3 Questions to Ask When Developing an Adaptive Security Awareness Program
INTRODUCTION

Most people working in or near cybersecurity have felt the influence of the NIST Cybersecurity Framework (CSF), which provides organizations guidance for insuring they are protected from ongoing information security threats.

An intriguing element of the CSF—particularly for those in the awareness space—is the depiction of the various “tiers” at which an organization could meet the standards. At the top is the Tier 4: Adaptive program.

Per the CSF, a Tier 4: Adaptive program has three basic attributes. Such a program is:

• Based on lessons learned and predictive indicators
• Continuously improved via active adaptation to combat evolving threats
• Part of the overall organizational culture
Let’s take a look at how the NIST Cybersecurity Framework (CSF) defines Adaptive:
(Text taken directly from the CSF document)

**Tier 4: Adaptive**

**Risk Management Process** - The organization adapts its cybersecurity practices based on lessons learned and predictive indicators derived from previous and current cybersecurity activities. Through a process of continuous improvement incorporating advanced cybersecurity technologies and practices, the organization actively adapts to a changing cybersecurity landscape and responds to evolving and sophisticated threats in a timely manner.

**Integrated Risk Management Program** - There is an organization-wide approach to managing cybersecurity risk that uses risk-informed policies, processes, and procedures to address potential cybersecurity events. Cybersecurity risk management is part of the organizational culture and evolves from an awareness of previous activities, information shared by other sources, and continuous awareness of activities on their systems and networks.

**External Participation** - The organization manages risk and actively shares information with partners to ensure that accurate, current information is being distributed and consumed to improve cybersecurity before a cybersecurity event occurs.

Those who have tried to apply these principles to an ongoing cybersecurity education program know how difficult creating such a program can be. We’re talking about creating a highly flexible and visible program that is woven into the very culture of the organization. MediaPro has been in the business of helping organizations build awareness programs for over a decade, and we rarely see programs reaching this level of flexibility and sophistication.
We recognize that the challenges of creating such a program are many, but the rewards are well worth the effort (see “Five Benefits of Being Adaptive” later in this paper). Just as an adaptive approach to cybersecurity risk management is quickly becoming the preferred practice, we believe that an adaptive approach to security awareness should become the new standard.

We know that building a security-aware culture will require an awareness program that has three key attributes:

• Direct relevance to the organization and the different roles people play within it

• Ongoing reinforcement activities to motivate and sustain the behavior changes needed to keep your organization secure

• Tools for measuring what is working and what isn’t

The more sophisticated programs already have many of these components. But an adaptive awareness program has the added benefit of dynamic flexibility toward new risks, flexing the deployment of the education program to accommodate the changing risk environment. The result is an awareness program that does more than maintain a defensive posture: it is also builds customer trust, increases customer loyalty, and impacts profitability.

But how does an organization with a burgeoning security awareness program (or none at all) reach the top tier of a truly adaptive awareness program? In this white paper, we’ve provided three key questions any organization should ask as they seek to develop, implement, or mature an effective adaptive security awareness program.
QUESTION 1: How well do you understand your risks?

First things first: to create an awareness program that is aligned to your vulnerabilities, you’ll need to develop a clear understanding of your unique risks (as opposed to just assuming that your risks are the same as everyone else’s, thus creating a generic program). Many tools are available to understand risk, and many of them are technical in nature (that is, they help you understand technical vulnerabilities).

But the key to effective awareness programs, which address the impact your employees and their behavior have on cybersecurity, is to measure human-centered risks: those risks that are directly associated with the behavior of your employees. A comprehensive risk assessment, performed by your own team or by an external resource, will identify some of those human-centered risks, but such assessments can be costly and time consuming. That’s why many organizations use analytical measures like phishing simulation programs (to identify susceptibility to the pernicious risks associated with phishing), other social engineering simulations (including vishing, smishing, and USB drops), and knowledge assessments (to identify existing knowledge in the employee population). Using these alongside a technical risk assessment will go a long way toward more accurately understanding your risks.

A major addition we anticipate in the near future is the ability to integrate human-focused risk insights into the various technical tools you may already use. These include security information event management systems (SIEMs), data loss prevention software (DLPs), incident reporting, and especially user behavior analytics (UBA) tools. Traditionally, the focus of these tools has been to identify system vulnerabilities, or to detect and thwart external threats. However, we expect that these tools can and will evolve to provide us with real intelligence about the risks our employees pose to security, either through intentional or (more likely) unintentional actions.
The goal of understanding these risks, no matter what tools you use to understand them, is to generate an accurate depiction of your unique risks in order to create an awareness program that effectively addresses them. We recommend that such an effort end in a targeted list of 5 to 10 human-centered risks that can be addressed through education and communication. The more specific you can be in expressing those risks and the more action-oriented you can be in describing the behavior change you expect to see in your employees, the better off you'll be. With a set of defined risks and desired behaviors, you stand a great chance of accurately measuring your ability to improve your risk posture through an effective program of training and communication.

For example, say you conduct a knowledge assessment and find your employees' knowledge of password best practices is lacking. So you implement a simulated phishing campaign that sends official-looking emails asking employees to enter their passwords into a "Password Strength Tester" site. Now you know how many employees have fallen for the bait, and can tailor your awareness program to include anti-phishing and password best practices components. Six months later, you run a similar phishing simulator to see if your employees' behavior has changed for the better.

**RECOMMENDATION:** Develop a targeted list of between 5 and 10 human-centered risks that can be addressed through education and communication. Then, you can measure the effectiveness of training that addresses these risks.
QUESTION 2: What capacity do you have to deploy a program?

If you’ve got your risk-based battle plan, the next thing you’ll need to consider is your own capacity to deliver a program. Let’s use a climbing analogy: if you’ve identified the mountain that you want to climb, the next step is to ask yourself how prepared you are to climb it.

“ If you’ve identified the mountain that you want to climb, the next step is to ask yourself how prepared you are to climb it.”

Do you have the time set aside to train and then to climb the mountain? Have you identified the climbers you’ll summit with (and do they know what they’re doing)? Do you have the gear to make the climb? These are all important considerations that shouldn’t be taken lightly. (And if you’re going for Tier 4, remember: that’s like climbing Mt. Rainier in Washington State. It’s no walk in the park!)

In a similar way, you’ll want to consider the following when developing an awareness program: Do you have support and resources needed to deliver required online training? If so, do you have specific time limits or other constraints on the training? Do you have capacity and permission to deliver other content to all employees (things like videos, games, and posters)? Do you have the support of executives who will champion your message in their communications? Finally, do you have the personnel to help you carry out whatever program you design? You don’t want your ambition and enthusiasm to outstrip your organization’s capacity to support the program, so it’s best to be realistic.
Figuring out the answers to these questions—that is, your organizational capacity to deploy a program—is essential to laying out your plan of attack. Your capacity will determine whether you release only a single required training class, or you go all in with a sustained campaign of phishing simulations, animations, posters, games, etc. in a year-round effort to build a risk-aware culture. Remember, not every organization needs to get to Tier 4 right away; for some companies, just getting a basic program started would be a step in the right direction.

Question 3: How do you get the right content to the right people?

Even if you know your risks and you’ve got the capacity to deploy training, one of your great challenges will be to find training content that allows you to educate employees about your unique risks (ideally in a way that won’t bore them), and then to adapt that content to your environment and to risks that change over time. We believe that it’s the ability to be adaptive with content that will provide the biggest challenge to those trying to build a Tier 4 program.

If you’re working toward a higher-level program, you’re going to need a deep, diverse, and highly-flexible library of content that includes coverage of a variety of different risks and that corresponds directly to the needs of unique roles within the organization.

If you’re working toward a higher-level program, you’re going to need a deep, diverse, and highly-flexible library of content that includes coverage of a variety of different risks and that corresponds directly to the needs of unique roles within the organization. For example, you’ll want awareness training for those in finance that covers different ground than that directed at those in human resources. You’ll also need the ability to swap content in response to new or emerging risks, which will undoubtedly change over the course of the year. This is why static content doesn’t work; it doesn’t adapt to the current landscape.

RECOMMENDATION: Determine your capacity to deliver a program and create a “wish list” of program features. If you need third-party assistance, use the three questions in this white paper to guide your search.

"If you’re working toward a higher-level program, you’re going to need a deep, diverse, and highly-flexible library of content that includes coverage of a variety of different risks and that corresponds directly to the needs of unique roles within the organization."
Conclusion

In order to achieve a Tier 4 awareness program in line with the structure of NIST's Cybersecurity Framework, an organization needs to:

• Understand its unique set of risks
• Have the capacity to deliver the necessary training
• Have the flexibility to deliver the right training to the right people

Cyber threats will continue to evolve, and quickly. Despite employees' best efforts, the human factor continues to play a major role in breaches. Organizations and their employees must continually adapt to new and emerging threats, and the best way to do this is with a truly adaptive awareness program.

RECOMMENDATION: List the different types of role-based or customized content you'll need, and use this list to guide your search for an e-Learning firm.
5 BENEFITS OF BEING ADAPTIVE

Though striving for adaptability in security awareness is challenging, the value it brings is worth it. Here are five benefits of an adaptive security awareness program:

1. **You can respond quickly to new threats**
   This is perhaps the top reason for seeking a truly adaptive program. Cybersecurity threats are ever-evolving. With an adaptive awareness program, additional educational content can be implemented quickly in response to new threats. “Adapt to survive” is more than a catchy phrase; it’s vital.

2. **Your program will be risk-aligned**
   An adaptive program will be based on sound research into what your organization’s risks are. This means frequent, context-specific use of analytical tools to understand risks, and communicating changes in these risks to stakeholders and end users. Once your risks are known, designing an awareness program to address these factors is just that much easier.

3. **You get what’s needed to the right people**
   Different employees, all with different specialties, will benefit most from awareness training content that’s tailored to their specific positions. An adaptive program will include multiple training elements, including role- and risk-based elements that are customized to meet individual employee needs in your unique corporate culture. The more relevant your employees find your awareness program, the more likely they are to retain what they’ve learned.
4 You know how to reinforce your training
The best awareness program in the world will fall short without steps in place to remind employees of the things they need to know and do to reduce risk. Your employees may have completed training on phishing threats or malware, but what happens six months after the training is complete? This is where reinforcement comes in. An adaptive program will include regular deployment of a wide range of reinforcement resources, such as videos, posters, and games, aligned with known and emerging risks revealed through regular program analysis.

5 You can answer the ROI question
Any good adaptive program involves a process of continual analysis and improvement. Sounds like the perfect opportunity to provide proof that your program is working to the ones signing the checks, doesn’t it? With a truly adaptive program, you’ll have a built-in set of analysis tools, be they regular employee knowledge assessments or phishing simulations, to show the program’s benefits. This data will come in handy the next time your CEO asks if your training is worth the cost.

Developing an effective security awareness culture involves many factors, but the foundation of all should be adaptability. With this as your goal, you’ll be well on your way to a program that is predictive of risks, can be continuously improved upon, and that becomes part of the organizational culture while achieving real, measurable results.
ABOUT MEDIAPRO

MediaPro creates engaging e-Learning experiences that transform behavior, improve performance, and achieve business results. We offer a suite of security awareness, privacy awareness, and compliance tools and services that are used by the most risk-aware companies in the world. We deliver award-winning awareness training courseware, reinforcement resources, and a SaaS-based LMS solution.

For more than two decades, MediaPro has been helping enterprises of all kinds improve the professional performance of their people. We’re passionate about our work in adult learning, and it shows in the quality of our courses, the delight of our clients, and in our industry recognition.

For more information, visit www.mediapro.com.