protect it. While most wish there was a magic bullet that would guarantee 100% ...

Jim Boomer • Aug. 31, 2016

Security continues to be a top priority for firms today. Clients trust CPAs with some of their most sensitive data and it's our responsibility to do everything possible to protect it. While most wish there was a magic bullet that would guarantee 100% security and keep the bad guys out, the reality of today's environment makes that notion unrealistic. The fact remains that even if we do everything possible to try to eliminate security risk we are only as strong as the savviness of our people.

public sites and social media? If not, your firm needs to invest in security awareness training for your entire team. But where do you start?

Where to Start

The first step is determining where you are today. To do so, you probably need to bring in an outside party to perform a security assessment that includes penetration testing, social engineering and a complete review of your security infrastructure, as well as your team's knowledge.

Many of the firms we work with have had an assessment done in the last few years and the results have identified vulnerabilities that were previously blind spots. While some were the result of inadequate technology, the majority were caused by the human factor.

Training the Front Lines

The only way to mitigate against the risks of uninformed and careless individuals is to provide them with ongoing security awareness training. Although programs may vary, here are some of the key characteristics you should keep in mind.

- **Include Everyone** – Security awareness training applies to everyone in the firm. Leadership should not be excluded. In fact, top level executives are some of the most vulnerable individuals. Criminals have become more sophisticated and regularly target those who have access to the most sensitive and valuable information.
- **Link it to Their Personal Lives** – Most, if not all, of the best practices apply to your employee's behavior in both their professional and personal lives. The more you can show how it impacts them individually through personal examples, the better it will stick.

- **Protect People from Themselves** – The more IT can do at the desktop level to not

Risk Based Approach

Gartner lists Adaptive Security Architecture in its Top 10 Strategic Technology Trends for 2016 and states, "Relying on perimeter defense and rule-based security is inadequate. IT leaders must focus on detecting and responding to threats, as well as more traditional blocking and other measures to prevent attacks." This indicates we need to think differently about security than we have in the past. Traditionally, organizations have spent the majority of the security budget on eliminating risk. In today's environment, you must balance your resources between proactive prevention and reactive response. In other words, we must view security from a risk management perspective rather than risk elimination.

Conclusion

If you are currently relying on technology alone to prevent cyber-attacks, you are likely exposing your firm and clients to unnecessary risk. Make sure you address the weakest link in most organizations – the people. Educating them on the best practices and proper behaviors is the best way to protect yourself against the bad guys. At the same time, invest appropriate resources to prepare your firm to respond to a security event. Start the journey today to make your firm more security savvy.

Firm Management • Security • Technology