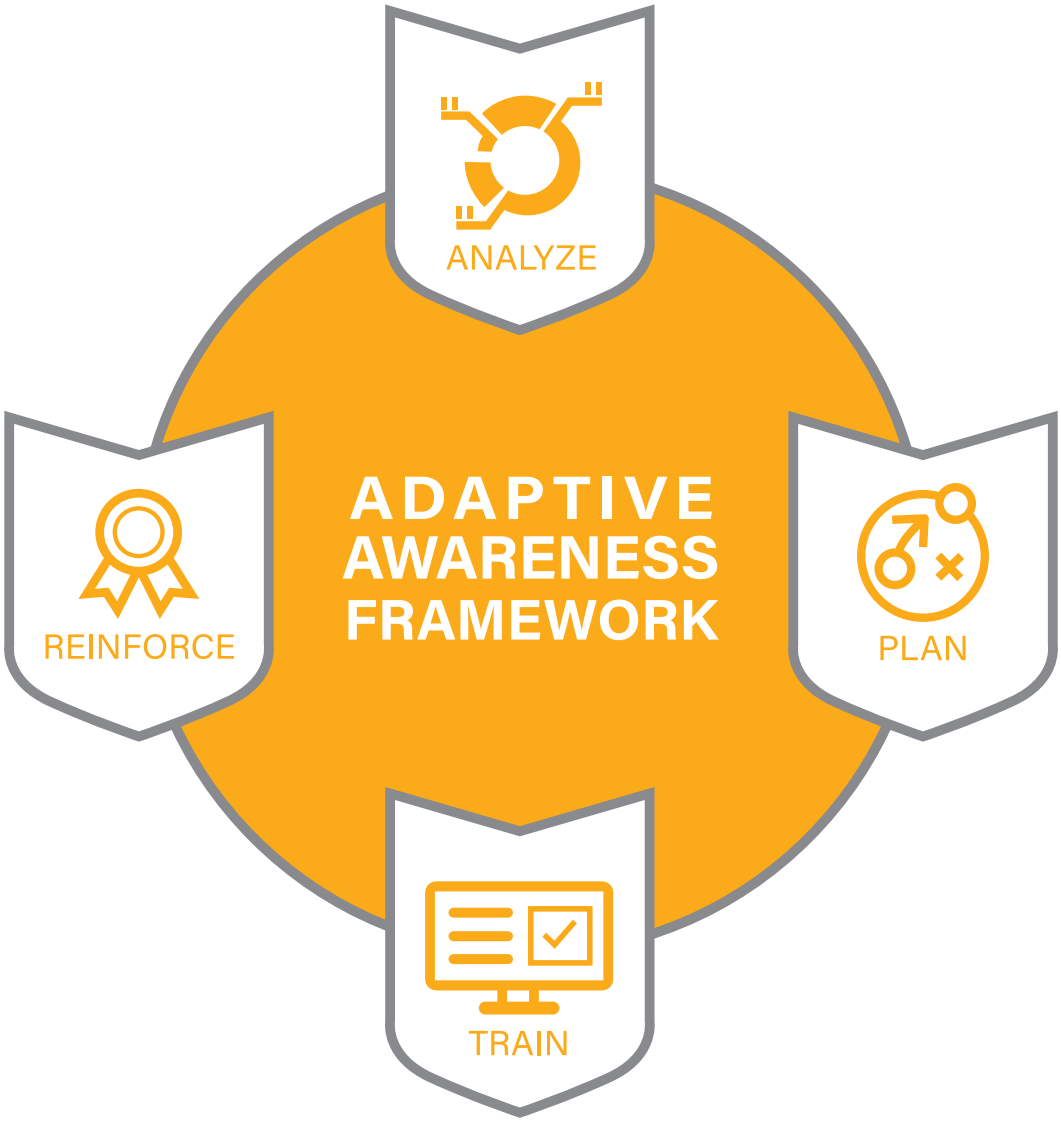
# A Best Practices Guide for Comprehensive Employee Awareness Programs




MediaPRO
Cybersecurity & Privacy Education

# INTRODUCTION

Today, security and privacy professionals find themselves in an enviable position. Global trends-from always-on connectivity to cloud computing to rising concerns for privacy and associated privacy regulation—have elevated the importance of both security and privacy personnel within all organizations, in both the public and private sector. Professionals in these fields have a voice at the upper levels of decision-making like never before, and the job market reflects intense demands for people skilled in these areas.

There is a dark side to this story, of course. Cybercriminals recognize the possibility for riches in the flow of information that makes the global economy go round, and they are coming after your data with ever-increasing tenacity. As you know, technological advances have helped tighten and control many security and privacy risks. However, because these technologies have improved so much in recent years, cyber attackers have shifted their focus to the ever-vulnerable human. While you can build a wall of technical protections around systems and information, it is ultimately the actions and behaviors of your people that will determine just how secure your data, and ultimately your bottom line, really are.

Cybercriminals are coming after your data with ever-increasing tenacity.

Our own 2017 survey of more than 1,000 employees across the United States revealed that 70% lack the awareness to stop preventable cyber incidents. Broader, industrywide research paints the same picture. The 2018 Verizon Enterprises *Data Breach Investigation Report,* for example, found that malicious emails were involved in 96% of data breaches in 2017, up from 88% the year before. And falling for scam emails is just a sampling of the dangers posed by employees lacking security or privacy awareness. A 2016 CompTIA report titled *International Trends in Cybersecurity* found that human error accounts for more than 50 percent of security breaches. Enterprises face threats that compromise the security of critical information due to unintentionally risky behavior

from employees with poor privacy and security hygiene. Left unchecked, these employees are putting their companies at serious risk of material loss due to a data breach or other cyber incident. The danger of sensitive client or customer data compromised by a data breach threatens organizations of all sizes and industries. Year after year, massive breaches affecting millions of people continue to make headlines. Reports of lost revenue, lost customers, and lost reputation often follow.

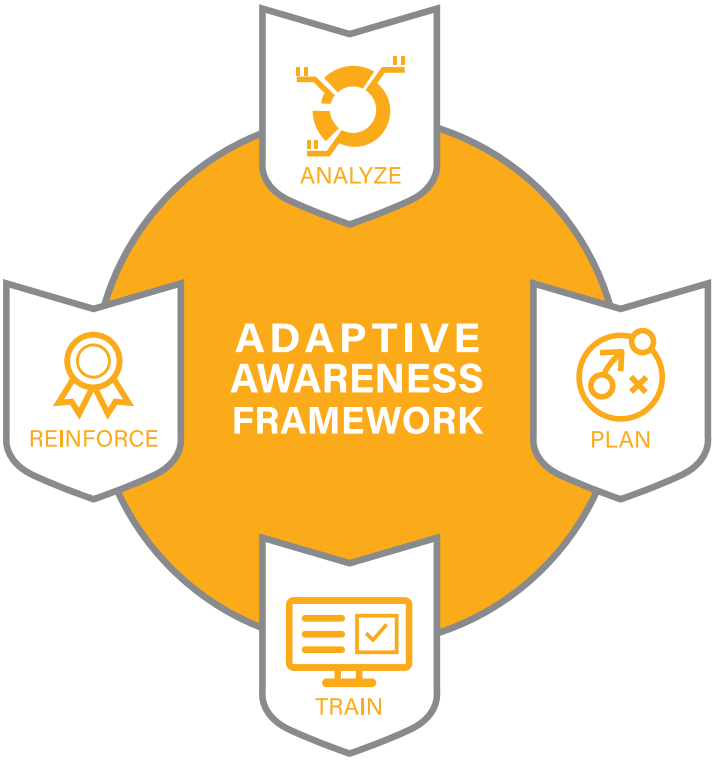
All the personal customer data and sensitive corporate information kept in your servers is only as secure as the humans who manage it.

Consider the analogy of a bank vault. No matter how much money may have been spent on construction and installation of this safeguard, it proves useless if it is left unsecure. The same is true in the security and privacy spaces. A vault is only as strong as its keepers. The keepers must know to properly close and secure the vault. Look at your organization in the same way. All the personal customer data and sensitive corporate information kept in your servers is only as secure as the humans who manage it. This is where the importance of employee awareness programs comes in.

It's no secret that security and privacy awareness programs do not always work or deliver the expected results. Often, the main purpose driving the awareness training is to officially "check the box" to satisfy various compliance requirements. If you've had the misfortune of implementing an inadequate security or privacy awareness program, then you already know that simply making users aware of the issues will not make them change their attitudes or behaviors. Unfortunately, the "check the box" approach is a very common practice.

There are many reasons an awareness program fails. Perhaps the training was simply a boring PowerPoint, converted for online delivery, with no thought given to engaging employees in considering the impact that security or privacy had on their lives. Perhaps it was a series of videos that amused people with animatronic malware bots—yet failed to convey the behaviors they needed to practice at work. If you are willing and able to promote awareness through training, why waste your money and your employees' time with training that is ineffective or boring?

With 25 years in the adult learning and employee awareness business, we like to think we know a thing or two about helping organizations teach their employees. In this guide, we'll explain what we believe are best practices for running employee awareness programs in security and privacy. We believe that if you're going to really change behavior within your organization, you've got to do four things: **Analyze, Plan, Train, and Reinforce.** These are the core components of our Adaptive Awareness Framework, a vision for how you can build an effective employee awareness program. Each of the four following chapters is devoted to one of these four components:




- **Analyze:** Using Data to Inform Your Awareness Program
- **Plan:** Drawing a Roadmap for Planning Your Awareness Program
- **Train:** Building Training that Achieves Real Behavior Change
- **Reinforce:** Battling the Forgetting Curve

## CHAPTER 1: ANALYZE
# USING DATA TO INFORM YOUR AWARENESS PROGRAM

Whether you are up to your neck in data on employee actions, or just starting to get statistics on human performance, you can take steps to use your data to improve your awareness program. One of the easiest ways to begin down this path is going straight to your employees. Knowledge assessments or surveys, for example, work well in this regard.

Technical tools to support data collection and analysis can also prove useful, and are rising in popularity. In Gartner's *2015-2016 Magic Quadrant for Security Information and Event Management (SIEM),* analysts reported that the SIEM industry grew 14% ($1.5 billion to $1.69 billion) in 2014. Gartner also estimates that by 2018, 90% of organizations will implement at least one type of integrated data loss prevention (DLP) technology. A quickly rising star is the concept of user and entity behavioral analytics (UEBA, sometimes simply called UBA or behavioral analytics). These systems are often designed to collate data gleaned from SIEM and DLP systems and sniff out anomalous, and potentially risky, behavior.

Increasing investment in this sort of data collection and analytics is no surprise as cyber attackers continue to bombard organizations with attempts to steal valuable

## Making Sense of the Data Analysis Alphabet Soup

**Security Information and Event Management (SIEM):** SIEM systems collect network event logs, such as a list of unsecure login attempts, and other security-related documentation for analysis.

**Data Loss Prevention (DLP):** DLP software is designed to monitor the transmission of sensitive information to make sure an employee, either maliciously or not, doesn't send it where it's not supposed to go.

**User and Entity Behavioral Analytics (UEBA, or UBA):** UEBA tools are a way to parse through all the information collected by SIEM and DLP systems and provide the IT professionals monitoring the network prioritized trend information.

personal information. All this data analytics work has the capacity to create reams of data and stunning visualizations of risk. And yet this vast effort at data collection will not have gone far enough if the information stays confined to the information security office and is only used to wow the higher ups in corporate board rooms.

No matter how you end up collecting data on employee-related risks, we think it's time to turn the immense power of this data loose on those who are constantly identified as the biggest source of risk: the employees. That's right, it's time to use the power of big data to change the way we run awareness programs. At its core, data on user behavior is really data about an organization's human-centered risks.

Such information will show you precisely where your employees misstep, and how badly. Drawing on that data in a well-defined "analysis" stage, in which you scrutinize your organization's human-related security and privacy risks, is vital to any comprehensive awareness program. Your understanding of these risks allows you to develop and deliver the kinds of content that ensure your employees get the most relevant training and reinforcement experience possible.

A well-defined "analysis" stage is vital to any comprehensive awareness program.

In Chapter One, we'll walk through some best practices for using data about your organization's human-centered risks to make the most of your security and/or privacy awareness education efforts. We'll discuss:

- **Collecting direct data about your employee-related risks**
- **Digging into technical tools to glean data on employee-related risks**

## DIRECT DATA INTO YOUR BEHAVIORAL RISKS

First thing's first: let's consider what data you can collect without the use an alphabet's soup of technical tools. This means going directly to your employees. Here are some ways to do that:

### *Knowledge Assessments and Surveys*

Knowledge assessments sent to employees are perhaps the most direct way to measure what they know and don't know about security and privacy best practices. The design of such a survey can take many forms, but the questions should be geared toward those aspects of security and privacy than could affect your organization the most. A good understanding of your organization's own goals and priorities will be needed here, to make sure you're ultimately asking the right questions. After all, why ask employees if they know how to connect to networks via VPN if they're not taking their computers out of the office?

We've developed an outward facing employee behavioral risk assessment designed to gauge the state of privacy and security awareness at individual organizations. These questions cover a number of scenarios, such as recognizing malware, proper sensitive data handling, and password security. Take the survey yourself, and find out how you can roll out this survey to your organizations here.

### *Phishing and Social Engineering*

Since phishing is one of the most common social engineering tactics in use today, it makes sense to run simulated phishing and social engineering attacks. These simulated attacks can employ a wide variety of clever techniques to obtain passwords, obtain access to sensitive information, or gain physical access through tactics as simple as an email or a phone call, tailgating, or dropping a dummy USB device. Simulated attacks like these can act as a sort of ad-hoc event monitoring system, as they reveal what risky actions your employees are most likely to take given the opportunity. A number of vendors offer phishing simulator programs as part of an awareness program package. But beware of vendors focusing too heavily on phishing as the be-all, end-all of cyber threats. Such an approach targets only one vector of attack, and doesn't do the work of helping employees see the multi-layered nature of threats.

Even if you do have automated data analytics tools in place, knowledge assessments and phishing simulator tools will still prove useful. Automated systems can't capture, for example, an organizational willingness to accept security or privacy awareness training (more on this topic in Chapter 2). A cleverly designed employee assessment can also shed light on how best to present educational content information to your people. Understanding your organizational culture around learning will help you deliver content in a way that's accepted and embraced. The most risk-aligned content in the world will do no good if it falls on deaf ears.

Understanding your organizational culture around learning will help you deliver content in a way that's accepted and embraced.

## DIGGING DEEPER INTO YOUR DATA

Additionally, you might already be gathering data related to information security and data protection, and you should definitely put it to use. What data do you already have? The answer could range anywhere from "next to nothing" to "enough to fill an oil tanker." If your organization does not have data collection measures in place, now might be the perfect time to begin researching vendors in this space. If your organization does have one or more event logging and data analysis systems in place, great! The information these systems collect can be a gold mine for determining what risky behaviors your organization's people most often take. Your IT staff will be the experts on these systems and the data they collect. They should be your first stop in accessing and helping to analyze this data.

The most common types of these systems are SIEM, DLP, and UEBA (forgive us for the alphabet soup). SIEM systems, in a nutshell, collect network event logs, such as a list of unsecure login attempts, and other security-related documentation for analysis. DLP software is designed to monitor the transmission of sensitive information to make sure an employee, either maliciously or not, doesn't send it where it's not supposed to go. Additionally, you may have incident

reporting and help desk data that you can tap. The concept of UEBA is quickly emerging as a way to parse through all the information collected by SIEM, DLP, and other sources and provide the IT professionals monitoring the network prioritized trend information. UEBA tools are providing real value in identifying patterns and signs that reveal the presence of bad actors in the IT environment.

But how can all this information help with your employee awareness program? We're glad you asked. Systems like these will be able to provide data on, for example, employees connecting unknown devices to the company network, or saving files to unapproved cloud storage locations.

These data will help you answer important questions about the kind of employee awareness program you'll need. What specific behaviors do you want (or need) to change? What tools will you need to bring about these changes? These questions are much more difficult to answer without a strong data set behind you.

## Data on these sorts of actions can be used to identify a number of different trends:

- Are we seeing a recent uptick in risky behavior?
- Is there a specific behavior that stands out?
- What sectors of the organization produce the most risky behaviors? (That is, are there certain behaviors that characterize sales vs. call centers vs. marketing, for example.)

## SUMMARY

You've probably heard it said that, "It's easier to drown in information than to profit from it." The sheer amount of data on information security threats flowing around your organization can seem overwhelming, but it should not be feared. Just as rivers can sweep the unsuspecting person away, they can also serve as commercial lifelines and economic generators. The key is how they're harnessed.

The same is true for the data we've discussed here. Whether technical or more subjective, smart data collection and analysis is the best way to tease out the risks that most impact your organization.

Continuous awareness program improvement through data analysis is one of the cornerstones for what we often refer to as an "adaptive" awareness program. By adaptive, we mean a program that is based on lessons learned and predictive indicators, continuously improved via active adaptation to combat evolving threats and changing regulation, and part of the overall organizational culture.

In Chapter 2, we discuss building a solid plan for your awareness program development or improvement.

## CHAPTER 2: PLAN
# DRAWING A ROADMAP FOR PLANNING YOUR AWARENESS PROGRAM

No journey should begin without a roadmap. When's the last time you traveled to a new location without first typing the address into your GPS, favorite mapping website, or app? Setting out without a clear direction can be an inconvenience at best, and a recipe for disaster at worst.

If you're responsible for establishing sound cybersecurity and privacy practices in your organization's employees, developing and maintaining an awareness training program for either area is one of the most important journeys you can take. Why? Achieving and maintaining a risk-aware workplace requires a well-mapped awareness program to effect the behavior changes needed to keep your organization safe.

In Chapter 1, we walked you through some ways to collect data on employee-related risks. Those risks that have a direct bearing on the security of your organization's sensitive information. In this Chapter, we'll discuss folding that risk-based data into a plan for a comprehensive awareness program. In this Planning stage, you'll consider the data you've gathered as well as:

- **The current state of your organization when it comes to security and/or privacy awareness**
- **What risks you'll need to address**
- **What challenges a new or improved awareness program could face**
- **What organization-specific factors you'll need to fold in to your training**
- **What your culture will support when it comes to awareness communication**

## WHERE DO YOU STAND?

A famous singing nun once said, "Let's start at the very beginning, a very good place to start." Great advice. The best way to start at the beginning is to look around you. Figure out where you stand now when it comes to cybersecurity and privacy concerns and what sort of awareness initiative is realistically possible. This may seem like the obvious way to begin, but you'd be surprised how many organizations decide to implement an awareness program and shoot for a top-of-the-line model from the start. We see this as akin to targeting Mt. Rainier, Washington State's highest peak, as your first-ever summit attempt. Ambitious, sure, but we'd recommend you warm up with a few smaller climbs first!

The takeaway here is to start gradually and build up in-line with your organizational capacity. Take the time to assess your current awareness program and the nature of the risks your organization faces. If program enhancements are what you're after, use this self-assessment time to make the wise decision about not biting off more than you can chew. Need outside help with your planning efforts? Need to add additional training elements, such as new courses or reinforcement materials? This is the time to figure it all out.

Even if you're working to develop an awareness program from scratch, these tactics are still the best place to start. Knowing your surroundings, what you need, and what your organization can take on are essential first steps in planning and developing an effective awareness program.

## WHAT ARE YOUR BEHAVIORAL RISKS?

After you've established where you stand, it's time to take stock of your risk landscape. When we think of "risks," we're thinking about the specific human behaviors related to security and privacy that you need to educate people about. (You may have already done a risk assessment in your organization, and this may or may not help you identify behavioral risks.) Are there certain types of behavioral risks that are not being addressed? You may want to prioritize those for the

year ahead. Have threats evolved since the last time the program was deployed? Risks change over time, and it does no good to wage war against yesterday's problems.

Risks change over time, and it does no good to wage war against yesterday's problems.

Here is where the work you did in the Analyze stage will help. If you've done an employee behavioral risk assessment, that may have already identified some key areas where your employees struggle, and phishing exercises shed a clear light on the extent of your phishing problem. You'll want to use this information to identify areas of emphasis for your training and reinforcement. You want to create an overall awareness program that is relevant, targeted, and focused on bringing about real improvements in employee knowledge and behavior. The more specific your risk analysis stage is, the more action-oriented you can be in describing the behavior change you expect to see in your employees.

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. Such a program ensures your employees are getting relevant information delivered to them, in a variety of forms that include, but should not end with, conventional training.

Using data analysis to guide your program is not, and should not be, a once-and-done scenario. The most mature awareness programs out there build regular data analysis and content alignment into an ongoing cycle of continuous improvement. Thus, if you started a program today, about six months from now you might want to "take your pulse" with another behavioral risk assessment or review of incident reports from your organization's SIEM or UEBA systems. This system feedback should be done on a regular basis to make sure the content you're providing is as relevant as possible. Regular assessments combined with your own knowledge of new and emerging risks will also help determine what to reinforce with additional targeted learning materials, such as games, animations, and posters (more on reinforcing key learning concepts in Chapter 4).

Regular risk assessment will also establish a framework for measuring your awareness program's effectiveness over time. Such a process is vital in demonstrating the relevance of your efforts and for making security and/or privacy awareness an ongoing priority for your organization. To this end, we recommend developing a set of quantifiable measurements to track during and after training occurs, such as a reduction in the number of incident reports. Another useful technique is to conduct a pre-assessment and post-assessment with employees to track an increase in security and/or privacy knowledge across the organization. Once you have recorded these results, communicate these metrics back to senior management and to the organization so managers and employees can see the results of the awareness efforts. You did the work, you deserve to be recognized for it.

Using data to tell you where to focus is one thing, but finding the right mix of training and reinforcement content can be difficult. Most programs typically generate some of their own content, such as videos starring your own executives discussing InfoSec best practices, or in-house awareness events ("Change Your Password Day," for example). But mature programs seek out skilled third-party providers to build content centered on the identified risks. Ideally, such vendors will have a library of available content to choose from so that you can mix and match learning materials over time. Such an approach will likely give you the best bang for your buck, as it will allow you to add new content as your organization's risks shift and new threats arise.

## WHAT ARE YOUR CHALLENGES?

With a good 360-degree view of where you stand and potential risks called out, it's on to the next step: determining what kind of challenges you face. By challenges (separate from "risks"), we mean all the things that could stand in the way of you developing the most effective security or privacy awareness program possible. This phase can seem daunting, as it may uncover barriers you didn't even know your organization had. But as with all obstacles, understanding them is the first step toward overcoming them.

First things first: you've got to figure out how much budgetary support you can get, and that means buy-in from the ones signing the checks. The key here is clearly answering the question: is it worth it? Explaining the cost of not equipping your employees with the know-how to avoid security and privacy threats is a great way to start this discussion. Did you know, for example, that the average cost of a data breach in 2017 was $3.6 million? The 2018 Verizon Enterprises *Data Breach Investigations Report* found that one in five data breaches in 2017 involved human error. Can you really afford not to properly train your employees?

First things first: you've got to figure out how much budgetary support you can get, and that means buy-in from the ones signing the checks.

While vital, executive support will not be all you need. You'll also have to learn what backing you'll get from your entire organization. We see this determination as twofold: logistical and cultural. From the logistics angle, do you have the people power to bring the awareness program to life? The technical know-how from IT, for example, to maintain the e-Learning modules? The human-facing support from HR to make sure your people are engaging with, and are engaged by, the training? Or simply the logistical support from Communications (if you've got such a department) to help you push out messages to the entire population in a way that they will be heard. Take this stage as an opportunity to identify potential in-organization partnerships that will allow your awareness program to get off the ground. The most successful programs we've seen have involved a productive collaboration between information security and privacy and other, supporting business areas. So don't go it alone; by all means, find allies.

The most successful programs we've seen have involved a productive collaboration between information security and privacy and other, supporting business areas.

Cultural support, however, is a whole different beast. In assessing cultural support, we're talking about your organization's overall willingness to accept security or privacy awareness training. This means trying to find out not just what your employees know about security and privacy best practices, but how they think and feel about these topics and any previous efforts in those subjects. Information gathering at this level calls for employee knowledge assessment on steroids, so to speak. One thought leader who has caught our eye in this regard is information security researcher Lance Hayden. Dr. Hayden, Ph.D. and author of *People-Centric Security: Transforming Your Enterprise Security Culture*, has developed a "Security Culture Diagnostic Survey" designed to identify and compare security cultures in your organization. Information gleaned from assessments like that will allow you to craft an awareness initiative that effectively speaks to your employee population. Shifting a corporate culture to one that's security and/or privacy aware will be no easy task, but gathering the right baseline information is a key first step.

Next, begin thinking about what technical hurdles you may have to jump. Do you know the state of your learning management system, or LMS? You'll need a system to deliver and track training, ideally with a built-in way to quickly add additional course content as needed. Your company may already have one, or you can find a cloud-based LMS from a third-party vendor. Speaking of the technical side, you'll also need to think about what kinds of devices your employees use to access training. Whether via laptop, tablet, or even smart phone, the training delivery method is almost as important as the quality of the training. You want to deliver education on the devices your people interact with on a regular basis.

Last but certainly not least, you'll need to consider perhaps the biggest challenge of all: making sure your employees actually learn something from your training (read more about what makes effective training in Chapter 3). This may seem so obvious that it doesn't need mentioning, but that doesn't make it any less challenging. This is where the expertise of the e-Learning provider

you choose comes into play (we highly recommend seeking outside help in this regard). Will your training be light-hearted or serious? Straight-forward or delivered in a unique way (using interactive games, for example)? You'll need to answer these questions, and more, all based on your organization's culture. Whatever method you choose, your training materials should be based on sound adult learning principles.  The potential pitfalls are many, but the benefits of a well-informed employee base will be well worth it.

## SUMMARY

The benefits of an effectively drawn roadmap have been known to humans since there were roads. A good map allows you to plan the best path to your destination. A good map will make clear what obstacles lie in your path. Put simply, a good map will answer the question "How do I get to where I want to be?" This is the true whether it's a journey to the top of a mountain, a road trip cross-country, or a development plan for an awareness program. As we've laid out, developing such a plan is key.

So you've analyzed your employee-related risks. You've developed a plan for your awareness initiative based on these risks, and other factors specific to your organizations. In Chapter 3, we discuss the meat of any employee awareness program: the training itself.

## CHAPTER 3: TRAIN
# BUILDING TRAINING THAT ACHIEVES REAL BEHAVIOR CHANGE

Imagine all your employees in a single room, waiting for cybersecurity and privacy training to begin. You've called them together because you know the value training can bring. You've done the research and discovered, for example, that "Companies that train their employees in information security best practices spend 76% less on security incidents than their non-training counterparts," according to a 2014 PWC report. That difference amounted to **$521,000 in lost revenue on average.**

As you stand before your gathered employees, your mind starts to race. "Is what I'm about to present going to work? Is it going to be enough?" Other research you've read on training effectiveness comes to mind. A joint Ponemon Institute/Experian survey found 55% of companies with security and privacy training had suffered a data breach or security incident due to malicious or negligent employees. This same survey found that many respondents felt their organization's training lacked the ability to effect real behavioral change. Forty-three percent said, for example, that their organization offered just one basic course meant to apply to all employees. Long story short: *if you're using the wrong training, you won't get the results you want.*

Long story short: if you're using the wrong training, you won't get the results you want.

As the statistics above show, not all training is created equal. Organizations both large and small continue to struggle with filling the human-shaped holes in their security and/or privacy strategy. In Chapters 1 and 2, we discussed using data about your employee-related risks to develop a plan for your awareness program. Knowing which behavioral risks you'll address, and having a plan for how to construct your overall program is a great start. But now, in Chapter 3, we will focus on how to present the needed training in these areas, how to make sure this training is as effective as it can be.

We're well aware that changing employee behavior is no easy task. Fortunately, there are some established ways to get a foothold. In this chapter, we'll discuss some awareness training best practices we know lead to real behavior change:

- **Getting users motivated**
- **Creating "Social Presence" to heighten engagement**
- **Providing interactive practice through all stages of training**
- **Using gamification to increase realism**
- **Managing training complexity**

## GET USERS MOTIVATED

You may expect to see an e-Learning best practices book section on training open with advice on juxtaposing multiple types of media or arranging the look on the page. But as Ruth Clark and Richard Mayer write in E-Learning and the Science of Instruction, the most fundamental lesson from e-Learning research is that learning is learning no matter the media. And the first job for any kind of training is to get users motivated, to get them to engage.

The most potent motivation comes from factors inside the learner or inherent in the task they're engaged in. So-called intrinsically motivated learners are more likely to process information in effective ways and achieve at high levels. So, the first step in motivation is getting the students' attention.

The first step in motivation is getting the students' attention.

The short path to motivation runs through identification. In order to hold your learners interest, you need to establish how the training content is relevant to them and how paying attention pays off for them. You can do that by addressing the student directly, or by presenting characters they identify with.

Once you've gotten their attention, you'll want to build their interest. A good way to do that is to show them that their actions at work have consequences, not only for the company, but also for them. You can do that, for example, by putting the characters they identify with in a situation that presents them with choices that have significant personal consequences.

## HEIGHTEN ENGAGEMENT BY CREATING "SOCIAL PRESENCE"

Motivation comes not only from the content you present, but also from the way you talk to students. You'll see a lot of training adopt a third-person voice ("To increase security, the 'strict' option is preferable,"), likely because use of third-person in academic circles lends an air of objectivity and authority.

The very objectivity of the voice, though, can waste the motivation we've been building. That's because learning, even e-Learning, operates at a deeper level when the learner experiences it as a social encounter. Students often experience the third-person objective voice as a disembodied voice. So, it leaves your learners less engaged and less likely to identify with characters you present.

The better approach for training is to address the user directly. You'll find that users parse second-person writing more easily, but that's not the only reason to prefer it. Writing in a conversational tone and addressing the reader in second-person ("You are our number one defense") triggers ingrained, unconscious, social conventions that cause learners to invest attention. Essentially, they react to the training as though it was a person talking to them and expecting a response. The result: learners engage at a deeper level.

Writing in a conversational tone and addressing the reader in second-person triggers ingrained, unconscious, social conventions that cause learners to invest attention.

You'll augment that sense of social presence by combining a conversational tone with the stories and characters we talked about above. Returning to Clark and Mayer, making the "author" visible

through story and images adds additional cues that encourage the learner to deepen their engagement with the content.

## PROVIDE PRACTICE THROUGHOUT THE STAGES OF TRAINING

We all know that if we want users to recognize information, we need to show them examples. And the best way to learn a skill is to practice it, not just to read about it. Learners learn what they do, so it's important that their exploration and practice be as true to reality as possible. If we want employees to recognize security features on a bank card, for example, we show them the features on the card. If we want them to tell the difference between sensitive and non-sensitive information, we ask them to separate the two into different folders. But there's more to practice than that.

Learners learn what they do, so it's important that their exploration and practice be as true to reality as possible.

In the past, the e-Learning industry has thought of practice as an end-point, the last step in a cascade which starts with an introduction and ends with a test. But research shows that practice doesn't have to work that way. Practice accomplishes varying ends depending on when and how you present it in the course.

Sometimes practice makes sense as part of the initial learning. That can be true when the content is simple. Introducing small challenges can combat "cognitive miserliness," the tendency for brains to conserve energy by attending less closely or falling back on heuristics to solve problems.

Practice can work well even when it's staged as a pre-test, literally a quiz students take before they've seen the content of the course. You might think it's unfair or counterproductive to pre-test. In fact, students get three benefits from getting practice before being exposed to the content.

First, as Clark and Mayer point out, students are notoriously poor (OK, terrible) at gauging their own ability. Graded practice before the lesson can alert them to holes in their learning so they pay attention when it makes sense. Second, pre-tests give students who already know the information a chance to test out of sections so they can focus on those areas where they need help. Finally, pre-testing gives students a preview of the content and vocabulary that will feature in the lesson, so they begin to build cognitive structures to fit the content into when they encounter it.

## HEIGHTEN REALISTIC PRACTICE WITH RELEVANT GAMIFICATION

Ambient Insight predicts the market for game-and simulation-based learning will rise to $7.3 billion in 2021 from an already impressive $1.7 billion today. Yet, gamification is double-edged sword. Done well, it can make training much more inviting. Done poorly, it can literally waste your project budget by teaching the wrong skills.

The classic example is the rise and fall of the *Oregon Trail*, an educational game that featured pioneers moving their families out west. Instead of absorbing lessons about Westward Expansion, many students abandoned the instructional objectives, choosing to load up on virtual bullets and take down as many buffalo as they could.

Gamification is double-edged sword. Done well, it can make training much more inviting. Done poorly, it can literally waste your project budget by teaching the wrong skills.

Good game design that makes a difference in workplace performance compresses realistic job problems into a short timeframe in a safe setting where learners can succeed and fail safely. As our friends Clark and Mayer write, learning will get more reinforcement when it becomes essential to progressing through the simulation. You can facilitate this by weaving instructional objectives into the flow of the simulation.

Consider, for example, our own *Catch the Phish* game, designed to test a user's ability to tell a scam email from a legitimate one after receiving phishing training. The game invites users to sort received emails into a "Keep" folder or the trash, based on a number of attributes. If a phishing email is treated as legitimate, a warning window pops up with a brief description of what was suspicious about the email. Too many of these, and users have to start the game again.

Games and simulations are more effective when they include explanatory feedback rather than a simple correct or incorrect. Explanatory feedback works well as either a hint as feedback to learner responses.

## MANAGE COMPLEXITY

A current fad in instructional design is to create "discovery" spaces that are rich in interactivities with little direction. The intention here is to create a rich environment. But in practice, complex environments are often inefficient and can contribute to overload. According to Clark and Mayer, the more effective practice is to sequence content by starting with a simple task that has a low level of challenge and only partial functionality enabled. Then, progress to tasks that have more information and demand more skill or knowledge.

And complexity isn't just a matter of the number of images on a page, but the detail in those images as well. We often work with subject matter experts whose initial position is that photorealistic images are more appropriate for "serious" content while hand-drawn or simplified images should be reserved for less important topics. In fact, highly realistic images and sounds are busy and distracting, particularly for novice learners. Clark and Mayer say the best practice is to minimize realism that isn't aligned with an instructional objective.

Of course, there's abundant literature on the way to deliver multimedia content, the number of channels to use simultaneously, and how to manage it. And you'll find plenty of articles on the web discussing those issues. Before you get into those details, though, consider this.

In awareness training, poor design impacts your bottom line and your reputation in the market place.

Graphical and audio design are important. They underline and clarify. They direct attention. But only after you have the attention first, and only for learners who are interested and motivated. Shooting phishing email in an arcade is fun. But it alone doesn't build your employees' confidence or capability to make your information or your customers more secure. In awareness training, poor design impacts your bottom line and your reputation in the market place. It doesn't matter how pretty your screens look if your employees aren't engaged and taking your training to heart. Substance and appearance must walk hand-in-hand to effect real behavioral change.

## SUMMARY

You may hear arguments that training is dead, that it's too boring, and that all you really need to do is phish your employees to make them aware they're at risk. This is bunk. When done well, a good security or privacy course clearly communicates your company position on these issues and provides a single source of clear guidance on what you need employees to know and do to keep information safe. In other words, it sets your organization on the path toward a risk-aware culture. If you keep these five best practices in mind, you'll be well on your way.

But as we've argued many times before, training done once or even a few times a year cannot be expected to achieve that risk-aware culture all on its own. In our fourth and final chapter, we discuss the ever-important concept of making sure the key concepts your employees have just spent time learning stick around.

## CHAPTER 4: REINFORCE
# BATTLING THE FORGETTING CURVE

We've likely all had this dream, or one similar to it. You're back at college sitting in class when the professor announces a surprise test. Not a pop quiz, mind you, but a full-fledged test with essay sections, dozens of multiple choice questions, you name it. Your heart starts to race as you realize you barely know this material. You've spent barely any time on it over the past year!

Fortunately, this scenario is just a dream. But for employees who have undergone training on risks related to their organization's cybersecurity and data privacy only once or twice per year, this is a stark reality. Imagine sitting in their shoes: they're asked to tap their knowledge of security and privacy best practices on a nearly daily basis, based on training they received months ago. In our view, this just isn't right: employees cannot, and should not, be expected to serve as safeguards against these risks without consistent and regular education. Even the best training experience will be forgotten over time if there are no efforts made to reinforce key learning concepts. To make those concepts stick.

When reinforced, even with the simplest flow of supporting communications around the key messages, training changes behavior.

When reinforced, even with the simplest flow of supporting communications around the key messages, *training changes behavior.* Reinforcement can remind, refresh, encourage, and even entertain. And when you deploy reinforcement as a focused and ongoing series of communications around key risks, you take an intentional step toward building a risk-aware culture.

In the previous chapters, we discussed developing effective employee training through a robust risk analysis and planning process. Now that we have a firm handle on how the initial training should be done, let's turn now to making sure your employees remember it.

The goal of this fourth and final chapter is twofold:

- **Make the case as to why solid reinforcement of training principles is needed**
- **Provide concrete examples of reinforcement content we've seen prove most effective in reinforcing key concepts**

## THE FORGETTING CURVE

You've likely heard the term "learning curve" to describe the time it takes for someone to learn a new concept. But most people might not be aware of the learning curve's evil twin: the "forgetting curve." Theorized by the German psychologist Hermann Ebbinghaus (the same man who described the learning curve concept), the forgetting curve is a measure of how quickly new information is lost over time when there is no attempt to retain it.

No musical instrument has ever been mastered with practice sessions once or twice per year. The same goes for security and privacy awareness education.

And as it turns out, humans are remarkably forgetful creatures. In fact, without immediate and continual reinforcement, an embarrassingly high percentage of the knowledge gained in the training phase will tend to evaporate within weeks, if not days. While the phrase "forgetting curve" may have failed to enter our common psyche, the concept is at the core of the time-honored adage: "practice makes perfect." No musical instrument has ever been mastered with practice sessions once or twice per year. The same goes for security and privacy awareness education.

That's where the reinforcement phase of an effective awareness program comes in. A good reinforcement program is a deliberate, orchestrated, focused, and an ongoing campaign against the forgetting curve. It's designed to convert what would otherwise be transient short-term

memory into sustainable, second-nature behavior. Without immediate, persistent, and consistent reinforcement, the awareness training messages will be lost over time.

With reinforcement, you'll realize a positive and lasting ROI on your training investment. To achieve this end, an effective reinforcement program must target multiple communication triggers operating in many channels, and in the process apply proven learning techniques— over time—in order to bring about the desired changes.

## THINK LIKE A MAD MAN

But what makes effective reinforcement? Here we'd like to take a page out Don Draper's book. Think about what makes up an advertising campaign: a series of messages that share a single idea or theme, transmitted via different media channels on a regular basis, for an extended period of time—with the singular goal of influencing consumer behavior. Sound familiar?

The goal of a reinforcement program is not only to raise awareness, but to bring about a change in attitude that leads to a change in behavior.

Advertisers know that human behavior is complex. They also know that media can work to shift and shape attitudes and behaviors. Keep in mind that the goal of a reinforcement program is not only to raise awareness, but to bring about a change in attitude that leads to a change in behavior. As a case in point, your organization may have certain policies that are generally unpopular. Mandatory password changes come to mind. Such requirements often meet with resistance because they're considered a nuisance. But by acknowledging the inconvenience, and emphasizing their importance with consistent and frequent messaging, the displeasure eventually wanes, ultimately giving way to a positive attitude.

Repeated exposure goes a long way toward achieving this outcome. The same is true when employees must unlearn bad habits—especially the ones that have served them well over the years ("I've always done it this way and I've never had a problem"). A good reinforcement

program will help employees see the error of their ways, acknowledge and recognize the risks they present to the organization, and bring them fully on-board with the policy or procedure.

Another rule of advertising involves audience segmentation, or what we've called a role-based approach. That is, delivering the message where it will do the most good. Some messages are fairly universal (creating strong passwords or detecting phishing schemes, for example), but others might be specific to particular roles (e.g., properly classifying data or handling payment card information). Without segmentation according to the multiple responsibilities and levels of expertise within your organization, many messages may be ignored for lack of relevance, diminishing the effectiveness of the program overall. Happily, you can easily segment your reinforcement delivery by deploying content tailored to specific job roles (your C-suite, HR department, etc.) posting certain messages only in the appropriate departments, through the use of email groups, departmental events, and numerous other means that will improve audience targeting and relevance.

## KNOW THY COMPANY CULTURE

While it is important to know your audience, effective training reinforcement involves more than simply differentiating people by roles and responsibilities. Your company's culture will also influence how the initiative will play out. Your organizational culture provides subtle cues to employees about what to do, how to do it, and also what not to do. Your culture is an expression of the organization's practices, its values, and behavioral norms. And because culture is socially learned, a culture that values information cybersecurity and data privacy is best modeled by the executive leadership.

Many business leaders understand that culture plays an important role in their organizations, but most, it seems, have difficulty understanding how it can be leveraged to bring about risk-aware behaviors—or worse, how it might actually impede those behaviors. Nonetheless, with properly managed communications and consistent executive modeling, you can realize real change. To create a such a culture, it is helpful to think of the security/privacy function as a brand—your brand. As discussed in the previous section, a good reinforcement program is a lot

like an advertising campaign. To make it work, you've got to think like an advertiser. At this point you might be thinking, "In the training phase, I had to think like an educator. Now you're telling me I have to think like an advertiser, too?" Sorry, but yes. It is just this combination of domain expertise that distinguishes a rudimentary "check the box" awareness program from one that actually produces real results.

Just as with the training itself, reinforcement content must speak to your organization's unique culture.

Just as with the training itself, reinforcement content must speak to your organization's unique culture. Will humorous, tongue-in-cheek content hit home, or fall flat? Is a more serious (but by no means less engaging) approach warranted? No one knows your own culture better than you, and this knowledge must be brought to bear when planning and developing your training reinforcement strategy.

## WHERE THE RUBBER MEETS THE ROAD

Now that we've worked through the whys of a robust training reinforcement initiative, it's time for the fun part: what types of content work best. The answer to this question will undoubtedly depend on who you ask (and also on your culture; see above). In general, though, we've collected some consistent themes over our 20-plus years of developing award-winning training and reinforcement. Read on to learn more about the reinforcement types that we've seen work the best. Keep in mind that in general, our clients have found that reinforcement initiatives incorporating multiple media and delivery methods yield the best results.

### *Animations and Videos*

If a picture is worth a thousand words, then a video or animation must be good for at least a couple million. Think of any website you've visited recently, or the makeup of your social media feeds. Chances are videos can be found in both of them. The reason: they work. Adult learning research consistently shows that videos help provide an enjoyable learning experience, boost engagement, and improve the transfer of knowledge. These attributes are keys to effective training and should be part of reinforcement content, too.

The best videos get your message across quickly and powerfully and are aligned with the key concepts of your training (or they wouldn't be "reinforcement"). The best training vendors will provide a wide variety of reinforcement content covering myriad security and privacy risk topics such as ransomware, password best practices, bring your own device (BYOD) policies, safely downloading apps, or the use of public Wi-Fi. Additionally, the best vendors will make different styles available; funny animations for certain corporate cultures, for example, or live-action offerings for others.

Another attribute to look for is ease of distribution of this video content. Ideally, your chosen vendor should allow you to embed the assets on your Intranet, offer a hosted solution, provide the ability to track usage, and offer a stand-alone player. We see the flexibility of delivery almost as important as the content itself. You need to be able to access your employees where they are, be it at their personal machines or in break rooms, lunch rooms, or other common areas (via wall-hung screens, for example).

### *Games*

The terms "interactive" and "engaging" are likely the first things you think of when games are mentioned (if not, you're probably playing the wrong ones). Gamification of adult learning is of the most popular trends in the industry, and for good reason. Adult learning research has found time and again the benefits of melding education with game-playing. Well-designed game experiences encourage the learner to think of their lessons as real-world experiences, thus increasing the chances of retention. In this way, games are an effective means for engaging people and reinforcing the security and privacy awareness message. Games pose a challenge to the learner and should be both entertaining and fun. And because they are interactive, they provide excellent opportunities for feedback and instruction. Moreover, because the scores can be tracked, games can be used as remedial devices when a training intervention is triggered.

Adult learning research has found time and again the benefits of melding education with game-playing.

You can also track groups of people and create competition between departments to achieve the highest participation rate or average score. Like most awareness activities, games should be rotated on a regular basis to keep the experience fresh. There are many prepackaged games on the market, so you don't need to create your own. If you choose an outsourced solution, be sure that the games provide you the ability to update and rotate the challenge questions yourself without reengaging the vendor. And like the other elements in your awareness campaign, they should be customizable and support your own branding.


**Reinforcement games pose a challenge to the learner and should be both entertaining and fun.**

## *Posters*

Don't underestimate the power of a single, engaging image to drive home the importance of a key learning tenet. A wide selection of well-designed posters, each aligned to specific risks, is an effective and popular way to drive home the initial training message. As with the videos, each should address the kinds of behaviors your organization seeks to instill. Consider these posters "drive by" billboards that will help drive home an attitude of security and/or privacy awareness with memorable images and tag lines that will not only grab attention, but reinforce the behavior in ways that will encourage compliance.

The posters should be simple, direct, and easy to read, even by employees walking quickly by them. To increase relevancy, the posters should also carry your "branding," whether of the company or of your awareness campaign. The posters should be placed in the spaces your targeted audiences frequent: in respective departmental areas, at copy and fax

Consider these posters "drive by" billboards that will help drive home an attitude of security and/or privacy awareness with memorable images and tag lines.

machines, near shred bins, in lunch rooms, and conference rooms. Finally, they should be changed on a regular basis to keep the content fresh. The best awareness vendors will have both an arsenal of posters at their disposal and the ability to get them deployed quickly as the need arises (for example, if a new risk has emerged among your work force).

### *Articles*

One of the most cost-effective ways to keep your message fresh and in front of your employees is to provide relevant written content that is both interesting and personal. The content can be short sidebars or full articles within your company newsletter, regular email communication, or just presented as a page on any internal site employees visit. The most popular content typically addresses a personal benefit to the user, such as keeping the employee's children safe online or how to identify social media threats at home. While the concepts are typically similar to those covered in your initial awareness training, the personal perspective fosters an emotional connection with security awareness mindfulness, and thus reinforces it.

These articles can also be branded to integrate within your awareness campaign. Most awareness solution providers continuously monitor the threat landscape and should be well-positioned to source a stream of relevant "story-packaged" articles you can use in your reinforcement campaign. As with the other types of reinforcement content, a vendor with a library of pre-existing material will likely be the most cost effective.

## SUMMARY

Repetition is the mother of learning; a quote undoubtedly repeated in schools and colleges across the world. Though the source of that quote has been lost to history, it still rings true. In this chapter, we discussed the importance of establishing a strong training reinforcement campaign delivered in engaging and varied ways and provided concrete examples our clients have seen work. In our experience, the method of repetition can prove just as important as the content that is offered. Reinforcement is far more effective when it is delivered in different formats and through a variety of channels, providing a fresh experience of material that will be easily recalled.

# EPILOGUE: HOW YOU'LL KNOW IT WORKS

We started this guide by acknowledging you, as the person charged with running a security or privacy awareness program, have a tough job. Given that, we've tried to offer you some guidance on the nuts and bolts of setting up an awareness program that would bring about measurable results. The question that you should be asking right now is: how will you know that all this work made a difference? Let us conclude this book by identifying some of the results you should expect from a properly run awareness program.

You can appear before your executives with pride as you show them the measurable results of your work. You've got behavioral risk assessment scores that show your employees know way more than they used to, especially in the high risk areas you identified in your initial assessment. You've got evidence that your phishing program, which you've been running throughout the year, has directed targeted training to those who need it most, and that the majority of users have improved phishing detection over time. And you can clearly point to a roadmap that demonstrates the connection between the work you've done over the year and these results.

Numbers don't tell the whole story, however. You should also see a number of signs that the culture around data protection is changing. This may show itself as a decrease in employee complaints about having to take training, and a willingness to acknowledge that your training helped them understand why protecting information matters to the company. If training is optional, you may see that the rates of completion are much higher than before—and you can bet this is thanks to the support you've gotten from executives and management.

The most positive signs, however, may be really subtle. But you may notice, as you come into the office kitchen to get a cup of coffee, that your employees are talking about the latest humorous video you shared about tailgating. Or maybe they're discussing that really difficult simulated phishing email that most of your employees got right away. When your employees happily joke about data classifications, when they brag about the difficulty of their passwords, and when they argue about the right answer on the latest quiz you sent out, you will know that you have started to make real progress in creating a risk-aware culture in your organization.

## About MediaPRO

MediaPRO is nationally recognized for producing award-winning online training that reduces risk and improves end-user behaviors. Combine this training with our phishing, reinforcement, and assessment tools, and you've got an awareness program that meets your compliance requirements and safeguards business assets. MediaPRO's products are used by the most risk-aware companies in the world, have won more than 100 e-Learning awards, and have earned us a place as a Leader in Gartner's Magic Quadrant for Security Awareness Computer-Based Training.

**Find Out More About MediaPRO's Awareness Program Offerings**