tracesecurity

Practical, worry-free cybersecurity.

WHITE PAPER

Building a Successful Security Training Program

How to Avoid a Training Rut

Stephen Wyles

TraceSecurity Information Security Analyst

Executive Summary

The number of scams and social engineering schemes employees can fall victim to is only limited by an attacker's imagination. Spoofing emails, domains, phone numbers, even live personalities are all very real and growing threats to organizations today.

Educating employees and ensuring their ability to identify potential attacks is the first line of defense when it comes to protecting an organization and its assets. But how can organizations ensure employees are prepared, regardless of the attack vector, and avoid a security training rut?

This white paper highlights potential downfalls when it comes to security training programs and strategies organizations can implement to ensure employees are not only educated about current threats but prepared to identify and respond to attacks.

Train in Context

Rut: (noun)
1. A long deep track made by the repeated passage of the wheels of vehicles.
2. A habit or pattern of behavior that has become dull and unproductive but is hard to change.

It is easy to inadvertently create a rut when conducting any repetitive task. Just as is the case with all training, when it comes to security, it is important to create and repeat training that keeps employees alert and aware of common tactics used by attackers to gain access to sensitive information, systems, or facilities. However, with many organizations consolidating responsibilities and eliminating resources, it can be difficult to create and maintain an effective security training program that provides a smooth path to employee awareness.

Drafting, editing, proofing, and finalizing a good training program is not only difficult but time-consuming. For Human Resources, this can be a "one-and-done" exercise that generates a solid regimen for protecting the organization from lawsuits. However, due to today's rapidly changing and advancing threat environment, security and technology-related training must continually evolve. Combine constant change with the imagination of a motivated attacker and the average person can quickly become overwhelmed trying to figure out how to effectively convey necessary information to employees.

How can we keep the good guys as motivated to develop reliable training programs as the bad guys are at devising new ways to circumvent security protocols? The attacker has no timeline, punch clock, or supervisor to reject their overtime request, essentially working without a budget. Unlike the attacker, your payroll is already bulging, and you most likely have limited resources available to oversee training initiatives. This leaves your organization with a weakened defense shield or one that focuses on past attack vectors as opposed to current threats, which just rolls out the red carpet for attackers.

If only your budget and time were as limitless and flexible as an attacker's. If only you had your own team of cyber engineers compiling training documentation and processes as creative as those malicious parties waiting to devour your assets with a single leaked password. All it takes is one sensitive piece of network information or a whispered password from an employee who was caught off guard by the kind, gentle, and thankful caller who was presumed safe, to expose your entire organization.

To be effective, your security training cannot stop at just one or even one dozen possible phishing scenarios your employees may face. It must be comprised of the current practices and mindset used by attackers to ensure your organization begins thinking about cybersecurity in a new way. It is important to remember that any and all pieces of personal and organizational information can be used by attackers to draft a script intended to engage employees and entice them to reveal small chunks of information that can lead to a larger pothole down the road.

Beginning with guesses, attackers will call your organization, without fear of failure, to eliminate options and drill down to specific content, eventually crafting a script that feels comfortable and familiar to the employee. Once the employee is at ease with the caller, they begin to reveal more and more information. Eventually, the attacker calls or walks into the facility as a known and trusted friend welcomed and invited into the headquarters of your organization with open arms. Gift wrapped assets and sensitive information will be waiting for them, handed over by the CEO or manager themselves, without even realizing they are under attack.

Consider the following scenario. An attacker begins calling your organization in an attempt to gather information. They have no idea your regular delivery man is going on vacation, but when your receptionist reveals this information during a phishing call, the attacker quickly modifies their plan of attack. The attacker had no intention of posing as a delivery man, but once the employee revealed that Frank, the normal delivery man, was going to be on vacation next month, an opportunity presented itself. For the next few weeks, the assailant watches the building looking for the delivery truck. Once it shows up, they quickly build a costume to resemble the delivery man and note the day and time each week deliveries arrive. The week of the alleged vacation, a message is sent to the manager from a spoofed email notifying him that "Johnny" will be filling in for Frank.

When "Johnny" arrives a few hours earlier than the normal delivery time, no one suspects a problem, especially when the name tag on the uniform says "Johnny." And if the delivery truck is a plain white van, he can explain that away too. Since "Johnny" does not know his way around, when questioned, he is able to justify why he is in the wrong part of the building. Meanwhile, the person who questioned him has no idea that "Johnny" just plugged a USB thumb drive containing small scripts into an unmanned computer, and he and his partners now have full access to that computer and potentially the entire network.

Perhaps your USB ports are blocked on all devices owned and operated by your organization. If this is the case, on his way out "Johnny" can easily drop a few USB thumb drives around the parking lot that are labeled with enticing words such as "Honeymoon Photos" or "Patent Ideas." An employee might take one home, plug it into their personal computer and after a few seconds, the attackers are logging every keystroke on the family laptop, gaining access to email accounts, your VPN, and maybe even company directories, all of which can help build on the attack or bust your security gates wide open.

Unfortunately, the threat of an attack does not stop when employees exit your building. It does not stop when they are on vacation or having dinner with friends. Social engineering attacks can happen anywhere at any time. Once your organization becomes a target, all of your employees become smaller, more vulnerable targets. An attacker will not only try to penetrate your firewall by hitting it with brute force, they will also target the weakest link and find a way around the firewall, as demonstrated above. This means they will test each and every employee to see who will unlock the door from the inside.

To combat this threat and ensure your security training progam covers a vast array of topics that continually evolve over time, try focusing on concepts as opposed to examples. Encourage employees to collaborate and use their imaginations and past experiences to identify and discuss potential vulnerabilities and attack scenarios. These scenarios can then be used to demonstrate how, when applied correctly, your policies and procedures protect employees, the organization, and sensitive data. Combining this strategy with current events and research enables you to implement a successful security training program that not only includes relevant topics, updated content, and scenarios that resonate with your employees but also results in improved behaviors and overall security posture.

Incident Reporting

Once your staff is successfully trained, tested, and retrained, they need a method for documenting questionable encounters and a notification process in the event they receive or click on a suspicious email. This can be tough to sell as it can be quite embarrassing for an individual to admit they fell victim to an attack. To ensure employees feel comfortable coming forward, consider adopting amnesty policies that afford first responders protection and anonymity when reporting an attack. After all, you should be concerned about avoiding future exploitation and recovering from the attack, not reprimanding employees.

Your reporting system does not need to be complex, it just needs to be secure and easy-to-use. Phone systems can be configured with a mailbox that can be used by employees to report potential attacks. Email addresses or text messaging systems can be installed that allow employees to quickly and easily communicate information using a mobile device or computer. These systems can then be set up to distribute notifications to your CTO, IT director, or the individual responsible for disseminating information regarding security-related incidents.

Incident Reporting

Regardless of size, no organization has the same amount of time, energy, or resources as an attacker. Your ability to invest in predicting and preventing attacks will always be outweighed by an attacker's desire to identify vulnerabilities and find new ways to exploit weaknesses. It is a never-ending battle. Continually updating your training program, educating your staff, allowing amnesty in communicating potential breaches, and publishing notification alerts can be challenging. But how difficult and expensive would it be to recover from a data breach? Proactive security training measures will keep your staff alert and save your organization from the fallout related to compromised systems or individuals.

By focusing on concepts and collaborating with employees to identify potential attack scenarios, you will create an engaging security training program. One that evolves over time, includes creative content and results in the ability to predict attack types and exploitable opportunities within your own environment.

Additionally, testing employees by simulating vishing (phone calls) and phishing (emails) attacks is essential and easy to do. When testing, don't be afraid of failure. Failed tests provide an opportunity to learn and expand security and defensive measures. They ensure your organization is testing outside the normal criteria and including all avenues of social engineering. Local visits by vendors, inspectors, or auditors are just as important as scheduled spam tests. Conducting spoofed email and caller ID tests are also important components of an overall security training program. Regular and ongoing testing is the best way to confirm your security training program is working and that your employees are aware of the threats that surround them.

Conclusion: Minimize Security Threats

NASCAR drivers use a simple maneuver to keep their tires warm and free from debris as they make the final pace laps before going full speed. They wiggle the steering wheel back and forth, and the cars zigzag, left and right, up and down the track. Collectively, they look like snakes in the grass. This same approach can be used to build an effective security training regimen. If you continue to follow the same path every time and fail to make adjustments, your organization will inevitably get stuck in a rut and be vulnerable to a method of attack your employees are neither expecting nor able to detect.

Continually work with employees to identify potential attack scenarios. Provide an easy way for employees to report incidents. Challenge yourself and your organization to be tested with the intention of failing. Allow third-party contractors to get creative with their testing methods and scenarios. The results will provide you with real-world examples, a baseline to expand content, and the ability to build and maintain a successful security training program that improves overall security posture.

About TraceSecurity

TraceSecurity is a leader in cybersecurity software and services that help organizations of all sizes reduce the risk of cyber breaches and demonstrate compliance. TraceSecurity offers a comprehensive portfolio of solutions that allow organizations to manage their information security program and supplement it with third-party validation and testing. TraceSecurity's suite of information security services includes but is not limited to IT risk assessments and audits, social engineering, penetration testing, and security training. TraceSecurity's award-winning TraceCSO is a revolutionary cloud-based solution that dramatically streamlines the management of IT governance, risk, and compliance (GRC) programs. It accomplishes this by tightly integrating and automating all eight critical IT GRC components: Risk Management, Compliance Management, Audit Management, Vendor Management, Incident Response Management, Vulnerability Management, Policy Management, and Training Management.

With market experience that spans over 2,000 customers, TraceSecurity offers the insight, products, professional services, and partners to support the security and risk management efforts of organizations across all industries.