**Four Common Mistakes in Employee Security Awareness Training**

*By Omer Taran*

For over a decade, I've been leading and developing content for security awareness training programs with various organizations. The type of training you might be familiar with, however, is likely not the kind I provide.

To understand why I've taken a different approach, it's important to take a hard look at the field.

Security awareness training has existed for decades—yet in all that time, it seems as if it hasn't reached the level of effectiveness we hoped for. Sure, today there is more of a focus on the need and various compliance demands to actually create effective programs. But the figures representing the blatant failure of our field are frightening: anywhere from 35% to 80% of security breaches start with some kind of employee involvement, usually with the employees being totally unaware of it.

Information security is a "wicked learning environment". Outside information security, employees' mistakes are evident—to them, to their customers, to their managers. Most employees work in a "kind learning environment," where facts are unambiguous and feedback is immediate enough to establish a connection between cause and effect.

This isn't the case in information security. A programmer creating faulty code or an employee clicking a fraudulent email usually will not receive any feedback from their peers, customers or the corporate IT staff, leading them to falsely assume they've made the right decisions.

How is this relevant to security awareness programs? **In order for security awareness programs to succeed, it is *not enough* to merely provide employees with information; we have to change their learning environment to support the development of an improved instinctive reaction to security threats.**

During the course of my work, I've seen many awareness programs and training solutions, most of which suffered from four common mistakes—mistakes that, if taken into consideration while creating the awareness program, could very well enhance its effectiveness and create better ROI for the organization.

1. **Singular events:** Most training programs focus on singular training events. Perhaps they're part of a security awareness week or even a month (if budget permits), but usually they fall into a standard bi-yearly training. If the CISO can manage it, they might provide some verbal training, which is less efficient, yet offers some engagement with employees. More often, the task would be left to some training video—an asynchronous method that leaves employees with the feeling that while information security is important, it's somehow not so relevant to their day-to-day operation. It also usually leaves employees with unanswered questions.

2. **Learning to swim from a textbook:** Knowledge can be divided into two types: declarative and procedural. Declarative is basically knowing the facts, such as being able to define symmetric encryption, malware or knowing the guidelines regarding taking work home. Procedural knowledge is the actionable knowhow: how to write a symmetric encryption algorithm, how to decide if a file is malware, and should I actually take my work home at this specific time—understanding security tradeoffs and potential compromises. Procedural knowledge is the knowledge we use when riding a bike or swimming in a pool. No one teaches that through computer-based training, and no one would board a plane where the pilot had only read the manual (and knows it by heart). Security decisions such as identifying a fraudulent email, handing out information over the phone or choosing a good password are all related to procedural knowledge, yet they are taught as if they were declarative knowledge. One can teach employees what fraud is, but identifying fraud as it happens is a totally different ballgame.

3. **Lack of feedback:** Turning a wicked learning environment into a kind learning environment requires supervisors to provide more feedback on daily tasks. This means going out of our way, abandoning training and embracing learning. There's a saying that "Training happens when it can, and learning when it's required" and it's logical to assume that in most corporate settings, training is a compromise between what is required (professionally or compliance-wise) and what is possible. Training only takes place when there's available time for employees, a trained instructor or when it's most convenient (via computer-based training, a vacant class, etc.) This has much to do with corporate needs; however, it does not transfer into learning.

Learning happens when an employee faces a challenge, resulting in a correct or incorrect action. Learning happens constantly, much more than formal training occurs, and if we wish to educate our employees, we need to tap into this natural learning cycle. Put into context within the corporate world, this means incorporating more and more exercises (creating the required challenges) and providing immediate and concrete feedback (creating a kind learning environment). It also means transforming our security audits into a learning and engagement tool which serves as a basis for employee feedback rather than scoring and benchmarking. Many CISOs use auditing; however, in order for an audit to act a learning tool, it should provide the audited person with immediate, clear and accurate feedback. For an employee to learn from a decision made, he or she will have to recall the precise situation that led to that particular decision, along with its specific nuances and stressors. As such, immediate feedback offers a better opportunity for employees to internalize the information.

4. **Repetitive training:** Think of driving, riding a bike, or even identifying malware. These are all tasks in which we always encounter new situations—none of which are exactly the same as the previous ones—and we must respond. Our minds develop a cognitive scheme that allows them to identify similarities within different data sets, and thus respond in a correct fashion.

Every corporate employee possesses cognitive schemes within their own profession—HR personnel can make quick and relatively accurate judgments on who might fit a given position, and finance personnel can identify financial irregularities easily—both tasks that security professionals might find difficult. Our minds create these cognitive schemes through the process of diverse exposure to different challenges and accompanying right and wrong solutions. As security experts, we don't feel or think about those cognitive schemes, but they are what drive our profession. *Yet we cannot teach them.* We can only create diverse training challenges and expose employees to various types of challenges so they will develop their own cognitive schemes.

For a training program to be truly effective—that is, to offer the highest level of protection to an organization—it requires the following aspects:

- The program has to be conducted year-round,
- It needs to be based upon exercises and challenges that utilize procedural knowledge,
- It must include immediate and concrete feedback,
- And it must use a combination of repetitive yet diverse scenarios.