Cyber Security Memo

June 9, 2017

We are not big enough to have a legal department and we are not lawyers, so we will try to answer some questions about how to address the cyber security issues we are all talking about. On the other hand, we have been around CNA and lawyers long enough to know there should be a disclaimer here. Most of this information is based on Windows operating systems and the recommendations are for a solo or very small firm without extreme security needs. You may very well have security in place that goes well beyond what we discuss here. Recommendations from your "insurance guy" do not take the place of actual due diligence on your part. With that said, we hope this will be a helpful starting point for your further investigation.

We researched recommendations for inexpensive services that would not only provide a one-time evaluation of your computer system for security issues but also help you implement solutions. This was not as easy as it sounded. However, from the ABA Buyers Guide and elsewhere, we found these options:

- eSentire, Inc. (a one-time vulnerabilities test of your system and report is $8,000)
- Cyber Revolution (their monthly service "starts at" $500 per month, but if you read further there is an option for sole practitioners at $175 per month)
- All Covered (this was the cheapest one-time vulnerabilities test at $995)
- Tenable (reportedly tests an unlimited number of PC's for $2,190)
- Trustware (their lowest tier of penetration testing is $7,500 and goes up to $28,000)

The following information may help you evaluate your own system and implement solutions:

Firewalls and Security Software

1. Make sure that Windows Defender (real-time malware protection) is updating automatically on all computers in your office. It is built into Windows 8, 8.1 and 10, but make sure it is on. Check the status by going to Start, Settings, Update & Security. If Defender is not running, it is just a matter of clicking a box or button to turn it on. *This program alone likely would have kept you safe from the recent WannaCry Ransomware attack.* For Windows computers running earlier operating systems, install the free Microsoft Security Essentials.
2. Consider adding another good anti-malware program. Malwarebytes Anti-Malware runs on all our machines and it reportedly catches things others do not. There are other good ones, but avoid running too many security software programs simultaneously. They may not work well together and could slow your system way down.
3. If you are connected via a NAT router (see the link to article #2 below), this provides an effective firewall - assuming you trust the computers on your side of the firewall. When you are connecting elsewhere on a laptop, always be sure to turn on the Windows firewall. You may want to just leave it on. (Control Panel, Windows Firewall and click to turn it on.)

Look for the official Windows answers to your questions when you Google. We rely on and recommend a computer knowledge site called Ask-Leo. Leo Notenboom gives practical advice for individuals and small businesses. The following Ask-Leo articles address some of the security software issues mentioned above.

Ask-Leo.com/What Security Software Do You Recommend
Ask-Leo.com/How Do I Know If I'm Behind a NAT Router?

Back Ups

This is essential not just for cyber security, but for the simple reason that hard drives fail, disasters happen, and things get lost. Make sure you are backing up all your data regularly *and keeping the incremental backups.* If you overwrite your only backup, you will not be able to retrieve that earlier data if needed. Incremental backups will save those previous versions of your data. If you have your data all on the cloud, that is just where it is; it is not a backup. One copy anywhere is not a backup. We use both a cloud back up program (Carbonite) and a hard drive back up system. The following Ask-Leo article is for small firms and home users, but it gives you a starting point if you are not doing this already.

Ask-Leo/What Backup Program Should I Use?
Ask-Leo/4 Important Rules to Safely Use Cloud Storage as Cloud Backup

Encrypting your devices

Encrypting your phones and computers can make the loss of those devices, while still very inconvenient, a non-issue for breach notification requirements. Arizona and New Mexico breach notification laws refer only to the loss of unencrypted data.

It's important to set up a good password or fingerprint scan as a requirement to open your phone, and all phones used for business should have a password/fingerprint option on them. Go to Settings/Security on your phone and set a password or pass phrase (not just a pattern) or enable the fingerprint option. Newer Android/iPhones may come encrypted by default, but go to Settings/Security/Encryption to check and encrypt if needed. Note: Encryption can take several hours and requires that the phone be plugged in.

Encrypting the hard drive on your computer requires some additional work but is still easy and, with most Windows computers, free. This is especially important for laptops, but even desktop computers can be stolen or hacked. Make sure you have a complete backup of your hard drive before you encrypt it and, assuming your backups are in a secure location, have unencrypted backups. It is essential that you save a copy of the recovery key somewhere that you (and someone else you authorize) can access it. Should you forget your computer password, the security key is the only way you can access the data on your computer.

The following article walks you through encrypting a hard drive using Windows Bitlocker.

Ask-Leo/How Do I Encrypt a Disk?
Ask-Leo/Will Hard Disk Encryption Protect Me from Network Attacks?

Finding Secure Vendors

Many law firm practice management systems, including those listed in CNA's Allied Vendor Program, provide cloud storage with bank grade security and may also include secure client communication options. The Allied Vendor list includes IronBox for secure, encrypted file transfer of sensitive data and Silent Circle for secure communications.

The ABA Legal Technology Buyers Guide is a list of vendors for a variety of computer services. While the ABA notes they are not recommendations, and the list is a paid ad, at least these vendors are attempting to target the specific needs of lawyers and law firms.