Gartner Research

How Midsize Enterprise CIOs Create an Effective Cybersecurity Operations Strategy

Patrick Long

11 March 2024

Gartner

How Midsize Enterprise CIOs Create an Effective Cybersecurity Operations Strategy

Published 11 March 2024 - ID G00802355 - 11 min read

By Analyst(s): Patrick Long

Initiatives: Midsize Enterprise IT Leadership

Cybersecurity talent shortages can disproportionately affect midsize enterprises due to scale and budget. Midsize enterprise CIOs must get creative and utilize all tools and services at their disposal to develop and execute a well-defined cybersecurity operations strategy.

Overview

Key Findings

- Midsize enterprises (MSEs) typically have between one to four dedicated cybersecurity full-time equivalents (FTEs), which are insufficient to properly run a security operations center.
- MSE IT departments are often staffed by versatilists as opposed to specialists, making defining roles and responsibilities for cybersecurity functions difficult.
- According to the 2023 Gartner MSE Baseline survey, 47% of MSE CIOs and the most senior IT leaders use external managed services to handle skills gaps in both cyber and information security.
- MSE IT budgets, cross-industry, are 4.6% of revenue and cybersecurity budgets are 5% of the overall IT budget, making cybersecurity spend very low. This limits the ability to add security tools and resources to the MSEs cybersecurity portfolio, which impacts the capabilities of a security operations function.

Recommendations

- Communicate the critical risk of low protection to leadership by utilizing outcome-driven metrics to show where there may be gaps in coverage.
- Identify and nurture skills within the IT department for tasks that do not require specific, specialized security skills by leveraging tools such as NIST's NICE Framework and upskilling training to assign security responsibilities.
- Augment your current security posture by leveraging third-party services, such as managed security service providers (MSSPs) and managed detection and response (MDR), as a way to outsource much of the tactical effort, allowing the internal IT staff to focus on the maturation of the security program.

Strategic Planning Assumption

By 2026, 70% of midsize enterprises' security portfolios will be outsourced, up from the 40% of outsourced security portfolios today.

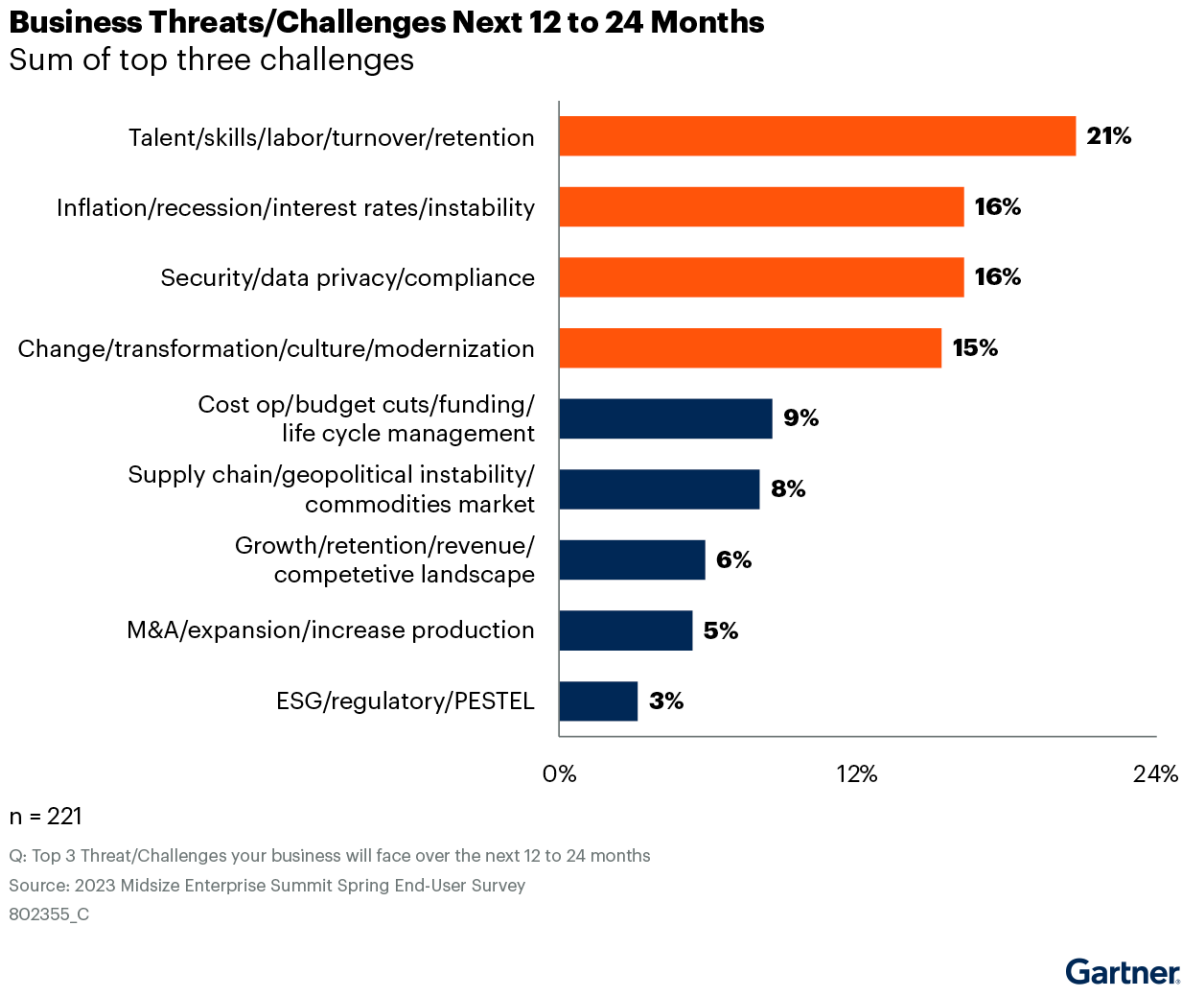
Introduction

MSEs Need Security Operations to Ensure Protection and Resiliency

With one FTE for every 20 IT FTEs, creating a security operations center or even fully leveraging its capabilities can be a significant struggle for MSEs. [1] Additionally, 73% of cybersecurity standard framework audit questions ask for the existence of a control as opposed to their performance. This means that if your focus is purely on following a framework like NIST or ISO, your MSE still runs the risk of not having an efficient security posture.

So it comes as no surprise that FTEs and their skill sets, uncertain costs, security, and the need to continue to grow and transform, are all key concerns for MSEs (see Figure 1).

Figure 1: Business Threats/Challenges Next 12 to 24 Months



MSEs must improve or establish their security operations to ensure protection and resiliency.

Analysis

Utilize Outcome-Driven Metrics for Cybersecurity

With 62% of MSEs not having a chief information security officer, it is often challenging for MSE CIOs to prioritize improvements and align those improvements with an appropriate level of protection. [2] Cybersecurity outcome-driven metrics (ODMs) provide a direct line of sight between the performance of security investments and business outcomes. They are constructed by aligning security controls that are measured with the intended protection outcome of the investment. In this manner, ODMs simultaneously reflect protection levels and value for investment (see Quick Answer: What Is a Cybersecurity Outcome-Driven Metric?).

MSE CIOs must measure security controls using data that reflects their business' requirements to help determine any potential pitfalls or gaps; whether in overall tool coverage or overburdened personnel. Taking this approach to cybersecurity metrics and auditing protection and resiliency levels allows MSE CIOs to allocate their resources to meet specific tasks, as opposed to blindly following a framework with no real end goal. The goal of any cybersecurity program should be to balance risk with the ability to run the business. Gartner has created 16 different control groups, that are currently being benchmarked, that MSEs can use to improve the efficacy of their security program (see Figure 2):

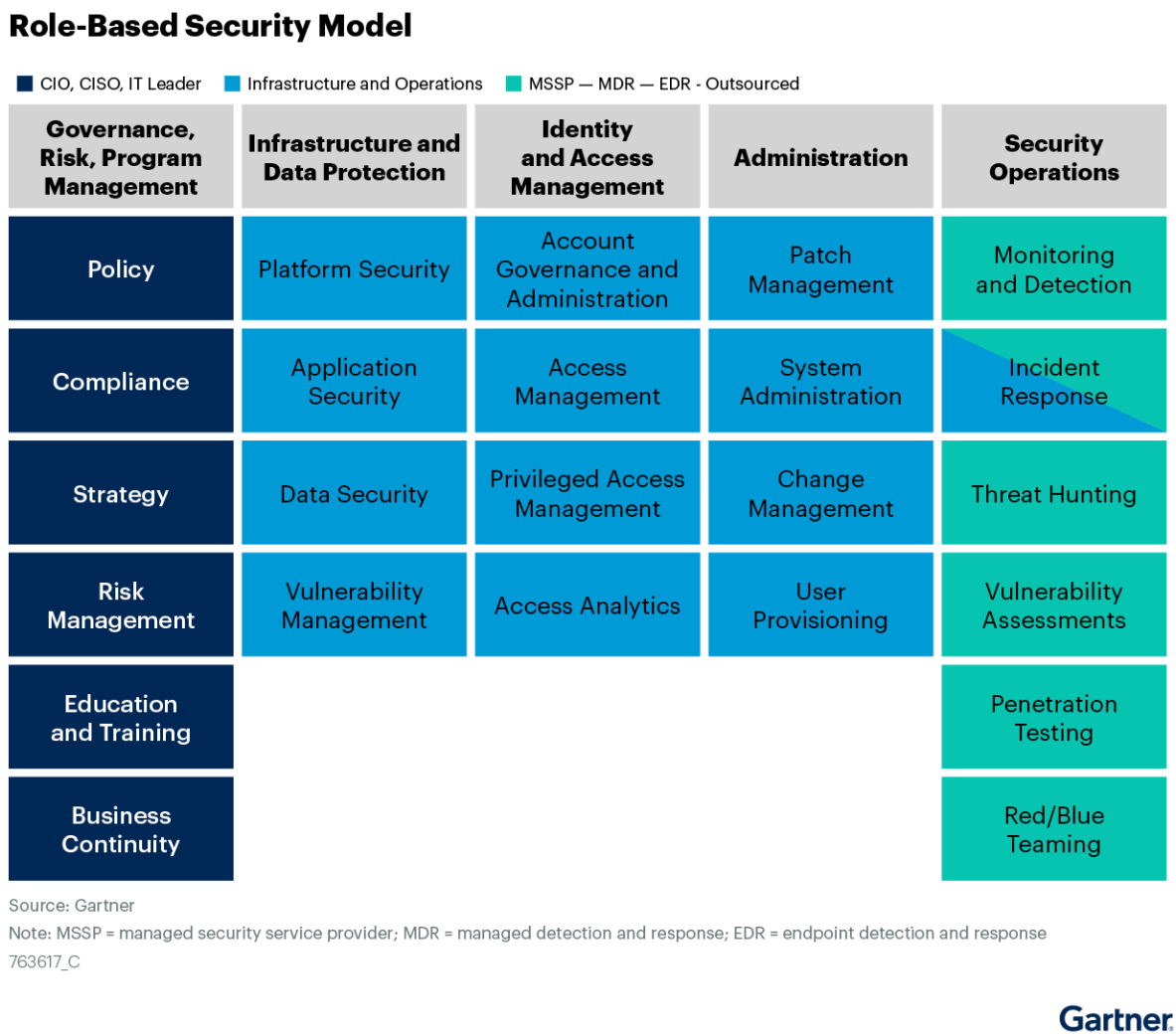
- Incident containment time
- Incident remediation time
- OS patching cadence
- Third-party risk engagement
- Unassessed third parties
- Expired policy exceptions
- Endpoint protection coverage
- Ransomware recovery exercise
- Ransomware downtime workarounds
- Cloud security coverage
- Multifactor authentication coverage
- Access removal time
- Privileged access management
- Security awareness training
- Phishing training click-throughs
- Phishing reporting rates

Midsize enterprise technology leaders should not try to “boil the ocean” when implementing cybersecurity ODMs. Instead, pick one to three different metrics where data already exists. This allows for quick wins and a foundation to build a more mature security organization, regardless of the number of individuals in dedicated, security operations positions. Cybersecurity ODMs will also help in advocating for additional resources or headcount for cybersecurity positions by showing where protection is not at a level the business deems appropriate.

Identify and Nurture Cybersecurity Skills Within the IT Department

In most midsize organizations, the group providing support for infrastructure and operations is often the same group tasked with securing those environments. In order to address the lack of dedicated headcount, midsize enterprise CIOs must focus on distributing security roles and functions to their existing team members; in particular, those roles and functions relating to incident response. Regardless of the size of the IT team, all facets of information security must still be addressed. Figure 2 outlines the five critical security categories and requisite areas that must be addressed. With small teams, it is not uncommon to have one individual responsible for several security roles.

Figure 2: Role-Based Security Model



Source: Gartner
Note: MSSP = managed security service provider; MDR = managed detection and response; EDR = endpoint detection and response
763617_C

Gartner

To help with assigning responsibilities, MSE CIOs can leverage NIST's Workforce Framework for Cybersecurity (NICE). MSE security functions are a collaborative effort and a responsibility shared among resources within the infrastructure and operations teams. Therefore, it is not uncommon for a network engineer to be in charge of the firewall or a desktop engineer to have responsibility for installing and maintaining antivirus software. This operating dynamic makes governance critical, especially when a small pool of resources is given multiple, sometimes conflicting, information about its next priorities. By leveraging the NICE Framework, MSE CIOs are able to identify those specific capabilities needed to maintain a good cybersecurity posture, while simultaneously showing evidence about how their FTEs are being utilized to mitigate business risk. Compiling the capability statements that are not able to be fulfilled enables midsize enterprise technology leaders to advocate for additional resources, headcount or third-party services to fill the gap.

Upskilling also plays a vital role in this dynamic. Regardless of whether a midsize enterprise technology leader decides to leverage the NICE framework (see How Midsize Enterprises Can Exploit the NICE Framework to Secure Cybersecurity Talent) or not, I&O FTEs who perform security functions must continue to be trained on the latest techniques and technologies.

MSE CIOs need to work with their human resource partners to offer upskilling opportunities for their staff. This needs to be a balanced delivery of both tactical learning and professional development. Consider internal mentorship programs, cross-role training, certification reimbursement and conferences as options to enhance your team's capabilities. This kind of training can also be provided through educational institutions, cybersecurity communities or through vendors focused on providing training exercises and environments.

Yes, there is a risk that training your staff will make them more marketable and they may leave, but that also becomes a high point in the employer value proposition. Focus on the fact that, as their skill sets improve, employees will provide improved security processes and practices within your organization. Failing to make the investment in training may actually accelerate their decision to find employment elsewhere. This ultimately introduces additional risk to the organization by potentially decreasing your ability to identify and react to emerging threats.

Utilize Third-Party Services to Expand Your Cybersecurity Resource Pool

MSE CIOs responsible for security operations must leverage their understanding of business risks and drivers, environments, users and other assets to best mitigate the threat techniques that target the organization. A minimum viable security operations center (SOC) takes 10 to 12 dedicated security FTEs working 24/7, 365 days a year, costing potentially millions of dollars including additional investment in tools (see SOC Model Guide). For MSEs unable to take advantage of an internal SOC, the best available alternative would be to outsource the tactical effort of operating a SOC. MSE CIOs are increasingly seeing this as the best option with 47% of MSE CIOs using external managed services to handle skills gaps in both cyber and information security. [3]

There are multiple types of managed services for cybersecurity, but the four most suited for MSEs are:

- **Managed security service providers (MSSP):** MSSPs provide organizations with a variety of management and operational services specific to security technologies and business outcomes for security. Capabilities include:
  - Security monitoring
  - Detection and response
  - Exposure assessment and management
  - Security consulting
  - Security technology implementation

MSSPs are delivered in a variety of modes: in the providers' cloud infrastructure, as consultative engagements or through staff augmentation and on-premises. MSS providers offer a variety of different engagement models. These include heavily customized and consultancy-led models and commoditized technology-management-driven experiences. MSSPs are most appropriate for MSEs that have made a significant investment in tooling, but don't have FTEs to actively monitor, administer and tune the tools.

- **Managed detection and response (MDR):** MDR services provide customers with remotely delivered security operations center (SOC) functions. These allow organizations to rapidly detect, analyze, investigate threats and actively respond through threat disruption and containment. MDR providers offer a turnkey experience, using a technology stack that commonly covers endpoint, network, logs and cloud, making it ideal for MSEs that have not made significant technology investments. This telemetry is analyzed in the provider's platform by experts skilled in threat hunting and incident management.
- **Endpoint detection and response (EDR):** EDR analyzes system, process and user activity to detect security threats. It provides remedial guidance for threats that bypass prevention controls and enables endpoint threat investigations. EDR capabilities are often included in endpoint protection platforms and delivered as software agents connected to centralized cloud-based security analytics and management software. EDR is often a requirement for cybersecurity insurance and is a good starting point for other kinds of managed cybersecurity services.

- **Extended detection and response (XDR):** XDR delivers unified threat detection, investigation and response (TDIR) capabilities. XDR solutions integrate threat intelligence and telemetry data from multiple sources, with security analytics to provide contextualization and correlation of security alerts (XDR relies on native sensors to obtain telemetry data). XDR can be delivered on-premises or as a SaaS offering, and is typically deployed by organizations with smaller security teams or to meet a subset of SecOps use cases. XDR can be delivered through both single vendor-specific tools (i.e., firewalls and endpoint agents) or an open format, leveraging current tools in an MSE's environment to deliver the service.

Regardless of what type of managed service an MSE uses, incident response (IR) will be a critical function of internal resources. Typically in all of these services, incident response is limited to very defined SLAs and does not include remediation. Incident response can also be outsourced, but often comes in at a higher cost.

The cost of these services is also an important factor when determining whether to try and hire more internal resources as opposed to utilizing a third-party service. For some MSE environments, it is possible to contract a managed service provider for less than the cost of one senior FTE. MSSP and MDR/XDR services range from $75,000/85,000 to $110,000/125,000 per year (dependent on number of monitored assets) with EDR services potentially coming in at lower price points. Additional benefits can include:

- Faster response times isolating compromised devices
- Freed-up staff to focus on maturity, and triaging and validating alerts
- Reducing burnout and becoming overwhelmed with alert triage
- Reducing staff costs by not having to hire for multiple shifts
- Reducing tool costs (i.e., not needing a security information and event management [SIEM] tool)
- Access to additional services such as risk assessments and/or incident response

Evidence

[1] **IT Key Metrics Data 2024: Industry Measures — Insights for Midsize Enterprises.** The ITKMD 2024 cohort represents over $15 trillion in total revenue and over $562 billion in total IT spend. In 2023, Gartner collected 4,139 data points in total from public and private enterprises from more than 80 countries in 21 industry sectors to contribute toward all of the IT Key Metrics Data series of reports. For more information, including the distribution of data points by region, see IT Key Metrics Data 2024: Demographics.

- For the key industry measures contained in this report, we collected 937 data points, from midsize enterprises. The result is the most comprehensive and authoritative IT spending and staffing data in the industry.
- For this IT spending and staffing report, "midsize enterprise" is loosely defined as any enterprise with between USD $50 million and $1 billion in revenue (for-profit enterprises) or operating budget (government enterprises).

[2] **2023 Midsize Enterprise Summit Spring End-User Survey.** Responses are based on results from 101 CIOs or the most senior IT leaders in a midsize organization (that is, organizations with an annual revenue of $50 million to less than $1 billion) in North America at the Channel Company's Midsize Enterprise Summit in April 2023. Disclaimer: The results of this survey do not represent global findings or the market as a whole, but reflect the sentiments of the respondents and companies surveyed.

[3] **2023 Gartner Midsize Enterprise Baseline Survey.** This survey was conducted to understand the most critical market differentiators in the midmarket and discover what midsize enterprises are doing differently when investing in and deploying technology. It also focused on monitoring changes in buying behaviors, staffing resources, budgets, outsourcing strategies and other conditions that drive midmarket IT leaders' IT decisions. The survey was conducted online from May through July 2023 among 366 CIOs or the most senior IT leaders in organizations with annual revenues from $50 million to less than $500 million across industries. Participants were from North America (n = 236), Europe (n = 100) and Asia/Pacific (n = 30). Disclaimer: The results of this survey do not represent global findings or the market as a whole, but reflect the sentiments of the respondents and companies surveyed.

Recommended by the Author

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

Quick Answer: What Is a Cybersecurity Outcome-Driven Metric?

SOC Model Guide

2023 Talent Outlook for Midsize Enterprises

How and When to Change Your Managed Security Service Provider

IT Key Metrics Data 2024: Industry Measures — Insights for Midsize

Enterprises Market Guide for Managed Detection and Response Services

Market Guide for Extended Detection and Response

Actionable, objective insight

Position your organization for success. Explore these additional complementary resources and tools for midsize enterprise leaders:

Research

Strategies for Midsize Enterprises to Mitigate Insider Risk

Understand the risk internal employees pose.

Download Now

Infographic

2024 CIO Agenda: A Midsize Enterprise Perspective

Deliver on your digital initiatives.

Download Now

Roadmap

2024 Technology Adoption Roadmap

Benchmark your technology adoption plans against your midsize enterprise peers.

Download 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 IT Leaders

gartner.com/en/information-technology

Stay connected to the latest insight

Gartner®