# End users must be part of cybersecurity solutions

RELATED

-

Credit: Thinkstock

It's time to stop blaming employees and enlist their help.

NetworkWorld | Jun 24, 2014 8:41 AM

As the old infosec adage goes, "people are the weakest link in the cybersecurity chain." Clearly, enterprise security professionals agree with this statement. In a recent ESG research survey, enterprise security professionals were asked to identify the factors most responsible for successful malware attacks. It turns out that 58% point to "a lack of user knowledge about cybersecurity risks" – the most popular answer by far *(note: I am an employee of ESG)*.

This data is not unusual; security professionals often bemoan end-user cybersecurity behavior. They don't pay attention in training classes, they click on suspect links, they are easily fooled by social engineering tactics, etc.

Yup, naïve employees are certainly part of the problem, but here's a news flash – that's not going to change. Cybersecurity threats evolve rapidly, so much so that many infosec professionals can't keep up. Given this, how can we expect any more from employees?

It's time to take a realistic and pragmatic approach to employees and cybersecurity. How? Based on my discussions with numerous CISOs, best practices in this area include:

1. **Awareness programs.** I've found that these programs include some basic training combined with ongoing awareness campaigns. Oh, and successful awareness campaigns combine education, communications, cheerleading, entertainment, and perhaps even some incentives. So cybersecurity messages and posters may be combined with a funny video featuring the CEO getting scammed by emails from the Central Bank of Nigeria. CISOs say keep all communications high-level and clear to avoid alienating employees with constant geek-speak.
2. **Leadership.** The CISO may be responsible for cybersecurity, but he or she should not be the face of end-user awareness programs. Rather, the CEO and business managers must take the lead here. The goal? Communicate to the troops that online behavior is as important as any other work-related task, such as arriving on time, treating others with respect, and meeting deadlines. In other words, business leaders must strive to make cybersecurity awareness and good online behavior part of the corporate culture.
3. **Notifying end users of policy violations.** Some security tools frustrate employees by blocking their actions without further explanation. In many cases, this is frustrating to employees who may not understand why they were prevented from doing their jobs. Rather than blindly enforcing policies, progressive companies also use electronic notifications to educate employees as to why their actions were blocked in the first place. For example, an employee may not realize that the file they were trying to email contained healthcare records or other regulated data. CISOs tell me that providing this kind of simple explanation can actually decrease the volume of policy violations by up to 90%.
4. **Proactive spear phishing.** This tactic involves sending bogus but authentic-looking emails to internal employees to see if they actively click on links, install software, or open attachments. On average, somewhere between one-third and half of employees will do so. Rather than compromise internal employee systems however, organizations use this as a "teachable moment" by sending the employee a notification of what just happened and reminding them about good online hygiene. While success metrics are hard to come by, anecdotal evidence seems to indicate that internal spear phishing can lead to improvements in user education and behavior.
5. **End-user feedback.** If employees are expected to become good cybersecurity citizens, then the security team should keep them up to date on how they are doing. Measureable

improvements should come with some type of “that-a-boy” message from the CEO or token reward from the company.

When I started my career at EMC back in the late 1980s, then CEO Dick Egan used to say “sales is part of everyone’s job description.” Enterprise organizations need to communicate a similar message with regard to cybersecurity and back this up with a commitment to continuous education, cultural changes, the right tools and awareness campaigns, a team approach, and a little bit of show biz.