PLF inBRIEF

ISSUE 137 | JUNE 2019

*Malpractice Prevention Education for Oregon Lawyers*

# Cybersecurity and Employee Training

***By Rachel Edwards, PLF Practice Management Advisor***

An important part of reducing your firm's risk of a cyberattack is proper employee training. According to Verizon's 2018 Data Breach Investigations Report, phishing or other forms of social engineering, which are defined as fraudulent attempts through manipulation in order to obtain sensitive information, cause 93% of all data breaches. Firm employers must make it clear to employees the importance of cybersecurity. Listed below are general tips for implementing cybersecurity employee training:

- **Require social engineering awareness training.** Social engineering is defined as the act of gaining access to buildings, systems, or data by manipulation and exploitation of human psychology rather than physically breaking in or using hacking capabilities. Social engineering awareness training develops awareness of ways that you can be exploited, such as phishing scams or people posing as vendors.

- **Create written security policies.** Update these policies regularly, and require all employees to review them upon hiring, annually, and after any change to the policies. Below are specific policies you may consider including:

  - *Use of firm technology*. Employees are prohibited from using technology resources provided by the firm, including Internet and email access for personal use.

  - *Malware protection*. Require all employees to use malware protection software.

  - *Protection of firm devices*. Require devices containing client data to be password protected and encrypted, especially if the device is taken offsite. Prohibit employees from leaving devices in their vehicle, even in a locked trunk. If employees travel for work-related activities, consider requiring employees to store the device in a safe in their room or at the hotel front desk. Also consider using a program that can track the location of a device and erase its contents remotely. Other options include requiring the use of "burner devices," which contain no client information on the device itself but allow for remote access through a web browser.

  - *Use of personal devices*. If allowing employees to use their own devices for work purposes, implement a policy to ensure the device is secure through password protection and encryption.

  - *Passwords*. Require employees to create strong passwords, which includes those that are 14 characters or longer, contain upper and lower case letters, numbers, and special characters. Also require that passwords be changed frequently, and cannot be recycled or used for multiple websites or devices. When storing passwords, consider requiring the use of a password manager program, or require storage in an encrypted document or locked cabinet.

  - *Updated operating systems and software programs*. Require all employees to use updated operating systems and software programs. Also require employees to notify a manager or administrator if their system is not providing automatic updates, which usually means the program is no longer supported by the vendor and must be upgraded.

- *Downloading programs*. Prohibit employees from downloading programs onto any firm device or the firm network without receiving prior authorization from a managing attorney or the IT department.
- *Clean desk*. Require employees to log out of their computer or other mobile device if leaving their desk for even a short period of time. Most devices have setting options that can be used to log a user out after a short period of time. Also require employees to clear paperwork from their desk so that client information is not exposed.
- *Opening electronic files*. Create a policy that requires electronic files received from outside sources, whether it be from a mobile storage device, file sharing program, or some other electronic source, to be opened on a standalone device that is not connected to any firm network. Or require the use of a virus scanning program.
- *Redaction and removal of metadata*. Train employees on how to redact confidential information and remove metadata.
- *Secure release of information*. Create a policy on appropriate methods for releasing information outside the firm network. For example, if providing discovery documents to opposing counsel, create a policy specifying that employees cannot mail thumb drives containing confidential client data, which are easily lost or stolen in transit. Instead consider the use of a secure file sharing program or encrypted email.
- *Internet use*. Develop specific Internet use policies. Examples include:
    - Require employees to use a secure Internet connection available only to firm members. While most WiFi connections are now password protected, some employees may work remotely, or in a building that has access to a public WiFi connection. Whichever connection is used, ensure that the connection is encrypted and a firewall is used to prevent unauthorized access.
    - Prohibit personal web browsing on firm devices.
    - Use secured websites. Only engage in online transactions if you are on a secure website, indicated by the "https" in the website address. Before entering any information, also check to be sure that the site address matches the one originally entered.
    - Require prior approval from a managing attorney or the IT department before adjusting your browser settings, such as allowing browser add-ons and plug-ins.
- *Email use*. Develop specific email use policies. Examples include:
    - Always use spam filters.
    - Beware of "red flags" in emails. Train employees to recognize red flags tied to phishing scams. For more information, go to *www.osbplf.org* > Blog > Evolving Scams: Don't Let Your Guard Down.
    - Never open attachments from strangers.
    - Never open attachments sent to you unexpectedly by people you know. Malware often finds its way into an infected person's contact list, so even if you know the person, if their system has been infected it can send a virus out to everyone in that person's contact list.
    - Do not download any attachment sent via email, especially if the extension ends in ".exe," which stands for "executable file" and is often used to transmit malware.
    - Prior to clicking on links contained in

emails, hover over the link to see if the website address is different than the link itself. Check to see if you know the sender, you were expecting receipt of the link, and that it is taking you to a secure website.

  - *Working remotely*. Establish a policy that requires employees who work remotely to use a secure Internet connection, such as through a VPN, mobile WiFi, smartphone hotspot, or some other encrypted connection. Prohibit employees from connecting to the office network through a public computer or a public WiFi connection.

  - *Cloud storage*. Lawyers have an ethical duty to ensure that client materials stored on a third-party server are kept reasonably secure. OSB Formal Ethics Opinion 2011-188. Don't use third-party file sharing or storage programs unless you understand the level of security and are familiar with the terms of service. Require employees to receive approval from a managing attorney or the IT department before using any cloud program for storage or sharing of electronic client materials. Or require the use of particular programs after review and approval by the managing attorney and IT department.

  - *Proper deletion of data and disposal of hardware*. Create a policy regarding proper deletion of data from devices as well as disposal of hardware. For more information, see an article written by Practice Management Advisor Hong Dao, available at *www.osbplf.org* > Practice Management > Publications > InBrief > April 2017 > Unwanted Data: How to Properly Destroy Data in Hardware.

  - *Employee departure*. Create a policy regarding employee departure, including things like return of keys or access cards, and disabling user access to the network or cloud storage programs.

- **Enforce the written security policies.** Create methods of supervision and reporting by fellow employees so that failure to follow the policies is made known to the supervisor and remedied.

- **Incident response plan.** Create an incident response plan, which is a set of protocols for managing the aftermath of a cyberattack or other type of loss, such as a lost or stolen laptop. See an article written by Practice Management Advisor Hong Dao regarding creating an incident response plan, available at *www.osbplf.org* > Practice Management > Publications > InBrief > October 2018 > Incident Response Plan.

- **Annual training.** Require mandatory cybersecurity training on an annual basis. Also consider periodic informal training, such as sending out emails reminding employees of potential threats and particular security policies.

- **Phishing tests to ensure compliance.** Consider hiring an IT person or company to conduct a phishing test, which simulates a cyberattack without the knowledge of employees in order to test their response.

Cybersecurity is crucial, but you don't need to have significant amounts of time or resources to implement cybersecurity training for your employees. The benefits of the time and resources invested will far outweigh the time and money spent recovering from a cyberattack.

## Additional Resources

Cybersecurity employee training courses:

BrightWise (*https://www.bright-wise.com*)

Inspired eLearning (*https://inspiredelearning.com*)

KnowBe4 (*https://www.knowbe4.com*)

Proofpoint (*https://www.wombatsecurity.com*)

Webroot (*https://www.webroot.com/us/en/business/security-awareness*)