KnowBe4
Human error. Conquered.

GLOBALCTI
Global Solutions. World Class Service.

Critical Considerations When Evaluating Security Awareness Training Vendors

INTRODUCTION

The vendor landscape for security awareness training (SAT) is as diverse as it is innovative. This market has changed significantly over the past several years as CISOs and security leaders now seek to ensure that any SAT program is changing user behavior and empowering their business to understand, reduce and monitor employee cyber risk.

An SAT vendor should provide a platform to accomplish this by:

- Helping you develop broader thinking around security culture and human risk management
- Provide the necessary tools to drive and measure behavioral change
- Ensure your users become your organization's human firewall and last line of defense against cyber attacks and data breaches

This white paper provides an overview of what to know before you evaluate SAT platforms, and most importantly, seven critical capabilities any SAT vendor should provide to help your organization achieve its goals.

EVALUATING SECURITY AWARENESS TRAINING PLATFORMS

Many, old-school SAT programs fail to account for something called the knowledge-intention-behavior gap. Simply put, just because you provide a user with information and data pertaining to security awareness doesn't mean they'll learn from it and/or care about it.

Information alone doesn't change actions. Ultimately, individuals will gravitate toward the path of least resistance or what is habitual. Ensure key stakeholders within your organization understand these three realities before evaluating an SAT vendor.

- **Just Because You Make Someone Aware Doesn't Mean They'll Care**
  Throwing lots of information, data and procedures at employees won't make them care about security awareness. When they receive a security recommendation, most employees will "take it under advisement" and will weigh it versus other priorities.

- **If You Attempt To Work Against Human Nature, You Will Fail**
  If there is a gap between your policy expectations and the previously mentioned behavioral realities, your SAT program will likely fall well short of expectations. Ultimately, you're training and setting expectations with humans, not programming data into a computer.

- **What Your Employees Do Is Way More Important Than What They Know**
  Knowledge alone has never stopped an organization from having a breach. It's behavior that will either strengthen an organization's security posture or result in a breach. Focus on behavior and not simply on providing information and policy.

SEVEN CRITICAL COMPONENTS THAT AN SAT VENDOR SHOULD PROVIDE

When evaluating SAT vendors, ensure they provide the following seven components. Doing so will help ensure a successful SAT program in the short term while setting up for future success by showing you what is possible moving forward.

#1 Varied and Engaging Content

Ensure any SAT provider supports mobile learning so users can digest content and complete exercises on the go.

Content is king. It's the informational component to any SAT program. It's also not a "one-size-fits-all" model. Users gravitate towards different styles of content that match individual learning preferences. Keep this in mind when evaluating SAT platforms. To change behavior and build a strong security culture within your organization, having an array of content that resonates with different groups of employees is critical. Look for a SAT platform that has a large library of continuously-updated, multilingual SAT content, including interactive modules, videos, games, posters, newsletters, assessments, etc.

Additionally, consider role-based or preference-based training. What you teach people in a call center will probably be different from someone in IT. Content must support these differences. Demographically, users will have different learning styles within your organization: some people will be better at absorbing three-five minute funny videos, yet an executive team may feel talked down to by this approach. The ability to have flexibility around your core training themes to ensure everyone gets the content they need is a critical consideration when evaluating SAT platforms.

Lastly, deploying training content to users is almost as important as the content itself. Ensure any SAT provider supports mobile learning so users can digest content and complete exercises on the go. Additionally, a user-friendly administrative interface that allows you to assign, track, measure and report training efforts is critical so you can draw meaningful and useful conclusions regarding increases/decreases of risk and pockets of the organization where more intervention is necessary. Also, look for flexible SAT platforms that will allow you to incorporate custom, third-party content.

#2 Localization

Localization is the crucial process of translating content in addition to providing examples, imagery and interactive elements that are region-specific to users. This is an in-depth process that goes well beyond simply translating content and is critical for organizations with a global footprint and with a multilingual employee base.

Partnering with an SAT vendor that allows your users to select the language/region they are located in - or the most comfortable with - is a crucial factor to ensure they are able to absorb and apply training material. Ensure the SAT vendor provides high quality localizations and uses local subject matter experts to ensure content and examples are relevant.

#3 Structure and Automation

SAT is not a "one-and-done" exercise. Building a security culture requires ongoing training and testing followed by reinforcement. Moreover, when you create an SAT program, remember that learning happens at three different stages, so it's critical to seek SAT platforms that have the content and tools necessary to target and deliver at each learning stage.

- **Formal Structured Learning (10%)** – this refers to things like classroom-based training, online learning deployed through a Learning Management System (LMS), training days, etc.
- **Informal Learning (20%)** – this means asking other team members for advice, collaborating, watching videos, or reading.
- **Experiential Learning (70%)** – this is mostly about day-to-day learning opportunities such as on-the-job, social interaction, when working within business workflows, or within corporate and departmental culture.

90% of a person's learning takes place outside formal structured settings.

As you can see, 90% of a person's learning takes place outside formal structured settings. Many SAT programs fail because they focus solely on this first 10%. Ensure that your SAT program addresses all three stages, and that any SAT platform you're evaluating has the tools to target all three stages of learning. A perfect example of this: putting a short password video on your organization's password change page, making it readily available at the moment of need.

Lastly, automation is also critical. Any SAT vendor should incorporate elements of automation within their program for easy user provisioning so training campaigns can be scheduled weeks in advance without direct action needed from program administrators. This automation should also improve ease of use and ROI by streamlining program management time and more effectively delivering content to the right users at the right time. Lastly, automation should also be leveraged to provide reactive/remedial-based events for "just-in-time training" and to provide scheduled reporting for management and executives.

#4 Testing

While training is the foundational cornerstone of any SAT program, testing users to see how they will respond to phishing simulations is how you will determine if you're changing security behavior and mitigating human risk. Will a user click on the email, report it or do nothing?

Additionally, users need a streamlined way to report phishing emails to help your organization build resilience. This reporting mechanism allows your IT team to learn more about potential attacks targeted at your organization as well as to alert everyone else.

While most SAT platforms provide various types of simulations and phishing templates, in addition to end-user tools that support phish reporting, the devil is in the details. Ensure you partner with an SAT vendor that stays ahead of the threat landscape, and as a result, provides phishing email templates based on real-world threats.

Also, if an employee fails a simulated phishing test, an SAT platform should provide "just-in-time" training to establish a learning moment around that specific incident while it's still fresh in the user's mind.

Just like content delivery and program development, phishing simulation programs will also benefit from automation and machine learning. A vendor's phishing simulation platform should leverage machine learning to recommend and deliver informed and personalized phishing templates based on a user's training and phishing history, and be able to recognize legitimate phishing emails and flip them into simulated tests.

#5 Metrics and Reporting

Measurement and reporting is another way to determine how effective your SAT program is at changing behavior and reducing human risk. It's also paramount for quantifying the success of your security awareness program to executives.

Knowing how well your program is performing against specific goals/targets and being able to clearly demonstrate improvement is critical to maintaining executive support. A good vendor will provide a robust reporting and analytics platform to allow your organization to measure what matters the most. This should also include executive reporting to allow SAT program managers to easily create reports specifically tailored for leadership.

Additionally, identify vendors that measure human risk and security culture metrics. Old-school SAT program metrics typically center around completion rates, quiz performance, engagement metrics, etc. It's critical to be able to measure the risk profile of individuals or departments so you can make data-driven decisions regarding adjustments to training. You should be able to evaluate how your organization's risk changes over time and truly measure the performance of your training program to understand where improvements need to be made to strengthen your organization's human firewall.

Additionally, users need a streamlined way to report phishing emails to help your organization build resilience. This reporting mechanism allows your IT team to learn more about potential attacks targeted at your organization as well as to alert everyone else.

While most SAT platforms provide various types of simulations and phishing templates, in addition to end-user tools that support phish reporting, the devil is in the details. Ensure you partner with an SAT vendor that stays ahead of the threat landscape, and as a result, provides phishing email templates based on real-world threats.

Also, if an employee fails a simulated phishing test, an SAT platform should provide "just-in-time" training to establish a learning moment around that specific incident while it's still fresh in the user's mind.

Just like content delivery and program development, phishing simulation programs will also benefit from automation and machine learning. A vendor's phishing simulation platform should leverage machine learning to recommend and deliver informed and personalized phishing templates based on a user's training and phishing history, and be able to recognize legitimate phishing emails and flip them into simulated tests.

#5 Metrics and Reporting

Measurement and reporting is another way to determine how effective your SAT program is at changing behavior and reducing human risk. It's also paramount for quantifying the success of your security awareness program to executives.

Knowing how well your program is performing against specific goals/targets and being able to clearly demonstrate improvement is critical to maintaining executive support. A good vendor will provide a robust reporting and analytics platform to allow your organization to measure what matters the most. This should also include executive reporting to allow SAT program managers to easily create reports specifically tailored for leadership.

Additionally, identify vendors that measure human risk and security culture metrics. Old-school SAT program metrics typically center around completion rates, quiz performance, engagement metrics, etc. It's critical to be able to measure the risk profile of individuals or departments so you can make data-driven decisions regarding adjustments to training. You should be able to evaluate how your organization's risk changes over time and truly measure the performance of your training program to understand where improvements need to be made to strengthen your organization's human firewall.

#6 Surveys and Assessments

The presence of formalized and continual security awareness training can seem out of place for employees, as they may perceive cybersecurity to be IT's job. Therefore, it's important to understand the attitudes within your organization and how they are changing with the presence of SAT. This will help you highlight areas where you are performing well or you need to take remedial action. It also allows you to gauge progress in terms of security culture and is different from the previously mentioned metrics because you're analyzing preference, opinion and frame of mind.

Surveys and assessments should include measuring not only sentiment and attitudes, but also knowledge and proficiency. Any SAT platform should provide the ability to execute skill-based assessments and security culture surveys to allow you to measure the security knowledge and proficiency of your users and measure your organization's overall security culture posture. The goal is to identify users that are more proficient at knowing how to respond to a certain situation and what it means to do the right thing. Additionally, any platform should provide the ability to benchmark your organization against peers within your industry, and standardize assessments with scientific validity to accurately measure what progress your organization has made.

This should also include the ability to measure employees' human risk score. Addressing human risk management is the ultimate goal. Once you understand the risk profile of an individual or department, you can adjust training and gain valuable insight about where to improve your security program, thereby bolstering your organization's security posture.

#7 Beyond SAT

The vendor landscape for SAT vendors has seen a fundamental shift in recent years. Leading vendors have moved from providing offerings focused solely on training users to platforms that now tackle more comprehensive issues such as building a security culture within an organization and addressing human risk management.

It's critical to partner with an SAT vendor that not only achieves your immediate goals, but that can also show you what is possible moving forward. Keep these key points in mind when evaluating an SAT vendor:

- **Focus on awareness, behavior and security culture**
  Ultimately, reducing human risk should be your goal. You want to partner with vendors that offer human risk quantification and risk calculation based on user behavior, according to Forrester Research.* SAT then becomes the cornerstone for shaping your security culture.

- **Does the vendor provide a suite of offerings that will allow your organization to move beyond SAT?**
  As previously mentioned, SAT is the foundational cornerstone for building a security culture within an organization, however it's not necessarily the only component. Other components, such as human detection and response, SOAR platforms, incident response and threat intelligence, are other key components which could be added to your security culture roadmap in the future. Ensure you're partnering with a vendor that fulfills your current needs in addition to your future ones.

Ultimately, these capabilities lay the foundation for ensuring your organization's SAT program changes user behavior and allows your business to truly understand, reduce and monitor cyber risk. SAT will serve as a platform for developing a broader understanding of security culture and human risk management, and turn users into your organization's human firewall.

* The Forrester Wave: Security Awareness And Training Solutions, Q1 2022

#6 Surveys and Assessments

The presence of formalized and continual security awareness training can seem out of place for employees, as they may perceive cybersecurity to be IT's job. Therefore, it's important to understand the attitudes within your organization and how they are changing with the presence of SAT. This will help you highlight areas where you are performing well or you need to take remedial action. It also allows you to gauge progress in terms of security culture and is different from the previously mentioned metrics because you're analyzing preference, opinion and frame of mind.

Surveys and assessments should include measuring not only sentiment and attitudes, but also knowledge and proficiency. Any SAT platform should provide the ability to execute skill-based assessments and security culture surveys to allow you to measure the security knowledge and proficiency of your users and measure your organization's overall security culture posture. The goal is to identify users that are more proficient at knowing how to respond to a certain situation and what it means to do the right thing. Additionally, any platform should provide the ability to benchmark your organization against peers within your industry, and standardize assessments with scientific validity to accurately measure what progress your organization has made.

This should also include the ability to measure employees' human risk score. Addressing human risk management is the ultimate goal. Once you understand the risk profile of an individual or department, you can adjust training and gain valuable insight about where to improve your security program, thereby bolstering your organization's security posture.

#7 Beyond SAT

The vendor landscape for SAT vendors has seen a fundamental shift in recent years. Leading vendors have moved from providing offerings focused solely on training users to platforms that now tackle more comprehensive issues such as building a security culture within an organization and addressing human risk management.

It's critical to partner with an SAT vendor that not only achieves your immediate goals, but that can also show you what is possible moving forward. Keep these key points in mind when evaluating an SAT vendor:

- **Focus on awareness, behavior and security culture**
  Ultimately, reducing human risk should be your goal. You want to partner with vendors that offer human risk quantification and risk calculation based on user behavior, according to Forrester Research.* SAT then becomes the cornerstone for shaping your security culture.

- **Does the vendor provide a suite of offerings that will allow your organization to move beyond SAT?**
  As previously mentioned, SAT is the foundational cornerstone for building a security culture within an organization, however it's not necessarily the only component. Other components, such as human detection and response, SOAR platforms, incident response and threat intelligence, are other key components which could be added to your security culture roadmap in the future. Ensure you're partnering with a vendor that fulfills your current needs in addition to your future ones.

Ultimately, these capabilities lay the foundation for ensuring your organization's SAT program changes user behavior and allows your business to truly understand, reduce and monitor cyber risk. SAT will serve as a platform for developing a broader understanding of security culture and human risk management, and turn users into your organization's human firewall.

* The Forrester Wave: Security Awareness And Training Solutions, Q1 2022