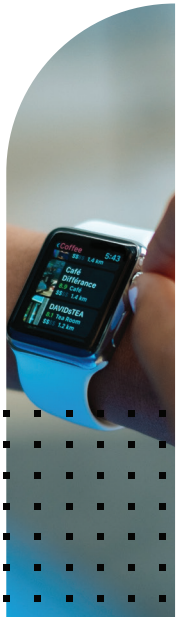
DEPLOYMENT GUIDE

Setting Goals and Planning Your Security Awareness and Training Program

A Guide for Building a Cyber Aware Workforce



There was a time when employees went about their daily tasks, oblivious to potential threats to their organization and to themselves. They trusted that their IT security team had data, networks, devices, and users protected. Fast forward, and today, employees have become high-value targets for cyber criminals. Educating employees about security risks is critical. One successful attack—driven by a single wrong click in an email—can reap millions of dollars for criminals, and cost an organization millions of dollars in loss of brand confidence, compliance fines, revenue, shareholder value, and the list goes on.

The human factor in cybersecurity can't be forgotten. Security is now everyone's business.

A security awareness and training solution needs to contribute to an overall security culture. Applying a "checkbox to compliance approach" to training does not foster a culture of awareness, nor is it responsive to the ever-changing threat landscape. It's important to make cybersecurity awareness an integrated and ongoing part of the organization's work culture. Awareness starts with the individual, and every employee has a responsibility to ensure the safety of an organization's information and assets.

But how do you engage your employees and build a culture of cyber awareness?

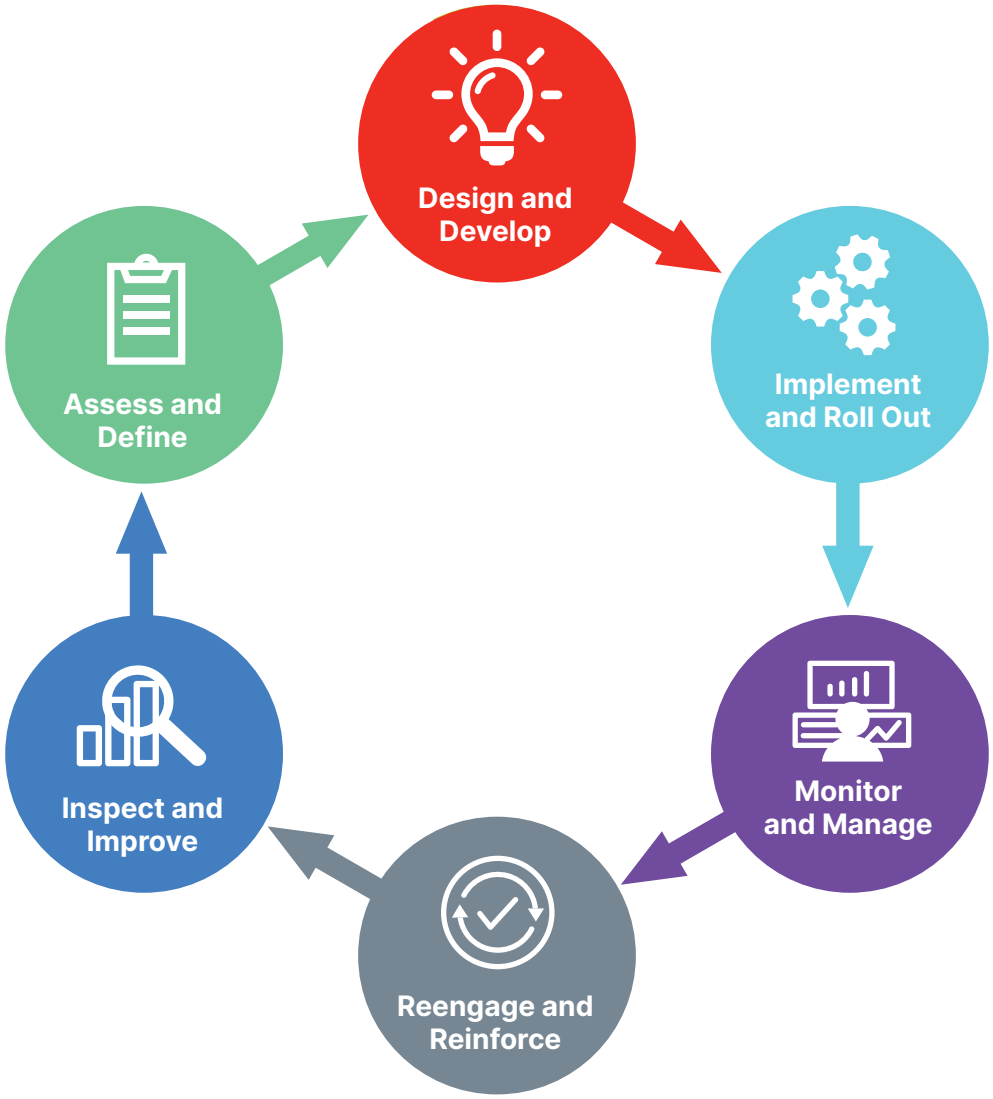


Figure 1: A Security Awareness and Training Program starts by assessing and defining needs.

Assess and Understand Your Baseline—Know Your Risks

Before you begin, it's crucial to establish a baseline of current security risks. Identifying the risks to your organization helps you develop your plan and allows you to evaluate whether your training program is making a difference in security habits over time.

A cybersecurity framework is a system of standards, guidelines, and best practices used to manage the risks that arise in the digital world. The framework typically matches security objectives and is used to develop the policies and procedures that define the best practices an organization follows to manage its cybersecurity risk.

Managers should ask, "What cybersecurity outcomes would be helpful in managing cybersecurity risk?" There are a number of frameworks, such as the World Economic Forum (WEF)–Cyber Resilience Principles and Tools for Boards and the National Institute of Standards and Technology (NIST)–Cybersecurity Framework (CSF), that you can refer to when developing a security framework aligned to your organization.

Employee Security Risks

It is a best practice to test employee security habits (or lack thereof) before you enroll them in training. Testing helps establish a baseline so that you know where the problem areas are and where to focus training and reinforcement efforts. There are a number of techniques and tools that you can deploy to understand the security habits of your employees.

1. Start by running some phishing simulation exercises. Record your results. Add follow-up training. Run your phishing simulation exercises again. What are the results now?
2. Monitor the access points and record any instances of tailgating (employees allowing people to enter access points without swiping an access badge). Record the results and retest in predetermined increments.
3. Perform an unannounced spot check on desks within your workplace. Look for locked devices, drawers, and confidential documents. Record the results and retest in predetermined increments.
4. Issue a survey asking key questions.

Secure Leadership Support and Define Your Goals

Your leadership team should be involved in establishing the mission and directive of your security awareness and training. Create a leadership task force with assigned roles and responsibilities, such as the identification of the goals and objectives for end-user training, management training, the adoption and incorporation of frameworks, and compliance mandates.

With executive sponsorship, identify the key reasons why your company wants to adopt enterprisewide security awareness and training. Start by identifying goals. Think about why you are implementing the training, and what you hope to achieve by training your employees. Typical goals are: to identify problem areas, to increase employee knowledge, to create change, and to reinforce expectations.

Ensure that your tasks and milestones have budget and funding approval.

Design and Develop Your Training Plan

Now that you have executive support and a clearly defined direction, you can begin to develop your training and awareness plan.

Here are some questions you may want your plan to address:

- What will the training cadence look like? How will you manage the onboarding process, yearly training, ongoing evaluation, and the training service as a whole?
- Do you need a phased rollout with an initial pilot test group? How will you capture user feedback?
- Do you need to target different groups at different times with different material?
- Which topics need to be addressed within your organization to create a program that meets your specific organizational needs? When picking topics, keep in mind the behaviors that you want integrated into the day-to-day activities of your employees.

- Does your organization need a communication plan that is centralized, distributed, or both? (Refer to NIST 800-50, section 3 for detailed guidelines.)
- How will you distribute all communication assets (posters, screenshots, or something else)?
- How will you test the success criteria?
- How will remediation actions be established and executed?

Roll Out—Get Everyone on Board

Now, you're ready to roll out your security awareness program and communicate it to employees. We recommend that you let your employees know ahead of time that you are enrolling them in security awareness training. We also recommend that you establish a deadline by when your employees must complete the training and send them reminders. Communicate the importance of training, your training plan, and your training schedule with your entire organization. Getting people on board is a key step to increasing security awareness.

Select the topics you want your team members to learn more about. You can choose topics based on your baseline testing, business requirements, or timely world events. Plan the timing of your training cadence. Establish when you will be distributing modules, assets, and resources to your team. To keep security top of mind, they should be distributed on a regular basis.

Monitor and Manage

Manage the progress of your security and awareness program by tracking employee progress. Who has taken the training? Who hasn't and why? Where are people performing poorly? Are you seeing some trends that can help you increase adoption?

In addition to monitoring the training progress of your employees, you will likely also want to evaluate if, and how, employee security behaviors improve over time. You can accomplish this by establishing a cycle of initial baseline testing, training, retesting, and remediation training for noncompliant employees.

As you review your program and uncover gaps, consider the following as you implement appropriate actions:

- Should you escalate gaps to management and should you take actions on stragglers?
- Should you be increasing or decreasing the frequency of training module distribution?
- What modifications should you make to the training campaign to meet the success criteria?

Reengage and Reinforce Learning

As you monitor your program, consider adjusting or adding new campaigns as needed. For example, if you are seeing the wrong behaviors or your organization is concerned about a current threat, consider deploying nanolearning or microtraining modules as remediation training or reinforcement of key teachings. Distribute tip sheets through email, or post them on your company intranet, to be featured at regular intervals.

You want to keep security visible throughout the year in order to help increase security awareness across your organization. Consider running campaigns connected to various themes, such as Black Friday, the Christmas holiday season, and so on.

Inspect and Improve

The key objective of any security awareness training program implementation is to increase awareness and positively alter user behavior, to reduce information security incidents.

The goal of a post-implementation plan is to strive for continuous improvement. Monitoring compliance, conducting formal evaluations, and collecting feedback are best practices that can be used to build continuous improvement within your organization.

NIST Special Publication 800-50 section 6.2 outlines tools and tactics for conducting formal evaluations and collecting feedback. These include:

- Design a feedback strategy
- Conduct surveys
- Create status reports
- Conduct interviews
- Make observations
- Implement focus groups
- Collect and compare metrics (comparison to baseline)

The publication also outlines several program success indicators for security awareness training. These include:

- The distribution of modules and awareness assets is supported.
- The executive team is on board with sending messages to staff about IT security.
- Metrics indicate a shrinking gap between existing awareness and identified needs, an increased percentage of users exposed to awareness materials, and so on.
- Managers are engaging in the process by enrolling in and completing their awareness training, and encouraging others to do the same.
- Security contributions are being recognized through awards, contests, and so on.
- Key players (managers, information security administrators, training coordinators, and others) appear to be motivated.

Use the success indicators to determine if the implementation of the program was successful. If you determine that it was not successful, use the indicators to determine where you can make improvements. Continuous improvement and measurable changes in behavior should always be the goals of any successful information security awareness and training program.

December 16, 2021 4:25 PM

1376805-0-0-EN