KnowBe4

The CISO Guide to Security Awareness Training

Cybersecurity threats loom large, making robust security awareness training (SAT) programs a necessity for organizations. To navigate this complex terrain effectively, a structured approach is paramount. In this article, we unveil the nine indispensable steps crucial for crafting a comprehensive and effective SAT program. From initial assessment to content development and reporting, here are nine best practices for building an SAT program that builds a strong security culture.

#1 What Is Your Starting Point?

Most organizations will find themselves in one of the following positions:

- You have an established program, but it is not effective
- A security awareness program does not currently exist

If you are currently using a provider, reevaluate and understand the quality of awareness training they're providing. Not all SAT providers are created equal; each will have a different approach to content, reporting, administrative functionality, automation/AI, etc. Ensure your provider is providing you with all the critical elements required for a successful SAT program.

Also consider who is leading your SAT program. Often, it's a security practitioner or IT admin that has it assigned to them. Ensure the person understands organizational development, has a background in training and knowledge of how to drive behavior. Look for candidates who have strong project management and communication skills and can lead up and across an organization.

#2 What Are You Trying To Accomplish?

In order to build a strong security awareness program, first determine your objective. Security awareness programs are anchored on having employees act in vigilant and secure ways in order to protect the organization. It may seem simple, but if you do not know what outcomes you want to drive, you will not know how to measure and represent your results.

#3 Who Are Your Advocates?

Capturing C-level support is paramount in both driving a more secure culture and ensuring that everyone within the organization understands their role and responsibility in creating the desired state. Executives are notoriously overlooked in the training ecosystem. The thinking is, because of their elevated role, they must have been trained. Wrong. They need the training as much as you need their support. In order to capture attention at the top, you will need to leverage partners across the organization, be highly persuasive and enact a level of diplomacy that gets to the point without becoming your own blockade.

#4 Engaging Content

It is no secret that people learn differently. Content needs to be provided in different versions and varieties that match your diverse learning population styles. There are many content providers in this space, but few bring the necessary content elements that make for good programs. Identify providers that have large libraries of security awareness training content; including interactive modules, videos, games, posters and newsletters.

Also look for a provider that offers a user-friendly administrative interface that allows you to assign, track and measure training efforts. It is imperative that you are able to use the dashboard data to draw meaningful and useful conclusions to what you are seeing regarding increase/decrease of risk and pockets of the organization where intervention is necessary.

#5 To Phish Or Not To Phish

Simulated phishing attacks should be delivered to every employee at least once a month. For those individuals who have escalated risk associated with their role, the number of simulated attacks should be increased to two or three. There needs to be a good cadence for the appropriate conditioning to take place and for behavior change to take hold. It is good practice and potentially a corporate policy, to notify the organization that you are conducting ongoing simulated attacks coupled with the accompanying rationale.

Simulated phishing tests should not be viewed or implemented as a “got ya” exercise. Explain that this is a company-wide initiative to help teach and strengthen their ability to spot and report an attack.

#6 Communication Is Key

When managing an SAT program, it’s critical to operate like a cyber attacker, but to think like a marketer. Look for ways to partner with other departments to give your messaging another outlet to get to employees. People receive information differently, so try to leverage as many communication styles and mediums as possible. Leverage digital banners, internal social media channels and team meetings as continuous means of driving messaging. Partner with your corporate communications or marketing teams (if available) to brainstorm ways to make your messages memorable and connect to the overall corporate messaging agenda.

#7 Build An Army

Champion programs are a great way to have advocates spread across the organization in every department, region and country who can further translate and embed the security message within your organization.

They don’t need to be security experts, but they should be influencers in their areas. Provide champions with the messaging content and give them the liberty to translate and communicate that content in ways that are most effective for their audience.

The recommendation is for champions to spend no more than two years in the role so that you can circulate fresh thinking continuously and provide others with the opportunity. Lastly, consider incorporating their participation into a formal performance review and or some other type of recognition.

#8 Rewards and Consequences

Rewarding secure behavior and upholding consequences for insecure behavior is relatively new thinking. Companies are evaluating whether using rewards like certificates, shout-outs on team calls, increments of time off, gift cards or swag can help to reinforce secure behavior in those demonstrating it while enticing others to jump on board.

On the other hand, companies are also looking at how consequences play a role in enforcing more secure behaviors. Companies are evaluating scaling back access to company systems or social platforms, incorporating into performance reviews and one-two-three strike policies. If you decide to test these approaches, clear and concise company-wide communication is key.

#9 Measure and Report

Quantifying the success of your security awareness program is paramount. When determining what metrics to focus on, select a few meaningful ones that can be quantified frequently in order to show the progress over time. It is important to understand the organization's top security concerns and then anchor your measurements to those concerns.

Although training completion rates and ongoing phishing click rates are important measurements to track, consider evaluating vulnerability instances and assessments or password resets as additional options. Being able to show the cost/risk of doing nothing is also important. The compelling piece of the narrative is that the organization is becoming more secure as a result of the efforts.

LEARN MORE **Contact us To Learn More About How Security Awareness Training Can Strengthen Your Security Culture**