Why Most Cyber Security Training Does Not Work by Joe Ferrara

There has been a lot of debate lately about whether cyber security training is worth the investment. To engage in this debate, it is important that all parties have a common definition of cyber security training. If we define cyber security training as the act of herding people into a classroom once a year (or upon hire) to sit through the boring, antiquated style of training session that emerged 15-20 years ago, then I would have to agree, don't bother with the investment. There are studies which prove this style of training does not work.

Unfortunately, as the rest of the cyber security industry has evolved, the basics of cyber security training have pretty much stayed the same. I have actually seen people using the same annual PowerPoint training material for 7+ years. This outdated model of training will not help defend a company against evolving cyber-attacks. But I have also seen companies achieve quantifiable results with new models of cyber security training that employ interactive software modules and games to engage users, coupled with simulated attacks to assess them.

I think it is more accurate to say that security professionals know that traditional training is not working, but they have not found other options. They either aren't willing to invest the time to update the content or aren't willing to invest money to change the training methods.

Why does most cyber security training fail today?

1) It is boring
2) It lacks user interaction and involvement
3) There is no measurement
4) We scare versus teach
5) Education is not a security team's core competency

However, based on our work with customers and extensive scientific research, security training does yield measurable results. Let us review in more detail why traditional training fails and how to approach it differently:

Make it Engaging: Traditional cyber security training is boring, out of context, and way too long! With today's attention deficient society, training has to evolve to be successful in reducing the threats for an organization. Many of today's training methods are not compelling to users and many times the content is so overwhelming that companies lose users a few minutes into the training session. They'll doze off, start checking their smartphone or politely zone out while looking attentive.

New methods of effective training can provide users with practical advice in a topically focused software-based training session that takes less than 10 minutes.

Involve the User: In addition to being boring, there is limited chance for users to interact and actually practice what they learn. Now, I am not talking about a quiz. Quizzes do not teach, they test. Answering quiz questions out of context should not be confused with practice. Practice helps users put concepts to use so they learn the right behaviors. We all know the scenario . . .you start the video at your desk, and then go about doing your other day-to-day business. At the end of the video, you guess your way through a few questions, hit enter and hope for the best. If you are a good guesser . . .Viola! . . . you get your shiny new certificate of completion and the security team can put a check mark on their annual objectives. But was anything learned?

Instead, cutting edge training deploys interactive techniques where users are asked to practice concepts as they learn them, thereby engaging the user and enforcing learning as they go. For example, employees can complete their session by making decisions in a variety of security scenarios to apply what they have just learned, thereby increasing learning retention.

Measure Success: If you do not measure, how do you know if you are being successful? What valuable data did you collect in the process? Was it actionable? The goal of security training has been to "check

the box" whether for an audit, compliance reasons, or to show to your managers that you are doing your job. Successful training needs to be measured and provide actionable data about the strengths and weaknesses in your organization. Anything less is a waste of time.
Effective training collects user interaction and data throughout the training to give security professionals intelligence on individual employee, as well as aggregate, strengths and weaknesses in their organization. This data also helps to show improved knowledge over time.

Enlighten, do not Scare: For some reason, we have come to believe that we need to scare people to get them to act differently. The problem is that by scaring workers we are impacting their ability to get their jobs done. They become afraid to open emails, to access systems, and to do their daily jobs. Yes, training needs to break through, but paralyzing an organization in fear is counter-productive. Instead, good training has the potential to empower employees to take full advantage of the Internet's benefits while protecting themselves and their employers from potential security breaches.

Use Learning Science Principles: If you are a hacker, are you automatically an effective teacher? If you know the technology and all of its weaknesses, then it seems reasonable you should be able to teach the same information to employees, right? Possibly, but not likely. If you ask a bunch of hackers whether training is working, what answer do you expect to get? Everyone has strengths and weaknesses, but generally, hackers do not make good educators and technologists are better off making technology decisions.

If companies want to see results with cyber security training, a shift in mindset is required. the science of learning dates to the early 1950s, and its techniques have been proven over time and adopted as accepted learning principles. Applied to information security training, these techniques can provide immediate, tangible, long-term results in educating employees and improving your company's overall security posture. Let us conduct training based on how people learn versus treating training as a check-box activity, and we'll see just how valuable an investment in security training can be.

In the words of Einstein, "Insanity is doing the same thing over and over again and expecting different results." Thankfully, when it comes to cyber security training it is possible to stay sane by embracing the advances in security training which are available today.

About the Author

Joe Ferrara is the President and CEO of Wombat Security Technologies, a leading security awareness training and assessment company. Joe has provided expert commentary and has spoken at numerous information security industry events including the CISO Executive Network forum, and ISSA International and regional conferences.