INTERACTIVE SECURITY

BUILDING A SECURITY AWARENESS PROGRAM: *It's not wise to assume that employees know even the most basic tenets of cybersecurity*

To prepare employees for a sophisticated cyberattack, a cybersecurity professional is needed who understands that security requires a proactive approach and is always current on all the latest tactics of cybercriminals.

Author: Shawn Corrigan
President / Managing Partner
Interactive Security
www.intactsec.com
267.824.2500

Today's business leaders may believe their company is too small to be concerned with cybersecurity awareness, or for that matter cybersecurity at all, because cybercriminals wouldn't waste their time targeting a small to medium sized business. "There's not enough for them to steal to justify the risk of getting caught", some may think.

Unfortunately, that train of thought is *dead wrong*!

All Businesses Need an Effective Security Awareness Program

According to Symantec, 43 percent of cybercriminals do indeed target small businesses. This is largely because smaller companies are typically unprepared to combat cyberthreats and less likely to pursue the attacker. And since, according to the same Symantec data, 55 percent of all cyberattacks directly target company employees, a company-wide security awareness program is crucial for modern business survival, regardless of company size.

Don't Leave Security Awareness Only in Your IT Team's Hands

It is not prudent to simply depend on an Information Technology (IT) team— whether inhouse or outsourced—to set up a cybersecurity program. While they're likely experts in the technical nuance of a smoothly running IT system, they are not dedicated security experts. In fact, security is often a side project for many IT teams and thus becomes only a reactive afterthought. To prepare employees for a sophisticated cyberattack, a cybersecurity professional is needed who understands that security requires a proactive approach and is always abreast of all the latest tactics cybercriminals use to steal confidential customer information and money.

The Best Solution: A Comprehensive Security Training Program for All Workers

With the help and guidance of an expert cybersecurity partner, it is a common best practice to setup a formal program to educate your employees about cybersecurity. It is not wise to assume that they know even the most basic tenets of online security. Employees may be highly skilled at what they do but may be unaware of the huge number of cyberthreats that face them every day at the workplace.

A security awareness program covers two main aspects of cybersecurity: Corporate Policies (which need to be updated frequently with the advice of security awareness consultant) and the Procedures that should be followed when working with any type of digital device, be it mobile or desktop.

The Key Ingredients in Your Business's Security Awareness Program

It's important to make sure client corporate policies are correct and current, so they can then be appropriately incorporated into the security awareness training program. This is not a one-size-fits-all program but rather should be tailored to the unique needs of each business.

As a first step, employees should be taught that data itself is often the lifeblood of a company and thus one of the company's most valuable assets. Many employees only regard financial data as valuable. In fact, customers' confidential information—even such mundane facts as their names and phone numbers--may be the most valuable

data cybercriminals can steal. It's important to teach the "why" as well as the "how," so employees are empowered to think on their feet when it comes to guarding data.

Next, its key to educate employees about the warning signs of a cybersecurity threat. They need to be informed on the chain of command: who they should contact if they believe they've found a security threat—and how quickly they need to report it. When it comes to cybersecurity, it's better to lose a few minutes work on a false alarm than to ignore subtle signs and risk a full-scale attack.

It's advisable to hold employee training sessions on a regular basis. This not only updates employees on new threats and tactics, but also provides an opportunity for new employees to get up to speed on the company's security protocols. Each employee needs to understand that security is ultimately everyone's responsibility.

Frequent training sessions are especially essential for organizations with high employee turnover rates. In fact, security training should play a major role in the company onboarding process for even temporary or contract workers. Keeping new personnel alert about security challenges is a key ingredient in avoiding most problems since human error accounts for over half of most companies' problems, according to IBM's SecurityIntelligence.com.

Furthermore, no one likes to think about insider threats—security breaches caused by dishonest employees—but they do happen. Employees need to be educated so they can recognize the signs of insider data breaches and how to properly report suspicious activity. Since these matters are highly sensitive, management personnel should be trained on proper protocols to follow during an investigation.

Finally, it's critical to measure how effectively a security awareness program is performing. The most simple and effective way to measure performance is to measure trends and look for a downward trend in the number of incidents a company experiences over time.

Proactive is always better than reactive. So now is the time to act—not after an incident occurs. To discuss setting up a cybersecurity security awareness program, contact the security experts at Interactive Security today.

About Interactive Security

Since 2007 Interactive Security, Inc. has been at the forefront of providing industry leading expert information technology security services to clients across the globe - focused on IT Security Auditing & Compliance.

Our team is comprised of highly skilled industry certified professionals with diverse experience serving technology consulting firms and enterprise security departments. We serve a broad base of clients and industries including the payment card industry, finance, legal, healthcare, education, government, restaurant and hospitality.

Our clients and partners choose Interactive Security because of our uncommon ability to provide expert custom IT security services that exceed both technical and business expectations.

We pride ourselves on Making ***IT COMPLIANCE OBTAINABLE, SIMPLE AND AFFORDABLE.***

*Vulnerability / Penetration Assessments * Application Security * BCP/DR Planning * PCI DSS * HIPAA * HiTRUST * ISO 27001-27002 * ISO 31000 * NACHA ACH * FEDRAMP * FISMA/NIST * GDPR * Privacy Shield*