KEY ASPECTS OF CYBERSECURITY AWARENESS TRAINING

By: Kevin M. Gold, Esq.

The familiar refrain in the cybersecurity world is not if a company will be hacked, but when. One of the more effective ways to delay this unfortunate inevitability is to implement a strong employee cybersecurity awareness training program.

While there is much written about the need for effective training, there is often little practical guidance offered on the key topics for such training. Since so many breaches and incidents are caused by human error, developing an effective cybersecurity awareness program is a key tool for financial institutions to mitigate risk. This article will briefly explore some of the key areas to include in a cybersecurity awareness training program and offer some best practices.

PROTECTING SENSITIVE DATA

All employees must protect sensitive data and files. Securely storing this information is an important step that should include a secure physical environment. Further, a bank should describe in a written policy the types of devices on which data and files may be stored and require that they be encrypted when stored or used on any mobile device.

Personal computers and laptops should be locked when unattended and should automatically be set to lock after a set period of inactivity, such as 10 or 15 minutes. A password should be required to log back into the system.

PASSWORD STANDARDS

Strong passwords are another simple but effective method of security. Requiring passwords that have upper case, lower case, numeric and non-alphabetic characters and at least 8 characters is key. In addition, passwords should be changed frequently, such as every 60-90 days, and should not be repeated. In addition, it is a good practice to use different passwords for different sites and to avoid repeating passwords.

Users should be cautioned not to share their passwords with anyone or write them down and keep them in plain sight. Computers should automatically lock after a reasonable number of password attempts and users should be instructed not to configure their browser to automatically remember and save passwords.

SECURITY UPDATES

Another effective strategy to protect valuable computers and information is to force automatic security updates and patches. Policies should require employees to regularly and consistently update their computers and their operating systems. Further, security and ant-virus software that can scan email, attachments, downloads, webpages, etc. should be installed and configured to perform regular scans when a computer is started and at shut down, at a minimum. Some security and anti-virus software can even provide real-time protection.

EMAIL

An employee's email account is one of the key areas of vulnerability and demands significant training attention. The number and frequency of threats directed via an employee's inbox continues to expand. The goal of a malicious email is to get the reader to click on something, whether it be an attachment, photograph or a website link.

Training here can go a long way in preventing issues. Having paranoid and skeptical employees is particularly valuable when it comes to email. For example, employees should pause and think about any attachments or links in an email and evaluate them carefully before opening or clicking. If a user cannot identify the source of the email, or if it looks suspicious or unusual, they should be instructed not to open the attachment or click the link.

Banking institutions are particularly vulnerable here, as there are a growing number of email fraud schemes in which the goal is to deceive a financial institution into making illegitimate wire transfers.

INTERNET

In the same way that employees should think carefully and suspiciously about emails that they open, the same goes for websites on the Internet. Here, the threats come from malicious links that can direct a user to a malicious program or risky websites. Employees should learn to carefully consider a link before clicking on it. A good strategy here is to train an employee to hover over a link with a mouse to see the website that the link directs to and whether it appears to be trustworthy or familiar. Unfortunately, the growth of social media websites has only compounded the problem, as they can make clicking on videos, pictures and the like more appealing.

The cybersecurity risks that exist in today's work environment are numerous and growing. Banks and financial institutions would be wise to keep up with these threats and regularly train employees in these and other areas to mitigate the growing risk to sensitive data and files.

KEVIN GOLD IS AN ATTORNEY WITH PILLAR + AUGHT.
HE CAN BE REACHED AT 717.308.9626 OR KGOLD@PILLARAUGHT.COM.

PILLAR + AUGHT IS AN ASSOCIATE MEMBER OF PACB.