Market Guide for Security Awareness Computer-Based Training

Published 27 July 2020 - ID G00718853 - 21 min read

By Analysts Brian Reed, Richard Addiscott, Claude Mandy

Initiatives:Security and Risk Management Leaders

Adversaries exploit ineffective security awareness, often exposing vulnerable human behaviors. Security and risk management leaders must define strategies and deploy effective tactics to perpetually evolve their security awareness training programs to mitigate people-centric threats.

Overview

Key Findings

- Organizations must view security awareness as an ongoing component of their broader information security program, not as simply a technology spend decision or an annual training expense.
- While phishing testing remains the most used method to measure effectiveness of training, it is not the only method an organization should use to measure security awareness effectiveness.
- Successful security awareness programs must include both executive sponsorship and organizationwide involvement.
- Organizations without a full-time equivalent (FTE) employee dedicated to security awareness should look for security awareness platforms that can automate and orchestrate many elements of security awareness training.

Recommendations

Security and risk management leaders responsible for security awareness training programs should:

- Build security awareness programs around platforms that offer diverse, contextually appropriate content and innovative delivery capabilities, and that measure success through meaningful metrics.
- Utilize additional information security metrics beyond phishing testing “click rates” to determine program success, such as incident response metrics, employee monitoring reports, unsanctioned application usage and sensitive data metrics.

- Involve and actively solicit groups and individuals outside of IT and information security to help ensure widespread support and approval for your security awareness program.
- Evaluate security awareness training as a managed service if there is a gap in security awareness expertise on staff, or if other budgetary, financial or program-driven constraints exist.

Strategic Planning Assumption

By 2024, 25% of midsize enterprises will adopt security awareness training as a managed service, up from less than 5% today.

Market Definition

This document was revised on 30 July 2020. The document you are viewing is the corrected version. For more information, see the Corrections page on gartner.com

The security awareness computer-based training (SACBT) market is characterized by vendor offerings that include ready-to-use, interactive content modules. These modules are available as cloud-hosted SaaS applications or on-premises deployments via client-managed learning management systems (LMSs) and also support the Sharable Content Object Reference Model (SCORM) standard to support integration with corporate learning management systems. The vendors included in this Market Guide support multilingual and multicultural audiences; that is, they are available in English and support several other languages, either natively or through some degree of subtitling or partial translation. In many cases, the language support is diverse and localized. Vendors typically offer security awareness content delivery through a variety of digital endpoints and provide a platform to operationalize a security awareness program.

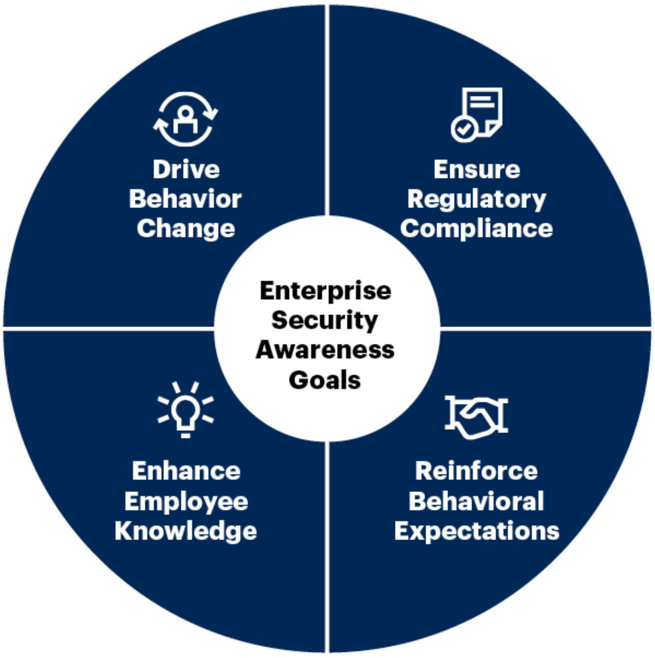
Market Description

People directly affect security outcomes more than technology, policies or processes. The market for security awareness computer-based training remains driven by the recognition that perfect cybersecurity protection is not possible, resulting in people frequently on the front lines of potential security incidents. Individuals’ awareness of potential security concerns relates directly to their behaviors when challenged by adversaries. Organizational culture plays a strong role in placing importance on users and their development and understanding of information security issues.

Organizations should strive to accomplish several goals when establishing an enterprise security awareness program. Figure 1 describes four commonly cited goals of establishing an enterprise security awareness program.

Figure 1. Four Common Enterprise Security Awareness Goals

Four Common Enterprise Security Awareness Goals


Drive Behavior Change
Ensure Regulatory Compliance
Enterprise Security Awareness Goals
Enhance Employee Knowledge
Reinforce Behavioral Expectations

Source: Gartner
718853_C

Security Awareness Goals

End-user-focused security awareness is a rapidly evolving market. Demand is fueled by the needs of security and risk management (SRM) leaders to help influence the behaviors that affect the security of employees, citizens and consumers. Ideally, positive influence will result in progress toward an overall corporate culture that is security-aware and rewards understanding of potential security issues. The organization can then avoid the consequences of people-centric threats through meaningful and thoughtful awareness and education programs.

Interactive CBT platforms are a central component of comprehensive security education and behavior management programs. The focus and structure of the content delivered by CBT vary, as do the duration of individual CBT modules and the type of computing endpoints supported. Understanding the diversity of people in the organization is as important to SRM leaders as understanding how security fits into an organization's larger goals.

An effective security awareness program requires executive sponsorship, organizational buy-in and interactive involvement from a number of constituents. CIOs and chief information security officers (CISOs) must support security awareness programs through technology support and delivery to end users, as well as ensuring meaningful and relevant content is shared appropriately. Employee communication leaders, such as human resource (HR) managers, and corporate communications departments can also play a pivotal role in helping to verify that security awareness program content is both relevant and effectively communicated to everyone.

Market Direction

Security awareness CBT is both a growing and rapidly evolving market. Within the past year, we have been faced with both the COVID-19 global pandemic and significant global economic instability and uncertainty. Both of these macrolevel events have resulted in significant changes in how the workforce operates and interfaces with technology. A natural byproduct of changes in normal work location and normal work operations is the requirement to accurately and effectively communicate what these changes mean to end users across the entire organization, and any resulting security implications. This is where security awareness computer-based training can help.

The COVID-19 global pandemic broadly affected information security markets. Short-term spending increases became evident in very specific tactical spending, in particular, in areas directly related to supporting a remote workforce. Solutions that could help to verify a secure posture (see "Securing the Fully Remote Workforce"), and solutions that enable and ensure secure remote access (see "Solving the Challenges of Modern Remote Access") remain pivotal to securing ongoing remote operations. Many security awareness providers have created and shared security awareness "starter kits" or "work from home" packages to help with this shift in workplace productivity.

Market Analysis

Security Awareness Must Not Be Treated as a Technology Issue Buried in IT

Gartner clients cited building a security culture, measuring security awareness activities and tailoring messages to different audiences as the top three challenges for their security awareness programs. Far too often, many of the IT — and specifically information security technology — spend decisions that organizations make are buried in the IT and information security departments, without soliciting outside counsel or expertise. Since security awareness training should ideally be utilized by the entire organization, it only makes sense that buyers should carefully evaluate provider content and solicit feedback from a wide variety of constituents across the organization. There are a number of techniques that can be used to measure the success of the security awareness program (see "Measure the Success of Your Security Awareness Program Without Asking").

Most Organizations Will Want Centralized Management of Security Awareness Programs

The vast majority of organizations will require some centralized means to manage all aspects of their security awareness program. Many of the providers in this Market Guide have scalable platforms that allow for importing various users, groups and organizations into a centralized management structure in order to manage the security awareness journeys of participants. Most solutions will also have support for SCORM, which is a de facto standard to ensure that metrics related to your security awareness content are accurately captured. Security awareness metrics can then be shared among other corporate learning platforms (see the “Market Guide for Corporate Learning”).

Security awareness platforms aid in measuring training completion and mapping required training that may be mandated by regulatory compliance requirements. Completion of training on a wider range of information security topics, such as acceptable use policies, sensitive data handling guidelines, and other legal and compliance training, could indicate whether or not employees are properly engaged in their security learning journey. Some government entities are even passing legislation requiring government employees to successfully complete a security awareness training certification program. Texas passed House Bill 3834 into law in 2020, which details the frequency, type of training and others mandates that Texas state employees must abide by as they relate to cybersecurity training.

Many security awareness training platforms offer some degree of automation and orchestration of content. For example, once a participant successfully completes a learning module, there may be several other modules that would be appropriate after the previous training has been delivered and the user’s knowledge of that content has been successfully checked and verified. For end-user security awareness training, the predominant method of testing users has been through the use of phishing testing through corporate email systems.

Innovative Approaches to Security Awareness and Development of Diverse Content Are Important

Many security awareness providers have taken an innovative approach to security awareness content development and delivery. This content diversity is a welcome change from the CBT modules of the past, which were often an exercise in participants clicking “Next → Next → Finish” and receiving a digital certificate of completion.

As far as the amount of time that these security awareness modules take to complete, the market includes descriptors such as “nanolearning,” “microlearning,” episodes, “Netflix-style” training, and so on. Nanolearning typically refers to very short content modules (often 60 to 90 seconds) that cover one specific point about security awareness. Microlearning refers to content a bit longer than nanolearning (usually a couple of minutes in duration), and usually follows the “one topic, one message” format. Other training content styles, such as episodic or series-based training, might have recurring characters or narrators and build upon the knowledge learned in previous content modules. Many of these types of content will be incredibly diverse visually, such as animations that might be stylized or adapted in a variety of ways (e.g., cartoons, corporate-to-casual look and feel, specific cultural or geographic relevance). Many of the security awareness providers are starting to use professional voice-overs and even using celebrity voices in their training content to better engage a wider audience and to drive positive experiences and outcomes for participants.

There are a number of innovations in measuring user engagement within security awareness training platforms. For example, measurements and reports can often detect user-level engagement. Some of these platforms can detect and report if users are multitasking while a training module is being played, if the module is running in the foreground/background, or if end users are using input devices (keyboard and mouse activity) while training content is being actively delivered.

Another innovative delivery approach involves the use of gamification. The idea of gamification is that organizations can make meaningful changes to security behaviors through harnessing individual (and in some cases group) human competitiveness. Support for gamification varies greatly between providers. Organizations must also understand if their organizational culture supports gamification techniques, such as displaying a leaderboard, and awarding digital badges and certificates based upon games or completion of exercises that demonstrate subject matter expertise. In some privacy-sensitive organizations, gamification might not be a motivator or viewed as a positive element of your security awareness program. Virtual reality (VR) is another capability that many security platforms have begun using to further extend security awareness gamification. Some innovative examples of this are VR simulated scenarios and even cyber "escape rooms."

Phishing Simulation Testing Is Not the Only Way to Test Your Users

Several studies have shown that email remains a primary threat vector for organizations. Gartner clients cited email phishing as the strongest focus area for security awareness for 2020 and 2021, followed by providing security awareness for remote workers. However, not all security awareness problems are solved by achieving a mythical 0% click rate on phishing. There is no such thing as perfect protection, and there is also no such thing as human perfection. People click on phishing links, it is not a matter of "if," but rather of "who, when and how frequently." Metrics matter, but the context and deeper understanding of why users take certain actions or exhibit specific behaviors are more important than a static "click rate."

Many of the more sophisticated email attacks are not even link-driven, so simply testing on click rates without any additional context is a fallacy. Ideally, your security awareness program should contain several elements of awareness. These would address what to look for in a suspect email, or what to do before you click or take other actions, as well as behavior recommendations, such as "Should I right-click on this email and report it as suspicious?" or "Should I block/report this sender?"

Email security vendors have historically been the primary integration point with SACBT. However, there are a number of other security product integration points that also make sense for SACBT. Employee monitoring and insider threat management programs, which are often remediated through proper user awareness and education efforts, are a logical integration point for SACBT. Another natural integration exists within cloud collaboration platforms, since increasingly users are transferring data and using applications in ways that may not have protection capabilities enabled. Some security awareness providers are also delving into human risk management. These platforms use training content along with integrations or feeds from other security platforms (e.g., threat intelligence sources, social media monitoring, and workplace productivity analysis). They aim to better identify who risky users in your organization might be, and how to work to influence security behavior modification with at-risk users.

End-user organizations constantly struggle with how to appropriately handle users who repeatedly fail phishing simulations. There is no shortage of opinions on dealing with consequences, and how much positive reinforcement versus punitive action should take place. This is a problem that is ultimately organization- and individual-specific, and is rooted strongly in culture, psychology and trust. One approach might be to apply additional protections to end users who struggle with recognizing certain types of threats, such as web browser isolation. Another approach might involve forcing users to a restricted text-only view within their email client (disabling HTML email). These remediations can vary widely and should be made on a case-by-case basis.

In organizations without a dedicated program for security awareness, phishing simulation testing and some security awareness content are often delivered as “checkbox” exercises, frequently as the result of some compliance initiative or other tactical concern. All organizations should think about ways to test their users’ security awareness knowledge and to influence behavior beyond simply phishing testing exercises.

Security Awareness Training as a Managed Service

Many resource-constrained organizations, specifically midsize enterprises, struggle with providing adequate security awareness training to their users, let alone developing cohesive enterprise security awareness programs. For these organizations, security awareness training delivered as a managed service offering might be a good fit. These services often combine a subscription-based security awareness platform, along with dedicated services to help establish, operate and maintain the program. The service offerings will typically include expertise to help you get started with a security awareness platform, help profile and build learning tracks for different users or groups, and even help with internal communications to build support for your security awareness program. These services also usually deliver a certain number of phishing testing campaigns during a time period (monthly testing for a year) and work with you on developing specific targeted phishing testing campaigns.

Future possibilities for automating security awareness service offerings include improving upon the use of chatbots and virtual assistants. Deeper integrations with other security platforms that measure, analyze and contextualize end-user behaviors could change and improve how clients utilize security awareness. In addition to these integrations, natural language processing (NLP) and natural language understanding (NLU) platforms can help form an autonomous system to detect, protect and respond to user-specific security concerns.

Security Awareness Training Market Dynamics

We expect spending and security needs to continue to shift due to the short-term upheaval and uncertainty of organizations returning to some semblance of normalcy throughout the rest of 2020 and into 2021 (see “Forecast Alert: Impact of COVID-19 on the Information Security Software and Services Markets”). However, all of that change will undoubtedly result in the need to continue to communicate with employees effectively and efficiently. Organizations must offer end users up-todate information on security awareness in order to make them both educated and aware of changes that impact their behavior toward information assets.

Attempts to properly size the addressable security awareness training market are difficult due to several factors. In the previous "Magic Quadrant for Security Awareness Computer-Based Training," Gartner estimated significant growth in the market through 2019 of 47%, resulting in a market size of approximately $660 million. Overall information security and risk management spending growth is expected to slow to 4.2%, but remain positive for 2020. Taking into account this more modest growth forecast through 2020, it is likely that the addressable market for SACBT is approximately $700 million globally, and expected to grow more significantly in 2021 and beyond. The single biggest route for growth is through fundamental changes in the way that users are having to adapt to location-based disruptions, and through changes in workplace responsibilities that can alter the way information assets are being utilized.

Several mergers, acquisitions and partnerships in the security awareness market have taken place in 2019 and 2020. Below are some of the highlights of notable acquisitions and partnerships:

- Proofpoint acquired The Defense Works — May 2020
- Microsoft and Terranova Security announce a strategic partnership — February 2020
- Trend Micro's partnerships with multiple security awareness providers (AwareGO, GoldPhish, Infosec, NINJIO and Awaretrain [formerly NextTech Security]) — February 2020
- KnowBe4 acquired Twist and Shout Group — September 2019
- KnowBe4 acquired CLTRe — May 2019

Gartner believes that there will be additional vendor consolidation and new partnerships in 2020 and beyond. Many of these vendor relationships will be driven by combining the value of security awareness with other information security initiatives, such as employee monitoring and insider threat management, cloud collaboration security, and improved data security governance.

Representative Vendors

Market Introduction

The representative vendors (see Note 1) listed in this Market Guide have a generally available offering at the time of this publication that is specifically designed to deliver SACBT to end users. To help potential customers identify which vendor offering best addresses their use case, we have grouped the following 40 vendors into four categories (see Tables 1 through 4). A given vendor offering will be listed in the table that best describes its primary use case focus.

The four categories below and a vendor placement in a category does not, nor is it intended to, indicate in any way exclusive or limited focus on a category or capability. In addition, many of the vendors represented often can provide multiple SACBT capabilities. Again, this is not a definitive and exhaustive list of each provider's services, and many vendors in one section can perform multiple (or all) features and capabilities.

The representative vendors are listed in one of four primary groups:

1. **Security Awareness Program Platforms** (see Table 1): Include vendors that can offer a holistic and complete platform to effectively manage all aspects of a cohesive security awareness training program. This includes content delivery capabilities, sophisticated and scalable reporting metrics, integrations with broader corporate learning systems, and the ability to test and evaluate awareness training effectiveness across the end-user population.

2. **Security Awareness Content Development and Delivery Systems** (see Table 2): Includes vendors offering unique approaches to developing compelling security awareness content, or an innovative approach to delivery or distribution of security awareness training content to end users across the organization. Some of these vendors also have OEM relationships or partnerships where other providers might redistribute and resell their training content.

3. **Phishing Simulation Testing and Remediation/Response Platforms** (see Table 3): Includes vendors who predominantly focus on the aspects of phishing training and end-user phishing testing. Many of these vendors have close integrations with email security systems and can also integrate into the mail flow to help with user-submitted suspicious email content. They may also have a button in the email client or other workflow action to help end users report emails.

4. **Security Awareness Training as a Managed Service** (see Table 4): Includes vendors who offer their security awareness training capabilities as cloud-hosted, subscription-based managed security services. These managed service offerings can often alleviate the effort and learning curve required to establish and launch a security awareness program. These offerings typically include wizard-driven workflows, to help easily develop security awareness training campaigns or a library of modules on security topic areas to choose for managed security awareness campaigns. They may also offer a means to deploy phishing simulation testing for end users, collect results, and then automate reporting of training program metrics.

Table 1: Security Awareness Program Platforms

Vendor ↓	*Product, Service or Solution Name* ↓
CybSafe	CybSafe
CyberProtex	Security Awareness Training Software
Infosec	Infosec IQ

Vendor	Product, Service or Solution Name
Inspired eLearning	Security First Solutions, PhishProof Anti-Phishing Software
KnowBe4	Enterprise Security Awareness Training, PhishER
MediaPRO	MediaPRO TrainingPacks
MetaCompliance	eLearning, Phishing, Awareness Management, Policy Management, Privacy
Proofpoint	Proofpoint Security Awareness Training
SANS Institute	Security Awareness Training
Security Mentor	Security Awareness Training
Terranova Security	Security Awareness Training

Source: Gartner (July 2020)

Table 2: Security Awareness Content Development and Delivery Systems

Vendor	Product, Service or Solution Name
AwareGO	Online Training Solution and Security Awareness Content
Circadence	Project Ares
Curricula	Security Awareness, Phishing
Cyber Risk Aware	Security Awareness Training, Phishing Simulation
Cyber Intelligence 4U	Enterprise Cybersecurity Program

Vendor ↓	*Product, Service or Solution Name* ↓
ERMProtect	Awareness Training
Elevate Security	Human Risk Management Platform
Habitu8	Learning Platform and Videos
Infosequre	Security awareness e-learning, VR game, Cybersecurity culture scan, escape room, phishing simulation
Living Security	Cybersecurity Training, Cybersecurity Escape Room
Lunarline	Cybersecurity Workforce Maximization
NINJIO	NINJIO AWARE ANIME, NINJIO AWARE CORPORATE, NINJIO AWARE NANO, ENTERPRISE
OutThink	Adaptive Security Awareness Training, Phishing Simulations, Human Risk Management Platform (SaaS)
Security Innovation	Security courses

Source: Gartner (July 2020)

Table 3: Phishing Simulation Testing and Remediation/Response Platforms

Vendor ↓	*Product, Service or Solution Name* ↓
Barracuda	Barracuda PhishLine
Boxphish	Boxphish
Cofense	Cofense PhishMe, Cofense LMS,Cofense Reporter, Cofense Triage, Cofense Vision, Cofense Intelligence, Cofense PDC

Vendor ↓	Product, Service or Solution Name ↓
Hoxhunt	Gamified Phishing Training Platform
IRONSCALES	Phishing Simulation and Training, Phishing Emulator
Mimecast	Awareness Training, phishing testing
PhishingBox	Phishing Awareness Training, Phishing Simulator
PhishLabs	Email Intelligence & Response
Sophos	Phish Threat

Source: Gartner (July 2020)

Table 4: Security Awareness Training as a Managed Service

Vendor ↓	Product, Service or Solution Name ↓
CyberHoot	Cybersecurity Training Platform
Digital Defense	SecurED, Security Training, Education and Awareness Module (TEAM)
Global Learning Systems	Security Awareness, Managed Services for Security Awareness Program
LUCY	Awareness Training, Attack Simulation
Secure Mentem	Security Awareness as a Service
Stridepoint	Relay Managed Security Awareness

Source: Gartner (July 2020)

The vendors listed in this Market Guide do not imply an exhaustive list. This section is intended to provide more understanding of the market and its offerings.

Market Recommendations

Before purchasing a security awareness platform, establish an enterprise security awareness program and have a detailed list of requirements for that platform to support your program. Solicit feedback on the security awareness platform, content modules and reporting outputs from constituents beyond just IT and information security. Strongly consider involving your marketing or corporate communications teams to ensure strong communication of your program.

Pricing across the security awareness training market has been facing downward pressure and will continue to trend that way. There are several reasons for this. Many large platform security providers, such as Cisco, Microsoft and Trend Micro, are beginning to bundle security awareness training content at certain license levels or into enterprise license agreements. If you already have a high-level license from a large security provider, evaluate your current licensing to see what elements of security awareness are included, and if you can (or should) make additional spend for additional security awareness features.

There are a large number of security awareness training providers in the marketplace, thus you should carefully map your needs to these providers' capabilities. If your requirements are tightly aligned to phishing detection and prevention, this might steer you toward certain providers that not only provide awareness training, but also offer a wide array of preventative capabilities.

Internationalization, and multilanguage support is another key area to investigate when looking at security awareness training platforms. If you have a global organization, localized content will help improve receptiveness to your program. Carefully consider providers that have strong language support, as some of these providers have their content translated into more than 50 languages. Gartner recommends that organizations verify the accuracy of languages with their own in-country personnel before deploying translated materials. Although some vendors promote many languages, carefully check whether only some of the content has been localized or if all of the content has been translated into other languages.

Note 1
Representative Vendor Selection

The representative vendors listed in this Market Guide have a generally available (GA) offering at the time of this publication specifically designed for providing end-user security awareness computer-based training. The 40 vendors divided among four groups are meant to show a representative sampling of diverse vendors that offer solutions that can help organizations with multiple facets of establishing, operating and measuring an effective security awareness program.

Note 2
Gartner's Initial Market Coverage

This Market Guide provides Gartner's initial coverage of the market and focuses on the market definition, rationale for the market and market dynamics.

Recommended by the Authors

3 Ways to Gain Support for Your Security Awareness Program

How to Design a Security Champion Program

Measure the Success of Your Security Awareness Program Without Asking

10 Ways to Improve Security Awareness on a Tight Budget

Security Fundamentals — The Services and Processes You Must Get Right

Security Awareness: A Cost-Effective Way for Midsize Enterprises to Reduce Risk

How CIOs in Midsize Enterprises Can Best Fill Staffing and Skills Gaps in Security

Market Guide for Corporate Learning

Recommended For You

Magic Quadrant for Security Awareness Computer-Based Training

Gartner Peer Insights 'Voice of the Customer': Security Awareness Computer-Based Training

4 Teaching Tactics to Boost Your Security Training Efforts

Peer Lessons Learned: Implementing Security Awareness Computer-Based Training Tools

3 Tactics to Boost Awareness of Phishing Attacks