Cybercrime and law firms:

The risks and dangers are real

Historians may well look back and call 2013 "The year of the hacker." There have been numerous high-profile data breaches involving major corporations and online services: Facebook, Apple, Twitter, Adobe, NASDAQ, The New York Times and LexisNexis, to name just a few. Everyone reading this article likely has information stored by at least one, if not several, of these companies.

And it doesn't stop there. Millions of other business entities and individuals have experienced data breaches this year, either directly on their own computers or systems, or indirectly where there was a data breach involving information about them that was stored with a third party. Countless others will have lost money after being duped in various online scams.

Law firms and lawyers take notice: cyber criminals are specifically targeting *you* because they want your data or the money in your trust account. Law firms are actually very appealing and sought-after targets for cyber criminals for three reasons. Firstly, law firms have large amounts of sensitive and confidential information that can be very valuable. Secondly, law firms tend to have very large sums of money in their bank accounts. Lastly, and not the least, relative to their clients and based on anecdotal information, law firms tend to have weaker security protection in place on their networks and systems.

Cybercrime has hit very close to home. In 2011, several major Bay Street firms were targeted by hackers traced to China who appeared to be seeking information on a multi-billion-dollar commercial transaction. In late 2012, LawPRO handled a claim involving a significant theft from a firm trust account by a Trojan banker virus (see sidebar on facing page). There have likely been thousands of attempts to breach Ontario law firm systems this year, and probably some actual breaches as well. But we will likely never hear about them because firms that experience breaches usually try to keep their names out of the news.

Information on cybercrime tools and techniques is widely available online, making it easy for even non-technical people to undertake malicious cyber activities. But make no mistake, while rank amateurs may launch attacks on law firms, industrial espionage on high value targets can involve the most skilled hackers in the world including, potentially, foreign governments.

Cyber criminals will use every tool at their disposal to attack law firms. They will send spam and phishing messages. They will try to install malware and create backdoors into your firm's computers.

LawPRO claim involving significant theft from firm trust account by Trojan banker virus

In December, 2012, an Ontario law firm provided notice of a claim involving the infection of one of its computers by a Trojan banker virus. This was a very sophisticated fraud in which the firm's bookkeeper was induced, by a fraudster posing over the phone as a bank representative, to key in account and password information on her infected computer. Through the virus, the fraudsters were able to capture this information which they then used to access the firm's bank account. Over the course of several days, fraudsters wired several hundred thousand dollars from the firm's trust account to offshore accounts.

A more detailed review of how this fraud happened will help you appreciate how sophisticated these frauds can be. It appears the bookkeeper's computer was infected when she clicked on a link on a popular news website. Despite being the most current version with all updates, the antivirus software running on her computer did not recognize or stop the infection.

After being infected, the bookkeeper's computer appeared to have difficulties accessing the bank's website. She got a "This site is down for maintenance" message. This was actually not a page from the bank's website; rather, it was a fake or "spoofed" page pretending to be the bank's website. On another screen that appeared on her computer – which also looked like it was the bank's real website – she was asked to enter her name and phone number. This appears to have given the fraudsters her contact information, as later that day the bookkeeper received a telephone call from someone, allegedly from the firm's bank. That caller said she was aware of the login attempts and stated that the site had been down for maintenance. The caller said the site had been fixed and asked the bookkeeper to try logging in again. The bookkeeper did so, entering the primary and secondary login passwords for the account on screens that appeared on her computer – the passwords were not given to the person on the phone. The second password came from a key fob password generator. This appears to have given the hacker both passwords and access to the firm's trust account.

On each of the following two days there were similar phone calls to the bookkeeper from the woman who allegedly worked for the bank to "follow up on the website access problems." On each occasion, the bookkeeper tried to log in again and entered the primary and secondary passwords on screens that appeared on her computer.

The fraudsters went into the account during or immediately after each of the three phone calls and wired funds overseas. An amount less than the balance in the account was wired out each time. This was an infrequently used trust account and the firm had never done wire transfers from the account. The bank did not detect these frauds or stop the wires. The people behind this fraud appear to have had intimate knowledge of how to send wires from a bank account. By the terms of the banking agreements the firm had signed with the bank, the firm was responsible for replacing the funds that were taken out of the firm's bank account.

Lawyers should not underestimate the sophistication of frauds targeting trust accounts. To better protect yourself from one of these frauds, see "Increasing your online banking safety" on page 14.

They will look for weaknesses in security configurations and exploit them in order to access firm networks. In very devious ways, they will try to trick you or your staff into helping them. It is quite possible they would target you individually, including attacking your home computer to hack into your office systems.

The bottom line: cybercrime is a real and present danger for law firms. All firms should work to understand the cybercrime risks they are exposed to and take steps to reduce the likelihood they will experience a data breach at the hands of cyber criminals.

How prepared are you?

To assess your cybercrime preparedness, see if you can answer the following questions:

- Are your passwords secure enough?
- Would you or your staff be duped by a phishing message?
- How would your firm respond if one of its servers was hacked?
- Is your anti-malware software the most current version and is it updated?
- Could you tell if your computer had malware on it?
- Are your computer's security settings adequate?
- Is there a backdoor into your network?
- What would happen if a firm laptop or smartphone were lost or stolen?
- How would you deal with a major data theft by an ex-employee?
- Is your home computer safe?

The remainder of this article, and the next one, will start you on the journey to help you understand and answer these questions. Tread carefully and thoughtfully as the health and the future of your practice could well rely on how well you address cybercrime risks.

The menace of malware

*Mal*icious soft*ware* ("malware") is one of the most common ways law firm computers and networks are infiltrated and compromised by cyber criminals. The malicious intent behind malware usually involves gaining unauthorized access to computers or networks to steal money, passwords or valuable information, or to cause disruptions or destroy data. Malware can affect individual computers, firm networks and even the operation of the Internet. In many cases, people will not know their computer is infected with malware (see "How to recognize if your computer is infected with malware" on page 16). Worse yet, removing malware from a computer is often very difficult.

There are many types of malware and they usually do one or more of the following tasks or damaging things:

- Record your keystrokes to capture usernames, passwords, credit card numbers and other personal information you enter while making purchases or doing online banking. This information is then sent to cyber criminals who will use it to hack your online accounts or systems.
- Create a "backdoor" that allows hackers to access your computer or network without your knowledge by bypassing normal authentication and security mechanisms.
- Disable your security settings and anti-malware software so the malware won't be detected.
- Use your computer to hack into other computers on your firm's network.
- Take control of individual programs and even an entire computer.
- Use your computer to send email messages to the people in your address book, who will in turn become infected if they click on links or open attachments in these messages.
- Use your computer to send spam to thousands of people, usually with the intent of infecting them.
- Steal the data on your computer.
- Alter or delete your files and data.
- Display unwanted pop-up windows or advertisements.
- Slow down your computer or network or prevent access to your firm website.
- Allow someone to secretly watch you through your webcam.

Malware employs varying mechanisms to self-replicate and infect other computers. Malware often requires some kind of deliberate action by a user to infect a computer or hijack an online account. For example, you can become infected with malware by doing the following things – most of them are common tasks that occur many times a day in every law firm:

- Opening an infected email attachment.
- Just visiting a website (no need to click on a link).
- Triggering a download by clicking on a link on a website.
- Triggering a download by clicking on a link in an email, instant message or social media post.
- Plugging an infected USB stick or external hard drive into your computer.
- Downloading a program to your computer, or an app for your tablet or smartphone.
- Installing a toolbar or other add-on to your browser.

Documents created on an infected computer can be silently infected, and if those documents are sent as an email attachment, anyone opening them can be infected. USB sticks or external hard drives that are plugged into an infected computer can become infected, and they in turn can infect other computers they are then plugged into. Once malware gets into a firm network, it will often spread to other computers on the same network. As they often have mixes of people from many different firms or online communities, deal rooms and document sharing sites can be a breeding ground for malware.

In some cases the computer user doesn't have to do anything – some types of malware (e.g., worms) can spread on their own without any user actions.

While viruses and worms are the most common types of malware, there are many other types which are described in more detail in the adjacent "Common types of malware" sidebar.

Cybercrime dangers can originate inside your firm too

Many people assume, incorrectly, that the biggest cyber dangers come from outside a law office. Statistics actually show that the majority of incidents involving the destruction or loss of data are perpetrated by current, soon-to-be dismissed or recently dismissed employees. Few, if any, know more about your firm's systems than your employees; and few, if any, are in a better position to cause major damage. In particular, your IT staff, employees with advanced technology knowledge, and outside technology support people are potentially the greatest threat. They have the greatest knowledge about your system configurations, the technical know-how to be very destructive, and they are often savvy enough to cover their tracks – erasing evidence of their presence and activities. Your cybercrime prevention efforts should address these internal dangers as well.

Now that you are familiar with basic cybercrime dangers, review the next article to gain an understanding of the steps you need to take to reduce your exposures to the cybercrime dangers that occur in law firms. ■

Dan Pinnington is vice president, claims prevention and stakeholder relations at LawPRO.

Common types of malware

Malware is classified by how it propagates itself or what it does. The names and a brief description of the common types of malware appear below:

Viruses:

Viruses are one of the most common types of malware and will do one or more of the tasks and damaging things listed in the adjacent text. Like their biological namesakes, computer viruses propagate by making copies of themselves. When an infected program runs, the virus will attempt to replicate itself by copying itself into other programs, usually while completing the malicious actions it is designed to do. Viruses often arrive in infected email attachments or via a download triggered by a click on a link in an email or on a website. Even just visiting a website can start an automatic download of a virus. Some viruses will send themselves to everyone in your contact list; others will use your computer to infect strangers as they come with their own address lists.

Worms:

After viruses, worms are one of the next most common types of malware. Unlike a virus, a worm goes to work on its own without attaching itself to programs or files. Worms live in a computer's memory and can propagate by sending themselves to other computers in a network or across the Internet itself. As they spread on their own, they can very quickly infect large numbers of computers and may cause a firm's network – or even parts of the Internet – to be overwhelmed with traffic and slow down or stop working all together.

Trojans:

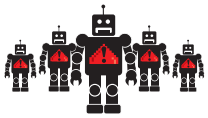
Trojans are named after the wooden horse the Greeks used to infiltrate Troy. A Trojan is a malicious program that is disguised as, or embedded within, otherwise legitimate-looking software. Computer users often unwittingly infect themselves with Trojans when they download games, screensavers, utilities, rogue security software or other enticing and usually "free" software from the Internet. Once installed on a computer, Trojans will automatically run in the background. Trojans are used for a variety of purposes, but most frequently they will open a backdoor to a computer or capture keystrokes so that sensitive information can be collected and sent to cyber criminals. See the sidebar on page 7 for details of a large fraud involving a Trojan infection.

Spyware:

Like Trojans, spyware also often comes in the form of a "free" download, but can also be installed automatically when you click on a link or open an attachment. Spyware will do many different things, but usually it will collect keystrokes or other information about you that will be shared with third parties without your consent. This can include usernames, passwords and surfing habits.

Adware:

Adware works like spyware, but will focus on your surfing habits and will slow down or stop your browsing by taking you to unwanted sites and/or inundating you with uncontrollable pop-up ads while you are browsing the web.



Botnets:

A botnet is a collection of software robots ("bots") that together create an army of infected computers (known as "zombies") that are remotely controlled by the originator. Your computer may be part of a botnet and you may not even know it. On an individual level, bots will do most of the typical malware tasks and damaging activities. When working together, botnets are used to execute denial-of-service attacks (DoS attack) or distributed denial-of-service attacks (DDoS attack). A DoS attack is accomplished when thousands of computers are told to visit a particular website or server at the same time, thereby crashing it and/or making it impossible for regular users to access it.

Rootkits:

Once malware is installed on a system, it is helpful if it stays concealed to avoid detection. Rootkits accomplish this by hiding inside the host computer's operating system. They can be very hard to detect and will do most of the typical malware tasks and damaging activities.

Scareware:

Scareware is plain devious. While visiting a website, a pop-up advertisement will appear with a "Your computer may be infected with harmful spyware programs. Immediate removal may be required. To scan, click 'Yes' below." If you click "yes," you download malware onto your computer.

Ransomware:

Ransomware infections are becoming much more common recently and are usually spread by infected email attachments or website links that trigger a download. The most common type, Cryptolocker, will scramble all the data files on your computer with virtually unbreakable encryption. You learn you are infected when a pop-up window tells you that your data has been scrambled and will be deleted unless you pay a ransom within a very short period of time, typically 48 hours or so. The ransom is typically in the range of $100 to $300 and payable only in Bitcoins, a type of virtual currency that makes payments untraceable. It is a relatively low amount so you have an incentive to pay it as a nuisance; but as you are dealing with criminals, paying it does not guarantee that you will get your data back.