Security Awareness Efforts Fall Short! Now What? (Survey Results Analysis)

Published 21 February 2023 - ID G00778935 - 6 min read

By William Candrick, Richard Addiscott, **and 2 more**

Initiatives: Cyber Risk **and 1 more**

Enterprises typically enforce security awareness training, but program maturity, level of investment and gaps between ambition and reality significantly vary. Gartner's Security Awareness Survey examines how CISOs and their teams approach — and plan to advance — their security awareness programs.

Overview

Key Findings

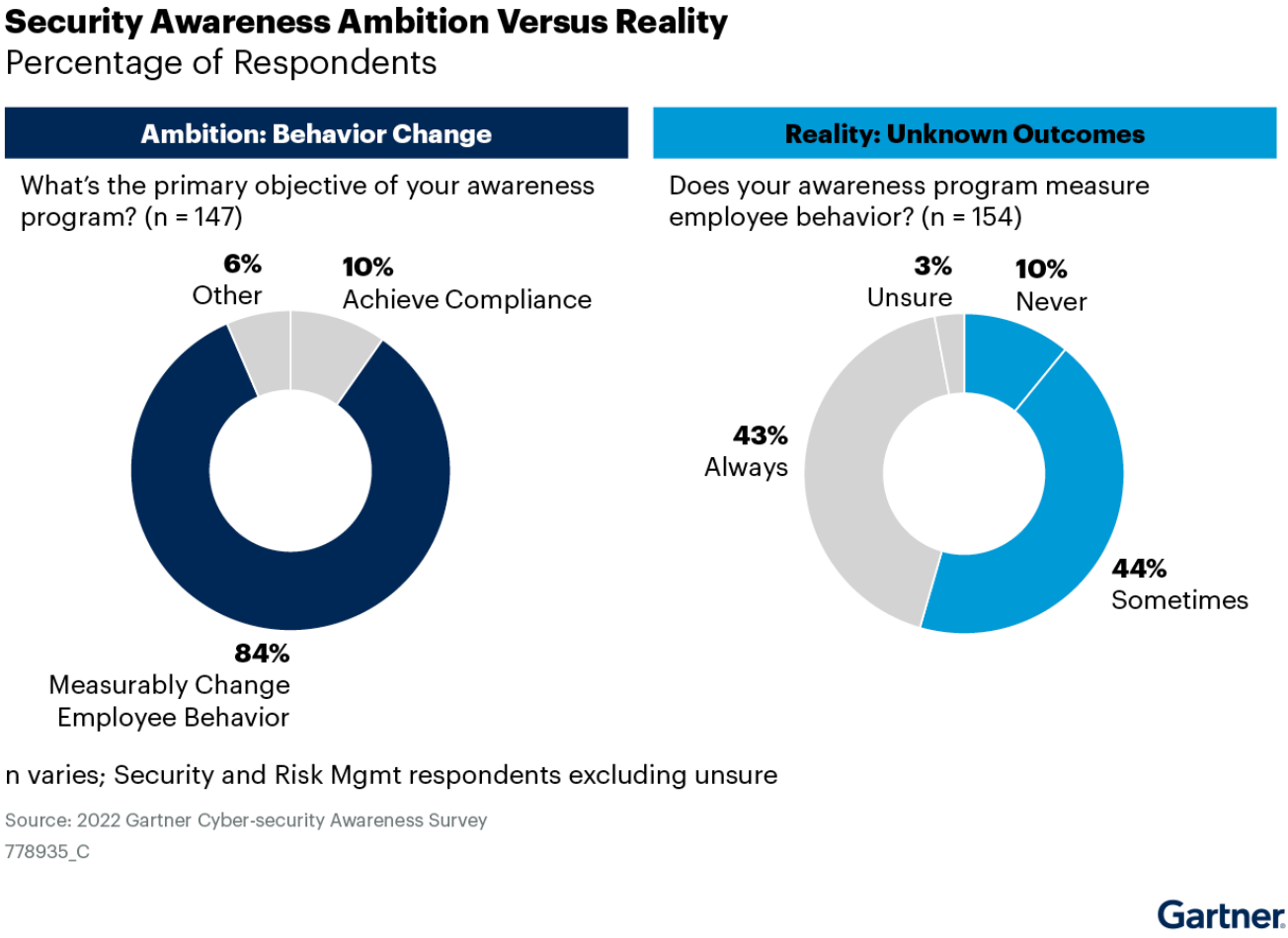
- **Security awareness programs are failing at behavior management.** Over 90% of cybersecurity functions have an awareness program, yet 69% of employees admit to intentionally bypassing their enterprise's cybersecurity guidance. [1]
- **Awareness programs are lean — with low staffing and funding.** Eighty percent of all cybersecurity functions have less than one full-time employee (FTE) dedicated to the awareness program, and 50% of all functions have less than half an FTE.
- **Cybersecurity leaders hesitate to invest more in awareness.** Nearly 60% of cybersecurity leaders plan to keep awareness staffing levels flat, and only 10% of cybersecurity leaders plan significant increases to awareness spending over the next 18 months.
- **Awareness programs struggle to measure success.** Measurable employee behavior change is the primary objective of the vast majority (84%) of awareness programs; yet less than half (43%) of programs consistently measure employee behavior.

Data Insights

Security Awareness Ambitions Don't Reflect Reality

Cybersecurity leaders face a gap between security awareness ambitions and reality. What they set out as the primary objective is not consistently measured as an outcome (see Figure 1).

Figure 1: Security Awareness Ambition Versus Reality



Further, even when employee behavior is measured, the actual actions taken by employees reflect a willingness to ignore the lessons from security awareness training:

> **CISOs aspire to change employee behavior and reduce risk. However, these aspirations are not realized: over 90% of cybersecurity teams have an awareness program, yet 69% of employees admit to intentionally bypassing their enterprise's cybersecurity guidance during the past year.2**

The maturity of awareness programs simply does not align with stated ambitions. For example, only 43% of awareness programs consistently measure employee behavior, and 10% never

measure behavior. And — when behavior is measured — it's often via a simple metric, such as simulation click rate, that fails to fully capture changes in employee behavior. Further, as explored below, security awareness staffing is lean — with many programs receiving only part-time effort (less than 1 FTE). This lean staffing means cybersecurity teams have limited capacity to improve behavioral measurement or fully adopt manual features offered by service providers.

This gap between ambition and reality is not surprising.

Security awareness computer-based training (SACBT) has existed for over a decade — yet the vast majority of breaches (82%) in 2021 involved human error. In particular, social engineering attacks, such as phishing, remain high-impact attack vectors. For example, social engineering alone accounted for 21% of breaches in 2017, 23% in 2019 and 21% in 2021. In fact, since 2012, social engineering has accounted for 21% of breaches or more each year. [3]

This decade of data suggests past investment is not driving more secure behavior in employees — which makes cybersecurity leaders understandably cautious to invest more in awareness efforts.

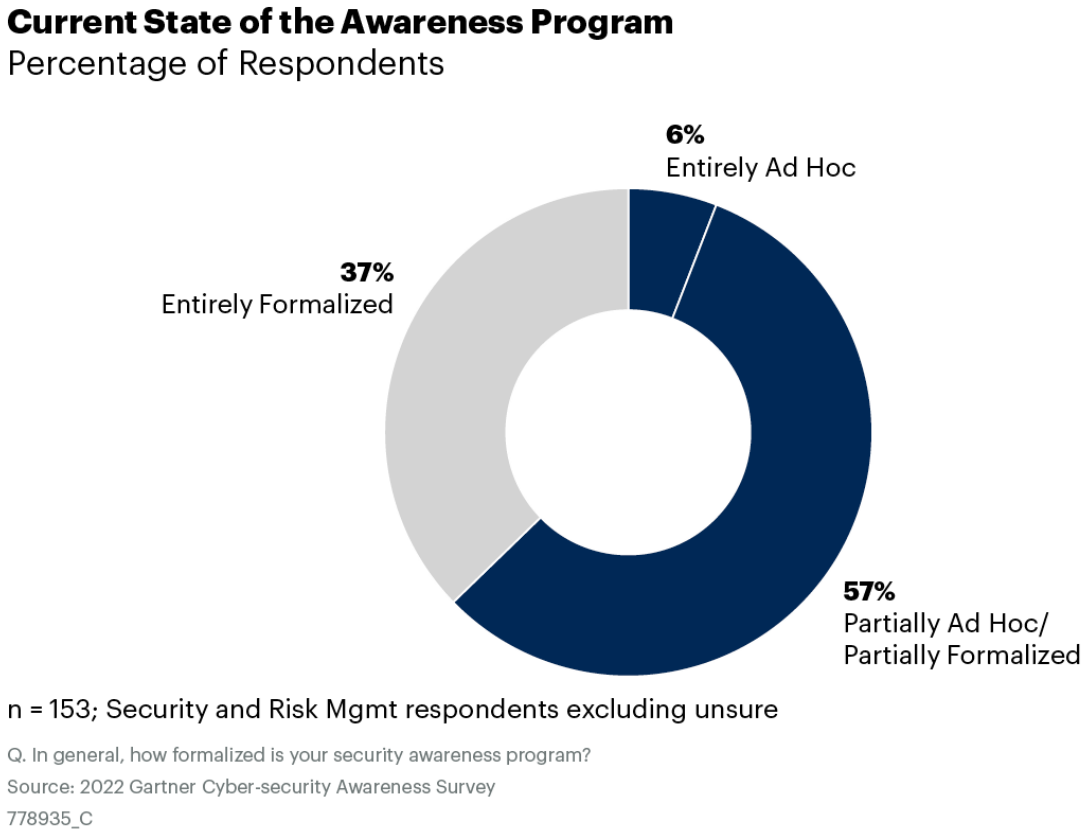
In short, the ambition of most awareness training — employee behavior change — does not reflect the reality of how programs are actually measured and managed. This gap will persist until cybersecurity leaders have confidence that additional investments and effort will achieve their awareness ambitions.

The Current State of Awareness Programs

Ad Hoc Effort and Lean Staffing

Security awareness programs are often ad hoc (e.g., part-time effort, informal reporting, few if any metrics), with lean staffing and moderate spending (see Figure 2).

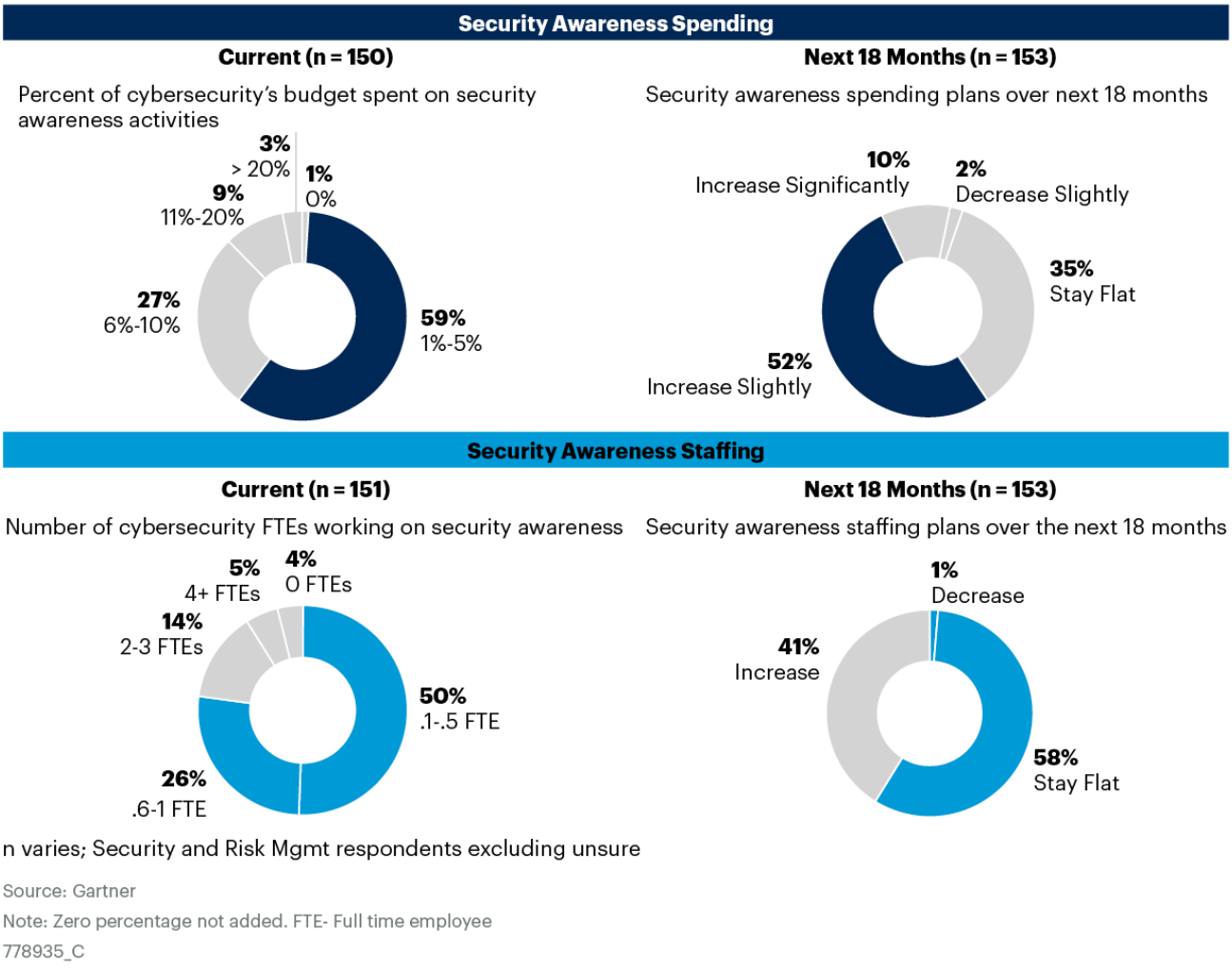
Figure 2: Current State of the Awareness Program



The prevalence of ad hoc awareness programs reflects the low staffing and funding levels awareness programs receive (see Figure 3). Sixty percent of cybersecurity teams spend 5% or less of their budget on awareness activities — including people, processes and technology; and only 10% of cybersecurity leaders plan significant increases to awareness spending over the next 18 months.

Figure 3: Security Awareness Spending and Staffing

Security Awareness Spending and Staffing



n varies; Security and Risk Mgmt respondents excluding unsure

Source: Gartner

Note: Zero percentage not added. FTE- Full time employee

778935_C

Gartner

Staffing levels of security awareness programs are even lower.

> **Security awareness is typically a part-time effort. Eighty percent of all cybersecurity functions have less than one full-time employee (FTE) dedicated to the awareness program, and 50% of all functions have less than half an FTE.**

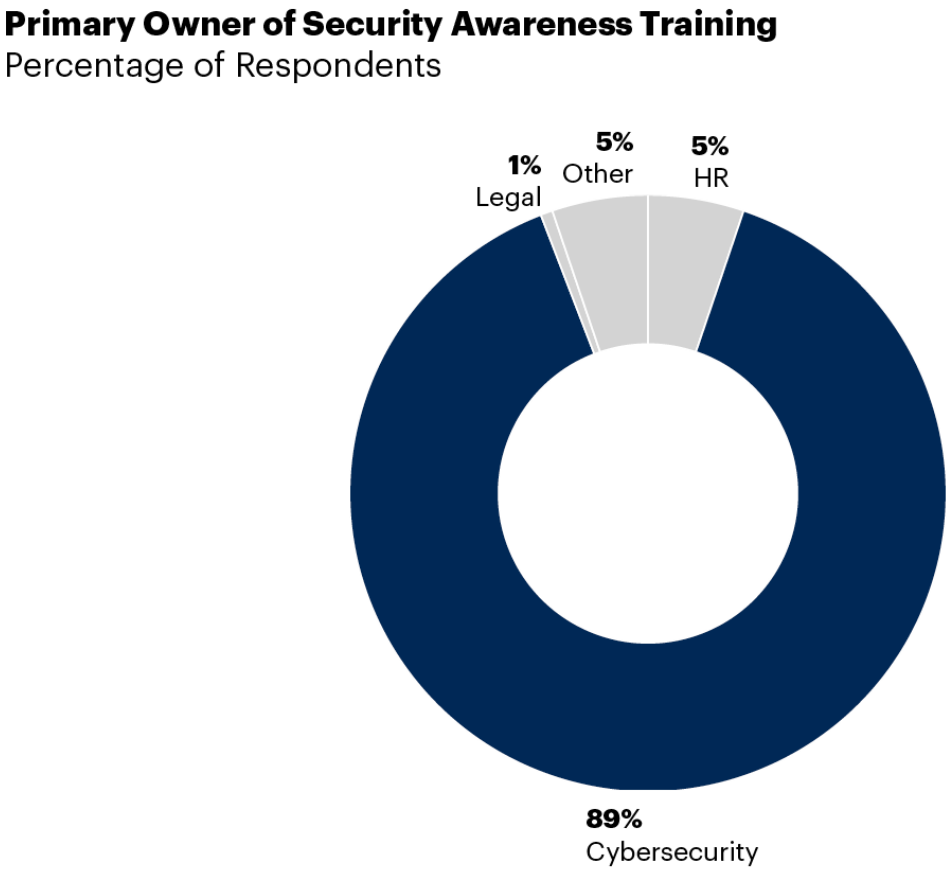
Severely lean staffing will persist for the foreseeable future, as nearly 60% of cybersecurity leaders plan to keep awareness staffing levels flat. Though 41% plan to increase staffing levels, the low starting point suggests security awareness programs will remain stretched thin.

Even with lean staffing, awareness programs manage to deploy a portfolio of tactics.

Many Tactics, But Little Payoff

Most cybersecurity functions own awareness (see Figure 4), with many adopting a portfolio of awareness tactics (see Figure 5). However, most struggle to turn engagement into tangible, measurable behavior change.

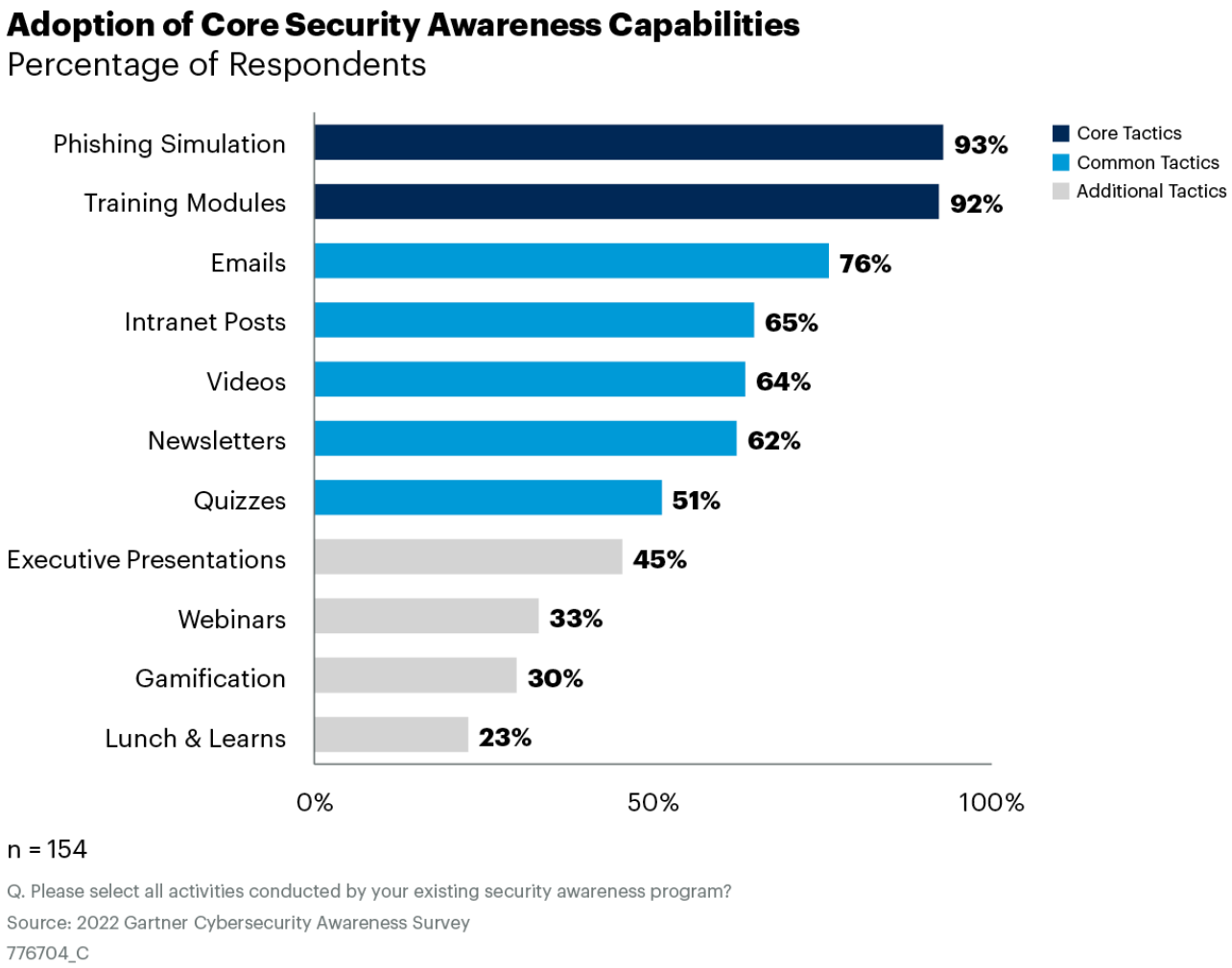
Figure 4: Primary Owner of Security Awareness Training



Gartner

Security awareness programs consist of two core activities: education (computer-based training modules) and testing (phishing simulations); and over half of awareness programs adopt common tactics, such as email engagement, intranet posts, video content, newsletters and knowledge quizzes (see Figure 5).

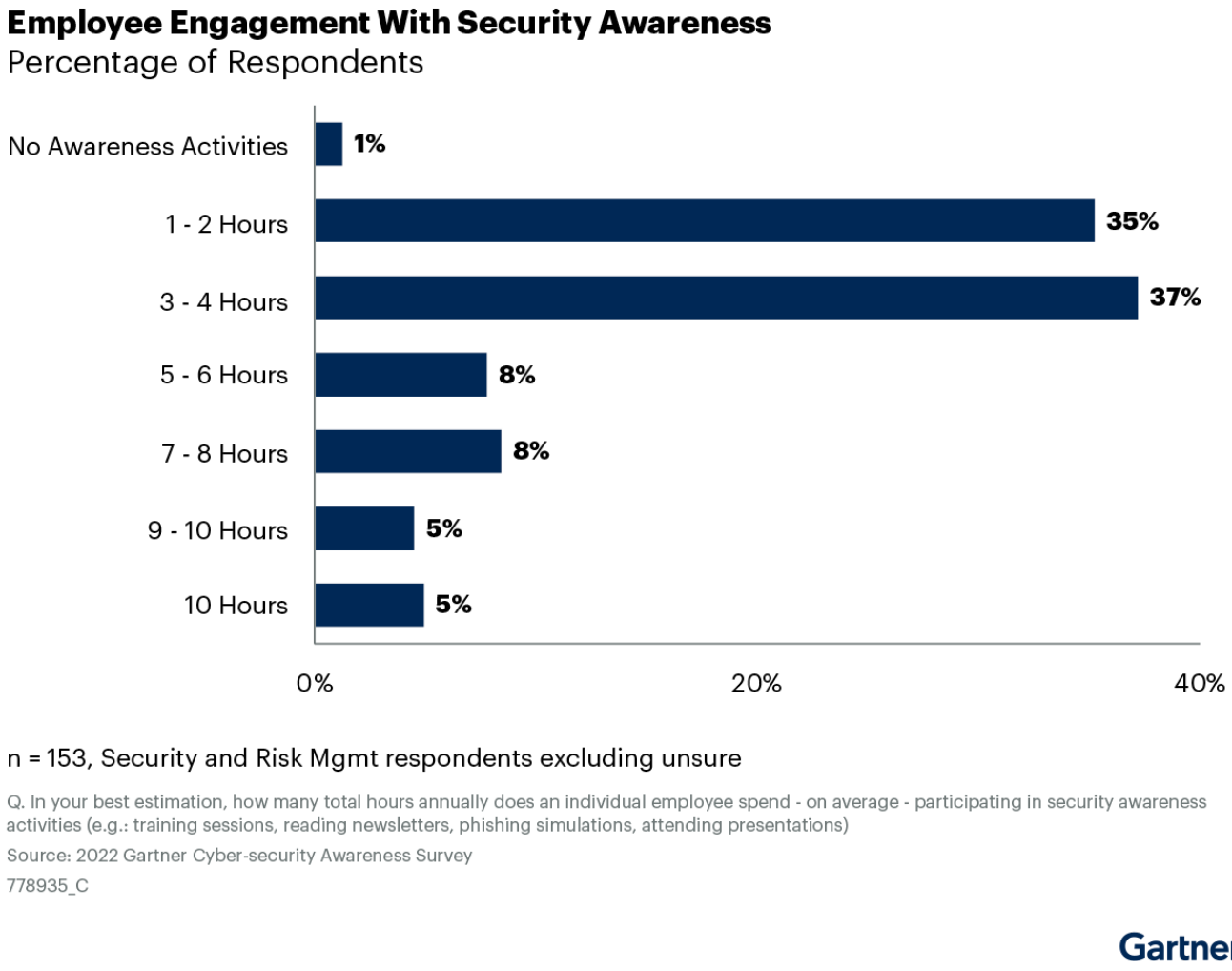
Figure 5: Adoption of Security Awareness Tactics



However, these awareness tactics have limited impact on employee behavior.

Sixty-four percent of organizations estimate their employees spend three hours or more consuming awareness content (see Figure 6) — including training, newsletters, videos, quizzes, etc. Yet, as established earlier, this considerable effort fails to drive sustained, measurable behavior change.

Figure 6: Employee Engagement With Security Awareness



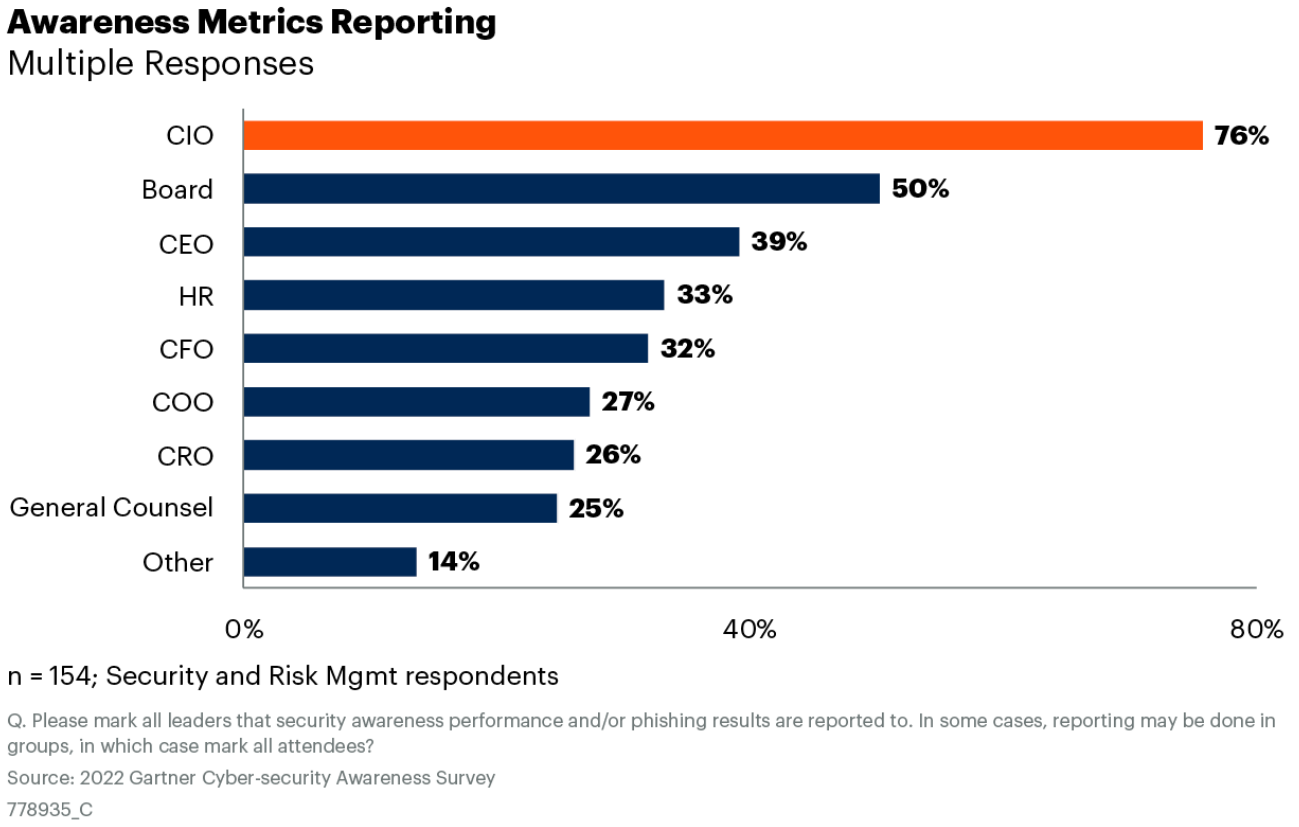
Doing more of the same things is not the answer. More staffing, more spending and more employee engagement does not guarantee employee behavior change and risk mitigation.

Security Awareness — Time for a New Path Forward

Cybersecurity leaders send mixed messages to leadership.

On one hand, social engineering attacks are so concerning that half of boards review awareness metrics (e.g., phishing simulation click rates); and well over a quarter of most C-suite executives receive security awareness reports (see Figure 7).

Figure 7: Awareness Metrics Reporting



On the other hand, security awareness efforts remain largely ad hoc, success metrics are narrow in scope and outcomes do not meet ambitions. Cybersecurity leaders need a new way forward to drive employee behavior change.

Gartner recommends refocusing efforts to build a **security behavior and culture program** (SBCP). This approach focuses on four primary components of the PIPE framework to drive tangible and sustain behavior change: practices, influences, platforms and enablers. Explore the PIPE framework in CISO Foundations: Build a Culture of Security Consciousness: Introducing the Gartner PIPE Framework.

Building a security behavior and culture program also requires new capabilities that go beyond common (and ineffective) awareness tactics. These emerging capabilities include behavioral science, automation, data integration, omnichannel engagement and personalized engagement. Learn about these emerging capabilities in Innovation Insight on Security Behavior and Culture Program Capabilities.

Evidence

This research draws upon multiple data and information sources.

- **Gartner's Security Awareness Survey (2022):** 153 respondents from North America, EMEA and Asia/Pacific across industries and enterprises with annual revenue of more than $1 billion.

- **Gartner 2022 Drivers of Secure Behavior Survey:** 1,310 employees surveyed across functions, levels, industries and geographies. The survey examined the extent to which

employees behave securely in their day-to-day work, root causes of insecure behavior and the types of support and training that they received from their organizations to drive desirable secure behaviors.

[1] Gartner 2022 Drivers of Secure Behavior Survey, n = 1,164, Q48. Over the last 12 months, how often did you intentionally bypass your enterprise's cybersecurity guidance?

[2] Gartner 2022 Drivers of Secure Behavior Survey, n = 1,164, Q48. Over the last 12 months, how often did you intentionally bypass your enterprise's cybersecurity guidance?

[3] Social Engineering, Verizon Data Breach Investigations Report.

Objectivity." Gartner research may not be used as input into or for the training or development of generative artificial intelligence, machine learning, algorithms, software, or related technologies.