**Suggested Title: Security Awareness Training – Time to Jump on the Bandwagon**

****

Human-error; we talk about it all the time, but what exactly do we mean? Human-error occurs when an individual performs a task or does something with an unintended outcome. It’s easy to point the finger at employee’s as being an organization’s weakest link, but without appropriate security awareness training provided by the employer, how can employees truly know what to watch out for?

An IBM study found that human-error accounts for 95% of security incidents, yet security awareness training for employees often ends up on the back burner.

In a recent [survey](https://www.welivesecurity.com/2018/05/21/cybersecurity-training-still-neglected/) by ESET, we learned that cybersecurity training is not a top priority for many organizations, with 33.3% of employees feeling that their employer has provided them with absolutely none. Only 17.9% of survey respondents felt their employers were providing them with “A lot” of cybersecurity training.

With the need for security training clear, even the most surprising organizations are jumping on the bandwagon, offering security awareness training as part of their services.

Since security incidents are often a result of employee mistakes, it is evident that technology alone is not enough to protect an organization. While antivirus (AV) companies may have previously found success in offering their virus protection services alone, the realization that employees are an organization’s weakest link has led many AV vendors to one conclusion: to be successful and provide services that can truly defend against cybercrime, providing education through security awareness training is key.

Educating employees on security awareness is crucial to organizations, especially those with sensitive data, so why is the AV industry just recently making a push to offer this service? Cybercriminals are relentless in their efforts to carry out their attacks, and while AV companies have historically been embarrassed to admit their products are not the catch-all for fighting cybercrime, they have since recognized that these criminals are becoming more sophisticated in their attempts. In the digital era, criminals have become masterminds at forming social engineering attacks to trick their victims, a scheme that no antivirus can protect against.

In addition, a fierce competition and the desire to generate more revenue could be contributing factors. With free AV software that provides enough coverage for organizations to feel protected, they may look to use those funds in other areas to defend themselves.

AV does play a crucial role in defending an organization, but it’s important to remember that a layered security strategy is necessary for adequate protection.  We must not forget that without appropriate training provided by organizations, employees cannot effectively act as that first layer of defense.

Security awareness training will certainly help employees learn how to spot malicious attempts by cybercriminals, but it is also required to comply with federal and in some cases state regulations. A lack of training will open the door for cybercriminals and may result in a breach, causing potentially significant fines and penalties as well as likely damage to an organization’s reputation.

The time is now to jump on the security awareness training bandwagon! After all, employees can’t help defend against cybercrime if they aren’t provided with the necessary tools to do so.