Five Cybersecurity Worries to Give You the Willies

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

There are lots of cybersecurity worries to give you the willies in the wee hours of the morning, but we were asked to pick five, so here are some of the most common ones.

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

Overwhelmingly, 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 backup and then disconnect the backup from the network. For others, it means running an agent-based backup system rather than one which uses drive letters. Make sure your IT consultant has your backup engineered so that backups are 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 made frequently to avoid any significant data loss).

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

Oh, and they 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. This means 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. And you have no way to manage the data 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. Someone has you in their sights – they often have done research on your law firm. They may know what cases you are involved it – and who your opponents are. They may know the managing partner's nickname. Everything they know about you they may use to get your click on something (say, an e-mail from an opponent referencing a specific case and saying "The next hearing in _____ case has been rescheduled as per the attachment.) Many a lawyer has clicked on such attachments – or a link within an e-mail.

The best solution to protect yourself from targeting 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 e-mails questioned their authenticity. Forget the loss of billable time. The loss of money, time 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 (including our own). Frankly, if they want your data and they have sophisticated tools, they will get it. So shame on you if you are not employing encryption (which is now cheap and easy) to protect confidential data via voice, text, and e-mail. Encryption, today, 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 of encrypting.

Failure to Use Technology to Enforce Passwords Policies - First, let us say that you should use multi-factor authentication where available and use it to protect sensitive data. But failing that, we recognize that passwords are still king in solo/small/mid-size firms.

Therefore, have your IT consultant assist you in setting up policies that can be enforced by technology, requiring that network passwords be changed every 30 days, not reused for an extended period of time – and mandating strong passwords, 14 or more characters in length, utilizing upper and lower cases

letters, numbers and symbols. Passphrases are best. Iloveattorneyatwork2016! would do nicely.

There are many other “willies” out there, but address them a digestible chunk at a time!