Security Awareness Training for Law Firm Employees

by Sharon D. Nelson, Esq. and John W. Simek

Introduction and stats

Sadly, your greatest asset – your employees – are also the greatest threat to your cybersecurity. We know this because we regularly see data breaches and ransomware infections caused by click-happy employees. You also have rogue employees determined to use their own devices, go where they want on the Internet, irrespective of firm policies. When we train them, they tell us that they are scared – and you know what? That means we did our job. One of the great fallacies that employees believe is sometimes called "The IT Shepherd" – they simply have faith that the flock (employees) is protected no matter what they do by the shepherd (technology). You need to make them understand that no technological defenses are ironclad.

Let's look at a few statistics. The Computing Technology Industry Association (CompTIA) released the results of a study of 1200 full-time employees in October of 2015. 63% used work mobile devices for personal activities. 94% used mobile business devices to connect to public Wi-Fi networks. 78.5% used public Wi-Fi to check work e-mail and 60% access work documents.

45% have never had any cybersecurity training from employers. 41% don't know what 2FA is. If you don't know, it is two-factor authentication, a more secure way to protect data than using a password alone. 27% know the name 2FA but not how it works.

When researchers salted 200 unbranded USB drives in public, at airports, coffee shops, and parks in Chicago, Cleveland, San Francisco and Washington D.C., 17/% were picked up and used. The flash drives had a trackable link and a text file to tell them to mail an e-mail address. Even IT workers did this – and they should know better!

The Association of Corporate Counsel published *The State of Cybersecurity Report* in December of 2015: Over 1000 General Counsels responded. The dismal result of the survey included the fact that only 1 in 3 track attendance at mandatory cybersecurity training, only 19% give a test, and only 17% have "simulated security events."

Who should do the training?

Certainly not law firm owners. Even if they think they know something about cybersecurity. The biggest hammer is a third-party consulting firm that clearly knows what they are talking about and can answer a fusillade of questions, which generally come fast and furious during training sessions. They bring credibility with them because of their credentials.

If you are an Am Law 200 firm, you are likely going to hire one of the big guns with a hefty price tag. If you are a smaller firm, there are likewise plenty of smaller companies who do cybersecurity training. You want a company that has something of a specialty in training. Hopefully, they have sample phishing e-mails and tests they can give your employees to demonstrate that they are aware of security risks. If an employee repeatedly fails such tests, is that really an employee you want around sensitive data?

Using paper manuals to train is worthless. Online training is not as engaging or effective (our opinion) but 32% of employers use it. In-person group workshops seem to work best. And for heaven's sake, don't bellyache about the loss of billable time. If you think training is costing you money, just think about what a data breach would cost you – that may put it in perspective.

Training Tips

It sounds silly, but make training (as much as you can) fun. Encourage interactivity – make sure you ask your outside training company HOW they train. You want to hear about sample phishing e-mails, post-training testing, on-the-fly interactive responses as to whether an e-mail shows any evidence of being a phishing e-mail (the number one way law firms are breached). Better yet if you hear that they make a contest out of it, have a whiteboard to list the phishing methodologies they discover – even giving out small prizes. Use real life scenarios. They should tell stories. They may have attendees watch short security videos from YouTube (Sophos makes great ones). We love their tag line: "Skip the book and just watch the movies." And they are right – this is a vital part of effective training.

Time of day? Best done in the morning, when folks are most alert. Spring for breakfast and keep the coffee coming. Cybersecurity can be mind-numbing if not done right.

Make it mandatory? Absolutely. Take attendance. When we trained at one law firm, the managing partner told us he had sent around a memo stating bluntly that the training was mandatory and that he would be at the training and expected to see everyone from the firm there. Splendid idea –and everyone did indeed show up.

How often should you train? At least annually. Threats change and defenses to threat change. Both technology and security policies change. You should assess these changes and your security policies on a regular basis to stay ahead of the curve. You can never "set it and forget it" in cybersecurity.

One famous story that may give you pause: Weeks after falling victim to a data breach in 2015, JPMorgan sent a fake phishing e-mail, which 20% of its employees clicked on. If your results are anything like that, you are in desperate need of cybersecurity training for your employees. JPMorgan got the point – having spent $250 million on cybersecurity in 2014, it vowed to double its cybersecurity budget to $500 million over the next two years.

Physical security

Trainers should be talking about physical security too – not leaving files in stacks around the office, being aware of strangers in the office, etc. One of our friends dressed as a custodian and followed a real custodian right into an office building and got into a law firm. Easier than you think. The infamous "office creeper" in the D.C. area during 2015 got into all sorts of "secure" buildings, once getting into a law firm. She was a standard issue thief, taking money from drawers and purses, lifting laptops and cameras which were easy to pawn. But what if she had been after data?

She got through building security by piggybacking and tailgating. Your trainer will explain those terms if you don't know them. And we're betting most readers do not.

Don't be stupid!

This is the essential message of training. Above, we told you about "salted" flash drives in public places. That's called "baiting" – and people fall for that tactic all the time.

Likewise, if you know that another employee is engaging in insecure behavior, you should inform a supervisor. “See something? Say something” doesn’t apply just to possible terrorism, but to cybersecurity as well.

Encryption

Every training session is going to include encryption. Not the math, which employees don’t need to understand, but the critical need for encryption to protect confidential data. They will learn about encryption on all of their devices and e-mail encryption. There was a day when encryption was costly, cumbersome and a royal pain, but those days are long gone. It is now cheap, simple and easy. More and more ethicists are stating that lawyers should use encryption “where appropriate” – which is pretty much anywhere that data which ethically must be protected exists.

Don’t be mad at your employer!

Employees dislike many aspects of information security. A good trainer will have your back on this one. They will explain why your security policies are needed and why they must be enforced. They’ll talk about how the firm may protect its data through application whitelisting, logging of certain events, installing software or hardware that “reports” when certain files (or a certain large number of files) are accessed. They will talk about the dangers of bringing your own device, bringing your own network and bringing your own cloud. They will explain why such things may be forbidden or why they are tightly managed.

They will explain if your technology prohibits employees from opening attachments without asking for the attachment to be released by your IT or information security department. If you control where they go on the Internet, they’ll explain that too. They will explain why employees have to give up their beloved (name your software of choice) because it is no longer receiving security updates.

Trainers explain the importance of strong passwords, especially log-on, screen saver and financial credentials. They will encourage the use of two-factor authentication where it is available and they will report on the new Carnegie Mellon studies showing that password length is more important than complexity, which is agreeable news since it is easier to remember a lengthy passphrase than a complex password. There is a new draft document from the U.S. National Institute for Standards and Technology (NIST) which recommends password length over complexity. The rules keep changing, don’t they? But that too is why you train on a regular basis.

And trainers will preach the value of encrypted password managers – darn near a necessity if you are going to follow the cardinal rule of not reusing passwords everywhere which often leads to one breach compromising your security, and that of the law firm, in many places rather than just one.

Social engineering

People who are experts at penetrating businesses through social engineering say it generally takes them less than an hour to get into your network. We are so anxious to be helpful. Your employees need to know that Microsoft Tech Support will never call and ask for access to their machine (yes, we’ve seen lawyers duped). They also need to understand that someone who calls and says they are from your IT company and need log-in credentials to fix a problem may not really be from your IT company, even if they know the company name.

Phishing

As we said before, phishing is the easiest way into law firms. Even good enterprise anti-malware software doesn't catch everything – and there are plenty of zero day (no known defense) exploits sold on the Dark Web every day. Lots of studies have shown that roughly 20% of phishing e-mails will be opened.

The worst threat comes from targeting phishing attacks, where the hackers are specifically targeting your law firm. Law firms are at a disadvantage here – so much legal data is public. A hacker may know what cases you are involved with, who the attorneys are, which courts cases are in, etc. And they can spoof the e-mail address of an attorney or a court – how many folks can resist opening something that appears to come from a court?

Law firms are also at a disadvantage because they are "honey pots" – they hold the data of so many clients. Hackers may do a little research on the firm's website or on an attorney's LinkedIn page where they may find personal information that they can insert into a targeting phishing e-mail. Trainers will get them to PAUSE, THINK, INSPECT and REPORT before clicking on any attachment or links in the e-mail.

There are obvious phishing clues to pass on to employees:

- You don't know the sender
- You do know the sender but if you look closely, the address is one letter off (this one happens a lot)
- Nothing in the note seems personal to you
- You weren't expecting the e-mail
- Reference is made to a bank/product/service you don't use
- Words are misspelled
- The grammar is poor
- The e-mail doesn't address you by name
- The message asks for personal information
- There is an attachment which seems suspicious in conjunction with other factors or a link to a website (and no, hovering over the link doesn't necessarily ensure that you will go to the address shown – drive-by malware infections from visiting malicious sites are quite common)

The list goes on and on – you need to advise your employees to be alert to anything suspicious and not to be quick to click!

If they end up with malware, they may not know it. But some possible signs might include, sudden slowness of devices, strange messages appearing on the screen, the inability to open a file, machine crashes, running out of hard drive space, a high volume of machine activity, suddenly having a new browser home page or tool bar the employee didn't install, new programs appear that start automatically, etc.

Ransomware

Ransomware is an international epidemic. Your employees need to understand that it is usually contracted via phishing e-mails. Click on a link in the e-mail or an attachment and the malware is downloaded invisibly irrespective of what you see on the screen. Then it sets about encrypting the firm's data, file by file. If the backup is connected to the network at the time, it will encrypt that too.

Employees really need to understand how dangerous ransomware can be, how prevalent it is, how the ransom to get your data back is more and more expensive – and that you are out of business until you slog through trying to figure out how to get sufficient funds in bitcoins (which the hackers generally want as payment) – and then there is a delay after receiving the decryption key in restoring the files (assuming you do in fact get the key).

While you can be protected from ransomware by having a properly engineered backup, if you get ransomware, you still have to live through some period of time while the files on an unaffected backup are restored. And we are now seeing ransomware on mobile devices, including phones – most from downloading apps from unsanctioned app stores, a very common practice among employees!

Business e-mail compromises

These are also known as CEO scams and the FBI reports that they have netted more than 3 billion dollars thus far. From January 2015-June 2016, there was an increase of 1500% in successful attacks. That's one heck of a statistic. Basically, someone who has authority to order money wired appears to be e-mailing someone who actually does the wiring. Law firms have been hit hard by these scams, so it is critical that employees understand how they work and that they be conditioned to seek affirmation of any order to transfer significant monies.

More in the Morass

Clearly, there is a wealth of threats that employees need training on – more than we can possibly address in a single article. Employees need to be trained on the dangers of metadata, the safe use of public Wi-Fi, the safe use of file syncing software in the cloud, the perils of using social media, the need to protect all devices (including Apple devices), the malware that may be present on public computers in hotel business centers, public libraries and Internet cafés, the need to make sure (if they work from home without a VPN) to make sure that their home Wi-Fi is secure, how to secure their smartphones (especially if they are allowed to connect personal devices to the firm network), and the need for managed vendor access.

Hopefully, you have a sense of how critical it is that you train your law firm employees on cybersecurity. We know of one firm in California that averted disaster because all employees had recently received training on phishing e-mails and when they were on the receiving end of a targeted attack against their law firm, the employees recognized the phishing e-mails and quickly spread the word. Disaster averted. We have no doubt that the firm invested time and money in the training, but we're betting that, having survived the attack, the firm counted every dollar as well spent!

The authors are the President and Vice President of Sensei Enterprises, Inc., a legal technology, information security and digital forensics firm based in Fairfax, VA. 703-359-0700 (phone)
www.senseient.com