Magic Quadrant for Security Awareness Computer-Based Training

Published: 25 October 2016 **ID:** G00293102
Analyst(s):

Perry Carpenter, Joanna G. Huisman

Summary

Humans can be either the strongest or weakest defense against threats. Security leaders are, more than ever, seeking to increase security awareness and influence end-user behavior while also boosting security performance, as well as supporting productivity, accountability and compliance.

Strategic Planning Assumption

By 2019, the market for security awareness computer-based training (CBT) will evolve to incorporate integration with employee monitoring and endpoint detection and response (EDR) solutions as part of the standard, expected feature set.

Market Definition/Description

End-user-focused security education and training is a rapidly growing market with demand fueled by chief information security officers' (CISOs') and employee communication leaders' need to help change or improve the security behaviors of employees, citizens and consumers.

The market for security awareness computer-based training is driven by the recognition that, so long as technology-based security systems do not provide perfect protection, humans, with all of their inherent strengths and weaknesses, play an undeniable role in an organization's overall security and risk posture. This reality, coupled with enterprise and employee adoption of mobile, Internet of Things (IoT) and cloud solutions, requires CISOs to recognize and manage the increasing impact of employee behavior on enterprise security and risk management efficacy.

The phrase "security awareness" is commonly used to refer to a broad range of education, communication, and behavior management activities and learning outcomes. These activities and outcomes include:

- Complying with regulations and policy

- Supporting disciplinary actions
- Increasing employees' knowledge concerning threats, risks and security options
- Changing and maintaining employees' security behavior

In this research, Gartner uses the phrase "security education" to refer to the overarching set of activities and objectives that elevates security competence and motivates employees to make security decisions for themselves and the organization that align with enterprise security performance objectives and expectations. Awareness of threats and mitigating actions is one possible tool in a security education program. Direct behavioral conditioning (for example, anti-phishing projects; see Note 1) is another form of security education, as are security communication/marketing campaigns involving posters, competitions and advertising-style messaging.

Security education can fulfill multiple objectives and requirements, including compliance with regulations that mandate security training, establishment of clear behavioral guidelines to support disciplinary processes (as typically described in acceptable-use and/or security policies), improving employee knowledge of security and risk topics, and motivating desired security behaviors in the appropriate context. All these types of objectives share the goal of supporting enterprise requirements for the management of security risks.

Effective security education and communication are critical elements of a people-centric security strategy (see"Definition: People-Centric Security").

Most organizations have invested in some form of security awareness activities for decades. New technologies, new threats and new patterns of work compel organizations to seek more sophisticated behavioral support approaches (for example, corporate culture development) that incorporate a broad range of deployment models, increased frequency of learning opportunities, context-specific training content and structure, and metrics that support continued investment in awareness and security education. Demonstrating the effectiveness, or ROI, of the security awareness program is of increasing importance to many CISOs, which has manifested in the increasing demand for measurement of persistent learning outcomes, or offering preassessment so that some employees can "test out" of some courseware if able to demonstrate knowledge mastery.

Interactive CBT is one component of a comprehensive security education and behavior management program. It is a mechanism for the delivery of a learning experience through computing devices, such as laptop computers, tablets, smartphones and IoT devices. The focus and structure of the content delivered in CBT vary, as do the duration of individual CBT modules and the type of computing endpoints supported.

The market for CBT for security awareness is characterized by vendor portfolios that include ready-to-use, interactive software modules. These modules are available as Internet services or on-premises deployments via client-managed learning management systems (LMSs) and vendor support for the Sharable Content Object Reference Model (SCORM) standard. The products included in this Magic Quadrant support multilingual and multicultural audiences (that is, they are available in English and at least one other

language), delivery via a variety of digital endpoints, and assessments of trainee participation and completion. Vendors that support this market target end-user organizations of all sizes; however, enterprise clients commonly demand ancillary capabilities, such as customization of content, creation of new content, and advanced assessment and reporting capabilities.

Security education CBT is generally licensed on a per-user, per-year pricing structure, with limited exceptions. Vendors that offer traditional CBT and anti-phishing solutions consistently have separate licensing and pricing for each type of solution, although package contracts are common. Pricing can be per CBT module or for a bundled number of modules, or it may include access to all content under a single license fee.

Security education CBT is suitable for organizations of all sizes and is of particular utility to geographically distributed organizations that seek common security performance across all employee groups. The increasing diversity of CBT offerings requires prospective buyers to clarify the learning outcomes (see "Effective Security Awareness Starts With Defined Objectives") they seek prior to vendor engagement, and to integrate security education CBT into a consistent program of security maturity improvement across the enterprise.

Market Trends

As products within this market mature, there are a variety of ways in which each vendor seeks to differentiate. Whereas from 2011 through 2014, many vendors sought to distinguish themselves by adding anti-phishing behavior management capabilities to their product set, this has now become less of a differentiator, because the vast majority of vendors have now incorporated that functionality or have very well-established partnerships with anti-phishing behavior management vendors.

Each of the following areas received increased focus and weighting in this year's Magic Quadrant evaluation scoring. Vendor differentiators in 2015 and 2016 include:

- **Learning management systems (LMSs):** Some vendors now provide well-refined, robust SaaS-based LMS platforms that allow at least some content customization, full-featured management dashboards/reporting, and an integrated view into the intersecting metrics related to both phishing simulation tests and CBT performance.
- **Gamification:** Some vendors include a focus on gamification. This is broader than just including games as learning tools. In this context, "gamification" includes the establishment of multidepartment leaderboards so that departments are ranked against each other in various ways.
- **Multilanguage support:** Most long-standing vendors offer support for all major language groups. However, many vendors are now distinguishing themselves by offering out-of-the-box language support for 20 or more languages, and some offer more than 50 languages, including cultural variants/dialects of languages. However, Gartner recommends that organizations verify the accuracy of languages with their own in-country personnel before deploying pretranslated materials.

- **Large supplemental content libraries:** In recognizing that CISOs and security awareness managers are not full-time content writers, graphic designers or marketing experts, many security awareness CBT vendors offer large libraries of predesigned content to serve as additional/supplemental campaign artifacts or for ad hoc communications. These can include materials for newsletters, intranet postings, emails, security alerts, security information for families, and so on.
- **Variety of content formats, lengths and styles:** Many clients and vendors are also recognizing that their security training cannot be effective if approached with a "one size fits all" mentality. As such, they are developing content of different lengths (such as short-burst 1-to-2-minute microlearning lessons) and in different styles (for instance, extremely corporate-friendly and "safe" to more edgy styles using humor). This allows audiences to potentially receive the same information in multiple forms — thereby increasing the possibility for information absorption — as well as allowing for the custom-tailoring of content suited to particular roles or audiences. For instance, training for call center employees should be different from the training for executives.
- **Integration partnerships and possibilities:** Some vendors are also exploring interesting partnerships with core security technology vendors, such as employee monitoring vendors, endpoint detection and response (EDR) vendors, endpoint protection platform (EPP) vendors, secure email gateway (SEG) vendors, and others. The goal of such partnerships is to be able to leverage the real-time data as well as log data to provide injective, just-in-time learning based on observed unsecure behavior exhibited by an employee. Additionally, when unsecure or risky behavior is logged, the behavior could trigger autoenrollment into a contextually relevant training module. This is a natural evolution of the anti-phishing behavior management market — it is all about observed and individualized behavior-based training that is specifically relevant to the learner. This is an emerging area that Gartner will continue to track.
- **Competitive pricing:** The security awareness CBT market is very crowded, with a large number of competitive vendors providing a combination of CBT modules, anti-phishing behavior management and supporting materials for awareness campaigns. From a distance, many of the offerings can seem very similar and, as such, many features that were once distinctive have become commodity. A number of vendors have adjusted pricing downward in an attempt to differentiate on price and also to seek a large share of the SMB market that will not tolerate traditional pricing for products in this market.

Market Growth

The market has experienced greater than 55% growth from 2014 through 2015 and is currently projected to continue at a similar rate as 2016 draws to a close, with projected 2016 market size of approximately $240 million (see Note 2: Calculating Market Size for Security Awareness CBT). Of the vendors rated in this Magic Quadrant, the vast majority (15 of 18) experienced year-over-year revenue growth of greater than 25%,

with multiple vendors experiencing over 70% growth and four vendors with 100% or greater growth.

The investment community is taking note. In 2016, Gartner received a number of inquiry calls from the investment community taking note of the continued market presence and the success of a number of vendors. Signs of strong interest from the investment community were solidified as Elephant invested $8 million in Series A funding for vendor KnowBe4 (see Note 3) and as well-known market veteran PhishMe received $42.5 million in Series C funding led by existing investor Paladin Capital Group (see Note 4).

A Word to CISOs Seeking to Purchase Security Awareness CBTs

CISOs and other purchasers of security awareness CBT products should resist basing their vendor evaluations solely on technical/functional requirements. Deployment of security awareness materials — in many ways — becomes the overt face and voice of the security department to the rest of the organization. As such, ensuring that the tone, production value, and overall look and feel of the solution are a good match for your specific organization is fundamental to success. If the solution you are evaluating does not have content and an interface that is as good as or better than anything else your company has released, other vendors should be evaluated.

Magic Quadrant

Figure 1. Magic Quadrant for Security Awareness Computer-Based Training

Source: Gartner (October 2016)

Vendor Strengths and Cautions

BeOne Development

BeOne Development's goal is to enable learners to learn anywhere, anytime and on any device. The solution includes a growing library of more than 35 modules presented in varied formats and lengths ranging from general courses, to in-depth learning, to very short microlearning sessions. Multiple levels of customization are supported, from easy-to-replace branding to comprehensive customer-specific customization. In addition to CBT, BeOne Development also offers anti-phishing behavior management functionality.

Content is currently offered in 41 languages.

STRENGTHS

- Robust multilingual capabilities provide strong support for consistent training across diverse audiences in multinational enterprises.
- The variety of CBT duration and structure enables highly flexible curriculum scheduling to enhance skills retention.
- BeOne Development enables customers to craft very specific learning paths that are customized to a diverse range of needs, roles or competencies.

CAUTIONS

- With most of its customers based in Europe, BeOne Development faces brand awareness issues outside of its core region. This is partly because BeOne is a relatively new corporate entity founded in 2013 via MeeMaken's acquisition of InfoSecure. The InfoSecure brand name is still well-known both inside and outside Europe.
- Customers needing a diverse set of stylistic variations (for instance, both serious and humorous) may find that BeOne Development does not immediately provide that variety.
- While BeOne Development does offer an anti-phishing behavior management solution, it is not as full-featured as many competitors.

Digital Defense

The SecurED suite of CBT is produced and marketed by Digital Defense. In addition to 12 modules of CBT, the SecurED portfolio includes services for training needs assessment, instructional design, curriculum development and performance assessment. All modules are SCORM-compliant and available as SaaS or an on-premises deployment. Digital Defense provides LMS functionality as a service, with robust analytical and reporting capabilities.

Content is currently offered in nine languages.

STRENGTHS

- SecurED's sitcomlike style of using humor (referred to as reliable modern-day scenarios) can be appealing to companies looking for innovative and nontraditional security awareness presentations.
- SecurED has the ability to customize content and curricula to satisfy clients' needs. Additionally, SecurED offers a nonhumorous version of its content for organizations seeking more-traditional content.
- Digital Defense also offers customers the ability to purchase content outright (and without recurring fees) for customization/modification or internal hosting.

CAUTIONS

- A U.S.-centric direct sales channel limits support for clients headquartered outside the U.S.
- SecureEd content is not currently offered in as many languages as has become the market norm.
- The current SecurED video content can be polarizing for some, and is getting dated. However, Digital Defense is in the process of creating its new "season" of content, which should rectify this potential issue.

Global Learning Systems

Global Learning Systems (GLS) offers robust services in the design, development, deployment and ongoing management of training. The vendor offers a wide range of content around the theme of building your "human firewall." Topics range from traditional security awareness information to regulatory compliance. Content is available as SaaS or in SCORM-compliant modules for on-premises deployment. Its SaaS includes extensive LMS functionality, anti-phishing services, and delivery of content optimized for smartphone and tablet presentation. GLS's inclusion of anti-phishing and other social engineering assessment services creates a comprehensive portfolio for security education and behavior management.

Content is currently offered in 20 languages.

STRENGTHS

- The interactive training content and varied formats are designed to keep learners engaged, reinforce core messages and aid in knowledge retention. Optimization for content presentation on smartphones and tablets provides strong support for modern endpoint portfolios and digital workplaces.
- GLS approaches each customer in a consultative manner, allowing customers to leverage GLS content in the most effective manner given their current maturity.
- GLS offers an out-of-the-box solution for security awareness managers needing an immediate multiyear roadmap with prestructured campaigns and supporting materials.

CAUTIONS

- U.S.-centric sales and service may inhibit uptake of the solution by clients outside of North America; however, GLS has a prioritized strategy for growing its base of customers outside of North America in 2017.
- Customers needing a diverse set of stylistic variations (for instance, both serious and humorous) may find that GLS does not immediately provide that variety. GLS is in the process of expanding content to address this concern.

Inspired eLearning

Inspired eLearning provides a large portfolio of annually updated, role-based content that includes an anti-phishing solution. Delivery options include SCORM, SaaS and a fully managed service. The CBT portfolio is augmented with newsletters, security alerts/reminders, and instructional design and customization services. Multilingual support across multiple media is available for culturally diverse employee populations.

Content is currently offered in 40 languages.

STRENGTHS

- Inspired eLearning provides the ability to provide companies with up to nine years of nonrepeated training centered around five themes.
- Highly innovative presentation styles combine video and immersive situation-based role-playing scenarios into an engaging and still corporate-friendly learning experience.
- Inspired eLearning's analytics platform provides organizations with useful metrics to measure training effectiveness and is enhanced by its adaptive training capabilities, which present each user only with information he or she doesn't know while giving users credit for information they do know.

CAUTIONS

- Pricing may seem high when compared with other competitors (which may not be as feature-rich).
- The lack of a physical presence outside the U.S. may be an obstacle for clients based outside of North America; however, multilanguage support is strong, and the company is now building a more robust global strategy to expand its reach into multiple regions.

Junglemap

Junglemap focuses on delivering security awareness via NanoLearning CBT (two- to four-minute modules intended to be delivered every few weeks), which features content in short, tightly focused packages delivered to trainees with high frequency via email and other message systems. Frequent contact with security content is intended to support high levels of knowledge retention and performance support, with some clients providing weekly training events to employees. Junglemap offers NanoLearning Classic and NanoLearning Flow. Classic focuses on creating and keeping organizational focus

on a topic throughout the year. Flow focuses on respecting different knowledge levels and creating individual progression.

Content is currently offered in more than 50 languages.

STRENGTHS

- The short duration of each module minimizes impact on employee productivity.
- Continuous expansion of the topic list via vendor and client contributions enables highly topical CBT.
- Junglemap's NanoLearning Flow offering enables companies to focus on supporting individual learning paths/needs based on each learner's personal readiness level and mastery.

CAUTIONS

- The lack of sales or service channels outside the Nordic countries and Europe limits vendor visibility.
- Although effective, Junglemap's innovative format, frequency of delivery and structure may not align with how some individuals and enterprises define what "training" looks like.

KnowBe4

KnowBe4 markets anti-phishing behavior management and basic security awareness CBT with a strong focus on testing through social engineering. KnowBe4 has capabilities to improve employee resistance to various forms of social engineering attacks through various forms of penetration tests. CBT content is offered in a variety of module lengths and styles.

Content is currently offered in 26 languages for the 15-minute training module.

STRENGTHS

- KnowBe4 continues to innovate new technology-based paths based on real-world social engineering methodologies to measure social engineering vulnerability within client organizations at the individual employee level.
- KnowBe4's aggressive pricing structure is very attractive to companies looking to purchase security awareness and anti-phishing behavior management solutions on a limited budget.
- KnowBe4 is currently the fastest-growing company within this market and is growing its sales force to keep pace with demand.

CAUTIONS

- Much of KnowBe4's content doesn't currently resonate with large organizations seeking highly sophisticated awareness solutions that support adult learning principles. However, KnowBe4 is working to augment its content library to address this growing need.

- KnowBe4's alignment with the Kevin Mitnick name can be polarizing to some potential buyers.
- While KnowBe4's growth has been explosive and is impressive, it is yet to be seen if it can continue to experience high customer satisfaction and innovation while dealing with the complexities associated with such growth.

MediaPro

MediaPro provides a highly flexible awareness platform that contains customizable CBT content, reinforcement materials (animations, games, posters and articles), phishing simulations, knowledge assessments and planning tools. These products can be licensed separately or as bundles. CBT content is provided as preconfigured modules and as libraries of flexible microlearning CBT content topics that can be rapidly assembled into various unique instructional programs. A broad range of topics structured around common roles and use cases, including privacy, secure application development and corporate compliance, is supported. Content is interactive, with a nearly continuous assessment of skills and knowledge acquisition. MediaPro's phishing and knowledge assessment services are integrated with its CBT and LMS, enabling dynamic delivery of CBT topics based on user behavior and assessment responses.

Content is currently offered in 19 languages.

STRENGTHS

- MediaPro offers one of the most flexible integrated content solutions within this market. This allows clients to simulate course customization and creation capabilities in an easy, drag-and-drop environment.
- MediaPro has a large library of reinforcement materials that can be easily downloaded and leveraged in ad hoc communications or as strategic components in planned campaigns.
- A high level of interactivity in CBT builds trainee competence and skills retention.

CAUTIONS

- While one of MediaPro's main strengths is the flexibility of its course builder, some clients may not have the sophistication to build effective modules.
- MediaPro does not currently enjoy the same amount of brand awareness as many of its competitors. As such, it may be prematurely dismissed from customer shortlists simply because it is not a known name.
- Although language support is good, MediaPro does not currently support as many languages as some other leading/global vendors.

Optiv Security

In 2015, Accuvant and FishNet Security merged to form Optiv Security. The combined organization has an extensive portfolio of solutions focused on cybersecurity. Optiv Security offers three content options: standard (out of the box), tailored (branding and

changes in content for predefined slides) and custom (custom themes, imagery and verbiage). Optiv's CyberBOT format uses a variety of learning modalities in an illustrated style, whereas its Security Awareness Circuit Training (SACT) option is presented in a customizable photo-realistic style. Assessment of trainee performance is incorporated into each module, as well as content branching and remediation that simulates "choose your own adventure" scenarios. Customers have access to a large portfolio of security topics that extends into content for security professionals (for example, security infrastructure administration). In addition to traditional SCORM or hosted LMS options, Optiv Security can also provide a completely managed security awareness program. Anti-phishing behavior management can be provided via a partnership with PhishMe.

Content is currently offered in 32 languages.

STRENGTHS

- Content focused on executive roles via the company's Executive Vulnerability Simulations provides strong support to target specific audience needs.
- Offering multiple stylistic and immersive learning scenarios can have broad appeal for organizations seeking both traditional and more innovative awareness and training programs.
- Optiv's additional resource catalog is created with full alignment to its CyberBOT and SACT courseware, providing a sense of continuity and purpose across the campaign elements.

CAUTIONS

- U.S.-centric sales and service limit market reach and client support outside North America.
- Optiv Security does not currently enjoy the same amount of brand awareness within the security awareness CBT market as many of its competitors. However, Optiv is very well-known as a credible consultancy, so lack of brand awareness in the CBT market can certainly be overcome.
- Optiv's current SaaS LMS has some limitations when compared with the market norm (for instance, it does not yet have the capability to send individualized reminders or late notifications via email); however, LMS improvements are on its stated roadmap.

PhishLine

PhishLine is an anti-phishing behavior management and security awareness CBT provider with a particular focus on the data science of phishing measurement and with the ability to provide security awareness CBT modules from multiple vendors through its Content Center Marketplace. PhishLine's social engineering behavior management solution includes phishing, USB, SMS and voice channels, and is usually delivered as SaaS but can be run via an on-premises deployment or as a fully managed service. Extensive analytics enable more-complex behavioral assessment and targeted

education than is common with competitive anti-phishing solutions. Comprehensive LMS functionality is provided as a service, or the solution can integrate with an in-house LMS. Assessment capabilities include a variety of social engineering and phishing simulations that allow users to apply and demonstrate acquired knowledge.

Content is currently offered in 12 languages.

STRENGTHS

- Continual analysis of employee performance enables highly individualized training curricula for each employee based on the actual security performance of that employee.
- PhishLine offers a "data scientist" level view into the facets of how to create a simulated phish and how to measure/report on the data gathered and available through simulated phishing tests and CBT assessments.
- PhishLine's Content Center Marketplace provides a simple platform for customers to pick and choose from a large variety of CBT modules and associated content from multiple vendors (currently PhishLine, Security Innovation, The Security Awareness Co. and Ninjio), which is then aligned to specific PhishLine-created social engineering testing.

CAUTIONS

- While the solution has all of the features and functions of a leading product within this market, much of that can be obscured by the complex look and feel of the administrative interfaces. Clients looking for a simple, out-of-the-box awareness CBT vendor may find the number of options and the potential complexity of the solution overwhelming.
- Some clients (especially international clients) may be fearful of the amount of data that can collected and analyzed. Customers with data collection and privacy concerns are encouraged to work with PhishLine to ensure that they are taking advantage of the advanced configuration options that map to their individual regulatory or other security/privacy needs.
- Although language support is good, PhishLine does not currently support as many languages as some other leading/global vendors. However, for clients leveraging PhishLine's Content Center Marketplace, many of the modules are offered in over 30 languages.

PhishMe

Based on the number of clients served and revenue generated, PhishMe is currently the largest provider of anti-phishing CBT and enjoys global name recognition. PhishMe's focus on phishing behavior management and its large market base enable it to benchmark client performance against industry performance. This capability is supported with flexible analysis and reporting capabilities. In addition to anti-phishing, PhishMe also offers a large library of interactive content that incorporates games, video and a variety of learning artifacts. The PhishMe brand is well-known throughout the

security industry, and the success of its marketing program and technical innovations has established it as the company to beat when it comes to anti-phishing solutions. PhishMe's 2015 acquisition of phishing threat intelligence vendor Malcovery demonstrates a new and interesting growth area for the company.

PhishMe's CBFree (general security awareness) content is currently offered in nine languages. Content contained in its phishing platform is currently offered in 47 languages.

STRENGTHS

- Flexible analysis and reporting enable training optimization and phishing susceptibility vulnerability assessment.
- While PhishMe has, in many ways, become the most recognized vendor in this market, it continues aggressive reinvestment of revenue into product improvement, new capabilities and services.
- PhishMe's PhishMe Reporter and new PhishMe Triage product allow users to report suspected phishing emails via a "report" button in their email client and also enables significant automated analysis and risk ranking of the phish for incident response teams.

CAUTIONS

- PhishMe focuses on phishing and provides a number of security awareness and training artifacts and a free CBT package (CBFree). However, much of the CBT package is not as robust and innovative as many of the market leaders.
- An increasing number of vendors provide anti-phishing solutions that could erode PhishMe's value proposition for its anti-phishing suite. However, as demonstrated with the acquisition of Malcovery, PhishMe continues to find new innovation paths and differentiation.

Popcorn Training

Popcorn Training is a small regional developer of security CBT. Popcorn Training's staff has significant instructional design skills that are leveraged to optimize the impact of client investments in training. The CBT includes story-based end-user security content, as well as content specific to regulations within South Africa. CBT can be delivered via SaaS or on-premises, and it can be integrated with LMSs. Optimization of CBT for on-premises deployment enables Popcorn Training to successfully target markets characterized by low- or poor-quality bandwidth in rural regional locations. All content is interactive and customizable. The standard offering incorporates multiple episodes in a continuing storyline with various animated, as well as live-action, characters, but the vendor also produces customized motion-graphic versions without animated or acted characters for more conservative audiences.

Content is currently offered in nine languages.

STRENGTHS

- Popcorn Training's CBTs are innovative and visually engaging — targeting a media-savvy culture — with content that is continually updated to remain relevant and persuasive and delivered via a video-app-style interface.
- The vendor is highly responsive to customer needs for content modification.
- Vendor capabilities in instructional design and training needs assessment maximize the ROI of customization investments.

CAUTIONS

- Popcorn Training's sales and service channels outside South Africa are limited.
- The range and variety of topics covered by Popcorn Training may become a limitation as the program grows in maturity and seeks to support varied and deeper learning content.
- Limited support for languages restricts applicability to multicultural enterprises and audiences.

SANS Institute

SANS Institute is a major force in the training market for IT security professionals, offering well-regarded certification and degree programs, such as the Global Information Assurance Certification (GIAC). Its "Securing The Human" CBT portfolio is extensive and focuses on general security awareness, as well as on specific vertical industries, regulatory environments and roles, including senior leadership. The offering also includes an anti-phishing behavior management functionality for social engineering testing. SANS Institute offers a flexible solution that can supply security awareness "out of the box" for organizations just beginning their programs, and it can equally support the individual and varied learner needs associated with intermediate or mature-level security awareness programs.

Content is currently offered in 28 languages.

STRENGTHS

- SANS recently revamped its LMS as a strategic move to also support its full catalog of offerings (including technical training). The result is one of the most robust SaaS LMS platforms offered by a security awareness vendor.
- A deep knowledge of IT security management combined with adult learning psychology and design principles is reflected in the content and delivery of materials.
- The large CBT portfolio covers the topics and roles that Gartner clients commonly request, using formats (such as videos, games and quizzes) that suit many organizations that are seeking a wide variety of CBT training options that can support individual learning styles and cultural needs.

CAUTIONS

- Many organizations recognize the SANS brand as offering very technical training and may fear that its end-user training would be over the heads of "common" folk. While this is not the case with the Securing The Human product, this is still a perception barrier that the vendor faces.
- While SANS offers 28 languages for its online training, large global companies may still find that it does not yet support one or more of the required languages.
- Support is currently available only during working hours in the U.S. Clients in distant time zones may struggle to gain adequate support. SANS is addressing this by adding support personnel in the U.K.

Secure Mentem

Secure Mentem is focused on driving improvement in security outcomes through culture change, and has a highly consultative and individualized approach to helping clients shape their security culture. Secure Mentem offers a broad range of services and products that are structured around the concept of a security awareness program life cycle. This includes services for assessment, performance baselines, program design, security metrics, curriculum design and administration. Typical services and products that accompany the CBT offering are cultural assessments, posters, newsletter articles, event planning guides and security messages for internal distribution to trainees.

Internally developed content is currently offered in eight languages.

STRENGTHS

- Secure Mentem's individualized approach and focus on culture change and management are well-suited to clients seeking to change the corporate dynamics that drive poor security behavior.
- Secure Mentem's ecosystem of content partners, along with its ability to create custom CBT, helps to provide a large catalog of CBT covering a wide variety of security topics and regulatory requirements.
- Pricing is typically extremely competitive when compared with other vendors in this market.

CAUTIONS

- Secure Mentem currently has limited sales and service channel support outside North America.
- Secure Mentem does not currently enjoy the same amount of brand awareness as many of its competitors. As such, it may be prematurely dismissed from customer shortlists simply because it is not a known name.
- Limited support for languages restricts applicability to multicultural enterprises and audiences.

Security Innovation

Security Innovation offers a wide and diverse set of content and supporting resources, including traditional CBT, supplemental videos, tip sheets, posters, lunch-and-learn activities, customer care assets, securing-your-home information, and immersive and scenario-based learning modules, all offered in a variety of styles with full animation and narratives in local languages. Security Innovation also offers an extensive library of application security and IT security training, as well as consulting services that clients often bundle.

Content is currently offered in 10 languages.

STRENGTHS

- In addition to traditional CBT, Security Innovation has recently begun to offer "hack-a-thon" challenges that can be delivered via computer or in live situations. This type of immersive and situation-based learning can help participants understand attackers' strategies and best-practice defense strategies by putting them "in the shoes" of the attacker.
- Security Innovation's use of diverse media, mixed duration, interactivity and changing visuals in modules enhances the uptake and retention of new skills.
- The vendor's holistic, life cycle approach to training management promotes close alignment with enterprise risks and performance gaps.

CAUTIONS

- When compared with other market leaders, the range of topics covered by Security Innovation may become a limitation as the program grows in maturity and seeks to support varied and deeper learning content.
- Limited support for languages restricts applicability to multicultural enterprises and audiences.

Security Mentor

Security Mentor offers short-duration CBT (approximately 10 minutes per module) structured for frequent delivery to each employee. CBT modules include games and opportunities to practice new skills with the remediation techniques provided (when appropriate). Security Mentor's LMS functionality is robust and intuitive. Security Mentor offers the ability for clients to upload their organizational policies to Security Mentor's system for compliance attestation and tracking. All content is interactive, with a continually growing and refreshed curriculum composed of both basic and more-advanced content, as well as utilizing gamification. Security Mentor also provides consulting services to assist in customization of educational programs and optimization of client learning outcomes.

Content is currently offered in 11 languages.

STRENGTHS

- The short duration of the CBT modules is attractive for clients that are seeking to limit the productivity impact of training participation while maintaining a high-impact curriculum.
- Lessons are interactive, graphical and instructionally designed for trainee engagement and learning.
- Security Mentor is in a growth phase, focusing on rapid expansion of global partnerships, as well as refinement of its curriculum and platform.

CAUTIONS

- While language support is good, Secure Mentor's language support is not yet as expansive as many competitors. The use of Flash may be problematic for clients utilizing web browsers that do not support it. However, the vendor is currently converting to HTML5.
- Security Mentor does not currently offer anti-phishing behavior management functionality. Customers seeking that component will need to consider a multivendor solution.

Symantec (Blackfin Security)

In August 2015, Symantec acquired Blackfin Security, a provider of security awareness CBT, anti-phishing behavior management, and technical training for security professionals. Symantec's Security Awareness CBT offering is composed of short, focused videos and accompanying quizzes across a wide range of security topics, and Phishing Readiness (an anti-phishing behavior management solution). Symantec's presence and brand recognition as a provider of security-related products and services give it unique entry points into client buying cycles as the vendor is well-positioned to help clients create large-scale overall security program strategies.

Content is currently offered in seven languages.

STRENGTHS

- The short duration of the CBT modules is attractive for clients that are seeking to limit the productivity impact of training participation. Symantec's Phishing Readiness offers a variety of reporting capabilities, enabling customers to drive behavior changes based upon results and their Security Awareness programs' needs around phishing assessments.
- Symantec has a large library of content (approximately 50 modules) of consistent look and feel that is refreshed frequently.
- Symantec's solution may be particularly appealing to companies that are already large Symantec customers and those that partner with Symantec for security program development.

CAUTIONS

- Limited support for languages restricts applicability to multicultural enterprises and audiences.

- Symantec currently does not offer an online LMS for its security awareness modules.

Terranova WW

Terranova WW provides a large library of CBT modules and supporting materials primarily focused on general security awareness. Interactive content is supported by posters, newsletters and short videos, as well as by assessment and customization services. Terranova WW also provides anti-phishing simulation training. Preassessments and postassessments are available, and employee skills retention is tested in each CBT module. Terranova WW provides strong support prior to implementation to enable clients to select appropriate content for different user populations, and develop effective communication and deployment strategies.

Content is currently offered in 37 languages.

STRENGTHS

- Terranova WW supports each customer in a very consultative manner, ensuring that proper customization of content is achieved and that the learning paths are clearly defined and well-suited to the organization's selected roles and groups of learners.
- Lessons are highly interactive, graphical and instructionally designed for trainee engagement and learning.
- Ongoing assessment of trainees aids in the fine-tuning of curricula to meet security performance objectives.

CAUTIONS

- A strong focus on the North American client base may limit the availability of regulatory training required in other jurisdictions.
- While Terranova does possess a large library of content and resources, some organizations may not immediately resonate with the content's distinctive look and feel. However, Terranova offers customization services to match customer needs.

The Security Awareness Co.

The Security Awareness Co. provides one of the largest and most diverse security awareness content, CBT and resource libraries of any vendor. Its portfolio is both broad and deep, including an extensive collection of CBT, interactive learning modules, videos, animations, games, posters, tipsheets, newsletter content and other supporting downloadable resources. Traditional CBT is augmented with "security express videos," which offer one- to three-minute reinforcement messages for security content. A variety of assessment mechanisms is also available. The Security Awareness Co. has content presented in virtually every stylistic preference and delivery medium. Anti-phishing behavior management functionality is offered via partnerships with PhishLine, KnowBe4 and Social-Engineer. The vendor regularly works with clients to design an effective curriculum and to customize content based on training needs analysis.

Content is currently offered in 20 in-stock languages.

STRENGTHS

- The use of diverse multimedia, in addition to CBT, reinforces targeted skills and knowledge retention.
- The Security Awareness Co. has a large offering of available-for-purchase, as well as free, materials that will complement any program (from beginning to advanced), using a continuing and sustained security awareness "marketing" campaign approach.
- The vendor's large variety of content is well-suited for organizations seeking great diversity and variation in how they target communication styles to different roles or contexts.

CAUTIONS

- While The Security Awareness Co.'s library of several thousand learning artifacts can be compelling, it can also be overwhelming for organizations just beginning their program and needing a simple path. However, its Demo Center allows customers to see all content, create favorites and organize their programs.
- Although language support is good, The Security Awareness Co. does not currently support as many languages as some other leading/global vendors.

Wombat Security Technologies

Wombat Security Technologies is a leading provider of innovative security education and behavior management CBT, and features on nearly all customer shortlists. In addition to a portfolio of CBT on traditional security awareness topics, Wombat provides an effective anti-phishing solution that also supports simulated attacks through USB devices and SMS. Wombat acquired ThreatSim in 2015 and has integrated that product into its platform. Partnership with Carbon Black enables just-in-time training based on any user behavior that can be identified through and reported via connection to Carbon Black. Wombat provides extensive services in training needs analysis, content development, CBT customization, and security essentials training for executives. Wombat provides guidance on curriculum scheduling based on continuous assessment, refinement, targeted education and behavioral metrics to optimize retention of learned behaviors.

Content is currently offered in 27 languages.

STRENGTHS

- Continuing innovation in support of measurable security performance also supports the clients' need to enhance risk mitigation through the management of user behavior.
- Wombat is very well-suited to large enterprises seeking to deploy broad-base security awareness and anti-phishing training with a consistent corporate look and

feel that utilizes adult learning principles applicable across a variety of learning styles.

- Wombat's approach to "teachable moment" learning engages participants in the learning process through a variety of methods that encourage application of knowledge in scenario-based modules.

CAUTIONS

- Organizations seeking a wide variety of presentational formats and styles (for instance, extremely corporate-friendly and "safe" to more edgy styles using humor) may find Wombat Security Technologies' content limiting.
- Wombat's pricing is relatively high compared with many competitors depending upon the solution being purchased.

Vendors Added and Dropped

We review and adjust our inclusion criteria for Magic Quadrants as markets change. As a result of these adjustments, the mix of vendors in any Magic Quadrant may change over time. A vendor's appearance in a Magic Quadrant one year and not the next does not necessarily indicate that we have changed our opinion of that vendor. It may be a reflection of a change in the market and, therefore, changed evaluation criteria, or of a change of focus by that vendor.

Added

No vendors were added this Magic Quadrant.

Dropped

- Aujas
- Scipp International
- ThreatSim (acquired by Wombat Security Technologies)

Inclusion and Exclusion Criteria

Gartner's view of the market is focused on transformational technologies or approaches delivering on the future needs of end users. It is not focused on the market as it is today.

Gartner defines the security awareness CBT as the delivery of a standardized set of interactive security education and/or security behavior management content to a trainee/user via an endpoint computing device (such as a laptop, desktop or tablet). Training content focuses on general users of IT, not security or IT professionals. Although customization of this content may be provided as a service, the essential element is a catalog of core training content.

The security education CBT definition does not include solutions delivered through vendor personnel on-site (such as live training sessions), content delivered to trainees through noncomputing mechanisms (such as printed manuals or newsletters), nor services that produce novel and unique CBT solutions for a single client.

Inclusion Criteria

The inclusion criteria represent the specific attributes that Gartner believes necessary for inclusion in this research. To qualify for inclusion in the 2016 Magic Quadrant for Security Awareness Computer-Based Training, vendors must:

- Compete in the market for security education CBT, as defined above.
- Demonstrate a competitive presence in end-user organizations.
- Demonstrate ability to provide training content in English and at least one other language.
- Provide a diverse set of security content/curriculum.
- Provide trainee performance assessments against defined learning outcomes.
- Offer (via vendor-owned technology or through a partnership) an automated social engineering simulation tool (such as anti-phishing behavior management) capability for measuring current behavior and promoting behavior change.
- Demonstrate security education CBT revenue of over $1 million or a security education CBT customer count of over 400 client organizations.
- Be the original developer of the solution. Although we examine strategic partnerships as part of our analysis, we do not rate resellers.

Evaluation Criteria

Ability to Execute

Product or service: This includes service and customer satisfaction in deployments of the security education CBT. Execution considers factors involved in the selling, deployment and support of the education solution. Strong execution indicates that a company has clearly demonstrated that its solution has been successfully deployed and maintained, and that the company wins a large percentage of engagements in competition with other vendors. Companies that execute strongly generate persistent and pervasive brand awareness and loyalty among Gartner clients, and they are mentioned regularly in inquiries with Gartner analysts. Execution is not strongly correlated to company size or market share, although these factors can influence a company's ability to execute over time. Although sales success is a factor in the Ability to Execute, continuing innovation and quality of the solution portfolio have greater impact. Key features are weighted heavily. These include multiple modules of software, content that covers topics commonly raised by Gartner clients, customization of content,

interactive learning experiences and support for multiple types of endpoints. Support is rated on quality and breadth.

Overall viability: This includes overall financial health, prospects for continuing operations, company history and demonstrated commitment to the security education market. All vendors were asked to disclose comparable market data, such as revenue, quantity of customers, quantity of trainees and competitive wins.

Sales execution/pricing: Gartner evaluates the company's pricing, deal size and installed base. This analysis includes the company's sales and distribution operations and relationships. Pricing is compared in terms of typical deployment models. The robustness of sales channels is a strong factor.

Market responsiveness/record: Gartner's analysis focuses on the company's ability to support changing client requirements for security performance management.

Marketing execution: This ranking includes competitive visibility in client RFPs and competitive visibility with other vendors. The prominence of solution innovations in the market is a key factor, as are pricing innovations. Support for multiple endpoint platforms is heavily weighted, as is the depth of support for customization of content and structure of the solution.

Customer experience: Given the culture-specific and subjective nature of training effectiveness, this factor is heavily weighted in our analysis. Customer satisfaction throughout the client-vendor relationship is examined.

Operations: The experience and track record of company management in training design/development and the security marketplace are critical factors. Effective training solutions can be developed and marketed by small organizations. As a result, this factor focuses on the quality of staffing, rather than the quantity of personnel.

Table 1. Ability to Execute Evaluation Criteria

Evaluation Criteria	**Weighting**
Product or Service	High
Overall Viability	Medium
Sales Execution/Pricing	High
Market Responsiveness/Record	High
Marketing Execution	Medium

Table 1. Ability to Execute Evaluation Criteria

Evaluation Criteria	Weighting
Customer Experience	High
Operations	Low

Source: Gartner (October 2016)

Completeness of Vision

Market understanding and marketing strategy: Gartner assesses these factors via interactions with vendors, feedback from Gartner customers, and direct interactions with vendor solutions and materials. We evaluate the vendor's proven ability to anticipate market changes and lead customers to optimal performance. We also examine the company's understanding of and commitment to the security education market.

Sales strategy: This includes customer relationship management before purchase as well as during and after deployment of the solution. Companies need to demonstrate an understanding of the various decision makers and influencers within client organizations for security education solutions. Channel and third-party ecosystem strategies also apply.

Offering (product) strategy: This factor focuses on a vendor's solution roadmap, current solution features, variety and volume of content types, and solution performance. Integration of the CBT solution with other systems and capabilities (for example, LMS integration and LMS as a service) is also examined. Strong emphasis is placed on vendor support for reporting mechanisms that provide credible evidence of trainee progress, as well as improvement of security performance in the context of defined learning outcomes.

Business model: This includes R&D spending as well as the vendor's approach to developing new capabilities and features.

Vertical/industry strategy: While this Magic Quadrant is primarily focused on general end-user security education, training for security and data handling requirements aligned with specific verticals/industries is taken into account.

Innovation: This factor is heavily weighted and focuses on innovation in the core solution and supporting services and solutions.

Geographic strategy: This Magic Quadrant is global in scope, but many vendors demonstrate the strongest performance in their home geographies (for example, U.S. vendors perform best in North America). As a result, our analysis closely examines vendors' ability to support geographic markets beyond their home territories.

Table 2. Completeness of Vision Evaluation Criteria

Evaluation Criteria	Weighting
Market Understanding	High
Marketing Strategy	Medium
Sales Strategy	Medium
Offering (Product) Strategy	High
Business Model	Low
Vertical/Industry Strategy	Low
Innovation	High
Geographic Strategy	Medium

Source: Gartner (October 2016)

Quadrant Descriptions

Leaders

The security education CBT Leaders quadrant is composed of vendors that: (1) provide solutions that are a good match to market requirements; (2) have been the most successful in building a customer base and revenue stream within the CBT market; and (3) have a relatively high viability rating (due to CBT revenue). In addition to providing CBT that is a good match to customer requirements, Leaders also show evidence of superior vision and execution for anticipated requirements. They typically have relatively high market share and/or strong revenue growth, and provide a range of CBT capabilities that target education and behavior management. They have demonstrated positive customer feedback for effective CBT and related services, as well as focusing intently on anticipating market needs and evolving accordingly.

Challengers

The Challengers quadrant is composed of vendors that have a sustainable customer base and revenue, proven market relevance and adaptability, and solutions that meet the majority of market requirements. Vendors in this quadrant typically have strong

execution capabilities, as evidenced by financial resources, significant sales, customer counts, and brand presence garnered from the company as a whole or from other factors. However, Challengers have not demonstrated as rich a capability or track record for CBT offerings as vendors in the Leaders quadrant.

Visionaries

The Visionaries quadrant is composed of vendors providing CBT solutions that are good functional matches to general security education market requirements; however, these vendors have a lower Ability to Execute rating than the Leaders. This lower rating is typically due to a smaller presence in the market than the Leaders, as measured by installed base, revenue size or growth, a smaller overall company size, or general viability. Visionaries may also be vendors that specifically choose to focus with excellence on an innovative subset of market needs.

Niche Players

The Niche Players quadrant is composed primarily of smaller vendors providing security education CBT that matches specific security education use cases, which are a subset of CBT market requirements. Niche Players focus on a particular segment of the client base, or a more limited product set. An ability to outperform or innovate may be affected by this narrow focus. Vendors in this quadrant may have a small installed base, or they may be limited, according to Gartner's criteria, by a number of factors. These factors may include limited investments or capabilities, a geographically limited footprint, or other inhibitors to providing a broader set of capabilities to enterprises now and during the 12-month planning horizon. Inclusion in this quadrant does not reflect negatively on the vendor's value in the more narrowly focused service spectrum.

Context

The security education CBT market is a rapidly growing market focused around delivery of content for end-user security awareness. The market is currently evolving as it seeks to provide demonstrable benefit to organizations rather than just being a regulatory compliance "checkbox." Innovations are currently focused on:

- Behavioral intervention (which began with anti-phishing behavior management toolsets and is evolving into other integrations with more traditional security controls)
- Wide, diverse content sets, styles and supporting materials to support multiple learner contexts
- Robust LMS platforms to enable content assignment as well as reporting of metrics
- Support for large sets of languages to enable global delivery of content
- Intersection with threat intelligence, endpoint detection and response (EDR), and incident response to enable tailored, context-relevant training/testing content, as well as the ability to quickly analyze reported/suspected phishing emails and determine their risk.

The structure and content of solutions remain dynamic in response to changing threats and employee behaviors. Continual changes in the devices that workers use and the locations where work is conducted are forcing organizations to influence employees' security behavior and improve their security performance in workplaces. This ongoing change in the digital workplace erodes the efficacy of static education programs, driving enterprises to seek regular updates and improvements to the structure and focus of security education. Demand for innovative solutions that drive validated improvement in security performance is increasing, as is the demand for robust training performance metrics and reporting.

Market Overview

Market growth in security education is driven by changes in threats to the enterprise (such as continuing expansion of cybersecurity regulations targeting employee actions, threats that target employees and their devices, and utilization of technology that is beyond the control of the IT security organization), as well as increasing recognition that internal security departments are rarely able to produce effective security education or behavior management programs. The combination of increased risks and a lack of internal expertise pushes many CISOs to seek solutions in the market that are capable of producing measurable improvements in employee security behavior. In order to support security objectives, employees require skills, knowledge and motivation. Security education focuses on developing secure employees who, in turn, enable security performance and regulatory compliance.

The challenge of capturing market numbers for security education is exacerbated by the extreme diversity of activities, products and services that are present in the market. For example, security education programs can include security policy communication systems, live instruction (on-premises), posters/handbills, games/contests, manuals and videos. This Magic Quadrant focuses on the portion of the overall security education market that is most often discussed by Gartner clients: security education delivered to employees via digital endpoints. Within that context, market growth is extremely robust.

The market has experienced greater than 55% growth from 2014 through 2015 and is currently projected to continue at a similar rate as 2016 draws to a close, with projected 2016 market size of approximately $240 million (see Note 2: Calculating Market Size for Security Awareness CBT). Of the vendors rated in this Magic Quadrant, the vast majority (15 of 18) experienced year-over-year revenue growth of greater than 25%, with multiple vendors experiencing over 70% growth and four vendors with 100% or greater growth.

Given that most organizations of any size need to provide some level of security training for their employees, there is a very large anticipated total addressable market (approximately $1.5 billion depending on solution price tolerances) for solution vendors to continue mining. As such, Gartner anticipates sustained year-over-year growth in the 40%-to-60% range through at least 2018.

Anti-phishing behavior management continues to be a popular segment of the security awareness CBT market, with vendors seeking to innovate into new areas of behavior

management, measurement and influence. This popularity is due to both the demonstrable and evolving threat of phishing — phishing attacks have been the initial attack vector in multiple, large, high-profile breaches — and the ability of anti-phishing solutions to demonstrate behavior improvement in targeted employees. Nearly all vendors now offer some form of anti-phishing behavior management through in-house development of a solution, licensing of technology from another vendor or partnership with an anti-phishing solution provider. While anti-phishing behavior management is still a driver for this market, vendors with such solutions are no longer differentiated by having the solution … it is now the market norm and expectation.

The use of simulated attacks that trigger employee behavior and remediation training — all of which can be measured and analyzed over time — has increased client expectations for demonstrable ROI for security education investments. Vendors have responded by incorporating more curriculum management and trainee assessment capabilities into their offerings, and by producing software modules that are of shorter duration (that is, the current average duration is approximately 11 minutes) than traditional CBT approaches, which last 45 minutes and longer. An increasing number of vendors are introducing even shorter videos (one to three minutes in duration), and enterprise clients are reporting positive results from such short-duration, but high-frequency, media packages. Clients that treat security education as an inherently unproductive investment are a diminishing group, and the overall market is increasingly focused on security education that is proven to be effective and efficient at driving enterprise security performance.

Privacy regulations and other governmental controls in various jurisdictions may have an impact on the viability of vendor solutions that require transportation and out-of-country storage of employee identity and performance information related to training activities. Enterprises should seek legal counsel concerning the impact of such regulations on the use of vendor infrastructure located outside of the enterprise's legal jurisdiction. If transborder exfiltration of employee data is prohibited, clients should consider the use of on-premises or in-country LMS, CBT and anti-phishing solutions.

Gartner anticipates continued growth in the security education CBT market through 2018. Increasing numbers of end-user organizations will license CBT from regional and global vendors. Vendors will expand their support for diverse endpoints (for example, mobile and IoT devices) and presentation styles (that is, increased interactivity of content). The low barriers to market entry enable new vendors to enter the market, and Gartner expects to see a steady increase in the vendors competing in the security education CBT arena. Executive ROI expectations will drive security teams to invest in mechanisms that measure, record, analyze and report on employee performance in the context of security. Vendors are moving to support enterprises' appetite for metrics by analyzing user behavior via user and entity behavior analytics (UEBA) solutions and providing just-in-time remediation training based on actual employee behavior. The ability to deliver the right training experience to the people who need it, when they need it, will transform the security awareness market and drastically improve enterprise security outcomes that are dependent on employee behavior.

Other Vendors of Note

It is important for potential buyers to appreciate the dynamic nature of this market. Gartner is continually being briefed by new vendors seeking to meet the market demand for quality and innovative CBT content, delivery mechanisms, or adjacent functionality. While not formally rated in this year's Magic Quadrant, we believe that the vendors/products listed below are worth note and may support one or more use cases well.

- Axelos Resilia Awareness Learning
- eLearning Corner
- InfoSec Institute SecurityIQ
- Ironscales
- Kaspersky Labs Cybersecurity Awareness Training
- Lucy Phishing
- Navex Global
- Ninjio
- PhishLabs
- PhishThreat
- Rapid7 Security Awareness Training
- Restricted Intelligence
- Scipp International
- Vectorx Labs

Acronym Key and Glossary Terms

CBT	computer-based training
EDR	endpoint detection and response
EPP	endpoint protection platform
LMS	learning management system
R&D	research and development

ROI	return on investment
SCORM	Sharable Content Object Reference Model
SEG	secure email gateway
UEBA	user and entity behavior analytics

Evidence

- Gartner customer inquiries and information sharing related to security awareness CBTs
- Gartner customer inquiries and information sharing related to security awareness program development and trends
- Analyst interactions with Gartner customers via inquiries and meetings
- Survey of security awareness CBT vendors
- Survey of security awareness CBT reference customers

Note 1
Anti-Phishing Behavioral Conditioning

A number of vendors (for example, KnowBe4, PhishLine, PhishMe and Wombat Security Technologies) provide solutions that focus on reducing the frequency with which employees click on URLs in phishing emails. Although each vendor provides a unique solution, the basic approach is the same:

- Phishing emails are sent to employees.
- Employees who click on the URLs therein are immediately pushed into a CBT session.
- Click rates and refusals to click on URLs are recorded for longitudinal trend analysis.

This approach has proved to be effective at diminishing the success of phishing attacks. By tightly coupling the clicking on URLs with participating in CBT, these solutions are able to provide valid evidence of a causal correlation between CBT participation and behavior change. In turn, this provides support for claims of positive ROI from investment in such solutions.

Note 2
Calculating Market Size for Security Awareness CBT

The revenue projections for vendors rated in this Magic Quadrant account for approximately $172 million for 2016. The $240 million anticipated revenue for 2016 is calculated by looking at the combined revenue for the vendors tracked as part of the Magic Quadrant process. We then add an additional 40% to account for other vendors that are not tracked/rated as part of this process, which are small/regional vendors, or which are unknown to us.

Note 3
KnowBe4 Series A Funding Press Release

"KnowBe4 Raises $8 Million in Series A Funding Led by Elephant Partners"

Note 4
PhishMe Series C Funding Press Release

"PhishMe Raises $42.5 Million In Series C Funding Led By Paladin Capital Group And Joined By New Investor Bessemer Venture Partners"

Evaluation Criteria Definitions

Ability to Execute

Product/Service: Core goods and services offered by the vendor for the defined market. This includes current product/service capabilities, quality, feature sets, skills and so on, whether offered natively or through OEM agreements/partnerships as defined in the market definition and detailed in the subcriteria.

Overall Viability: Viability includes an assessment of the overall organization's financial health, the financial and practical success of the business unit, and the likelihood that the individual business unit will continue investing in the product, will continue offering the product and will advance the state of the art within the organization's portfolio of products.

Sales Execution/Pricing: The vendor's capabilities in all presales activities and the structure that supports them. This includes deal management, pricing and negotiation, presales support, and the overall effectiveness of the sales channel.

Market Responsiveness/Record: Ability to respond, change direction, be flexible and achieve competitive success as opportunities develop, competitors act, customer needs evolve and market dynamics change. This criterion also considers the vendor's history of responsiveness.

Marketing Execution: The clarity, quality, creativity and efficacy of programs designed to deliver the organization's message to influence the market, promote the brand and business, increase awareness of the products, and establish a positive identification with the product/brand and organization in the minds of buyers. This "mind share" can be driven by a combination of publicity, promotional initiatives, thought leadership, word of mouth and sales activities.

Customer Experience: Relationships, products and services/programs that enable clients to be successful with the products evaluated. Specifically, this includes the ways customers receive technical support or account support. This can also include ancillary tools, customer support programs (and the quality thereof), availability of user groups, service-level agreements and so on.

Operations: The ability of the organization to meet its goals and commitments. Factors include the quality of the organizational structure, including skills, experiences, programs, systems and other vehicles that enable the organization to operate effectively and efficiently on an ongoing basis.

Completeness of Vision

Market Understanding: Ability of the vendor to understand buyers' wants and needs and to translate those into products and services. Vendors that show the highest degree of vision listen to and understand buyers' wants and needs, and can shape or enhance those with their added vision.

Marketing Strategy: A clear, differentiated set of messages consistently communicated throughout the organization and externalized through the website, advertising, customer programs and positioning statements.

Sales Strategy: The strategy for selling products that uses the appropriate network of direct and indirect sales, marketing, service, and communication affiliates that extend the scope and depth of market reach, skills, expertise, technologies, services and the customer base.

Offering (Product) Strategy: The vendor's approach to product development and delivery that emphasizes differentiation, functionality, methodology and feature sets as they map to current and future requirements.

Business Model: The soundness and logic of the vendor's underlying business proposition.

Vertical/Industry Strategy: The vendor's strategy to direct resources, skills and offerings to meet the specific needs of individual market segments, including vertical markets.

Innovation: Direct, related, complementary and synergistic layouts of resources, expertise or capital for investment, consolidation, defensive or pre-emptive purposes.

Geographic Strategy: The vendor's strategy to direct resources, skills and offerings to meet the specific needs of geographies outside the "home" or native geography, either

directly or through partners, channels and subsidiaries as appropriate for that geography and market.