MEASURING AWARENESS TRAINING SUCCESS:

7 METRICS THAT MATTER

MediaPRO
Cybersecurity & Privacy Education

MEASURING AWARENESS TRAINING SUCCESS

1 TRACKING BEHAVIOR

2 REPORTED INCIDENTS

3 PHISHING

4 REMEDIATION COSTS

5 EMPLOYEE ASSESSMENT

6 EMPLOYEE TRAINING

7 LISTEN TO EMPLOYEES

7 METRICS THAT MATTER

HOW TO SHOW YOUR AWARENESS INITIATIVE IS WORKING

As a security professional, proving the worth of the work you're doing can be a challenge.

Those tasked with managing awareness programs often ask the question: "How can we show that security and privacy awareness training is worth the money?"

Whether you're just starting your journey toward establishing an awareness initiative or looking to upgrade an existing program, setting measurable goals for behavioral improvements is crucial.

Either way, the stakes are high.

Lack of ROI for awareness training can lead to funding cuts when budget season rolls around.

Fortunately, there are clear ways to track effectiveness and set the stage for a successful awareness training initiative.

Here are seven metrics that help articulate the benefits of training to measure your hard work.

1. Tracking Risky Employee Behavior (With IT’s Help)

Chances are your IT department has systems in place to track employee behavior in the form of network event and data loss prevention logs. There are a variety of software programs that might be running behind the scenes of your corporate network, such as SIEM, DLP, or UEBA, that can aid in monitoring risky behavior.

HELPFUL PROGRAMS FOR TRACKING RISKY EMPLOYEE BEHAVIOR

SIEM

Security Information and Event Management systems collect network event logs, such as unsecure login attempts, virus scans, and other security-related documentation for analysis.

DLP

Data Loss Prevention software monitors the transmission of sensitive information to make sure an employee doesn’t send it to unauthorized destinations.

UEBA or UBA

User and Entity Behavioral Analytics tools are a way to parse information collected by SIEM and DLP systems and provide IT professionals prioritized trend information.

The information these systems collect can serve as a gauge for determining which employee behaviors are putting your organization at risk.

WHAT TO DO

Work with your IT team to set a baseline by logging risky events prior to your training event. A few months after your initiative starts, revisit these numbers to see if logged events have decreased.

2. How Often Incidents Are Reported

Though technology plays a key role in security programs, employees are vital to your company's information security posture. No network monitoring system can spot confidential information left by the printer or deter non-badged visitors from gaining access into a secure area. Your company should have procedures in place that allow employees to report suspicious incidents.

WHAT TO DO

Review the frequency of reported incidents before training begins. Check if these reports increase as training progresses and in the months following. More reported incidents mean your employees have developed sharper eyes for suspicious activity (not necessarily that more incidents are actually happening!).

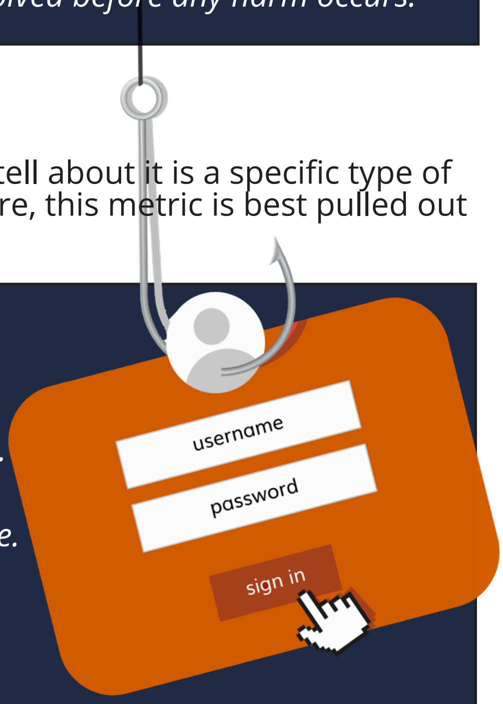
Consider combining this information with SIEM or DLP data to identify decreases in how long it takes for a security incident to be detected (called "time to detection"). Also, look for increases in the number or percentage of breaches detected and resolved before any harm occurs.

3. Reported Phishing Email Percentage

Spotting the dreaded phishing email and knowing who to tell about it is a specific type of incident reporting. But given how frequent these attacks are, this metric is best pulled out and recorded on its own.

WHAT TO DO

If your company has incident reporting procedures in place, how to report a suspected phishing email is likely one of them. Collect numbers on frequency of reported phishing emails vs. phishing emails not reported to develop a reported percentage. Clicked phishing emails should also be included in this initial data gathering to help set a baseline of your employee's proficiency with recognizing and correctly addressing this threat.



After your primary training has run its course, review these numbers to see how they changed. The goal is to see an increase in the percentage of phishing emails reported and a decrease in clicked phishing emails (ideally to zero!).

If you're deploying a simulated phishing tool as part of your awareness efforts, the metrics above still apply. Such a tool should provide a low-lift way of setting a baseline for phishing susceptibility before training by means of a simulated phishing campaign launched before training begins. After training has been delivered, run subsequent campaigns to see how employee behavior around phishing emails has improved.

4. How Much Incident Remediation Costs

No cybersecurity measure is 100% effective.

Chances are your organization has had a run-in with a data breach, malware infection, or another kind of cyber incident. Such an event may even be the reason you're in the market for security and privacy awareness training in the first place.

Typically, recovering from such an incident isn't cheap. In fact, the average total cost of a data breach is $3.92 million. Fortunately, independent research suggests an awareness training program significantly impacts the potential cost of recovering from an incident.

A commissioned study analyzing the ROI of MediaPRO's approach to awareness training found that organizations experienced fewer malware incidents when training employees with MediaPRO, leading to a $58,968 reduction in incident remediation costs. A separate PWC study found that companies that trained their employees spent 76% less on security incidents than companies that offered no training.

WHAT TO DO

If you have experienced a security incident, capture the cost of remediation and use it as a baseline before you launch your training initiative. Keep these figures in your back pocket in case another incident occurs and determine if training reduced overall incident remediation costs. However, the greatest return will be if you don't have any need for remediation because you've managed to avoid all security incidents!

5. Direct Assessment of Employee Knowledge

Assessing employee knowledge through surveys is a direct way to measure what they know about security and privacy best practices.

WHAT TO DO

In designing a survey, create questions that address your organization's most pressing security and privacy risks.

Connect with your HR department to help deploy your survey. HR may already use a survey tool for sending out surveys on employee benefits or other company-wide topics. Stick to 15 to 20 questions, with a 10-minute completion time for most employees. Deploy the survey at least twice: once before your initial training event and once after. The responses will tell you if your training stuck with your employees or if reinforcing materials (in the form of short videos, posters, or articles) are needed.

6. How Many Employees Complete Training

Training completion numbers become vital when compliance requirements come into play.

We're vehemently against the "check-the-box" approach to awareness training. But if you're in a specifically regulated industry (healthcare) or under the boot of regulations like the GDPR or CCPA (which require training), showing that your employees have taken training is vital.

WHAT TO DO

Any learning management system (LMS) worth its salt will be able to tell you how many employees have completed a given course in a specific timeframe. Though completion rates don't capture the impact of training, they are necessary to show the minimum goal of a training initiative is met.

7. Noting Employee Talk Around the Water Cooler

Beyond numbers-based metrics, consider assessing your employees from a "softer" point of view. Take time to understand if employee behavior change is occurring.

WHAT TO DO

Keep an ear open to discussions about your training topics before, during, and after your primary training deployment to see what conversations the content is generating.

You may notice that your employees are talking about one of the videos you shared during training. Or maybe they're discussing that particularly tricky phishing email that made its way to your marketing department.

When your employees happily joke about data classifications, brag about the difficulty of their passwords, or 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.

This is also an opportunity to gauge the quality of the training. Did that specific attempt at humor completely miss the mark? Was that physical security scenario too hokey? Keeping your ear tuned to discussions around the water cooler is a good way to find out.

BRINGING IT ALL TOGETHER

When evaluating the success of your program, it's important to remember to look at the metrics comprehensively.

Beware of falling into the trap of hyper-focusing on one metric. For instance, singling in on phishing catch rates will only result in employees who are adept at mitigating one threat. However, this will do little to support a comprehensive understanding of topics like identifying personal information or creating physical office security.

A comprehensive awareness program that addresses multiple risk factors deserves a comprehensive approach to tracking success. Fortunately, a multi-topic awareness initiative gives you the opportunity to do just that. The more topics you address, the more data points you can collect and analyze to see the impact of your awareness initiative. Additionally, continual data gathering will help you continue to evolve your program and address additional risks.

Since training should never be a one-and-done affair, keeping these assessment methods in mind when a training refresh or update is needed will allow you to alter your training program to address emerging risks.

One of the core elements of all of MediaPRO's TrainingPacks is the ability to monitor training effectiveness and prove compliance requirements.

Learn more about TrainingPacks by connecting with one of our experts.

SPEAK TO AN EXPERT