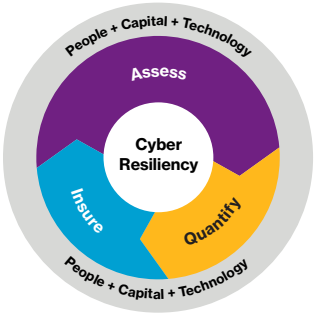

Decode human threat.

4 Essentials for effective security awareness training

Reprinted with permission from SecurityIntelligence

Educating employees on security is more crucial than ever. Willis Towers Watson claims data points to internal employees – whether through negligence or deliberate offense – as the cause of 66 percent of all cyber breaches. Figures like this are prompting security managers to put more resources into security awareness training.

The path to effective security awareness training

When the Financial Services Information Sharing and Analysis Center (FS-ISAC) reached out to security managers about cyberdefense for its 2018 CISO Cybersecurity Trends report, 35 percent said they consider employee training a critically high priority for improving security posture. While awareness training is indeed not a new concept, gone are the days when merely giving employees a series of videos to watch was considered sufficient – especially in the absence of any follow-up measures.

Security awareness training programs need to be interesting, engaging and memorable to be effective, said Lisa Plaggemier, director of security culture and client advocacy at CDK Global. Plaggemier believes the entire concept of awareness programs needs a revamp. (She even gave a talk on the subject, Let's Blow Up Security Awareness and Start Over, at the 2018 RSA Conference.)

"As far as what is not working – no offense – to my technical friends – but I think we are hiring the wrong skill set for this position," said Plaggemier. "We're hiring people without the right skill set to be good communicators. I think we need more people who have had experience with selling something. We are trying to influence behavior, and that requires being able to get buy-in from employees."

What are the essential ingredients for a successful security awareness program? The experts we interviewed had four key recommendations.

Use real-life hacking and phishing examples

"Nobody likes to sit in front of a computer where the speaker does all of the talking. They will be bored easily," said Aleksandr Yampolskiy, CEO and co-founder of Security Scorecard. "The best presentations show concrete examples. When we conduct training here, I will pull up a website and then show up some tools hackers can use to hack a computer. I always show examples of how they can be phished, and I play a video recording where I show how people try and phish me."

Willis Towers Watson

Create engaging security training programs

"Before you can get into tactics, you need good creative," said Plaggemier. "You need a good character. Something that's funny or interesting." At CDK Global, Plaggemier relies on an ad agency with great writers to craft compelling awareness programs.

Yampolskiy has experimented with gamification around awareness lessons at previous organizations where he has run awareness programs. "We bought two iPads and encouraged people to try and hack the company," he said. "People got creative and would call and pretend to be IT, among other things. This kind of competition resulted in amazing findings that professional demonstrators never discovered." Yampolskiy said the winner of the competition was titled the company's security champion and received a plaque from the CEO, which got people excited about the training.

Adjust your approach: No one cares

"In awareness, we suffer from the curse of passion," said Plaggemier. "You presume your audience has a certain level of knowledge. I've met so many people in security, they want to help everyone. They are really passionate about it, and they presume that the audience cares too. But that's just not the case. You need to start every awareness campaign with this premise that no one cares."

This brings us back to that hook that draws the audience in that we mentioned earlier: It needs to be funny, interesting and engaging to get them to care in the first place, said Plaggemier. "You can use humor, you can – but you have to start with the premise that no one cares in order to see some success," she said.

Enlist top-down support

Building any culture starts by example, said Yampolskiy. "You need buy-in from the CFO, from general counsel. If they lead by example, people will copy that behavior and know that gets rewarded. People look at who is being commended," he said. The push for significant change should come from the top – otherwise, there may be less potential to create a culture of cyber awareness.

"CISOs [chief information security officers] need to get everyone on board with doing something different," said Plaggemier. "If you're going to get everyone's attention, you need to get everyone on board at the outset."