Stay Aware

Five cybersecurity worries you should know about.

BY **SHARON D. NELSON** AND **JOHN W. SIMEK**

There are many cybersecurity worries to give you the willies in the wee hours of the morning. Here are some of the most common ones.

Ransomware

We continue to see law firms struck by ransomware, which encrypts your data and follows with a demand for payment—usually in bitcoins—to get your data back. Training your employees not to click on suspicious attachments or links in emails will help. They need to stay away from suspicious sites as well since ransomware can be installed by just "driving by" an infected website.

From a technological standpoint, you can defeat ransomware by having a backup that is immune to it. This can mean, particularly for solo lawyers, that they back up and then disconnect that backup from the network. For others, it means running an agent-based backup system rather than one that uses drive letters. Make sure your IT consultant has your backup engineered so that it is protected—that way, even if you are attacked with ransomware, you can thumb your nose at the demands for money because you can restore your system from your backup (which means backups need to be done frequently to avoid any significant data loss).

Employees

Employees are rogues by nature. In every study that's been done, they ignore policies (assuming they exist) in order to do what they want to do. This often means they bring their own devices, which may be infected when connected to your network. They may also bring their own network or bring their own cloud. Certainly your policies should disallow these practices (in our judgment) or at least manage the risks by controlling what is done by a combination of policies and technology.

Oh, and they sometimes steal your data or leave it on flash drives, their home devices, etc. This means you have "dark data"—data you don't know about and over which you have no control. You may miss data required in discovery because you don't know it exists, your data may not be protected in compliance with federal or state laws and regulations, or you will have no way to manage it because you don't know it is there. Once again, a combination of policies and technology should be in place to prevent these issues.

Targeted Phishing

This is perhaps the greatest and most successful threat to law firm data. Hackers have you in their sights. They often have done research on your law firm. They may know what cases you are involved in—and who your opponents are. They may know the managing partner's nickname. Everything they know about you they may use to get you to click on something, such as an email from an opponent referencing a specific case and saying, "The next hearing has been rescheduled as per the attachment." Many a lawyer has clicked on such attachments or links within emails.

The best solution to protect yourself from targeted phishing is training—and more training—endlessly. One California firm had multiple target phishing attacks but survived them because attorneys and staff who receive such emails questioned their authenticity. Forget the loss of billable time; the loss of money and even clients due to a data breach can be far worse.

Interception of Confidential Information

Start with the proposition that everyone wants your data, including cybercriminals, hackers, and nation-states. Frankly, if they want your data and have sophisticated tools, they will get it. So shame on you if you are not using encryption (which is now cheap and easy) to protect confidential data. Today encryption is a law firm's best friend. You may choose to use it always or in cases where it is warranted, but you surely should have the capability.

Failure to Use Technology to Enforce Password Policies

First, let us say that you should use multifactor authentication where available and use it to protect sensitive data. But we recognize that passwords are still king in solo, small, and midsize firms.

Therefore, have your IT consultant assist you in setting up policies that can be enforced by technology, requiring network passwords be strong, changed every 30 days, not reused for an extended period of time, be 14 or more characters in length, and contain uppercase and lowercase letters, numbers, and symbols. Passphrases—sequences of words—are best. Something like Iloveattorneyatwork2016! would do nicely.

There are many other willies out there, but remember to address them a digestible chunk at a time. TBJ

This article was reprinted with permission of the authors.

SHARON D. NELSON and **JOHN W. SIMEK**
are the president and vice president at Sensei Enterprises, a digital forensics, information security, and legal technology firm in Fairfax, Virginia. They can be reached at (703) 359-0700 and sensei@senseient.com.