CORE COMPLIANCE & LEGAL SERVICES, INC.

CCLS Risk Management Update
May 2017

COMPLIANCE PROTOCOLS FOR DEALING WITH CURRENT CYBERCRIMES

According to a Data Breach Investigations Report published by Verizon in 2016,[1] there has been a definite upward trend in the number of people clicking on "phishing" emails since 2014. Phishing is a type of social engineering used by hackers to trick people into introducing a virus into their computer or revealing confidential information.

This month's Risk Management Update ("RMU") discusses some recent phishing expeditions and provides steps firms can take to help protect themselves against these threats. In an effort to provide practical and actionable guidance, this RMU references certain products and vendors; however, these are provided as suggestions only and should not be considered specific recommendations.

Examples of Phishing Attacks

Approximately 70% of cyber-breaches entail a compromised user. Unfortunately, hackers are getting very sophisticated. Below are three examples of current phishing scams that have trapped a high percentage of victims.

Example #1 – Phishing

An employee receives the following email, which appears to have come from an HR officer:

> *"It has been brought to our attention there was a problem with ADP that may have affected your 2016 W-2 form. Please read the attached memo and notify me if you have been impacted."*
>
> The employee clicks on the attachment, which reads:
>
> *"Please check your December 29, 2016 pay stub and reconcile the figures with your 2016 Form W-2. If the numbers match, you do not need to take any further action. However, if there are any discrepancies please notify HR and we will issue a corrected 2016 Form W-2."*

Of course, the pay stub and W-2 match, but the attachment contained a virus so the employee's computer and possibly the firm's network has been infected.

Example #2 – Whaling

All employees (except the CEO) receive the following email, which appears to have come from the firm's CEO:

> *"One of our largest clients is opening a Pizza Hut within walking distance of our office at 123 S. California Blvd. The owner wants to give each employee a free medium pizza! Please click on the button below to download your coupon for the free pizza, and please spread the word to support our valued client."*

---

[1] *See* http://www.verizonenterprise.com/resources/reports/rp_DBIR_2016_Report_en_xg.pdf.

The email has all of the Pizza Hut branding and that free pizza button looks inviting, but clicking on the button reveals an error message that reads "HTTP 404 – File Not Found," and a virus is deposited into the computer.

Example #3 – Spear Phishing

A firm has posted job descriptions on several bulletin boards stating interested parties should send a resume to humanresources@abc-company.com. A hacker trolls for companies that have posted job descriptions and attempts to "spear phish" the HR person by sending an email with a fake resume attached. Everything looks normal, and since the HR person is expecting to receive resumes, nothing appears suspicious. However, the resume has a virus attached that activates when the resume is opened.

Compliance Protocols Geared for Prevention

User Awareness Training

Knowledge is power, so it's important to continually train employees on current types of threats and what can be done to prevent cyberattacks. Below are some tips for identifying phishing emails:

1. Check the URL address to help determine legitimacy
2. Confirm the domain name in the sender email address appears correct
3. Check the content of the email (if viewable without opening) –
    a. Does it appear to be something that would normally sent from the sender?
    b. Does it contain any misspelled words?
    c. Is it asking for confidential information?
    d. Does it require opening a link or attachment?
4. Don't click on links or attachments if emails contain threats
5. Be alert and never trust without obtaining verification

Implement Phishing Simulations

Simulated phishing emails, which track who opens the email and who clicks on the associated link or attachment, can be sent periodically to employees. For this type of training to be effective, employees should not be informed of the simulated emails, and those who open the emails should receive a short, mandatory training session.

Phishing simulations and the subsequent training help to reduce the "click" rate. In addition, this improvement is measurable and documented.

Suggested Vendors: InfoSec Institute (www.infosecinstitute.com**)** and KnowBe4 (www.knowbe4.com) offer various user awareness training tools and educational services.

Two-Factor Authentication ("2FA")

Cybersecurity is a regime to prevent unauthorized access. The primary mode of authentication is a username and password, and misappropriating these credentials is one of the most common ways to breach a network.

2FA is an internal control that greatly enhances security by requiring a second form of identification in addition to the username and password. Examples of 2FA are answering challenge questions, recognizing chosen images on a website, SMS text message tokens (a six-digit one-time code that must be entered), and fobs that generate security codes.

2FA is becoming standard. In 2016, in the wake of the highly publicized breach of a government employee database, President Obama mandated 2FA for all government agencies. In addition, banks are required to use 2FA, and a number of popular websites and services have chosen to offer 2FA, including Microsoft Office 365, Amazon, Facebook, and Gmail. The capability is there. Users simply need to enable the additional security. 2FA is economical and can be very effective in preventing unauthorized access.

Suggested Vendors: RSA (www.rsa.com**)** and Yubico (www.yubico.com) offer a variety of 2FA products and services.

Endpoint Monitoring and Protection

Each electronic device that connects to a firm's network is an "endpoint," which needs to be protected. The endpoint device could be a mobile device, laptop computer, home computer, and/or workstation in the office. Endpoint monitoring allows a firm to oversee network access activity in real time and, in some cases, prevent attempted cyberattacks.

Suggested Vendors: Entreda (www.entreda.com**)** and Symantec (www.symantec.com) offer endpoint monitoring products.

Conclusion

Maintaining a strong cybersecurity program is a daunting task for firms given the barrage of cyberattacks that continue to undermine reasonable efforts. Compliance personnel need to work closely with IT personnel to help ensure adequate protections are in place. Risk assessments should be performed annually and ongoing employee training is a must. It's also very important that senior management ensures adequate resources continue to be allocated to the firm's cybersecurity program.

CCLS cybersecurity service offerings include performing risk assessments, providing employee training, and drafting cybersecurity policies and procedures. We also offer a six-point Cybersecurity Program package. For assistance or more information, please contact us at (619) 278-0020, info@corecls.com, or visit www.corecls.com.

Author: Craig Watanabe, Sr. Compliance Consultant; Editor: Tina Mitchell, Lead Sr. Compliance Consultant, Core Compliance & Legal Services ("CCLS"). CCLS works extensively with investment advisers, broker-dealers, investment companies, hedge funds, private equity firms and banks on regulatory compliance issues.