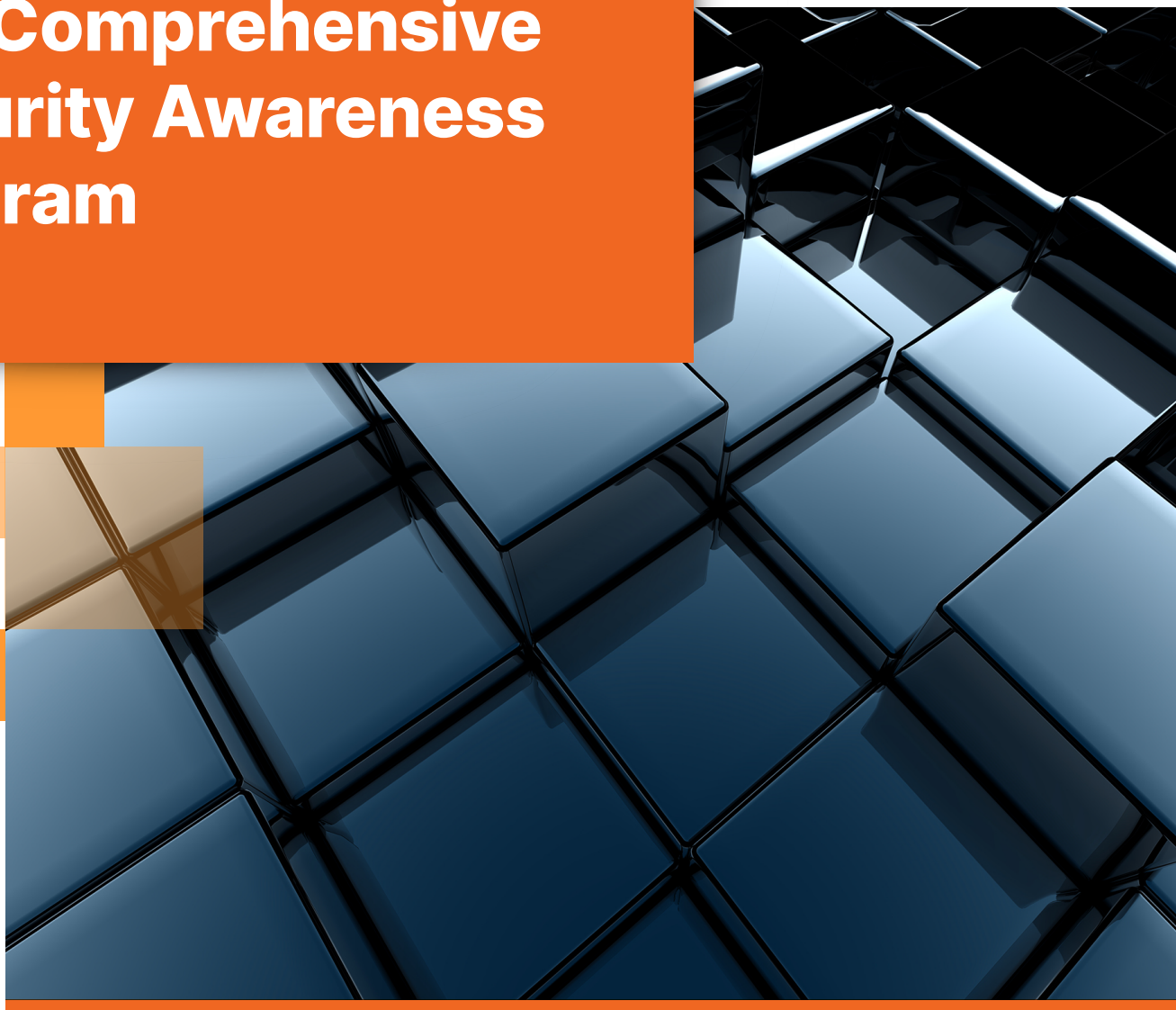
KnowBe4

Building an Effective and Comprehensive Security Awareness Program

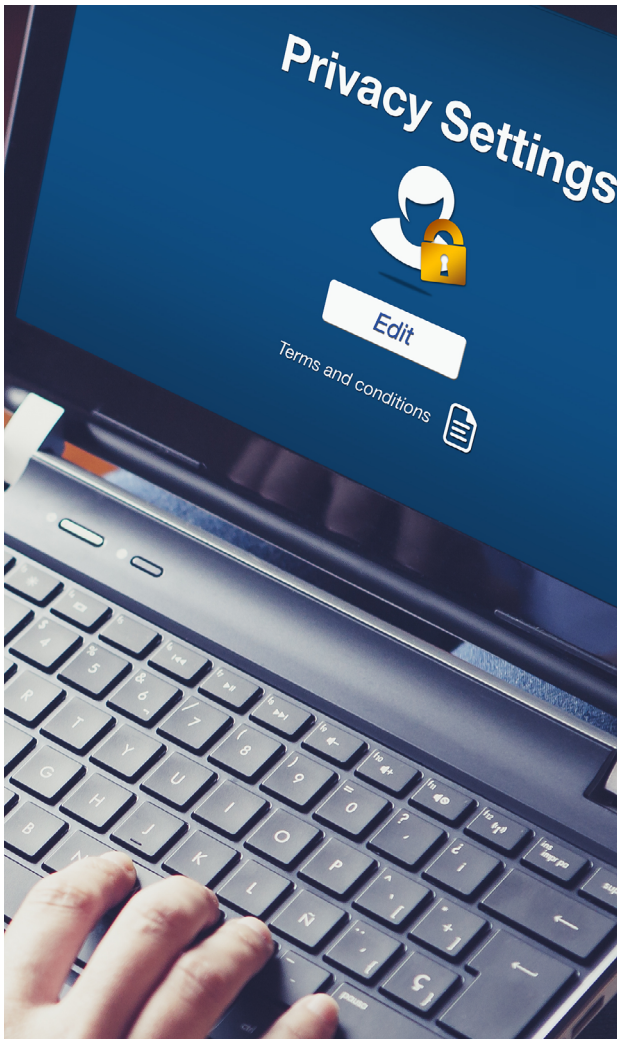


by Joanna Huisman

INTRODUCTION

Building an effective and comprehensive security awareness program seems like a daunting task to those who are fortunate enough to be in the line of fire...I mean responsible for it. There is a lot of information at your fingertips, but how do you turn that information into something useful? Like most security awareness professionals, understanding a program's critical components and connecting them together to design something comprehensive, continuous and engaging is an overwhelming task. It is a task we are taking on head-first in this white paper in order to provide you with a strong blueprint to get started.

What Is Your Starting Point?



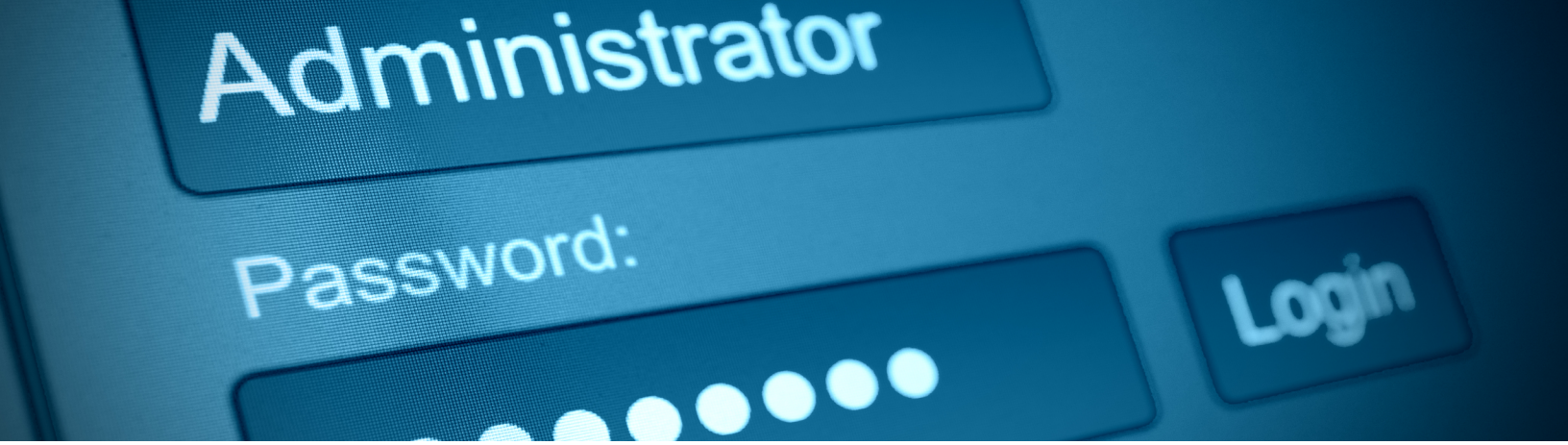
Let's first take a look at your organization's current efforts. You may find yourself in one of the following two positions:

- You have an established program, but it is not effective (you are not alone)
- A security awareness program does not currently exist (again, still not alone)

To start, let's determine where your program originates. Many organizations use internal corporate training teams to create program content. Security content is starkly different than other corporate or compliance content. There is a level of security expertise required to understand the critical elements that need to be included in a program and then how to marry those different elements into digestible bites creating one long, never-ending meal. You see, whereas some training has a beginning and an end, security awareness training is continuous; there is no end. It is worth evaluating the internally-created content against that of industry providers to see how they measure up.

If you are currently using a provider, it is time to look behind the curtain to better understand what you are paying for. All providers are not created equal. They will be different in approach, content, administrative functionality, reporting, etc... It is worth pausing to ensure that you are partnered with a provider that not only delivers the best, most comprehensive approach, but also helps you measure the outcomes of that program. The contents of this white paper will provide you with some comparative elements to get started.

It is also important to consider who is leading your security awareness team/program. What we find is that these programs are commonly led by security practitioners who drew the shortest straw or someone in security who had extra time to deal with this "training stuff". You are looking for individuals who understand organizational development, have 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.



What Are You Trying to Do?

In order to build a strong security awareness program, you first need to 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.

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.

What language is likely to seize their attention and get them to act with both resources and funding? It is not doom and gloom. It is language that connects the security awareness program to the success of core business initiatives. Many C-levels fall into the "technology will solve the world's problem" trap and throw all of the investment dollars there. Technology, although helpful and necessary in the fight against cyber crime, just is not enough. The human element is far more critical. Cyber criminals cleverly evade an organization's security controls, preying on the uneducated, distracted and naïve, knowing that where there are humans, there is also human error.

C-level attention is continuously fought for within an organization, leaving them to sift through what programs are most closely aligned to the core business and that will drive the most beneficial outcomes. A successful security awareness program will enable other parts of the overall business to prosper; and should be communicated that way. Additionally, the C-level's ability to act as an evangelist and lead advocate for the program will yield lasting benefits in adoption and engagement across the business.

The C-level must drive the organization's security culture; this is a need-to-have asset in the security toolbox. By assessing employees' security awareness, behaviors and culture, organizations can adapt their policies and training programs to the constantly-changing threat landscape. The alternative becomes less attractive by the hour: do nothing and see your organization crumble to a halt by ransomware, data theft or business interruption.

Still need help in painting the picture? KnowBe4's (Phishing by Industry Benchmark Report) provides conclusive data that helps show your industry risk when an organization takes action and does not take action. You will most likely be asked how your organization compares to the industry data... and that is your entry point.

Engaging Content

It is no secret that people learn differently, therefore, cookie cutter content just will not do. Content needs to be provided in different versions and varieties that match your diverse learning population styles. This is where you may dip your first toe into the "provider pool." There are many providers in this space, but few bring the necessary content elements that make for good programs.

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 use the dashboard data to draw meaning and useful conclusions to what you are seeing regarding increase/decrease of risk and pockets of the organization where more intervention is necessary.

Security awareness training has a reputation for being limited, boring and hard to understand. That is not the case anymore; awareness content has come a long way. Look for providers that have large libraries of computer-based security awareness training content; including interactive modules, videos, games, posters and newsletters. If you are looking for something really unique, take a look at KnowBe4's award-winning, Netflix-like series "The Inside Man". Three seasons in and customer reviews say it is binge-worthy content with relatable characters/scenarios and a gripping storyline. At the end of the day, buying engaging content for only one learning style will drive disinterest. Your ability to partner with a provider that allows your audience to connect with the content will help keep them engaged and increase content consumption.

To Phish or Not to Phish

Simulated phishing is not a trip out to the pond with a pole and some worms. It is a way to use simulated attacks to test your audience's ability to detect, report and prevent a cyber attack. A majority of successful data breaches started with a spear phishing attack, while phishing remains a top threat action used by cyber criminals. Emails, phone calls, SMS and other outreach methods are specifically designed to entice your employees to take actions which will allow criminals access to company data and funds.

Simulated phishing attacks should be delivered to every employee at least once a month...there is no end. 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. If employees believe that this is a punitive exercise to catch them doing something wrong, then they may be hesitant to open any emails, which could affect their overall work. Explain that this is a company-wide initiative to help teach and strengthen their ability to spot and report an attack.

Advise that these are transferrable skills that they can share with their friends, family and loved ones so that they can be more cyber safe in their personal lives.

Security awareness leaders should also leverage lots of different kinds of templates in their attacks. If you are only using simple templates, then you are not increasing the employee muscle in detecting difficult attacks. Think of it this way...at any time, you are either building, strengthening, or allowing atrophy to occur. Also, use a variety of template types. Test your audience with templates that contain attachments, links, meeting invites, known/trusted senders or sources. Cyber attacks are ever changing and evolving, so you need to continually change and adjust your template strategy, or better yet, use a platform like KnowBe4's that evolves with new attack models.

Communicate, Communicate, Communicate

When you are looking to evangelize across a broad, diverse population of people, you need to operate like an attacker, but think like a marketer. In addition to your communications that inform and reinforce the right secure behaviors, 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.

Be creative and continuous with your approach. You are looking for messaging that is sticky and memorable. Spend time determining what the right message approach looks and sounds like from a short-term and long-term perspective. Think of how you want people to feel, react and act as a result. 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.

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. By building a group of champions, you are ensuring that there will be a constant stream and reinforcement of security messaging moving through the organization. Consider these champions to be local extensions, culture carriers, of your overall program that act as evangelists.

Champions do not need to be security experts, but they should be influencers in their areas, having the ability to engage their peers in ways that are relevant and meaningful. Essentially, you are providing champions with the messaging content and giving them the liberty to translate and communicate that content in ways that are most effective for their audience. By localizing this messaging through champions, you now have a tremendous reach within the organization that you may not otherwise have had.

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. Consider having an application process coupled with an interview and manager recommendation. You are looking for people who know how to be heard and drive change. Champions are an integral part of driving the culture and sharing feedback on what is and is not working. Also, consider incorporating their participation into a formal performance review and or some other type of recognition. The champion role will become something coveted and will help you indoctrinate a continuous flow of new advocates.

Rewards and Consequences

Rewarding secure behavior and upholding consequences for unsecure behavior is relatively new thinking in the area of security awareness. 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. Human nature dictates that people like to be recognized in front of their peers, and that different types of recognition drive different people. Having a way to call attention to favorable behaviors may initiate this human desire to be appreciated and motivate employees to act in a more secure manner.

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, they must be communicated and equal. In other words, you should communicate to the entire organization what the rewards and consequences are and how they will be recognized and reinforced. Additionally, if you have an executive who gets three strikes, they should be dealt the same consequences anyone else in the organization would receive. Your approach should also be balanced, having both rewards and consequences in the equation.

How Is It Going?

Quantifying the success of your security awareness program is paramount. You should rely on metrics that reinforce the secure behaviors that are necessary in protecting company data, systems, finances and people. When determining what metrics to focus on, do not boil the ocean. Select a few meaningful ones that can be quantified frequently in order to show the progress over periods of 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 organization could suffer brand damage, revenue loss or reputational consequences that they cannot recover from. Also, executives are being held professionally accountable for breaches, losing their jobs and the ability to find future employment.

When reporting results, do not helicopter-up a data dump of information for executives to interpret. Tell the story with minimal numbers and charts. The compelling piece of the narrative is that the organization is becoming more secure as a result of the efforts. Show that in simple visuals using powerful, connecting and memorable words. The viewer should be able to understand and recommunicate the critical factors of the findings. Resist the urge to overcomplicate.

A FEW KEY TAKEAWAYS

- An effective security awareness training program should be both comprehensive and continuous… there is no end.
- Leverage engaging/interesting content, simulated attacks and insightful communications.
- Build a force of champions, advocates and executive support.
- Select a few critical metrics.
- Control the narrative.

Additional Resources

Free Phishing Security Test
Find out what percentage of your employees are Phish-prone with your free Phishing Security Test

Free Automated Security Awareness Program
Create a customized Security Awareness Program for your organization

Free Phish Alert Button
Your employees now have a safe way to report phishing attacks with one click

Free Email Exposure Check
Find out which of your users emails are exposed before the bad guys do

Free Domain Spoof Test
Find out if hackers can spoof an email address of your own domain

About KnowBe4

KnowBe4 is the world's largest integrated security awareness training and simulated phishing platform. Realizing that the human element of security was being seriously neglected, KnowBe4 was created to help organizations manage the ongoing problem of social engineering through a comprehensive new-school awareness training approach.

This method integrates baseline testing using real-world mock attacks, engaging interactive training, continuous assessment through simulated phishing, and vishing attacks and enterprise-strength reporting, to build a more resilient organization with security top of mind.

Tens of thousands of organizations worldwide use KnowBe4's platform across all industries, including highly regulated fields such as finance, healthcare, energy, government and insurance to mobilize their end users as a last line of defense and enable them to make smarter security decisions.

For more information, please visit www.KnowBe4.com

KnowBe4

KnowBe4, Inc. | 33 N Garden Ave, Suite 1200, Clearwater, FL 33755
Tel: 855-KNOWBE4 (566-9234) | www.KnowBe4.com | Email: Sales@KnowBe4.com

V041421