HOW CAN A LAW FIRM ENSURE THE SECURITY OF ITS DATA?

10 Security Measures Your Law Firm Should Consider

BY BRIAN MAUCH, BCOM LLB
CEO, BMC NETWORKS INC.

To paraphrase one of my favourite quotes about computer security, to be truly secure a computer would need to be (1) disconnected from the internet, (2) disconnected from any network, (3) powered off and unplugged, (4) cast in a block of concrete, and (5) sealed in a lead-lined room with armed guards. However, to describe such a computer as extremely inconvenient to use would be an understatement.

In the computer world, levels of security exist on a spectrum. One end of the spectrum represents a high level of security, and the other end of the spectrum represents a high level of convenience. It is impossible to have both high security and convenience because they each exist at the expense of the other. Put simply, a computer system that is convenient to use will have a low level of security and a highly secure system will be very inconvenient to use.

That said, modern businesses need to use computers, and law firms are no exception. In fact, law firms rely on computers more than many other types of businesses: to facilitate communication, record-keeping, scheduling, and the collection and analysis of data. One of the highest professional obligations on a lawyer is to safeguard their clients' confidential data. So how does a law firm do this, knowing that computers are inherently difficult to secure?

The key is for each firm to decide where they need to fall on the security/convenience spectrum, and to take reasonable precautions to meet that standard. Unfortunately, most law societies do not provide these standards because they take the approach that they are regulating lawyers, not technology. It is up to lawyers to do their due diligence to understand the risks involved and take reasonable actions. Some types of firms are at higher risk than others due to the type of law practiced, the type of data available, and the complexity of their network.

> Fortunately, there are many security measures that law firms can utilize to safeguard their network and data. However, none of these security measures are 100% effective. If there were a single security measure that was 100% effective, everyone would use it and there would not be such a thing as hackers, viruses or data breaches.

My firm's recommendation to its clients is to use a multi-layered approach to security, utilizing multiple best-in-class tools and best practices. Even if each measure or best practice has a 95% effectiveness (meaning that it is 5% ineffective), the combination of ten best practices each with a 95% effectiveness should yield something approaching (but never quite guaranteeing) 100% effectiveness. Think of using ten different strainers on a glass of orange juice – there probably will not be any pulp left over when you are done.

Here are 9 different "strainers" that law firms should consider:

1. ENDPOINT ANTIVIRUS PROTECTION

This is the security measure that most people are familiar with. It is the antivirus software that we install on our workstations and servers, and will one day install on our phones, cars, and connected homes. Endpoint antivirus software identifies and blocks malicious code using a list of known virus signatures, and tries to identify new threats using heuristics. This software needs to be updated on a regular basis to account for newly identified threats and is susceptible to new threats that have not yet been identified and blocked. As with all of the measures listed below, antivirus software needs to be monitored and acted upon by your IT team, so that it is not up to your staff to self-report that they clicked on a link they should not have – the natural instinct is to surreptitiously close an antivirus warning and hope that nobody noticed.

2. HARDWARE FIREWALL

This is a device that sits between your firm's internet connection and internal network. Good (i.e. expensive) firewalls inspect every packet of data that enters and exits your internal network and block packets that contain malicious code. Similar to antivirus software, firewalls are only as good as their latest update and are susceptible to new threats.

3. SECURE INTERNET GATEWAY

This is a new type of security measure that complements a hardware firewall by scanning all outbound requests from your firm's network and blocks any connections destined for a rapidly-evolving list of known malicious sites on the internet. This security measure is particularly effective against ransomware because most ransomware variants quietly enter a network like a trojan horse and then reach out to the internet to let the bad guys in.

4. EMAIL ANTISPAM

It may surprise you to know that an estimated 60% of all sent emails are actually spam. With that much spam coming in, it would be detrimental to productivity for users to have to sort out themselves the real emails from spam. Many people incorrectly assume that antispam software should be easy to use and maintain and have a 100% effective rate. However, teaching a computer how to identify spam email using heuristics is akin to artificial intelligence because spammers are constantly working to find ways around spam filters. It has become a long-running battle of attrition – some months the spammers are winning and some months the anti-spammers are winning. The only truly effective anti-spam measure would be to pay a reasonably intelligent person to read and filter all of your email for you, which would be inconvenient, expensive, and impinge on your privacy. We instead rely on anti-spam software, despite its less than 100% effectiveness.

5. TWO-FACTOR AUTHENTICATION

Remote access means accessing your data from outside your office, which removes the necessity to physically be in your office. Remote access is a mixed blessing because, while it is very convenient for you to access your data remotely, it also means that someone else can too. We typically protect our data using the time-honoured custom of having a username (which refers to you and can easily be guessed by someone else) and a password (which in theory only you know… and everyone else who reads that sticky tab on your monitor). Two-factor authentication introduces a second "factor" when logging into your computer. In addition to something you know (i.e. your password), logging in also requires something you have, such as a randomly-generated code texted to your phone, or a fob with a rotating set of random numbers.

6. PASSWORD POLICIES

Many users never want to change their password because it was hard enough to remember it in the first place. In fact, they use the same password for all of the online services we all use on a regular basis. This system of convenience breaks down when eBay, Target, Dropbox, etc. are hacked, and the hackers publish all of the username/password combinations they uncovered just for kicks. Other hackers then take a few minutes to research where these users work, figure out what type of remote access system they have, and try to log in using the username/password they found. The good news is that most hackers do not care too much about the confidential client data they will find on the network of a typical law firm but sometimes they do (e.g. the Panama Papers). However, the hackers know that the lawyers care about the confidential client data so they encrypt it with ransomware and will happily accept bitcoins in exchange for unencrypting it. To combat this, passwords need to be unique, complex, and changed on a regular basis.

7. MOBILE DEVICE PASSCODES

Law firms will sometimes go to great extents to secure their office computers and remote access but forget about the super-computers in their lawyers' pockets that contain the entirety of humankind's knowledge… not to mention also containing confidential client data and the ability to impersonate a lawyer by sending and receiving email as that lawyer. Smartphones have become indispensable tools of the trade for lawyers, and you would assume that they would all use alphanumeric passcodes or thumbprints to keep those devices locked at all times, but you would be wrong because that would be inconvenient. Complex passcodes (i.e. not "1212") with more than 4 digits need to be in place and phones need to automatically lock after a few minutes of sitting idle. If a phone is lost, stolen, or simply left in the back of taxi, law firms need to have the ability to remotely wipe that phone and all of the data on it. Fortunately, all of these measures can easily be enforced on a modern network.

8. SCREEN LOCKS FOR DESKTOPS/LAPTOPS

This precaution has more to do with physical security, which can sometimes be an issue in a law firm. Many users walk away from their computers for meetings, lunch, and to go home at the end of the day, leaving their computer logged in and accessible by anyone who sits down at it. However, law firms do not typically know every person who is in their office on evenings and weekends. Landlords provide cleaning and maintenance staff and they need to access the office at odd hours. If the wrong person were to walk into a typical law firm outside business hours, it would be very easy to steal data, infect a network with ransomware, or send and receive emails masquerading as a lawyer. Even if you told everyone to save their data, close all their programs and restart their computer at the end of every day, someone would forget, or they would be expecting to come back to the office later but changed plans and ended up going home instead. Best practice is to enforce that an idle computer locks with a screen saver after a short length of time and would require the password to unlock it. Our office has a 20-minute idle lock in place and to encourage our users to manually lock the computer every time they step away we use "social engineering". Upon encountering an unattended, unlocked computer, someone may sit down and send out a company-wide email stating "I love you guys, donuts are on me tomorrow." This usually only needs to happen once per user.

9. BACKUP

A reliable backup is the last line of defense for your data. A backup copy of your data will help you if embarrassing emails have been published on the web but it will help you if all your data has been encrypted by ransomware and a Russian teenager is demanding bitcoins to unencrypt it. A combination of onsite and offsite backup is necessary. An onsite backup will allow you to quickly restore files or emails, but it will no help you if your office has suffered a fire, flood or theft and the computers are unrecoverable. In that case, your data would also need to be backed up offsite in order to recreate your law practice.

CONCLUSION

There are more strainers available, if someone wants to try to catch every last bit of pulp. Email encryption, retina scanners, and other security measures may one day be commonplace but few law firms have felt the need to swing that far on the spectrum towards security and away from convenience. As with most things, there are diminishing returns when it comes to increasing computer security to the nth degree.

Implementing the preceding list of nine security measures will have a significant impact on improving your firm's security. Some of them will be inconvenient and some of them will be costly. Even if you had them all, your firm could still get hacked, but if you have these measures in place, the hackers will probably quickly move on to other unprotected targets because the lowest-hanging fruit gets picked first.

The tenth important security measure is to think of security as a fluid and evolving topic and not be fooled into thinking it can be addressed once and for all. New threats will evolve over time and new security measures will be developed. The cost of some measures may go down and we may find ways to make them less inconvenient. Law firms should review their security needs on an ongoing basis and be prepared to adapt to changes in the security landscape because the potential cost of a breach could be significant. V

Brian Mauch is the CEO of BMC Networks, a Vancouver-based outsourced IT provider that specializes in law firms. Brian obtained both law and commerce degrees from the University of British Columbia, and then combined his education with his passion for computers to form BMC Networks in 1997.