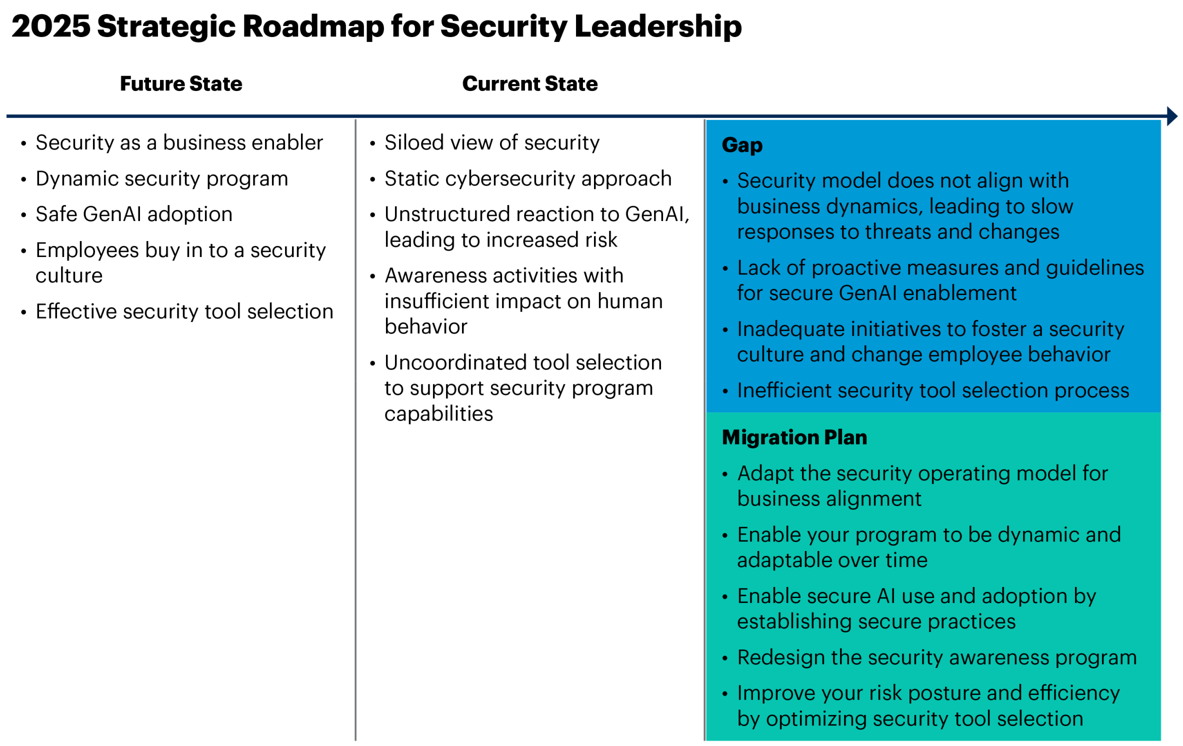
> **Cybersecurity strategy should always support and enable business priorities and outcomes. Yet only 60% of cybersecurity functions significantly change their strategies is response to shifting business objectives.[1]**
>
> *— 2023 Gartner Evolution of the Cybersecurity Leader and Their Function Survey*

Cybersecurity leaders should enable projects and add value by aligning with the organization's strategic direction and adopting a more dynamic operational model.

The 2025 Strategic Roadmap for Cybersecurity Leadership outlines a path for cybersecurity leaders to embrace innovation, enable inherently dynamic operations and adopt a forward-thinking approach to managing risks. The roadmap is structured around core components of a strategic roadmap (see Figure 1):

- A detailed analysis of cybersecurity's current state
- Top identified cybersecurity gaps
- A comprehensive migration plan
- The targeted future state

Figure 1: 2025 Strategic Roadmap for Security Leadership



2025 Strategic Roadmap for Security Leadership

Future State

- Security as a business enabler
- Dynamic security program
- Safe GenAI adoption
- Employees buy in to a security culture
- Effective security tool selection

Current State

- Siloed view of security
- Static cybersecurity approach
- Unstructured reaction to GenAI, leading to increased risk
- Awareness activities with insufficient impact on human behavior
- Uncoordinated tool selection to support security program capabilities

Gap

- Security model does not align with business dynamics, leading to slow responses to threats and changes
- Lack of proactive measures and guidelines for secure GenAI enablement
- Inadequate initiatives to foster a security culture and change employee behavior
- Inefficient security tool selection process

Migration Plan

- Adapt the security operating model for business alignment
- Enable your program to be dynamic and adaptable over time
- Enable secure AI use and adoption by establishing secure practices
- Redesign the security awareness program
- Improve your risk posture and efficiency by optimizing security tool selection

Source: Gartner
811077_C

Future State

Strong security leadership serves as the foundation for developing a robust security program, and it plays a vital role in guiding organizations toward achieving their goals. The future state goals that cybersecurity leaders should pursue include:

- Security as a business enabler
- A dynamic security program
- Safe GenAI adoption
- Employee buy-in to a security culture
- Effective security tool selection

Security as a Business Enabler

The democratization of technology acquisition, creation and delivery is reshaping the landscape of business operations. Today, these functions extend beyond the IT department, becoming part of the business lines themselves. In this evolving context, the future state will feature:

- **An adaptive security operating model:** Cybersecurity operating models must be inherently flexible and responsive, aligning with the business's needs for autonomy, innovation and agility. This alignment ensures that security not only responds to current challenges, but also anticipates and supports future business transformations.
- **Strategic role and responsibility distribution to foster collaboration:** Roles and responsibilities within security and business units will be clearly defined yet adaptable, promoting effective collaboration. This strategic distribution ensures that security considerations are seamlessly integrated into business initiatives, operations and strategic planning.
- **Security embedded in every business initiative:** Having an influential security team aligned with the business is key for effective security by design. This approach aligns security directly with business objectives, enhancing both resilience and agility. Security's active participation in business initiatives guarantees that security measures are effectively incorporated from the start.

A Dynamic Security Program

To address evolving threats and changes, cybersecurity leaders must continually adapt their programs. This ensures agility and responsiveness, balancing defense with business growth.

The future state of a dynamic security program will feature:

- **Embedded collaborative risk management and periodic assessments:** Collaborative risk management will serve as the strategic foundation, enabling informed decisions as threats and organizational context evolve. This will be complemented by carefully selected, targeted periodic assessments such as cybersecurity practices, control and functional maturity, compliance, and third-party cyber risk.

- **Strategic use of environmental scanning and scenario planning:** The practice of environmental scanning to identify external trends, threats and opportunities will become an indispensable input to sharpen security programs. This approach, combined with scenario planning, will equip organizations to navigate and prepare for diverse future landscapes, aligning security strategies with business goals.

Safe GenAI Adoption

For safe GenAI adoption, cybersecurity leaders should collaborate with stakeholders and GenAI initiative owners to manage associated risks. This will help to enable informed decisions, rather than block them, to harness GenAI's full potential safely, securely and ethically.

The future state will feature:

- **Robust AI security governance:** This includes comprehensive policies and guidelines tailored to manage the security risks inherent in GenAI technologies. They ensure the secure, safe and ethical development, deployment, and operational use of GenAI systems.

- **AI trust, risk and security management (TRiSM) implementation:** AI TRiSM ensures governance, trustworthiness, fairness, reliability, robustness, efficacy, security and data protection for AI models and applications. It encompasses model monitoring, interpretability, explainability, anomaly detection, data protection, model management, adversarial attack resistance, and AI-specific application security.

- **AI integration in cybersecurity:** Cybersecurity leaders consider leveraging the potential of AI capabilities to enhance the security posture and overall efficiency, which involves acquiring or implementing AI-driven tools to detect threats, automate responses and perform other key operations.

Employee Buy-In to a Security Culture

To encourage employees to be more security-conscious in all their actions, cybersecurity programs must change employee attitudes toward cybersecurity. This goes beyond traditional awareness training and aims to instill a security mindset throughout the organization.

This future state will feature:

- **Long-term behavioral improvement program:** A rolling multiyear initiative is firmly established, transforming, and then embedding, more secure employee behaviors. This program will systematically promote secure employee behaviors and mitigate practices that pose cybersecurity risks, effectively instilling security consciousness as a vital pillar of the organization's culture.

- **Cultivated security-conscious mindset:** Employees at all levels and in all roles across the organization will be mindful of cybersecurity and inherently undertake their work as securely as possible. Cybersecurity leaders will make sure that managers understand they are responsible for ensuring this.

- **Behavior-centric metrics for success:** The organization will use specific outcome- and behavior-driven metrics to gauge the effectiveness of its security culture. These metrics will provide quantifiable evidence of how security behaviors have improved over time.

Effective Security Tool Selection

Selecting the right security tools can greatly underpin the success of a security program, making some operations more efficient, facilitating cyber risk management, threat detection and other key operations. The goal is to maintain a minimum effective toolset for security.

The future state includes:

- **Maximizing and extending current technologies:** The organization will maximize the potential of its current technological investments. This approach prioritizes leveraging the capabilities of existing tools over acquiring new solutions, and includes exploring technologies or services provided by current vendors that could offer extended capabilities through contact adjustments.

- **Regular platform rationalization:** The organization will regularly assess and evaluate existing security technologies and services to find out opportunities for consolidation, always seeking to enhance the security operations and avoid redundant investments.

Current State

Cybersecurity leaders often focus on daily tasks, which, though essential, can divert attention from strategic activities needed to enhance and prepare the cybersecurity program for evolving threats and challenges.

Today, many security programs have these attributes:

- A siloed view of security and limited collaboration with business stakeholders
- A static cybersecurity approach that cannot adapt operations easily to changing environments and business priorities
- An unstructured reaction to GenAI, leading to increased risk
- “Awareness activities” that have insufficient impact on human behavior and culture
- Uncoordinated tool selection to support security program capabilities

Siloed View of Security

Security teams often operate in isolation, focusing on technical security measures without integrating a broader business perspective. This isolation stems from:

- Legacy perspectives that cybersecurity is purely an IT problem, often fostered by traditional organizational structures where the security team was part of the IT organization.
- A historical divide in the organization structure between security and business functions, where each has developed a distinct culture and language.
- A lack of effective understanding and communication about the strategic importance of security to the organization’s overall goals. Skilled staff shortages exacerbate this.

A siloed approach misaligns security efforts with business objectives, undermining effectiveness. The challenge grows with the increasing volume, complexity and dispersion of IT initiatives, making it infeasible for cybersecurity teams to make and review every decision.

Static Cybersecurity Approach

Organizations often rely on a static cybersecurity approach, characterized by repetitive practices and predetermined controls. While effective against known risks, this method struggles with novel and rapidly evolving cyberthreats, technological advances and shifts in organizational strategies.

Furthermore, cyber risk programs and investments within organizations are predominantly focused on compliance, potentially overlooking emerging threats. Additionally, these risk management efforts are generally periodic, which may not always consider significant organizational changes or new initiatives.

Scanning the external environment for trends and threats is often overlooked. Bypassing this action may restrict organizations' ability to anticipate technological shifts, emerging threats and regulatory changes, which can lead to misalignment between cybersecurity strategies and broader business objectives.

Unstructured Reaction to GenAI Leading to Increased Risk

Units within organizations often aggressively pursue technological advancements like GenAI to gain a competitive edge or streamline operations. However, rushing to adopt new technologies without considering risks increases vulnerability to threat actors.

The situation worsens when employees, motivated by productivity gains or curiosity, use these technologies without understanding their security implications. Consequences such as exposing sensitive company data are often the result. The lack of specific policies and comprehensive guidelines for safe technology use further compounds the issue, reinforcing a fragmented approach to cybersecurity. Additionally, security teams often exhibit a reluctance toward GenAI initiatives, instead of working toward appropriate risk management activities.

Awareness Activities With Insufficient Impact on Human Behavior and Culture

Organizations may try to boost awareness of cybersecurity, but awareness alone does not go far enough:

- Gartner research found that 93% of employees performing unsecured actions in the workplace already knew their behavior increased risk to their organization, [2] indicating that security awareness training alone has little influence on employee work practices.
- The Verizon Data Breach Investigations Report showed that 68% of all data breaches involved a human element, and nearly 30% of all data breaches involved phishing and other social engineering attacks. [3]
- Organizations often use training completion rates (84%) and phishing simulation click-through rates (72%) as the primary metrics to measure the effectiveness of their security awareness programs, according to a study by the National Institute of Standards and Technology. [4]

While these performance indicators might help meet cybersecurity compliance obligations, they do not demonstrate that security awareness training effectively reduces overall cybersecurity risk.

Cybersecurity leaders are increasingly acknowledging that merely raising employee security awareness is insufficient for minimizing cybersecurity risk from avoidable employee actions. When examining current security awareness initiatives, which primarily consist of delivering security awareness training and running phishing simulations, most organizations find that these efforts achieve little beyond regulatory compliance. The impact on changing human behavior and culture within organizations is very limited.

Uncoordinated Tool Selection

Organizations and specifically cybersecurity leaders sometimes tend to address productivity and efficiency challenges in security programs by acquiring new tools and technologies, frequently without an adequate and comprehensive analysis to ensure that the tools meet their specific needs. This habit can lead to increased costs of security programs without delivering expected returns.

Many organizations tend to overlook the potential of existing tools before analyzing a new purchase. They may then miss opportunities to enhance their security program and capabilities through extensions or additional features offered by current vendors.

Gap Analysis and Interdependencies

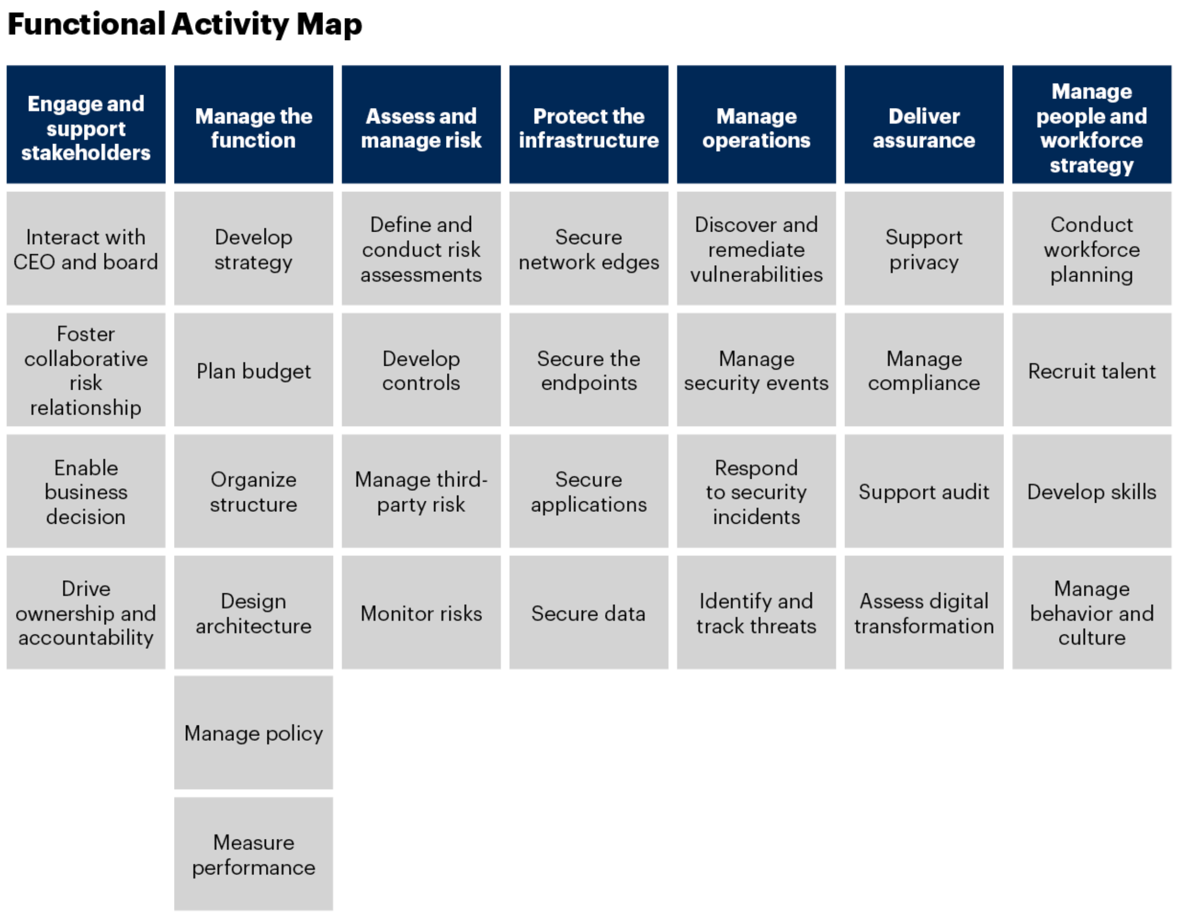
To successfully navigate the journey forward, cybersecurity leaders can conduct a comprehensive analysis to identify the gaps between the current state and the envisioned future state. This involves pinpointing areas where the organization´s current cybersecurity program and strategy may not fully meet the needs, and assessing the severity of these gaps to prioritize certain initiatives. To measure this severity, organizations can use a combination of cybersecurity functional and control-level assessments.

Gartner offers specialized tools to conduct these two types of maturity assessments, which also provide benchmarking data and help with the prioritization: capability maturity assessment and controls maturity assessment.

Capability Maturity Assessment

IT Score for Security and Risk Management (IT Score for SRM): This tool allows organizations to conduct a maturity self-assessment of the security function, allowing organizations to evaluate the capabilities of their cybersecurity program and help with strategic planning and resource allocation. It gauges the performance across seven functional security objectives and 30 key management activities (see Figure 2). Organizations can choose to assess all or a subset of these activities based on their specific needs.

Figure 2: IT Score for SRM: Functional Activity Map



Functional Activity Map

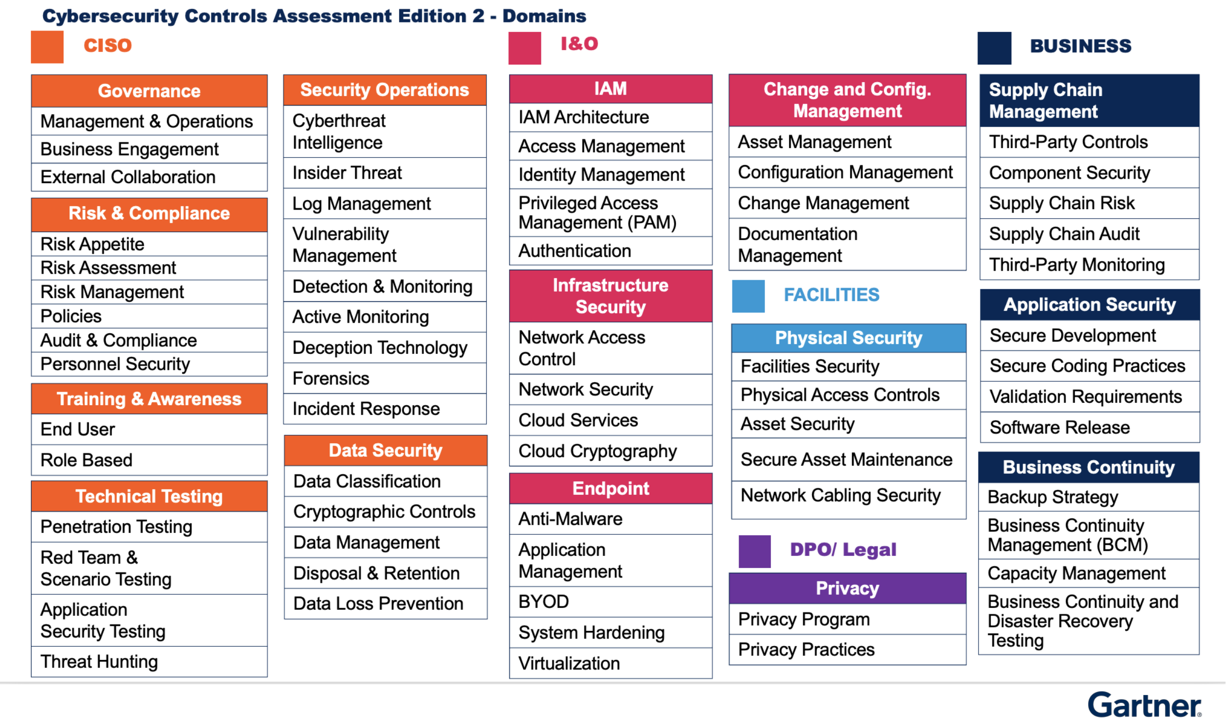
Engage and support stakeholders	Manage the function	Assess and manage risk	Protect the infrastructure	Manage operations	Deliver assurance	Manage people and workforce strategy
Interact with CEO and board	Develop strategy	Define and conduct risk assessments	Secure network edges	Discover and remediate vulnerabilities	Support privacy	Conduct workforce planning
Foster collaborative risk relationship	Plan budget	Develop controls	Secure the endpoints	Manage security events	Manage compliance	Recruit talent
Enable business decision	Organize structure	Manage third-party risk	Secure applications	Respond to security incidents	Support audit	Develop skills
Drive ownership and accountability	Design architecture	Monitor risks	Secure data	Identify and track threats	Assess digital transformation	Manage behavior and culture
	Manage policy					
	Measure performance					

Source: Gartner
804502_C

Controls Maturity Assessment

Cybersecurity Controls Assessment (CCA) : The CCA provides a view of the cybersecurity control maturity of the organization. It is aligned with industry-recognized frameworks and standards such as ISO 27002:2022, NIST 800-53 rev 5 and CIS 18 v8.0. This self-assessment also provides a peer benchmarking tailored to specific industry and risk exposure levels (see Figure 3).

Figure 3: Cybersecurity Controls Assessment



Cybersecurity Controls Assessment Edition 2 - Domains

CISO

Governance
- Management & Operations
- Business Engagement
- External Collaboration

Risk & Compliance
- Risk Appetite
- Risk Assessment
- Risk Management
- Policies
- Audit & Compliance
- Personnel Security

Training & Awareness
- End User
- Role Based

Technical Testing
- Penetration Testing
- Red Team & Scenario Testing
- Application Security Testing
- Threat Hunting

Security Operations
- Cyberthreat Intelligence
- Insider Threat
- Log Management
- Vulnerability Management
- Detection & Monitoring
- Active Monitoring
- Deception Technology
- Forensics
- Incident Response

Data Security
- Data Classification
- Cryptographic Controls
- Data Management
- Disposal & Retention
- Data Loss Prevention

I&O

IAM
- IAM Architecture
- Access Management
- Identity Management
- Privileged Access Management (PAM)
- Authentication

Infrastructure Security
- Network Access Control
- Network Security
- Cloud Services
- Cloud Cryptography

Endpoint
- Anti-Malware
- Application Management
- BYOD
- System Hardening
- Virtualization

Change and Config. Management
- Asset Management
- Configuration Management
- Change Management
- Documentation Management

FACILITIES

Physical Security
- Facilities Security
- Physical Access Controls
- Asset Security
- Secure Asset Maintenance
- Network Cabling Security

DPO/ Legal

Privacy
- Privacy Program
- Privacy Practices

BUSINESS

Supply Chain Management
- Third-Party Controls
- Component Security
- Supply Chain Risk
- Supply Chain Audit
- Third-Party Monitoring

Application Security
- Secure Development
- Secure Coding Practices
- Validation Requirements
- Software Release

Business Continuity
- Backup Strategy
- Business Continuity Management (BCM)
- Capacity Management
- Business Continuity and Disaster Recovery Testing

Source: Gartner

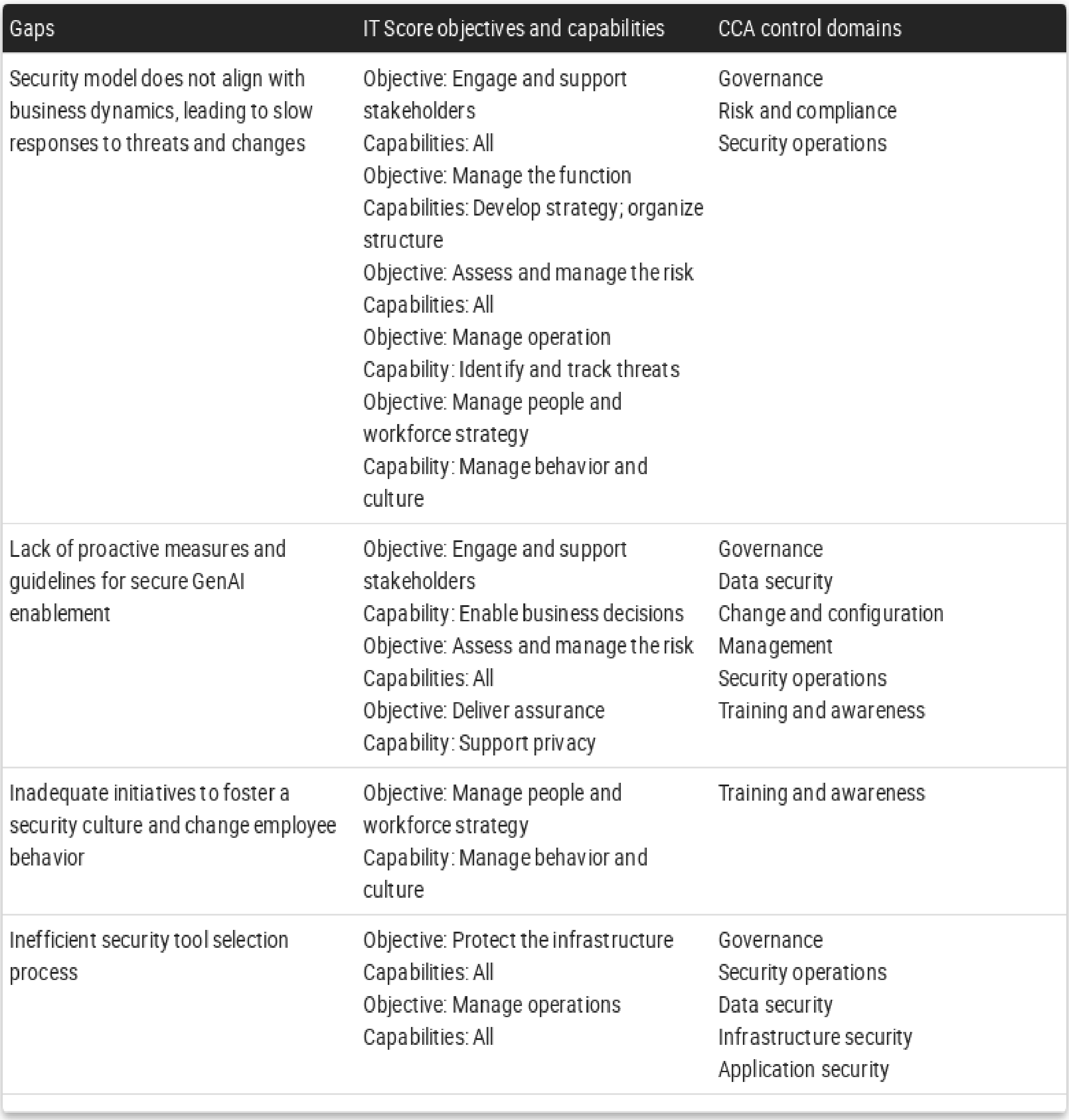
Unlike the IT Score for SRM, the CCA requires responses to all of the previous control areas without the option to select subsets.

Table 1 links the different aspects that are assessed in both tools to the gaps identified in Figure 1:

- The second column shows the recommended objectives and capabilities from the IT Score for Security and Risk Management (SRM) tool that help to determine the severity of the different gaps.
- Although the CCA tool does not allow analysis of specific control domains to analyze, the third column specifies the most pertinent control domains related to each identified gap. For these domains, the tool provides detailed maturity insights and benchmarking data regardless of the framework selected.

Table 1: Gaps vs. Objectives, Capabilities and Control Domains

(Enlarged table in Appendix)



Gaps	IT Score objectives and capabilities	CCA control domains
Security model does not align with business dynamics, leading to slow responses to threats and changes	Objective: Engage and support stakeholders Capabilities: All Objective: Manage the function Capabilities: Develop strategy; organize structure Objective: Assess and manage the risk Capabilities: All Objective: Manage operation Capability: Identify and track threats Objective: Manage people and workforce strategy Capability: Manage behavior and culture	Governance Risk and compliance Security operations
Lack of proactive measures and guidelines for secure GenAI enablement	Objective: Engage and support stakeholders Capability: Enable business decisions Objective: Assess and manage the risk Capabilities: All Objective: Deliver assurance Capability: Support privacy	Governance Data security Change and configuration Management Security operations Training and awareness
Inadequate initiatives to foster a security culture and change employee behavior	Objective: Manage people and workforce strategy Capability: Manage behavior and culture	Training and awareness
Inefficient security tool selection process	Objective: Protect the infrastructure Capabilities: All Objective: Manage operations Capabilities: All	Governance Security operations Data security Infrastructure security Application security

Source: Gartner (August 2024)

Assessment results offer a proposed prioritization of specific capabilities and controls based on three critical criteria: **maturity, importance** and **benchmarking.** These evaluations, when considered alongside organizational factors such as context and risk appetite, are instrumental in guiding cybersecurity leaders to set the target maturity levels for controls and capabilities, and therefore identifying the gaps.

Note that there are many alternative maturity assessments available, including proprietary and free tools. In addition, the results of risk assessments, vulnerability assessments, penetration tests and audit findings can provide valuable additional insights.

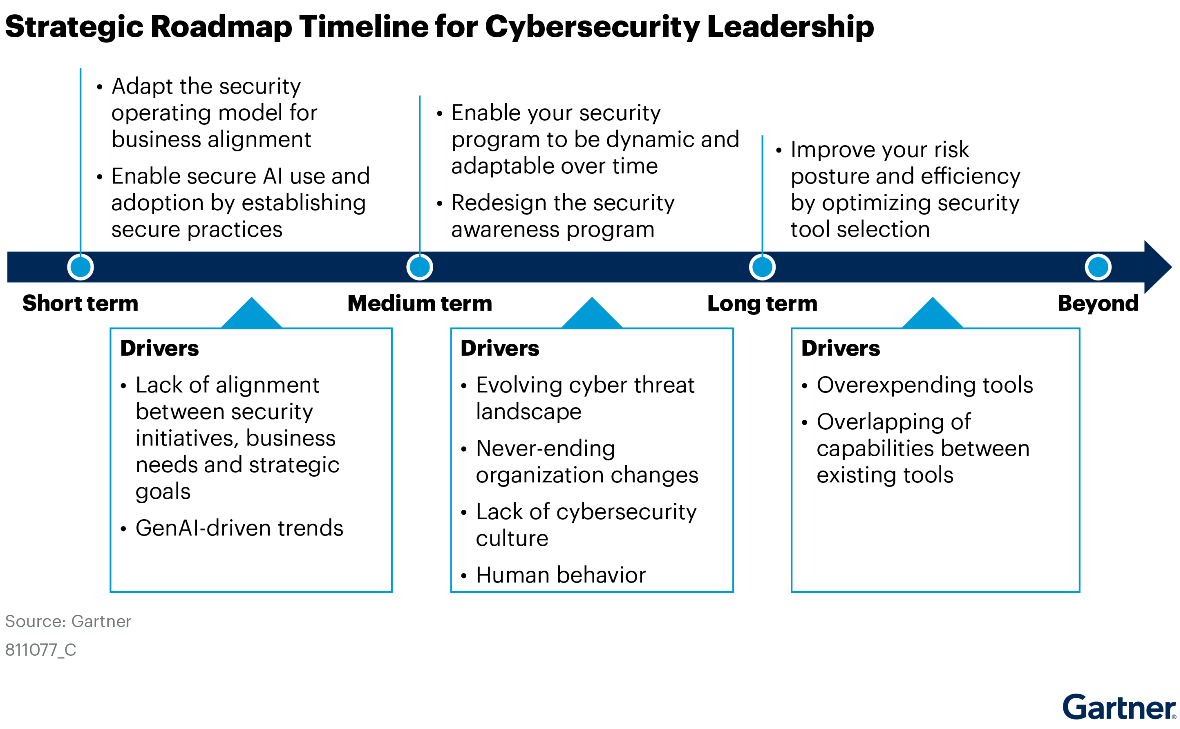
Migration Plan

Following the execution of assessments such as the Cybersecurity Control Assessment (CCA) and the IT Score for SRM, cybersecurity leaders will gain valuable insight about their gaps and their goals.

The reports from such assessments provide actionable information that will aid in bridging these gaps. These actions are instrumental in achieving the described future state.

Figure 4 outlines the actions.

Figure 4: Strategic Roadmap Timeline for Cybersecurity Leadership



Strategic Roadmap Timeline for Cybersecurity Leadership

Short term

- Adapt the security operating model for business alignment
- Enable secure AI use and adoption by establishing secure practices

Drivers

- Lack of alignment between security initiatives, business needs and strategic goals
- GenAI-driven trends

Medium term

- Enable your security program to be dynamic and adaptable over time
- Redesign the security awareness program

Drivers

- Evolving cyber threat landscape
- Never-ending organization changes
- Lack of cybersecurity culture
- Human behavior

Long term

- Improve your risk posture and efficiency by optimizing security tool selection

Drivers

- Overexpending tools
- Overlapping of capabilities between existing tools

Beyond

Source: Gartner
811077_C

This prioritization has been done based on Gartner analysts' observations from research and client interactions. Cybersecurity leaders must ensure that their teams are working on the actions from the strategic roadmap that offer the greatest business impact. The order of the actions can be adjusted according to the specific organization's context, priorities and other factors. For guidance on security portfolio prioritization, see Security Portfolio Prioritization: How to Structure and Assess Security Investment Decisions.

Higher Priority

Adapt Your Security Operating Model for Business Alignment

The security operating model adaptation requires redefining boundaries and responsibilities to enable quicker decision making and increased adaptability to evolving security landscapes. Each department and business unit must clearly understand its role in this dynamic setting. Organizations should adapt the security operating model to enhance business autonomy, innovation and agility. See CISO Effectiveness: Security Operating Models Are Evolving.

Cybersecurity leaders should strive to become facilitators of cybersecurity risk decisions by actively engaging with business stakeholders and promoting good cyber judgment. To that end, implement a well-defined responsible, accountable, supporting, consulted and informed (RASCI) matrix, approved, informed and periodically reviewed by the cybersecurity committee, to delineate clear cybersecurity roles and responsibilities across the organization. See Tool: Cybersecurity Program RASCI Matrix.

A well-represented security steering committee with members from various business units helps cybersecurity leaders to ensure a comprehensive understanding of business needs and serves as the primary mechanism to drive appropriate and timely investment and resource allocation decisions. See CISO Foundations: How a Steering Committee Enhances Cybersecurity Governance.

Finally, the roles and responsibilities previously defined in the RASCI matrix and the establishment of a security committee should be formalized as part of an enterprise information security charter. See Tool: Enterprise Information Security Charter Template.

Enable Secure AI Use and Adoption by Establishing Secure Practices

Due to the expanding use and adoption of GenAI, organizations should define and implement security measures to address the emerging risks that this poses. Cybersecurity leaders need to prepare for the impacts from generative AI and guide how their organizations build and consume it. To learn about these impacts and how to address them, see 4 Ways Generative AI Will Impact CISOs and Their Teams.

Owners of AI adoption initiatives are ultimately responsible for ensuring the monitoring of AI systems in use to actively identify and mitigate any deviations or unintended outcomes. Cybersecurity leaders can define the protocols and provide guidance on these aspects. The GenAI TRiSM market comprises multiple software and services segments that continuously support security, data protection and risk mitigation for adopters of GenAI applications and model interactions. See Innovation Guide for Generative AI in Trust, Risk and Security Management.

Rapid AI adoption is forcing cybersecurity leaders to quickly create security guidance for GenAI development, acquisition and use. To formalize these practices and provide a structured approach to managing AI risks, Gartner recommends developing a generative AI security policy. Use Tool: Generative AI Security Policy Template.

Medium Priority

Enable Your Security Program to Be Dynamic and Adaptable

A security program requires continuous evolution and should never be considered static or only updated annually. Ongoing refinement helps security measures and activities remain

Actionable, objective insight

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

Report

Cybersecurity Trends: Optimize for Resilience and Performance

Use this report to equip your cybersecurity function for greater resilience.

Download Now

Roadmap

IT Roadmap for Cybersecurity

Create a resilient, scalable and agile cybersecurity strategy.

Download Now

eBook

Leadership Vision for Security and Risk Management Leaders

Explore the top 3 strategic priorities for security and risk management leaders.

Download Now

Webinar

Strengthen Your Cybersecurity Leadership to Navigate Evolving Security Landscape

Explore this 5-part series for insights into the evolving landscape.

Watch Now

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

Connect With Us

Get actionable, objective insight that drives smarter decisions and stronger performance on your mission-critical priorities. 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 Cybersecurity Leaders
gartner.com/en/cybersecurity

Stay connected to the latest insight

Gartner