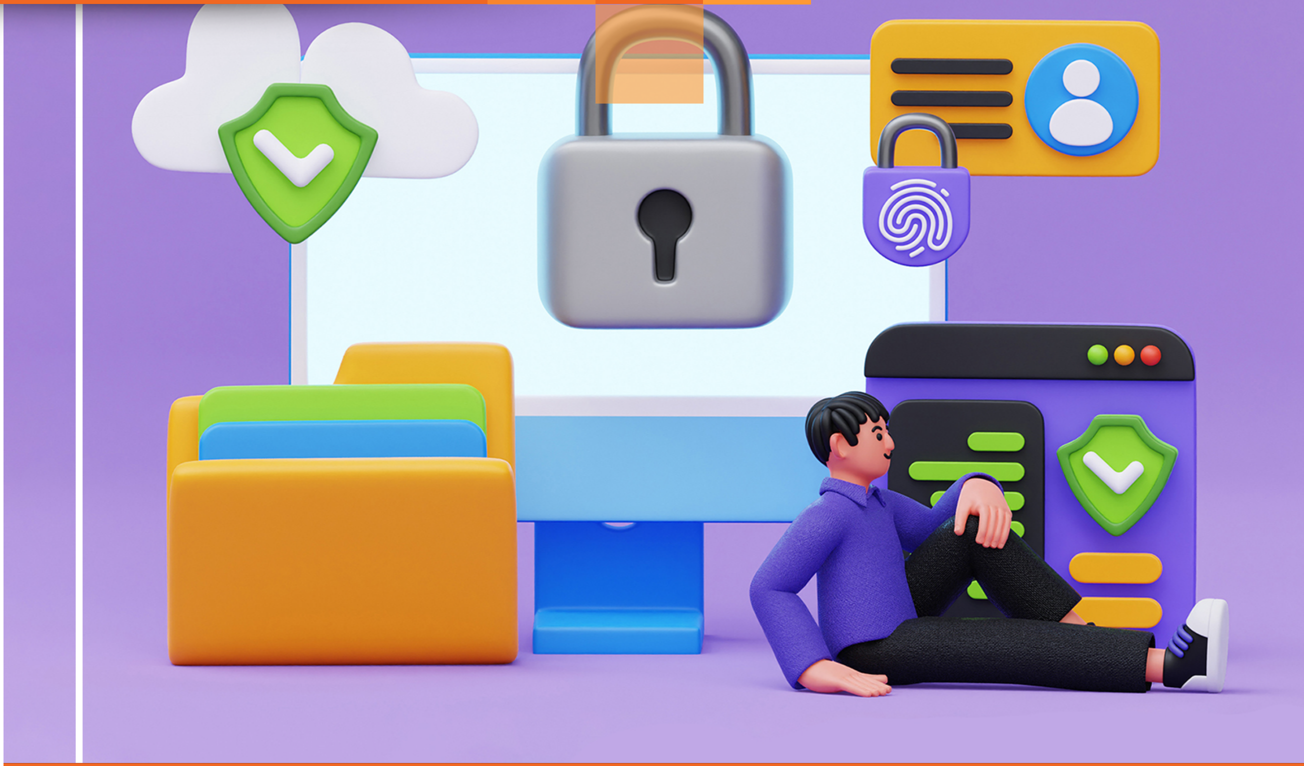
KnowBe4
Human error. Conquered.

Better Together: Security Awareness and Compliance Training



4 Strategies for Delivering a Cohesive Training Experience

Better Together: Security Awareness and Compliance Training

4 Strategies for Delivering a Cohesive Training Experience

Table of Contents

INTRODUCTION

In the drive to build a security culture, there are two components of a program that work hand in hand as the perfect combination: security awareness and compliance training.

These two elements, when combined in a comprehensive and continuous manner, improve the human defense layer to a higher state of readiness able to help organizations better secure employees' professional and personal digital, as well as physical, environments. Having a comprehensive approach to both security and compliance training can significantly lower the risks associated with fines, reputational damage, loss of customers and other results of noncompliance.

There is a strong overlap between security awareness and compliance training content. Learning needs to be packaged in a way where consumption of it translates to increased knowledge, not just noise. For example, conventional compliance topics that fall under the umbrella of Data Privacy or Data Protection fit well into a customary security awareness training program. While content topics like Diversity, Equity and Inclusion and Workplace Safety fit well under the broader scope of learning how to deal with and avoid challenging situations.

The same principles applied to a new-school security awareness training program should be applied to a compliance training program:

- Architect a plan that drives a more security and compliance aware culture by assessing employee behaviors and creating goals and objectives that connect with overall corporate objectives
- Deploy a diverse pool of content coupled with a simulated phishing program running phishing email tests, increasing the frequency by which you teach/test while decreasing the time spent in training
- Use a variety of communication tools to keep security front of mind and train more frequently with smaller, more concise pieces of training content
- Measure along the way (i.e. quizzes, survey results and informal touch bases)

In this whitepaper we'll explore some typical challenges to combining security awareness training and compliance training and take a closer look at each of the principles outlined above.

TO COMBINE OR NOT TO COMBINE? WE'VE GOT THE ANSWER

Combining security awareness and compliance training is not new, although most organizations still consider the two as separate entities. And even those organizations that have adopted a more unified approach still struggle to make sense and show necessary links between the two in ways that effectively keep employees engaged and interested.

Security awareness training is traditionally owned and run by the security team, while compliance training is often handled by the human resources department, further creating a divide in program, process and style. But, regardless of where the responsibility sits, there is a strong and natural connection between the two that needs to be optimized.

> *Traditional, old-school compliance training has been anything but effective. Generally offered through long, boring, complex modules, this approach is hard for individuals to connect with, difficult to retain and leads to pitfalls of noncompliance.*

Traditional, old-school compliance training has been anything but effective. Generally offered through long, boring, complex modules, this approach is hard for individuals to connect with, difficult to retain and leads to pitfalls of noncompliance. Employees find themselves multitasking through the courses, only paying enough attention to know when to advance to the next slide or take the next action. Generally, if they get 80% on the test, they pass and move on without learning much of anything. This once per year event comes with a big disruption to the business and not much to show for it. Wasted time and investment on the part of the organization, coupled with this false sense of security that behaviors will change based on learning that never occurred.

In the overall cost of doing business, compliance training is critical in giving your employees training they need to ensure that your organization complies with industry-specific laws and regulations. The importance of this content should not be taken lightly. Not having the most current, robust and engaging content could put your organization in a vulnerable position causing brand, reputational and even revenue damage that would be challenging to rebound from.

> *Creating a cohesive security awareness and compliance training program that is fluid in content, and the connection/progression of it, will provide your employees a more logical and organic approach to learning.*

Compliance content is also not one size fits all. While some of the modules will be required for all employees, some will be targeted for specific roles. Working with a provider that has both general compliance and role-based content will ensure you are meeting the needs and requirements at all corners of the business.

Compliance training on its own may feel like a misplaced puzzle piece: it doesn't make sense and it's hard to understand the overall fit because organizations treat it as one-off learning, which is less than optimal.

Creating a cohesive security awareness and compliance training program that is fluid in content, and the connection/progression of it, will provide your employees a more logical and organic approach to learning. Offering a program that encourages more frequent and smaller chunks of learning avoids disruption and provides employees more reminders and encouragement to comply and complete the assigned modules.

From the training manager perspective, deploying and maintaining two sets of training can feel like too many jobs for too few. When compliance and security awareness training are kept separate, those responsible for administering it often face twice the work across two (or more) different training platforms. Combining these efforts into a single platform or learning management system (LMS) puts all content and analytics in one place so training managers can get a more complete picture of training progress and results. This also makes it easier and faster to share training results with your leadership team since all training data is located in one place.

4 STRATEGIES FOR DEVELOPING A COHESIVE SECURITY AWARENESS AND COMPLIANCE TRAINING PROGRAM

So how do you get there and what are the best practices to accomplish this? Here are four strategies for building a comprehensive training program.

➔ Strategy #1: **Architect a plan that drives a more security and compliance aware culture by assessing employee behaviors and creating goals and objectives that connect with overall corporate objectives**

The most common items missing from any plan are solid goals and objectives. A good starting point is to determine the desired result you want and then outline the steps that will help you get there.

Not defining goals and objectives on the front end will only result in confusion and missteps along the way and ultimately not meeting the desired outcome.

When considering a set of goals and objectives to build a security awareness and compliance program, think of the general security/compliance knowledge required by all employees coupled with the specialized training required by only a segment of the employee population. Defining this at the beginning will ensure the right learning is assigned to the correct employee.

When considering a set of goals and objectives to build a security awareness and compliance program, think of the general security/compliance knowledge required by all employees coupled with the specialized training required by only a segment of the employee population.

For example, a legal department might be required to take the complete set of employment law training courses, whereas employees outside of legal might only be required to take the introductory course. Again, this is not a content dump. Remember that increasing the frequency by which you train employees while decreasing the time they spend in training is the optimal approach. Where there are requirements or best practices for a certain amount of time spent for a given subject, such as one hour per year, consider breaking this up into 15 minutes per quarter. The employees are more likely to retain this information if more frequently reminded and it will actually go smoother to train in smaller chunks.

Don’t forget to align the goals and objectives of your program to corporate objectives. If the executive team does not see how the program will help drive the overall business, they may reduce or limit the investment and support the program receives. So, whether your eye is on complying with regulatory requirements or driving more secure behaviors, this connection allows for maximum buy-in.

➔ Strategy #2: **Deploy a diverse pool of content coupled with a simulated phishing program to increase the frequency by which you teach/test while decreasing the time spent**

Content is king. Working with a provider that offers a variety of content styles and versions will help increase engagement of your audience.

Think of it this way; if you are looking to train your employees on creating strong passwords, you need to think about how your learners actually learn and absorb information. Their overall preference in learning plays a big role in their continued participation and interest. For example, IT might prefer content delivered through games, while the sales team likes short videos.

No matter the format, your training content should include clear "what's in it for me" moments for your employees.

No matter the format, your training content should include clear "what's in it for me" moments for your employees. If I like and can relate to the content, there is a higher likelihood that I will engage and stay engaged throughout the course and/or program. Additionally, making the lessons more relevant and real for your employees will increase the likelihood they'll use this knowledge both at work and at home.

Also, by threading a program with both security awareness and compliance content, you will deliver variety. Connecting the content through a single program not only allows for there to be a more fluid transition but also eliminates the divide in the two program components that were once visible to the learner.

This same thinking holds true for simulated phishing testing, which can be considered another category of content in your program. Increasing the frequency is critical in having enough comparative instances to understand how vulnerable your humans are and kind of training you need to include in your program. This is about building healthy habits and muscle memory. Conducting bi-annual or quarterly phishing tests only does not work. The recommendation is at a minimal monthly, and more than once a month for high-target employee groups.

Also, using the same, simple templates will decrease your overall click rate, but provides a false sense of security because cybercriminals use a variety of attack strategies to infiltrate your digital environments. Your program needs to include templates of all difficulty levels, and topical areas including security awareness and compliance. Your best defense is continuous content and testing.

➔ Strategy #3: Use a variety of communication tools to keep security and compliance front of mind

Start connecting security awareness and compliance training as a unified program. Thinking like an attacker and acting like a marketer is an important part in how you prepare your audience for the criminal behavior that is lurking around every corner, as well as the pitfalls of non-compliance that can occur.

Leverage every opportunity and medium, partner with other departments across the organization, and use unique marketing tactics to get employees engaged and keep them engaged. Effective internal communications help employees better understand why the organization is focused on this combination of training and why it is essential to them both professionally and personally.

By taking a fun and creative approach to security awareness and compliance training, your employees will be caught off guard. For example, embedding a message from the CEO in front of a training module explaining why this is important to the employee is unexpected and if they see the CEO is on board, they will be more likely to be too.

> *Continuous evaluation during the program is an essential part in determining if learning is occurring and your human defense layer is strengthening.*

Adopting the right approach is the difference between your audience dreading their required participation and looking forward to it, or at the very least understanding the value or it.

➔ Strategy #4: Measure along the way

Measurement is important before, during and after training occurs. As you build your plan and consider the outcome you are driving toward, an assessment on the front end provides you with information on your organization's security awareness and compliance strengths and weaknesses so you can develop a targeted campaign. Having this benchmark is critical to understanding and tracking progress, while also showcasing gaps in learning that need to be addressed.

Additionally, executing a few closely timed simulated phishing tests are necessary to understand your true starting click rate, that is, how susceptible your employees are to clicking on something malicious. You can determine the higher risk groups and adjust your frequency accordingly, remembering the goal is a minimum once per month.

Continuous evaluation during the program is an essential part in determining if learning is occurring and your human defense layer is strengthening. Adjustments can be made to keep you on track to attaining the goals you set. You may find that a portion of your audience is at a higher level of readiness and can move through the content at a faster pace or be assigned more challenging courses. Or you may start to notice areas of your population that need more time spent in a particular part of the program, and you can assign them additional modules. Whichever the case, these continuous checkpoints provide you the opportunity to pause and evaluate, reflect and adjust.

Completion percentage is one of the most common ways to measure the success of employee training, especially compliance content. For one, how many employees have completed required training is the main statistic auditors look for. Completion percentage should be one, but not the only, statistic you measure to track training success. This figure becomes more significant for optional training you deploy, as employees engaging with training on their own means you're doing something right. Our own experience and expertise supports frequent and varied training engagements to keep completion rates high.

It's easy to layer too many measurements in hopes of proving value. Keep it to a few that are meaningful and valuable and that meet the goals/objectives you set on the front end. Also ensure they are tied to the corporate goals. Last thing on measurement, when you are in the building phase, ensure that what you are measuring can be influenced by what you are training on. Your employees need to be able to drive the desired measurement and believe that they can help get to a favorable outcome.

CONCLUSION

The end result of your combined security awareness and compliance training program should help you optimize the valuable time you have with your employees and present a more cohesive learning experience for them. Keep your program focused and on track. Success comes by bringing the learning to the learner in a positive, relatable way versus dragging the learner to the learning through an inefficient experience. When learners are engaged and completing their training, your organization wins.

Additional Resources

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

Free Training Preview
See our full library of security awareness content; browse, search by title, category, language or content

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

About KnowBe4

KnowBe4 is the provider of 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 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
Human error. Conquered.

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

© 2023 KnowBe4, Inc. All rights reserved. Other product and company names mentioned herein may be trademarks and/or registered trademarks of their respective companies.