Innovation Insight on Security Behavior and Culture Program Capabilities

Published 16 November 2022 - ID G00776704 - 8 min read

By Analyst(s): William Candrick, Richard Addiscott, Andrew Walls, Alex Michaels

Initiatives: Cybersecurity and IT Risk

Security awareness computer-based training services offer a stable set of core capabilities yet risky employee behavior persists. New, emerging capabilities apply behavioral science principles, data analytics and automation to help cybersecurity leaders reduce risk via measurable culture change.

Overview

Key Findings

- Eighty-four percent of cybersecurity leaders want to mitigate risk by managing employee behavior, yet under half (43%) consistently track behavior and few deploy effective solutions.
- Core capabilities offered by security awareness computer-based training (SACBT) vendors achieve regulatory and audit compliance — and some rudimentary behavior change — but fail to make impactful changes to human risk.
- Security behavior and culture programs (SBCP) adopt emerging capabilities — including behavioral science principles, data analytics and automation — to reduce risk exposure via measurable culture change.

Recommendations

Cybersecurity leaders should take the following actions to prepare for and adopt new security behavior and culture program (SBCP) capabilities:

- Rescope the security awareness program to focus on human risk management outcomes, not just regulatory and audit compliance.
- Position the business case to senior leadership for investment in human risk management to combat cybersecurity challenges arising from a spectrum of unsecure employee behaviors.

- Evaluate vendors for SBCP capabilities that will meet requirements to measure and change employee behavior at scale.
- Adopt Gartner's PIPE Framework to guide the design, execution and performance monitoring of a secure behavior and culture program to reduce human-born cyber risks.

Strategic Planning Assumptions

By 2030, 80% of enterprises will have a formally defined and staffed human risk management program, up from 20% in 2022.

By 2030, all widely adopted cybersecurity control frameworks will focus on measurable behavior change rather than compliance-based training as the critical measure of efficacy for human risk management.

Introduction

Security awareness computer-based training (SACBT) services offer a stable, commoditized set of core capabilities. These capabilities focus primarily on basic training, testing (e.g., phishing simulations, surveys) and reporting (e.g., click rates, report rates, complete rates).

While these core capabilities provide value, they typically only focus on compliance plus rudimentary improvement to specific human behaviors. As a result, the current SACBT market fails to fully deliver on the promise of tangible, scaled and sustained employee behavior change to reduce cyber risk.

Most cybersecurity leaders report lofty aspirations for their security awareness programs, yet underinvest in this space because legacy solutions do not meet current CISO needs. Under half of cybersecurity functions consistently measure employee behavior, and almost 80% have less than one FTE dedicated to security awareness (Figure 1).

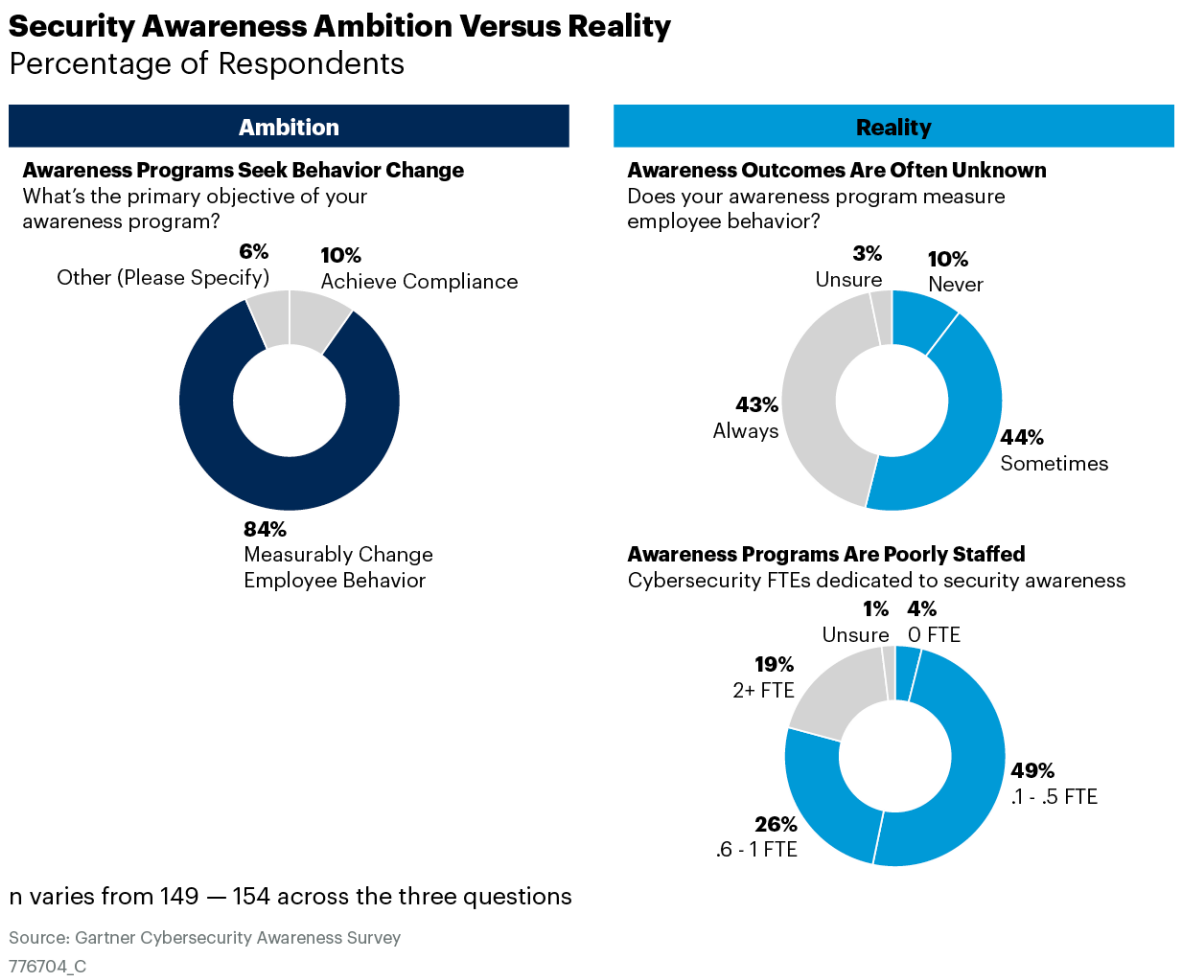
Cybersecurity leaders are hesitant to invest more resources and effort until solutions reliably deliver better risk management results.

Over 90% of cybersecurity functions have an awareness program, yet 69% of employees admit to intentionally bypassing their enterprise's cybersecurity guidance during the past year.

— 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?

These findings do not inspire confidence that additional spending on SACBT services is worth it.

Figure 1: Security Awareness Ambition Versus Reality



n varies from 149 — 154 across the three questions

Source: Gartner Cybersecurity Awareness Survey
776704_C

Gartner

New capabilities are emerging to meet the demand for improved human risk management. These **security behavior and culture programs (SBCP)** capabilities focus on risk reduction via tangible employee behavior management. Innovative solutions build their services based on behavioral science principles, and use data analytics and automation to reduce risk exposure via measurable culture change.

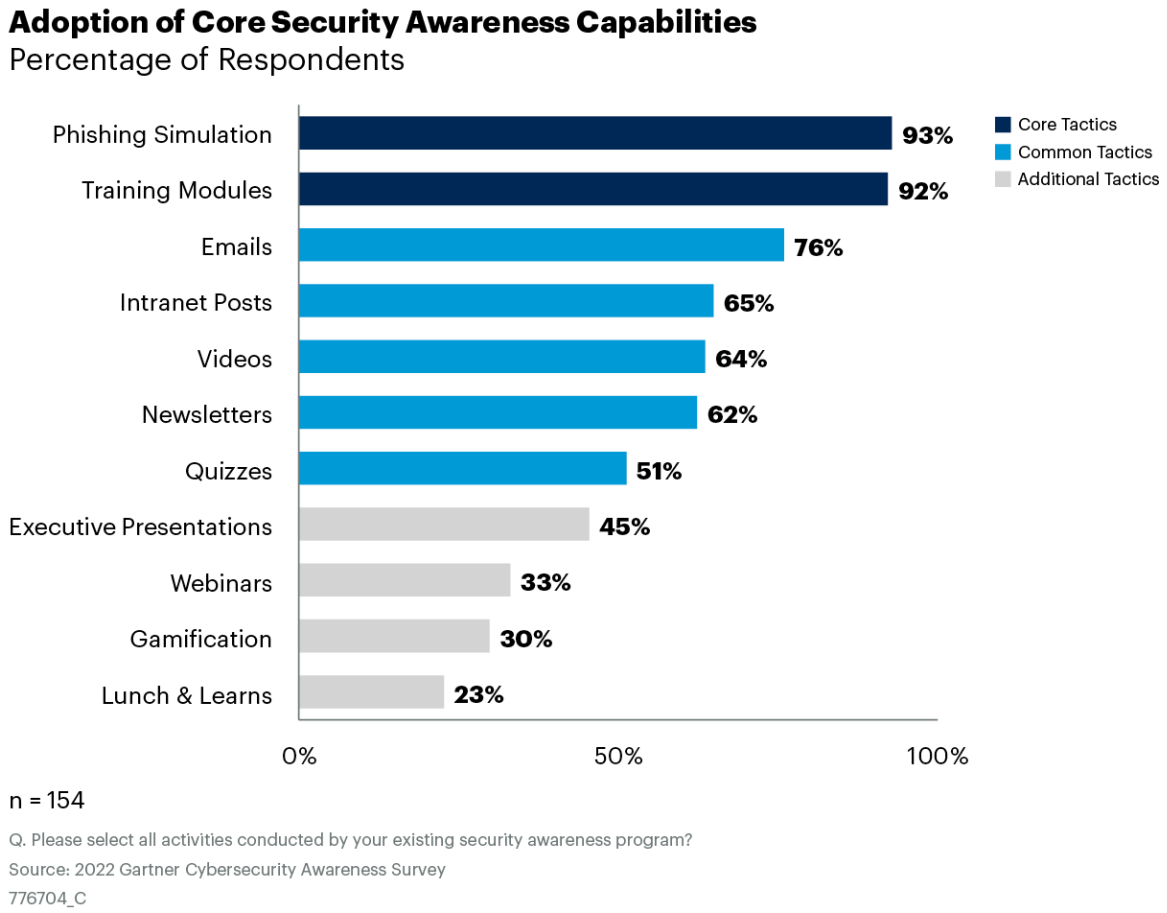
Description

The traditional **security awareness computer-based training (SACBT)** market has settled into a state of standard, stable and largely commoditized capabilities. These include:

- Training content (e.g., videos, quizzes, modules, etc.)
- Mock phishing simulations (e.g., templates, email integration, tracking)
- Report phish button (integrated with email security capabilities)
- Cloud-based platform to build and track campaigns
- Metrics and reporting dashboards (e.g., click rate, report rate, complete rate, human risk scoring)
- Industry benchmarking (e.g., click rate, report rate)
- Gamification (e.g., leaderboards, personal dashboards, interactive training)
- Learning management system (LMS) integration

CISO adoption levels of these capabilities shows that security awareness programs typically consist of two core activities: training and phishing simulations (Figure 2). Some organizations go further, adopting a range of engagement tactics — such as emails, intranet posts, videos, newsletters, etc.

Figure 2: Adoption of Core Security Awareness Capabilities



Gartner research shows that these core activities do not deliver and sustain the tangible behavior and culture change required to reduce cybersecurity risk exposure. Social engineering is a perennial top attack vector (see How to Respond to the 2022 Cyberthreat Landscape), and the vast majority of breaches (82%) involve human error. [1] While these core awareness capabilities achieve compliance objectives, they fail to sufficiently influence behavior.

Enterprises that are serious about human risk management must go further. New solutions and capabilities are emerging to meet this cybersecurity need:

Emerging SBCP capabilities focus on risk reduction via tangible employee behavior management. Innovative solutions adopt behavioral science principles, data analytics and automation to build and measure a digitally secure culture.

Security behavior and culture program (SBCP) solutions embrace both technical and nontechnical emerging capabilities, see Table 1.

Table 1: Emerging SBCP Capabilities

(Enlarged table in Appendix)

Emerging Capability	*Description*
Behavioral Science	Adoption of psychological concepts that encourage and reinforce tangible behavior change (e.g., nudge theory, choice overload, behavioral economics). **Benefit** Focuses effort on proven behavior change principles rather than raising general "awareness." See Use Behavioral Economics to Influence Security Behavior and Individual Decisions
Automation	Technology that automates continuous and targeted employee engagement without the need for manual analysis and campaign creation. **Benefit** Enables behavior management at scale without a linear increase in workload.
Data Integration	Platforms that collect, integrate and analyze data across multiple sources to gain better insight into human behavior and risk. **Benefit** Surfaces new insight on human risk and the most impactful tactics to change behavior.
Omnichannel Engagement	Engagement across multiple channels that meets employees where they are and integrates into existing workflows (e.g., Teams, Slack, Intranet, email). **Benefit** Engages employees based on where they are (physically and virtually) and how they work.
Personalized Engagement	Engagement that reflects individual preferences, abilities, strengths and opportunities in order to optimize behavior and reduce risky behavior. **Benefit** Meets people where they are and delivers context most likely to impact localized risky behavior.
Organizational Change Management	Nontechnical strategies to gain support and drive culture change across all levels of the enterprise (e.g., board presentations, business cases, middle-management buy-in). **Benefit** Funds the program, and prepares stakeholders for new-in-kind engagement with security.

Source: Gartner analysis

CISOs should note that not all SBCP capabilities are technical in nature. For example, organizational change management requires messaging, stakeholder mapping, relationship management and other soft capabilities. As SBCP solutions mature, they will increasingly integrate technical and soft capabilities that support CISOs efforts to better manage employee behavior.

Benefits and Uses

Emerging security behavior and culture program (SBCP) capabilities focus on the human element of cyber risk to achieve more ambitious outcomes. The full spectrum of human risk management capabilities spans traditional "security awareness" to SBCP, and falls into three distinct objectives (Figure 3).

Figure 3: Human Risk Management Objectives

Achieving these outcomes requires certain capabilities and metrics (to measure progress). The three objectives offer the following capabilities and metrics:

Table 2: Human Risk Management Capabilities and Metrics

(Enlarged table in Appendix)

Objective	Description	Capabilities	Sample Metrics
Achieve Baseline Compliance	Satisfy minimum audit and compliance requirements	■ Training modules (annual training) ■ Training completion rate tracking ■ LMS platform integration	■ Training completion rate ■ Knowledge checks
Teach Desired Behaviors	Educate employees on cybersecurity basics	■ Training modules (shorter, more freq.) ■ Mock phishing simulations ■ Click and report rate tracking/benchmarking ■ Human risk scoring ■ Mono-channel (email, training platform, LMS) ■ Awareness events (e.g., awareness month)	■ Click rate ■ Report rate
Change the Culture	Optimize employee behavior to manage cyber risk	■ Behavioral science/economics ■ Automation ■ Machine learning/artificial intelligence ■ Personalized engagement ■ Analytics (from multiple data sources) ■ Data integration (across multiple platforms) ■ Multi/Omnichannel engagement (Teams, email, Slack, etc.)	■ Actual incidents tied to user behavior ■ Actual detected attacks from users ■ Self-reported bad actions ■ Behavioral analytics

Source: Gartner analysis

Risks

CISOs and their teams should consider the following risks associated with emerging SBCC capabilities:

- **Worker and privacy rights** — Some SBCP capabilities require the collection, processing and even reporting of employee behavior at the individual or group levels. This level of data collection may not be possible or advisable due to local labor laws, privacy laws, cultural norms, corporate culture, etc.

- **Marketing buzz versus real innovation** — As SBCP capabilities continue to emerge, some solutions may make marketing claims that are not backed up by actual capabilities. In particular, some solutions may repackage legacy awareness capabilities and advertise them as newer capabilities that align with recent innovations.
- **Market dynamics** — SBCP capabilities are seen across many smaller, innovative players. As a result, the security awareness and training space may see an increase in merger and acquisition activity, including mergers between smaller players and acquisitions by larger players. In addition, the traditional SACBT market may not sustain all vendors, so some may go bankrupt or pivot to adjacent markets.
- **Pricing and contract changes** — Vendors may increase pricing or change contract arrangements as they expand their SBCP solutions. SBCP capabilities have the potential to offer greater value, but may command higher price premiums than the largely commoditized SACBT market.
- **C-Suite pushback on cost and scope** — Adoption of SBCP capabilities requires a shift in leadership expectations. SBCPs capabilities deliver measurable risk reduction, but these emerging capabilities require more resources to execute. CISOs and their teams may receive pushback from business leaders who still view “security awareness” as a low-cost, low-effort compliance activity.

Adoption Rate

In 2022, less than 5% of cybersecurity leaders have adopted emerging security behavior and culture program capabilities. This low adoption is due to the size and stability of smaller vendors, poor understanding of SBCP capabilities, reluctance to accept risks of early adoption and healthy skepticism of marketing promises.

Recommendations

- Rescope the security awareness program to focus on human risk management outcomes, not just compliance.
- Position the business case to senior leadership for investment in human risk management to combat cybersecurity challenges arising from a spectrum of unsecure employee behaviors.
- Evaluate vendors for SBCP capabilities that will meet requirements to measure and change employee behavior at scale.
- Adopt Gartner's PIPE Framework to guide the design, execution and performance monitoring of a secure behavior and culture program to reduce human-born cyber risks.

Representative Providers

- CyberconIQ
- Cybeready
- Cyber Risk Aware
- Elevate Security
- Hoxhunt
- Living Security Unify Insights
- OutThink
- Proofpoint
- SoSafe

Evidence

Gartner's analysis is based on over 200 end-user inquiries, 20 vendor briefings and 150 participants in our Security Awareness Survey.

[1] 2022 Data Breach Investigations Report, Verizon

Recommended by the Authors

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

Establish a Security-Conscious Culture Using Behavioral Economics

Infographic: When Security Awareness Falls Short: Why Employees Behave Insecurely

CISO Foundations: Build a Culture of Security Consciousness: Introducing the Gartner PIPE Framework

How Do You Prove That Your Security Awareness Program is Actually Working?

Take 3 Steps to Prove That Your Security Awareness Program Is Actually Working

Table 1: Emerging SBCP Capabilities

Emerging Capability ↓	*Description* ↓
Behavioral Science	Adoption of psychological concepts that encourage and reinforce tangible behavior change (e.g., nudge theory, choice overload, behavioral economics). **Benefit** Focuses effort on proven behavior change principles rather than raising general "awareness." See Use Behavioral Economics to Influence Security Behavior and Individual Decisions
Automation	Technology that automates continuous and targeted employee engagement without the need for manual analysis and campaign creation. **Benefit** Enables behavior management at scale without a linear increase in workload.
Data Integration	Platforms that collect, integrate and analyze data across multiple sources to gain better insight into human behavior and risk. **Benefit** Surfaces new insight on human risk and the most impactful tactics to change behavior.
Omnichannel Engagement	Engagement across multiple channels that meets employees where they are and integrates into existing workflows (e.g., Teams, Slack, Intranet, email). **Benefit** Engages employees based on where they are (physically and virtually) and how they work.

Emerging Capability ↓	*Description* ↓
Personalized Engagement	Engagement that reflects individual preferences, abilities, strengths and opportunities in order to optimize behavior and reduce risky behavior. **Benefit** Meets people where they are and delivers context most likely to impact localized risky behavior.
Organizational Change Management	Nontechnical strategies to gain support and drive culture change across all levels of the enterprise (e.g., board presentations, business cases, middle-management buy-in). **Benefit** Funds the program, and prepares stakeholders for new-in-kind engagement with security.

Source: Gartner analysis

Table 2: Human Risk Management Capabilities and Metrics

Objective	*Description*	*Capabilities*	*Sample Metrics*
Achieve Baseline Compliance	Satisfy minimum audit and compliance requirements	■ Training modules (annual training) ■ Training completion rate tracking ■ LMS platform integration	■ Training completion rate ■ Knowledge checks
Teach Desired Behaviors	Educate employees on cybersecurity basics	■ Training modules (shorter, more freq.) ■ Mock phishing simulations ■ Click and report rate tracking/benchmarking ■ Human risk scoring ■ Mono-channel (email, training platform, LMS) ■ Awareness events (e.g., awareness month)	■ Click rate ■ Report rate

Objective	*Description*	*Capabilities*	*Sample Metrics*
Change the Culture	Optimize employee behavior to manage cyber risk	■ Behavioral science/economics ■ Automation ■ Machine learning/artificial intelligence ■ Personalized engagement ■ Analytics (from multiple data sources) ■ Data integration (across multiple platforms) ■ Multi/Omnichannel engagement (Teams, email, Slack, etc.)	■ Actual incidents tied to user behavior ■ Actual detected attacks from users ■ Self-reported bad actions ■ Behavioral analytics

Source: Gartner analysis