# Why Customized Cybersecurity Training is Essential

**If you asked your employees to define “cybersecurity,” what would they say?**

July 1, 2014

If you asked your employees to define “cybersecurity,” what would they say? In many organizations, the answer may include: “It’s about firewalls and patches and other ‘tech stuff’ that keeps my work computer from getting hacked.” It’s highly unlikely that anyone would say “Cybersecurity starts with us.” That’s according to **Jerry Kruczek**, a Vice President at Foreground Security, responsible for customer training programs.

“The security of the apps, data and information within your enterprise is only as strong as the weakest link in that chain,” he says. “Yet, ironically, as professionals outside of the tech department have grown increasingly sophisticated in their consumer-driven knowledge about technology, they’re lapsing into practices that invite serious risks. They can pretty much get whatever they want out in cyberspace, and they’re more than eager to do it on the devices they use for work,” he says. “Well-conceived policies and enforcement certainly serve a vital function. But these measures can’t cover every conceivable scenario. With a formal training program in place, however, users can understand how their actions can potentially expose themselves and the organization to a wide variety of evil actors, and how some simple steps can protect them.”

According to research from Verizon, because of ill-conceived practices, nearly one-fifth of network threats over the last decade have been linked to inside users. What are the leading contributing factors?

First is unintended compromise. Users click on links they shouldn’t click. They keep sensitive data on their unsecured smartphones and tablets while they work at the local Starbucks.

Second is lack of password accountability. We depend upon so many passwords to get us through the day. Some of them are subject to rigorous oversight, such as email accounts, which mandate the changing of a password every 60 days and/or the use of various numbers, characters, capitalization, etc. But employees go to plenty of other password-protected places where the “rules” aren’t nearly as demanding. And these employees will often take a “path of least resistance” by not following proper password practices. Finally, they use the same passwords on their secure corporate systems and easily-exploited casual sites.

Third is password sharing, where an employee allows a colleague or contractor to borrow a password, and the subsequent “keys to the kingdom.”

Last is uncertainties about incident response. You'd be surprised at the number of users who don't know what to do once they see something suspicious.

There are many training companies out there, each one claiming to be the choice. So what do you look for in a training provider?

There are three must-have qualities. First is customized session content. If you sense that the provider can offer nothing more than a "check the box," one-size-fits-all program, then you should look elsewhere. The materials will merely scratch the surface with respect to what they need to know, with a generic presentation. Yet, the training will never speak to your organization's specific circumstances, roles, day-to-day situations and industry. As a result, the users won't really connect with the training and won't change their behaviors.

Second is customized delivery. This refers to the format of the training, and there is no "right" or "wrong" answer. Your company size, geographic location(s), industry and the experience levels of the participating employees should determine the format. Don't let a provider saddle you with strictly one choice. That's not good enough. Your provider has to accommodate all preferences.

Third is a lasting presence. What happens after the training provider "leaves the building?" Will there be any follow-up? Were any materials left behind? What will the provider do to ensure all of the awareness acquired doesn't fade over a short period of time? Will the training help the users decide what to do the next time they see a possible security incident?

What you're seeking is residual value. Does the provider distribute a post-session survey to evaluate what participants have learned and assess how to fill in remaining awareness gaps in a future presentation? Will they return for the training of new hires at some point in the future? Do they have printed and/or electronic materials to distribute to attendees, so they will always have reference points for guidance? And what about their capability to build a "cybersecurity presence" in your office, in the form of, say, posters to remind them of the core takeaways, thus building a culture of enterprise-wide security awareness?

By screening a provider for these qualities, you'll accomplish much more than a manager who simply wants to "check the box" and get it over with. You'll walk away knowing participants are getting the training that's right for them, not an endless sea of faceless masses. You'll gain confidence that your organization is now better positioned to compete within its specific industry while greatly reducing the risk of network threats. This is when you can conclude with conviction that you've completely addressed what could be the cornerstone of your cybersecurity program: verified user participation in the security process.