Practical Cybersecurity for Law Firms: How to Batten Down the Hatches

By Sharon D. Nelson, Esq., John W. Simek and Michael C. Maschke

Setting the stage

We're quickly approaching 2018 and a week doesn't go by without another variant of malware causing havoc across the globe. First it was the WannaCry ransomware worm, which infected more than 230,000 computer systems in over 150 countries demanding ransom payments in exchange for the decryption of files. More recently, a new variant using code from the Petya ransomware (named "notpetya") struck first in Ukraine followed by other European countries and disabled critical utility services such as the radiation monitoring system at the Chernobyl Nuclear Power Plant, as well the affecting the countries' banks and metro systems.

What caught the attention of lawyers was that an apparent infection in one of DLA Piper's European offices brought the law firm's normal operations to a halt. As we write, the extent of the damage is still unclear.

The times have changed since Cryptolocker first ran wild in 2013, but the results are still as devastating. The costs of ransoms have significantly gone up from a few hundred dollars to the $1,000+ plus range now for the decryption key to unlock the affected files – and more than half of those who pay up do not receive the decryption key. So much for honor among thieves!

Ransomware has continued to evolve and is the primary security concern for businesses of all types and sizes.

How do you protect your firm from ransomware, malware and other cyber threats? Before we get started, as we say all the time (and it rates all caps), **THERE IS NO SILVER BULLET THAT PROTECTS AGAINST ALL RANSOMWARE.** Or all malware for that matter. If a vendor promises you a 100% solution, you are being sold a bill of goods.

Backups

Backups are key. Backup all of your data. Don't forget to periodically conduct a test restore of the data and make sure your backups are impervious to ransomware – either backed up in the cloud or agent-based (talk to your IT provider to learn more) Backups should be encrypted with a user-defined encryption key, whether on-site, off-site or stored in the cloud. If using a cloud vendor, the vendor should not have access to the decryption key. Encryption should be treated as a must – no questions about it.

The simple solution for most solo/small firm lawyers? Use an external USB hard disk. Unplug the external USB hard disk after the backup job completes. Just make sure you have at least two USB hard disks and rotate them in case you are attacked while one disk is connected.

Passwords

Next up, passwords. Develop a password policy. The recommendations for password policies have recently changed. We still live in a password driven world, but the final guidelines from the National

Institute of Standards and Technology (NIST) for the federal government have now been published – see SP 800-63-3: Digital Identity Guidelines which you may find at https://pages.nist.gov/800-63-3/.

While this publication applies to government agencies, it represents new thinking that is sure to be embodied in the NIST Cybersecurity Framework, draft version 1.1, which is in the process of being finalized as we write – we expect the Framework to be finalized by the time this article is published. NIST is phasing out the requirement of periodic password changes – which has been the foundation of password policies for many, many years. Other recommendations include using a length of a least eight characters or more and choosing a passphrase rather than a "password." Some applications and devices allow users to include spaces and even *emojis*, which users can now include when setting their passphrase. As always, do not use dictionary words as these are easy to brute force and please, please force computers to require screen-saver passwords and ensure that passwords are required after a reasonable period of inactivity. Newly included is checking all passwords against a database of known compromised passwords, which will of course eliminate all of the dreadfully easy passwords that users are so fond of employing.

Users should never share their password, write it down or reuse the same password anywhere. It is particularly important that credentials used to access a law firm network **never** be used anywhere else. The use of a password manager can make this task quite easy. Consider enabling two-factor authentication (2FA) when available. Biometrics alone is not a good solution – once your biometrics are owned, they will always be owned. Remember the 5.6 million fingerprints stolen in the U.S. Office of Personnel Management data breach? You can't change your fingerprint.

A password policy should be part of an overall comprehensive security program, which should also encompass an incident response policy, disaster recovery plan and social media policy to name a few.

Patches and updates

Firms need to prioritize efforts to keep hardware and software as current as possible. Keeping up-to-date doesn't always have to cost money – see Windows Security Updates. You don't need to be first in line for the latest and greatest, but don't be the last in line either. Once software becomes unsupported, it is unethical to use it because it is no longer receiving security updates and is vulnerable to attacks. In January 2017, Microsoft stated that Windows 7 is so outdated that patches can no longer keep it secure. Extended support ends 1/13/20, so the operating system will not get any further enhancements and will receive security updates only. What does this mean? It is time to plan an upgrade to Windows 10 if you haven't migrated already. Windows 10 security is leaps and bounds better than what Windows 7 provides.

Firms need to apply patches **as soon as they are available** to reduce the vulnerability to attack or compromise. A perfect example – "notpetya" ransomware – attacks a vulnerability of Windows' Server Message Block (SMB) which is first believed to have been developed and exploited by the NSA – released by hackers in April 2017. Microsoft released a patch to address this security vulnerability in March of 2017, so if a computer system hasn't been updated with security updates since then, it could be vulnerable to this ransomware variant. If you have a Windows Domain environment, have your IT provider configure Windows Server Update Services to download and push out Windows Security Updates to all of your client computers and servers as they are released – a free solution to keeping your operating systems updated.

Encryption

Encryption, once just technical-jargon or something the German World War II Enigma machine used, is now becoming the de facto recommendation from cybersecurity companies. Why? It's no longer cumbersome and time-consuming, but is cheap and easy to set up and use (and maybe ethically required for attorneys – see the ABA's Ethics Opinion 477 (May 11, 2017) on encryption of attorney-client email. Your laptop should be protected with whole-disk encryption – no exceptions. Ditto for any external USB flash drive or hard drive used to store firm information. Stolen and lost laptops are one of the leading causes of data breaches. Many of the newer laptops have built-in whole-disk encryption. To state the obvious, make sure you enable the encryption, or your data won't be protected. For others, Windows BitLocker and Apple FileVault II are free encryption options included with Windows and macOS systems – there is no excuse for not using this free protection.

Also, encryption may be used in conjunction with biometric access. As an example, our laptops require a fingerprint swipe at power on. Failure at that point leaves the computer hard drive fully encrypted.

The same applies to mobile devices - encrypt, encrypt, encrypt. For modern phones – just enable a PIN or password lock code. We recommend six or more characters. Yes, if you use an Apple iPhone, the recommendation is still the same as these devices are not inherently more secure than other devices. You would not believe how many users (and attorneys) still believe that Apple products aren't capable of contracting malware. Apple itself refutes that thought. For the Samsung Galaxy S8, users can use a fingerprint, iris scan or facial recognition (don't use the selfie – this form of 'protection' was compromised within 24 hours!). And don't forget anti-malware software on your mobile devices, such as Sophos, Lookout, Kaspersky or McAfee – ransomware attacking mobile devices is on the rise.

Sometimes convenience causes issues. Providing remote or mobile users with access can create more vulnerabilities than you might realize. To combat this, mandate that all work-related Internet sessions be encrypted. Prohibit the use of public computers and unsecured open public Wi-Fi networks. Access to the office network must always occur through the use of a VPN, MiFi, smartphone hotspot or some other type of encrypted connection. For users that need to connect directly to their work computer, use an encrypted remote control solution such as Citrix, LogMeIn or GoToMyPC. The setup of this kind of software couldn't be any easier and we've seen many attorneys accomplish this on their own.

Employee security awareness training

Malware loves to prey on uninformed users. These victims are the primary cause for the continuing propagation of malware infections, with users clicking on things that they shouldn't be. Why, you might ask? Curiosity, fear, urgency, recognition (such as being named for an award) are generally recognized as the top four motivations for clicking. Over 91% of all hacking attacks begin with a phishing e-mail, which is why it's imperative that you train all of your employees.

Sadly, one of the most often-overlooked aspects of an organization's security readiness is end-user training. It is just as important that your employees know what not to click on as it is to have security software installed to help prevent malware outbreaks. Firms should provide mandatory social engineering and safe computing awareness training to everyone at the firm at least once a year. And make it mandatory!

Technology alone cannot protect your data. The greatest vulnerability comes from your greatest asset - the folks who use your network. Cyberattacks are successful because someone usually did something

stupid like clicking on a link, opening an e-mail attachment, or verifying an ID and password when they shouldn't have. With education and practice comes a more informed and safe user. Look into services that provide phishing assessments, such as Duo Insight (www.duo.com/resources/duo-insight) as a way to test and educate your employees against phishing e-mails. Integrating this testing into annual training is a great way to get your employees to learn, to have a fun competition and to identify those employees that may need some extra "attention" and practice. By the way, a single training session has been shown to reduce the risk of a successful phishing attack by 20% - not a bad return on your money.

Technical solutions

You can also augment your training with technical solutions. There are e-mail scanning services such as Mimecast, which convert attachments into a "safe" format such as PDF. There's also an option to scan URLs in messages and warn of any suspicious links.

There are some free and not so free solutions that your firm can implement to increase your security posture against ransomware and other malware threats. Much of what we describe is probably included in the software that your firm has already purchased. It is just a matter of turning the security settings and requirements on. Our list of security recommendations could fill a book, but we have tried to include the primary essentials above.

Doing nothing makes no sense - you are just begging to be "owned" by the next piece of ransomware or malware. By implementing some of the solutions described above, you are doing your "due diligence" to batten down the hatches, protecting your firm from becoming the victim of the threats that will continue to wreak havoc for the foreseeable future. Cybersecurity is a moving target – as threats morph, so will the defenses – keeping yourself educated on information security issues is a very high priority for all lawyers.

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