Protecting yourself from cybercrime dangers: The steps you need to take

Cybercrime dangers are many, complex and ever-changing. Hardly a day goes by without another news report of a data breach or other cyber-related scam or theft. Cyber criminals have considerable resources and expertise, and can cause significant damage to their targets. Cyber criminals specifically target law firms as law firms regularly have funds in their trust accounts and client data that is often very valuable. LawPRO encourages all law firms to make dedicated and ongoing efforts to identify and understand their potential cybercrime vulnerabilities, and to take steps to reduce their exposure to cyber-related dangers. This article reviews the specific cybercrime dangers law firms need to be concerned about, and how they can mitigate their risks.

It starts with support from senior management

Any effort to tackle cybercrime must start at the top. Senior partners and firm management must be advocates of cyber security, support the implementation of appropriate practices and policies, and allocate sufficient resources to address cybercrime exposures. While there are some quick fixes that can help make your office and systems more secure (to find them see "quick fixes" opposite), most firms will need to spend some time and money to better protect themselves from cybercrime. This may include upgrading or installing new technology, training staff, and changing how some tasks are done.

Firms should also put some thought into how a cyber breach – the loss of client data or hacking of a firm server – would be handled. Firms should have a formal incident response plan so they can avoid making bad decisions on an ad hoc basis in the middle of a crisis. See page 28 for an article on incident response plans.

You likely need expert help

Beyond the very practical issue of wanting to avoid being the victim of cybercrime, remember that when using technology, lawyers and paralegals must meet their professional obligations as outlined by the lawyers' *Rules of Professional Conduct* and the *Paralegal Rules of Conduct*. These rules provide that you should have a reasonable understanding of the technology used in your practice, or access to someone who has such an understanding [Rule 2.01 of the lawyers' Rules, Rule 3.01 of the Paralegal Rules].

It is unlikely that sole practitioners and smaller firms will have someone on staff who has the technical expertise to properly address all relevant cyber security issues. With their larger and more complex technology infrastructures, even medium and larger firms may also need to seek outside help. One of the biggest dangers here is that people just don't realize what they don't know when it comes to cybercrime dangers and how to prevent them. LawPRO encourages firms to seek appropriate help from knowledgeable experts when required. To identify vulnerabilities, firms may want to consider engaging an outside expert to do a formal security assessment.

Staff education and technology use policies

As you will learn in this article, despite being technology-based, many cybercrime dangers involve a human element. Cyber criminals create situations in which law firm staff and lawyers will unintentionally and unknowingly facilitate cybercrimes as they go about their

Immediately increase your security with these "quick fixes"

While some of the work that must be done to protect a firm from cybercrime will take time and effort to implement, there are a number of things you can do that are fast and easy and that can be done at little or no cost. These "quick fixes" are highlighted throughout this issue with this quick fix logo.

common daily tasks. Educating staff to help them understand, recognize and avoid cybercrime dangers is a critical part of reducing cybercrime risk.

Written policies that clearly establish guidelines and requirements governing the acceptable use of all firm technology resources can also help reduce cyber exposures. Through technology use policies, law firm staff should be given clear direction on what they are permitted and not permitted to do with law firm technology resources. These policies should use simple and non-technical language that all employees can understand. They should be reviewed with new employees at the commencement of employment, and on an annual basis with *all* staff. It is also essential that these policies be consistently and strictly enforced.

Every technology use policy should cover some basics. They should clearly state that technology resources provided by the firm, including Internet and email access, are to be used for legitimate firm activities. Staff should understand that they have an obligation to use resources properly and appropriately. Technology use policies should also direct firm staff to ensure that the confidentiality of firm and client information is protected at all times, that there is compliance with network system security mechanisms, and that resources are not used in a manner that would negatively affect others on the system. Technology use policies should also indicate that the firm retains the right to monitor any and all electronic communications and use of the Internet to ensure the integrity of the firm's systems and compliance with the firm's technology use policy. As well, the policy should indicate that there may be sanctions for failure to comply.

You can find some sample technology use policies you can use and adapt for your firm on practicePRO.ca.

The cybercrime dangers you need to address

The cybercrime dangers firms need to address are many and varied. This article reviews these dangers in more detail and will help you start on the work that is necessary to address them so you can reduce the likelihood that cyber criminals will breach your law firm's systems. These topics covered in the sections to follow are:

1. Avoid the dangers of email
2. Lock down your browser and avoid surfing dangers
3. Avoid infections with antivirus and/or anti-malware software
4. Lock things up by using passwords properly
5. Address security vulnerabilities by installing operating system and program updates
6. Keep the bad guys out with a firewall on your Internet connection
7. Stump hackers by changing key default settings
8. Lock down and protect your data wherever it is
9. Scrub confidential client information on discarded equipment
10. Be safe when using remote access and public computers
11. Secure your mobile devices to protect the data on them
12. Harden your wireless and Bluetooth connections and use public Wi-Fi with extreme caution
13. Be careful about putting your firm's data in the cloud
14. Inside people can be the most dangerous
15. Be careful of the dangers of BYOD and family computers
16. A backup could save your practice after a cybercrime incident

As they can be used as a point of access to your firm's systems, it is critical to address the above issues on your personal smartphones and tablets, as well as your home computers and networks.

You must address all the dangers

Don't be tempted to ignore any of the dangers listed above, or to skip or skimp on the steps suggested to deal with them. Remember, your data and systems are only as safe as the weakest link in your security plan. When you leave on vacation, you lock every door and window in your house. Leaving just one door or window open gives a thief easy and instant access. To protect yourself from cybercrime, it is critical that you fully and properly address all cybercrime dangers. Cyber criminals will look for and exploit holes in your security plan.

Note that some of the configuration changes suggested in this article will require you to have "administrator" access to your device or systems. Operating your computer or device with the administrator account (or an account that has administrator status) will allow you to freely change your configuration or settings. A regular "user" account will not have the ability to change many device or software settings. To prevent regular staff from changing their settings and intentionally or unintentionally causing damage to your systems, everyone in your office should be using a "user" account, not an administrator account or accounts with administrator status. Doing your day-to-day work while logged into a "user" account can also reduce the damage that a malware infection will cause. Without administrator access, the malware will be restricted in its abilities to change settings on your computer.

As a final note, you may find yourself unable to change your configuration if your firm centrally administers and controls the settings for computers and other devices. Speak to your technology support person if you have questions or concerns.

Avoid the dangers of email

1

Email has become a primary communications tool for the legal profession. It allows virtually instant sharing of information and documents between lawyers and their clients. Email is also one of the most dangerous tools in a modern law office. Infected attachments, spam and phishing attacks delivered by email make it easy for cyber criminals to deliver malware and breach law firm security protections. It is essential that you educate your lawyers and staff about these dangers and the steps they should take to use email safely.

Be wary of attachments

While email attachments are frequently used to share documents between lawyers, law firm staff, and clients, they are also one of the most common delivery mechanisms for malware. While most messages that have infected attachments will be stopped if your anti-malware software and/or spam filter are working properly and updated, some will make it through. For this reason, everyone at a law firm should follow these two simple rules:

QUICK FIX

1. No matter how interesting or enticing they appear to be (e.g., jokes, celebrity gossip or pictures), never open attachments from strangers.
2. No matter how interesting or enticing they appear to be, never open attachments unexpectedly sent to you by people you know.

The reason for Rule #1 should be obvious – enticing attachments from strangers usually have a malware payload. The reason for Rule #2 might be less obvious: to trick you into feeling comfortable about opening an attachment, some types of malware will send an email with an infected attachment to all the address book contacts it finds on a computer that it has just successfully infected. This is done intentionally with hope that people getting such a message will be comfortable opening the attachment as it came from someone they know – and bingo – the person opening the attachment will become infected and all *their* contacts will get a similar message.

Use spam filters to avoid annoying and dangerous spam

On a daily basis you undoubtedly receive unsolicited commercial junk email, advertising or other offensive messages commonly known as spam. Spam is not only annoying – it is also very dangerous as it is commonly used to deliver malware (if you click on a link in the message) and phishing scams (see the next heading).

To combat spam, many firms use spam filters that are intended to detect unsolicited and unwanted email and prevent those messages from getting into a user's inbox. Spam filters use various criteria to identify spam messages, including watching for particular words or suspicious word patterns, messages that come from websites that are known to send spam, etc. Anti-spam products also use "blacklists" that intercept messages from recognized spammers, and "whitelists" that let messages through only if they come from your personal list of recognized email addresses or domains (the domain is the main part of an email address or website, for example, lawpro.ca or gmail.com).

QUICK FIX

If your email program includes a spam or junk mail feature, you should turn it on. For additional protection, consider installing a third party spam filter. They are often included in anti-malware suites. See page 14-15 for more information on anti-malware software.

QUICK FIX

While spam filters can significantly reduce the amount of spam you receive, they are not perfect. They will sometimes let spam messages through. Advise firm staff not to open or respond to spam messages, and to flag them as spam so that the spam filter can learn to recognize and prevent a similar message from getting through in the future.

QUICK FIX

Links in spam messages will often cause malware to be downloaded to your computer. For this reason, everyone at a law firm should be told to never click on links in spam messages, no matter how interesting or enticing they appear to be.

Don't be fooled by phishing

Did you know that emails appearing to come from companies you trust may actually be from criminals trying to steal your money or identity? Because they are so successful at duping people, "phishing" emails have quickly become one of the most common and devastating scams on the Internet.

Phishing scams use spoofed (meaning faked or hoax) emails and websites to trick you into revealing your personal and financial information. By using the trusted brands and logos of online retailers, banks, or credit card companies, phishing scammers trick surprisingly large numbers of people. The phishing email directs users to visit a website where they are asked to confirm or update personal information such as: passwords; and credit card, social insurance and bank account numbers. In doing so, people are tricked into giving this information directly to cyber criminals, who, in turn, use it for identity theft, financial theft or other cybercrimes.

Legitimate companies will never ask you to update your personal information via an email message. Don't get tricked by phishing scams. See the "Could it happen to you" column on page 32 to learn how to recognize and avoid phishing scams.

Lock down your browser and avoid surfing dangers

2

After email, your Internet browser is probably the second most dangerous technology tool in your office. Even casual surfing on the web can expose you to malware and other cyber security issues. You and your staff need to know how to safely surf the web and configure your browsers so that surfing is less dangerous.

Safely surf the web

Teaching your staff the following surfing "don'ts" will help you reduce cyber-related surfing risks, and reduce the likelihood of a malware infection:

- Don't complete online transactions involving account information, passwords, credit card numbers or other personal information, unless you are on a secure connection as indicated by an "https" in the website address (see sidebar on page 14).
- Don't visit unknown websites, and especially music, video, or pornography sites because they are often loaded with malware.
- Don't use file sharing sites, or services unless you are familiar with them and know the people you are sharing files with.
- Don't download software, unless it's from a reputable and trusted site.
- Don't download new apps (wait until downloads hit the thousands and it is likely any malware in the app has been detected).
- Don't download browser add-ons, plug-ins or toolbars, especially from unknown or untrusted sites.
- Don't click on "OK," "Yes" or anything else in browser "pop-ups" (the small windows that sometimes open within a browser). These are sometimes made to look like "dialog boxes" (the windows you change settings or options in) to make you think you are clicking on options or settings you normally deal with. Quickly closing all browser windows and tabs can help, especially if you are being flooded with multiple pop-ups. On Windows-based browsers use Ctrl+W or Alt+F4 to repeatedly close the top-most tab or browser window. In Safari, ⌘+Shift+w will close all tabs in the current window and ⌘+q will close all Safari windows and tabs.

Run an antivirus or anti-malware program that runs in the background and scans for dangers (see below for more information on anti-malware software).

If you are doing online banking for your firm trust or general accounts, it is critical that you ensure all security risks are addressed. See the "Increasing your online banking safety" sidebar on page 14 for the extra steps you need to take.

Beware the dangers of social media

Many people are comfortable sharing a great deal of personal information on Facebook, Twitter, Instagram and other similar social media tools. While family and friends may enjoy this information, people should keep in mind that cyber criminals could use the same information to assist them in personal identity theft or the hacking of online accounts. Be cautious about the amount and type of information you share on social media. Posting vacation pictures while you are away or using apps that broadcast your location (e.g. Foursquare) tells the world you are away from your home and office.

Facebook, Twitter, LinkedIn and some other sites can be configured to only let you login on a secure connection (see the adjacent sidebar on https connections). This can prevent your account from being hacked since your login credentials and connection are encrypted, making it harder for someone to intercept them.

Lock down your browser

Malware programs can automatically and secretly install themselves while you are browsing. These are called "drive-by downloads." This occurs when websites run scripts (small bodies of code designed to perform a specific action) or ActiveX controls (a module of code that adds extended functionality to the browser).

All browsers allow you to change individual configuration settings, many of which can deal with these and other security issues. Some browsers let you easily change multiple security or privacy settings by choosing from different levels of security (Medium-high or high are best). While changing browser settings can provide greater protection, it may also prevent some websites from running properly. While the options and terminology will change slightly between the various browsers, these are some of the settings you should change to lock down your browser:

- prevent pop-ups from loading (or prompt you before loading a pop-up).
- disable JavaScript.
- don't accept third party cookies.
- delete cookies on exit.
- clear history at close.
- disable ActiveX controls (or prompt to run ActiveX controls).
- enable automatic updates.

See the "Browser Security Settings for Chrome, Firefox and Internet Explorer: Cybersecurity 101" webpage for detailed instruction on how to lock down these three browsers. "iOS: Safari web settings" on the Apple Support site has information on Safari security settings.

There are also various browser plug-ins and add-ons that can increase browser security and warn you about suspicious activity. Widely used WOT (Web of Trust) will warn you about untrustworthy sites (available for all browsers).

Pharming

"Pharming" is another common trick used to perpetrate scams. Pharming takes you to a malicious and illegitimate website by redirecting a legitimate website address. Even if the website address is entered correctly, it can still be redirected to a fake website. The fake site is intended to convince you that it is real and legitimate by spoofing or looking almost identical to the actual site. When you complete a transaction on the fake site, thinking you are on the legitimate site, you unknowingly give your personal information to someone with malicious intent.

You can avoid pharming sites by carefully inspecting the website address in the address bar. Make sure you are on the site you intended to visit and look for "https" (see sidebar on next page) before you enter any personal information, passwords, credit card numbers, etc.

The S in https means you are on a safe and secure connection

QUICK FIX

When logging in on any website, you should always check for a secure connection by checking to see if the web address begins with https://..., as opposed to http://... Look for the "s" which signals that your connection to the website is encrypted and more resistant to snooping or tampering.

Avoid infections with antivirus and/or anti-malware software

3

Good behaviour alone will not protect you from viruses or other malware infections. You must run software that will prevent and/or detect infections on your computers, and you may want to consider it for your tablets and smartphones too.

But what is the difference between antivirus and anti-malware software? As explained in the "Common types of malware" sidebar on page 9, viruses are a specific type of malware. Malware is a

Increasing your online banking safety

Many law firms manage their trust and regular bank accounts on the Internet, and some firms have the ability to initiate various banking transactions online, including account transfers and wiring funds. While the convenience and efficiency of online banking are huge benefits, the downside is that online banking exposes you to security risks. The steps outlined below will help law firms to understand, address and reduce online banking risks – for both your firm and personal accounts.

- **Know and understand the terms of your banking agreements:** As a starting point, carefully read your bank account and electronic banking services agreements. Make sure you understand the obligations these agreements place on you with respect to using the account. In particular, make sure you are familiar with the notice requirements for unauthorized transactions, and who is responsible for unauthorized transactions. In most circumstances it will be you, unless in specified and usually narrow circumstances you give prompt notice to the bank.
- **Remove account features you won't use:** If hackers ever managed to get into your account, the ability to access multiple accounts or to initiate transfers or send wires could allow them to easily remove funds from your account. If you don't intend to use your online banking facility for these types of transactions, have this functionality removed from your account.
- **Only do online banking from a secure firm computer:** The computer used for online firm banking should be a firm computer that has all software updates installed, is running updated anti-malware software, and is behind a firewall. To reduce the potential for other cyber risks, consider restricting the activities that occur on the computer used for online banking.
- **Have real-time protection running and run regular malware scans on your banking computer:** This should hopefully help detect an infection as it is happening, or detect one that occurred without triggering the real-time protection warnings. See "Avoid infections with antivirus and/or anti-malware software" on page 14.
- **Never use public computers to do banking for the firm:** If doing so, passwords or account data may be accidentally stored on the computer or captured by malware making it accessible to others.
- **Never conduct financial transactions over an unsecured public Wi-Fi network:** Communications on an unsecured Wi-Fi connection can easily be intercepted. See additional comments on Wi-Fi at page 20-22.
- **Use a secure and unique password that is changed regularly:** Your online bank account should not have the same password as any other account. It should be a strong password (see the Tech Tip on page 30 to learn how to create a strong password). Online banking passwords should never be stored on a mobile device or anywhere else that could make them easily accessible by another person.
- **Check your online bank account every day:** By monitoring your daily account activity, you'll be able to promptly identify any unauthorized transactions or other indications that your account has been hacked. Check the last login time and make sure it is consistent with the last time someone from your office accessed the account. Immediately report suspicious or unexplained activity to your bank.
- **Configure email or text message activity alerts:** Most banking websites allow users to sign up for notifications. You will then receive an email or a text message whenever a specified amount of money is withdrawn or deposited to your account, or if there is unusual activity such as international transactions. Some banks will also phone a firm for confirmation that a transaction that was initiated online is to go through.

broad term used to describe many different types of malicious code, *including* viruses, but also Trojans, worms, spyware, and other threats.

Does this mean antivirus software will only protect you from viruses and anti-malware software will protect you from all kinds of malware, including viruses? The answer is, unfortunately, it depends. While most of the more popular tools will scan for many types of malware, you need to look at the specific functionality of each product to know for sure what it will protect you from. From this point forward this article will refer to the broader category of anti-malware software.

The options

Windows computers are prone to infections so you must run anti-malware software on them. Microsoft Security Essentials is a free product you can download to help protect computers running Windows XP, Windows Vista, and Windows 7. Windows 8 includes Windows Defender, also free. Both offer good real-time anti-malware protection.

There are a number of widely used commercial anti-malware programs, some that come in suites that include other functionality like anti-spam, firewalls, remote access, device location and scrubbing.

The two most widely used antivirus programs are Norton™ AntiVirus (symantec.com) and VirusScan (mcafee.com). Expect to pay $40-$60 per computer to buy the software, plus an additional annual fee for virus signature file updates (see opposite). Buying antivirus software that is bundled with other products, such as firewall and anti-spam software, will save you money.

Until recently, it was generally felt it was not necessary to run anti-malware software on Apple computers as the Mac OS architecture prevented infections and there were no real malware threats targeting Macs. There are now potential malware threats, and consider ClamXav, an effective and free antivirus program for Mac OS X computers. Note: If you run a Windows emulator on a Mac computer you open yourself to the full gamut of Windows malware risks and you must use a Windows anti-malware tool.

Tablets and smartphones are, in general, much less likely to get malware infections, but you may want to run anti-malware apps on them for greater protection.

As no one tool will catch everything, you may want to consider using more than one anti-malware tool. To better protect yourself, install one security tool that scans for as much as possible and that runs all the time in the background with an on-access scanning engine. This will protect you from threats as you surf the web, install applications, open files and complete your other daily activities. Then, install another anti-malware tool that you can occasionally use on demand to make sure nothing got through or was overlooked. Scan your entire hard disk(s) at least weekly, either manually or automatically (automatic is better as you don't have to remember to do it).

Bitdefender QuickScan is a free online scan that is handy if you need a second opinion on a Windows computer.

But note, it is important to make sure you do not run two antivirus applications simultaneously. Anti-malware programs do not usually play well together, and running two at the same time can often lead to one identifying the other as a virus, or in some cases, file corruption. Running two at the same time will likely also slow your computer down.

Malware can be extremely difficult to remove from a computer, so it is best to prevent infections. However, if you do get an infection, Malwarebytes Anti-Malware is a good free tool for removing malware from a Windows computer.

QUICK FIX

Installing anti-malware software updates is a must

Installing anti-malware software is only the start. You also need to regularly update your virus definition or signature files. Anti-malware programs use the information in these files to recognize virus infections when they are occurring. As there are new viruses being created every day, you need to have the most recently released virus signature file to be protected against all known infections. These updates are available on your anti-malware vendor's website. Expect to pay about $30-$40 per year for these updates.

Most anti-malware programs can be configured to download these updates automatically, without user intervention. Make sure the automatic update feature is enabled as this helps ensure that your protection is always up-to-date.

QUICK FIX

Staff can help you spot malware infections

Sometimes anti-malware software will not detect that an infection has occurred. While malware can be on a computer and never give any hint of its presence, in many cases there are clues that a computer is infected with malware. See the "How to recognize your computer is infected with malware" sidebar for a list of these symptoms. Teaching your staff to recognize these symptoms could aid in the earlier detection of an infection.

4 Lock things up by using passwords properly

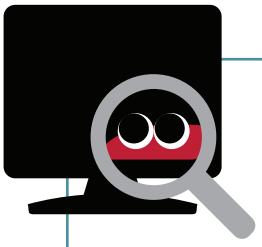
Like the keys that start your car or open the front door of your home or office, computer passwords are the keys that "unlock" your computer, your mobile devices and access to all the data on your network systems. We all have more passwords than we can remember. This tends to make us a bit lazy. We use obvious and easy to remember passwords – even the word "password" itself. Or worse: We don't use them at all.

Cyber criminals know and exploit bad password habits as they are often one of the weakest links in data security schemes. For this reason, it is critical that all lawyers and staff in a law office use passwords properly. The Tech Tip in this issue, "Keeping your passwords strong and secure" (see page 30), reviews the steps you can take to properly use and protect the confidentiality of your passwords, and how you can create passwords that are harder to guess or determine.

Address security vulnerabilities by installing operating system and program updates

5

There are millions of lines of computer code in the operating systems and programs that run on your computers, tablets and smartphones. These operating systems and programs will have hundreds or even thousands of settings and features. These settings and features are intended to allow you to do all the things you want to on these different devices.



How to recognize your computer is infected with malware

Ideally you have one or more types of properly updated anti-malware software running on your computers and networks. And hopefully that software detects and prevents any malware infections from occurring. However, because anti-malware software may not detect an infection, watch for the symptoms that can indicate a computer is infected with malware. These include:

- It takes longer than usual for your computer to start up, it restarts on its own or doesn't start up at all;
- It takes a long time for one or more programs to launch;
- Your computer and/or programs frequently lock up or crash;
- Programs are starting and running by themselves;
- Your hard drive runs continuously, even when you aren't working on the computer;
- Your files or data have disappeared;
- You find files with new or unfamiliar filenames;
- Space on your hard drive(s) is disappearing;
- The homepage on your web browser has changed;
- Your browser starts launching multiple tabs;
- Web pages are slow to load;
- There is a lot of network or web traffic, even when you are not browsing the web or using the computer; and/or
- Parts, or all, of your computer screen look distorted.

If one or more of the above things are happening, make sure your security software is up to date and run it to check for an infection. If the first scan finds nothing, try running a scan with a second product. If the odd behaviours continue or there are other problems, seek technical help.

Amongst all these settings and features, cyber criminals look for "exploits." An exploit is a particular setting, feature or sequence of commands that will cause an unintended or unanticipated behaviour to occur on a computer or other device. Exploits create security vulnerabilities because cyber criminals can use them to open a back-door to your network, allow malware to run, or do other damaging things. New exploits are discovered on a weekly or even daily basis.

Updates

When an exploit is discovered, software companies quickly rewrite their code and release updates or patches to stop the exploit from working. To protect against newly discovered exploits, devices must be updated with the latest versions of operating systems and programs.

To keep your computers and other devices safe, you should be checking for and installing updates regularly, ideally on a weekly basis. This is particularly the case for Microsoft products, which are prone to security vulnerabilities. While not as prone to vulnerabilities as Microsoft products, Apple products should be updated regularly as well. Don't forget to update the other non-Microsoft or non-Apple software running on your devices. Sometimes direct links to an updates webpage can be found on the Help menu. Otherwise, you should be able to find the software product's site with a search on Google.

If you are using Windows XP or Office 2003, note that Microsoft will no longer be supporting these products as of April 8, 2014. Using these products after this date will expose you to greater security dangers. See the "Stop using Windows XP and Office 2003 on or before April 8, 2014" sidebar if this applies to you or your firm.

Automatic updates

QUICK FIX

Enabling automatic updates can help keep your computers and other devices up-to-date. Both Windows and Apple operating systems have an "automatic update" feature that automatically notifies you when updates are available for your devices. Once activated, the device will periodically check for updates. Available updates will be downloaded, and depending how you configure things, installed with or without your knowledge. Some people prefer to set the automatic updates feature to ask for permission to install updates to avoid problems that might arise due to an update installation. Others prefer to have updates installed without intervention from the computer user (this can help make sure updates get installed).

QUICK FIX

The Ninite.com site can help Windows computer users check for and install updates (for free). Note, in some firms individual users will have no control over updates as the installation of updates will be centrally controlled and managed. The paid version of Ninite can be used for this purpose for Windows computers.

Back up before you install updates

It is very important to remember that installing updates can unintentionally interfere with the way your computer/device or individual programs/apps operate. It is possible that a program/app may not operate properly or at all, that data could be lost, or that a device will fail to restart after an update is installed. Creating a restore point (a temporary backup of your configuration and data) and/or making a proper backup of all the programs and data on a device before you install updates can help you recover if there are unanticipated problems. See page 24 for more information on backups.

6 Keep the bad guys out with a firewall on your Internet connection

When you are connected to the Internet, the Internet is connected to you. For computers to transmit data back and forth over the Internet, lines of communication must be established. These communications work through "ports" that are opened on each computer. The problem is that all the computers on the Internet can see one another, and these ports can allow unauthorized people to access the data on a computer and even take control of it.

Regardless of how your office connects to the Internet, your computer systems must be protected by a firewall – a type of electronic gatekeeper that ensures all incoming and outgoing communications are legitimate. A firewall watches these ports and will warn you about or prevent unauthorized communications.

Firewalls come in two varieties: software and hardware. Software firewalls are easier to set up, usually protect a single computer, and are adequate for personal or small firm use. Hardware firewalls are usually used to protect an entire network of computers. The more recent versions of both the Windows and Mac operating systems have a built-in firewall that you should enable. High-speed modems generally include a basic firewall. If you are using remote access software, you should consider using a hardware firewall to better protect the ports that must be opened for the remote access software to work.

7 Stump hackers by changing key default settings

Changing the default settings for the hardware and software used in your office is another critical step in safeguarding the security of your data and protecting yourself from cybercrime. This is probably the most technical of the steps outlined in this article and you may need expert help.

Every computer operating system, program, and app, and every piece of hardware has certain preset or default settings. These are necessary to make them operate out of the box in a consistent manner that the vendor and user will expect.

However, these default settings are common knowledge (and if you don't know them, you can find them with Google in about five seconds), and hackers can use them to compromise a network, computer or other device. For example, if the administrator account on a computer is named "Administrator" (it frequently is), a cyber criminal only has to work on figuring out the password to hack into a system or device. If you change the name of the Administrator account to something different, your computer is much safer as the hacker has to work much harder to figure out both the name of the administrator account and its password.

You can make your systems much safer by changing the following key default settings:

- administrator account names
- server names
- network or workgroup names
- ports (change to non-standard ports and close standard ports that you don't use)
- standard share names

Stop using Windows XP and Office 2003 on or before April 8, 2014

Microsoft will no longer be supporting Windows XP SP3 (Service Pack 3) and Office 2003 (SP3) as of April 8, 2014. After this date, there will be no new security updates, non-security hotfixes, support or online technical content updates from Microsoft for these products. Your computer will still operate, but if you continue to use Windows XP or Office 2003, you will become more vulnerable to security risks and malware infections. Undoubtedly, cyber criminals will target computers that are still using these programs. For this reason, you should immediately start planning to migrate to more current versions of Windows and Office on all law firm and home computers running Windows XP or Office 2003. Note that most current versions of these products are Windows XP SP3 and Office 2003 SP3. If you are using SP2 or earlier versions of these products, you already have greater security vulnerabilities; as a short-term fix, you should update to SP3 if you don't already have plans to move off Windows XP or Office 2003.

Lock down and protect your data wherever it is

8

Long gone are the days when you had to worry about a single file folder that held all the documents for a particular matter, which you could easily secure by keeping it locked in a file cabinet. Today, client data can exist in electronic form in many different places inside and outside your office. You need to know where that data exists, who can access it, and what steps should be taken to secure and protect it from cyber criminals.

Physical access to servers, routers and phone switches

Protecting your server(s) and other key telecommunications equipment such as phone switches and routers starts with physical security. Intruders who have physical access to a server can get direct access to files and data on the server's hard drives, enabling them to extract the usernames and passwords of every user on the system, destroy data, or give themselves a backdoor for accessing the server remotely. Even curious employees who want to change settings can unintentionally cause serious problems. Put your servers and other key telecommunications equipment in a locked room to protect them from unauthorized access. Be cautious about any wall jacks for your network in unsecured areas of your office.

Access to devices on startup

QUICK FIX To protect the information on them, and the information on any network they connect to, every computer, tablet and smartphone should be configured to require a password at startup. Devices without a startup password allow free and unfettered access to anyone that turns them on.

Better yet, in addition to a startup password, consider encrypting the data on devices. Passwords will prevent the average person from accessing your device, but can be bypassed by people with greater expertise. Encryption will make information on devices far more secure. QUICK FIX The operating systems on some devices have built-in encryption capabilities or you can install third party encryption programs or apps.

Put a password on your screensaver

QUICK FIX Activating a password-protected screensaver is a simple and very effective way to prevent an unauthorized person from rifling through the data on a computer or other device that's been inadvertently left on. All versions of Windows and Apple operating systems allow you to add a password to a screensaver. QUICK FIX Remember to log out of any applications containing sensitive data and lock your screen when you leave your desk, or set a fairly short wait time on your screensaver so that it locks automatically if you step away. BlackBerry, Android, iOS and Windows mobile devices also have an automatic screen-locking feature.

Access across a network

Almost every law office has a computer network with one or more central servers. Client and firm information can be stored on these servers, making it accessible to everyone in the office. To better protect information from unauthorized access, take time to understand what information is stored on your network servers, and who has access to that information.

"Network shares" make folders available and visible across a network. "Permissions" control what people can do with the data in a folder. Someone with "full access" can create, change or delete a file, whereas someone with "read only" access can open and copy a file, but not delete it. Segment your data and set appropriate access levels (e.g., public, sensitive, very private) so that access to sensitive information is limited or prevented. Remember that privacy legislation requires that you limit access to some types of personal information (e.g., financial and health-related data) on a need-to-know basis.

Restricting access to more sensitive data can help protect it in the event your network is hacked or an unhappy employee with bad intentions goes looking for data.

Your desktop or laptop computer can act like a server in some cases, and content on your hard drive could be shared and accessible to someone across a network or through the Internet. QUICK FIX To prevent this from happening, you need to make sure that file and printer sharing is turned off on your computer.

Scrub confidential client information on discarded equipment

9

Many of the technology devices used today are essentially disposable. When they get old or break down, they are simply discarded as it is too expensive to upgrade or repair them. As a result, law offices will frequently find themselves discarding older computers and other devices. This is problematic as these devices often have confidential client information on them.

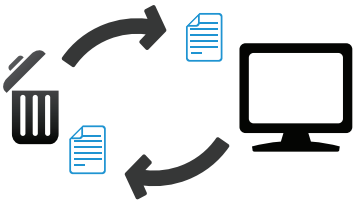
There are risks in donating your old computers to charity or a local school where a classroom of technology-savvy students will be itching to recover your data. Be sure to remove the hard drive from any computer you donate, or make sure the data on the drive has been thoroughly removed (see below).

Third party access to confidential client or firm information can also be an issue if you are sending your electronic equipment outside the office for repair or maintenance.

Client information can be in unexpected places. Most modern photocopiers and printers actually have hard drives on board that store copies of the images that go through them. This data can easily be found on, or recovered from, the hard drives on these devices.

Deleted doesn't mean deleted

It's a common misconception that deleted files are gone for good. In fact, the deleted files on most devices (e.g., computers, tablets,



smartphones, etc.) are easy to recover using widely available forensic recovery tools. Even reformatting or repartitioning a hard drive will not completely destroy all the data on it.

QUICK FIX Keep in mind that forensic technology can also be used to restore deleted files on portable media (e.g., CDs, DVDs, USB sticks, SD cards), so you should always use new media when sending data outside your firm.

Physically destroying a hard drive or other device with a hammer is the free and low-tech option. You can also use specialized software that will "scrub" all data from a hard drive so that it is not recoverable. Widely used free tools for this task include CCleaner, Darik's Boot And Nuke (DBAN), and File Shredder.

Being safer when using remote access and public computers 10

Being able to access your work network while you are out of the office can provide increased productivity and flexibility. However, opening your systems to remote access creates a number of security risks as external network connections are a ripe target for cyber criminals. And you should think twice about using public computers for firm work.

Setting up safe remote access

There are many tools that allow you to easily set up remote access (e.g., PCAnywhere, GoToMyPC, LogMeIn, TeamViewer, SplashTop). If properly configured, these are suitable for a smaller law office or home setting. Virtual private networks or VPNs may make remote access more secure. A VPN is a network connection constructed by connecting computers together over the Internet on an encrypted communications channel. VPNs are secure and fast, but may be expensive and harder to configure.

Securing remote access may require a degree of technical knowledge and advice from a computer expert. To make your remote access safe, you must secure your network and your remote access devices.

Do the following to secure your network:

- Use a firewall and security software to keep out unwanted connections.
- Only give remote access to people who really need it.
- In order to protect sensitive information, restrict the type of data that can be accessed remotely.
- Make sure all computers connecting to your network, including personal home computers, have up-to-date security software installed.
- Review firewall and other server logs to monitor remote access and watch for unusual activity.

Do the following to secure remote access:

- Ensure installation of remote access clients is done properly.
- Restrict access to the minimum services and functions necessary for staff to carry out their roles.
- Ensure that all staff use strong passwords on devices accessing your network remotely (see page 30).
- Change remote access passwords regularly. QUICK FIX
- Make sure that staff do not set their devices to login automatically and that they never store their passwords on them.
- Use strong authentication that requires both a password and token-based authentication.
- Have a formal remote access policy that clearly describes what staff are to do or not do with remote access.
- Delete staff remote access privileges if they are no longer needed, and immediately when a person leaves or is terminated (see "Inside people can be the most dangerous" at page 23).

The extreme dangers of using public computers

Public computers in libraries, Internet cafes, airports, and copy shops are an extreme security risk. While you can take steps to reduce these risks, it is still very dangerous to access sensitive client information on them. Start with the assumption that most public computers will have malware on them and let this govern your activities accordingly.

The following steps can reduce some of the risks associated with public computers: QUICK FIX

- Try to turn on the "private browsing" feature.
- Watch for over-the-shoulder thieves who may be peeking as you enter sensitive passwords to collect your information.
- Uncheck or disable the "remember me" or "log in automatically next time" option.
- Always log out of websites clicking "log out" on the site. It's not enough to simply close the browser window or type in another address.
- Delete your temporary Internet files, cookies and your history.
- Never leave the computer unattended with sensitive information on the screen, even for a moment.
- Never save documents on a public computer.

These measures will provide some protection against a casual hacker who searches a public computer you have used for any information that may remain on it. But keep in mind, a more sophisticated hacker may have installed a keylogger to capture passwords and other personal information entered on a public computer. In this scenario

the above steps won't prevent your information from falling into the hands of the hacker. This is why it is not a good idea to access sensitive client information or enter credit card numbers or other banking information on a public computer.

11 Secure your mobile devices to protect the data on them

Lost or stolen laptops, smartphones and USB sticks are frequently involved in major data breaches. This is because they often contain large amounts of confidential or sensitive information (e.g., client data, firm and personal information, usernames and passwords, etc.) and they are also easily lost or stolen as they are small and very portable. You can significantly reduce your exposure to breach involving a mobile device by doing the following things:

- Take steps to prevent mobile device theft or loss;
- Make it harder to access information on the device; and
- Configure remote "find and wipe."

Preventing theft or loss

Here are some very easy ways to prevent the loss or theft of your mobile devices:

- Never leave your portable devices unattended in a public place. In particular, don't leave them in your vehicle – even locked in the trunk is not safe;
- To be a less obvious target, use a briefcase or bag that does not look like a standard laptop bag;
- Inexpensive cable locks from Targus (targus.com) and others can help deter a casual thief, but are no obstacle for a determined thief with cable cutters; and
- If you are staying at a hotel, put the device in a safe in your room or at the front desk.

Making it harder to access data on the device

If a device is lost or stolen, you want to make it as difficult as possible for someone to access the information on it. This is very easy to do. As a first line of defence, you can enable the startup password. After enabling this feature, anyone turning the device on will be challenged for a password and they won't be able to see any information on the device. Most laptops and smartphones have this feature. However, while this should protect the data on the device from the average thief or person that might find a lost device, someone with specialized knowledge can bypass these built-in password-protection features.

For an extra level of security you can use encryption, which scrambles the data on a device making it very difficult for someone to access it. Some devices have an encryption feature in the device operating system, and, if not, you can use a third party encryption program or app. Truecrypt is a widely used encryption tool that works on many different platforms.

One other option to consider: if you allow remote access, have people travel with a device that has no client data or other sensitive information on it. They can use it to access client data in the office via remote access and if the device is lost or stolen there is no lost information to be concerned about.

You may want to keep in mind that current case law provides that law enforcement does not need the permission of a device owner to access information on a device that is not password protected.

Device locators and remote wipe

To prepare for the eventuality that of one of your smartphones, tablets or laptops gets lost or stolen, you should enable or install device locator and remote wipe functionalities. These features are built in on some devices, and there are many third party programs and apps that do the same things. Using GPS technology or the tracing of IP addresses, you can potentially view the location of your device on a web-based map, sometimes along with where and when it was last used. Just in case the device is lost in your residence, you can also trigger a high volume ring to help you locate it, even if the device is on silent or vibrate. If the worst has happened and it appears that the device is permanently lost or was stolen, you can usually lock the device so no one can use it or access the data, and you can also remotely tell the device to do a factory reset, which will delete all data on it.

Beware of data theft with USB sticks

Tiny, high-capacity USB sticks are commonly used for moving data around. A combination of three things makes them a major security concern: (1) they are very easy to use, (2) they are compact, light-weight and ultra-portable, and (3) they can store huge amounts of information. They are, in other words, the perfect tool for a disgruntled or soon-to-be ex-employee who plans to easily and quickly steal firm data.

How do you protect yourself? Make sure you have appropriate security and access rights to confidential client and firm information on your firm's computers and servers. Auditing file access may help you spot someone who is accessing information they should not. Consider disabling USB ports on firm computers used by people that have no reason to use USB sticks. Lastly, take extra care with employees who may be leaving the firm (see page 23).

12 Harden your wireless and Bluetooth connections and use public Wi-Fi with extreme caution

At home, coffee shops, restaurants, hotels, conference centers, airport terminals and many other locations, many of us use wireless and Bluetooth for our smartphones, tablets and even our computers without a second thought. While very convenient, anyone using wireless and Bluetooth should know that they are fraught with serious security issues. Unless you lock down your wireless network and

devices, someone sitting in a car across from your office or home could easily find and connect to them. Hackers known as "wardrivers" actually cruise around looking for networks they can hack into. There are even websites that list "open" networks by street address.

Hardening your wireless networks

Use wireless with caution, and only after you enable all possible security features on your wireless routers and devices. The hub of your wireless network is a router. It connects to your Internet service provider through a telephone line or other wired connection. Anyone connecting to your wireless network through your router can likely connect to the web and quite possibly access other devices on your network.

Completing these steps will make it much harder for strangers to connect to your wireless network:

- use WPA or WPA2 (WPA2 is better) or 802.1x wireless encryption. WEP encryption is found on older devices and it is recommended that you not use it as it can easily be cracked;
- turn off SSID broadcasting;
- disable guest networks;
- turn on MAC filtering;
- change default router name and password; and
- disable remote administration.

More detailed directions for completing these steps can be found on the practicePRO website in the "How to enable the security settings on a wireless router" checklist.

Bluetooth vulnerabilities

Bluetooth technology makes it easy for keyboards, headsets and other peripherals to connect to smartphones, tablets and computers wirelessly. Although security is available for Bluetooth, many vendors ship Bluetooth devices in Mode 1 (discovery/visible-to-all mode) to make it much easier for people using the devices to connect to them. In this mode they will respond to all connection requests. This introduces a number of vulnerabilities, including making information on the device more accessible to hackers and making the device more vulnerable to malware installation.

LAWPROFAQ

How do I get LAWPRO insurance coverage, now that I've been called to the bar?

Q. I have just been called to the Ontario bar, and will begin work for a law firm in a few weeks. I know I need insurance from LAWPRO – but that's all I know! How do I get started?

A. The LAWPRO program of professional indemnity insurance is approved each year by the Law Society of Upper Canada, and coverage under the program is mandatory for lawyers in private practice. When new lawyers are called to the Ontario bar, the Law Society provides LAWPRO with their contact information, and LAWPRO sends each new call a package of materials that includes information about the LAWPRO program and how to apply for coverage or, in certain cases, exemption from the coverage requirement. **Please note that you will not be automatically signed up for LAWPRO insurance coverage simply by virtue of being called to the bar.** LAWPRO and the Law Society of Upper Canada operate independently of each other, and you must contact each entity separately if you need to report a change in contact information or a change in practice status.

Applications for coverage or for exemption can be made online via a secure portal at lawpro.ca.

If you are a new call and you have NOT received a package (for example, because you have recently moved), please contact LAWPRO's customer service department to request a package.

More information

For more information about insurance requirements, exemption eligibility, run-off coverage, and other insurance issues, please visit the FAQ section of the LAWPRO website at lawpro.ca/faqs

If you have any questions regarding your coverage or practice status, please contact LAWPRO's customer service department by email at service@lawpro.ca, or by phone at 416-598-5899 or 1-800-410-1013.

To make your Bluetooth devices more secure, you should do the following:

- Configure devices so that the user has to approve any connection request;
- Turn off Bluetooth when not in use;
- Do not operate Bluetooth devices in Mode 1 and ensure discovery mode is enabled only when necessary to pair trusted devices;
- Pair trusted devices in safe environments out of the reach of potentially malicious people;
- Minimize the range of devices to the shortest reasonable distance;
- Educate your staff about how to safely use Bluetooth devices; and
- Consider installing antivirus and personal firewall software on each Bluetooth device.

Be extremely cautious with public Wi-Fi

Public Wi-Fi has become ubiquitous and a lot of people use it without a second thought. Unfortunately, there are major security issues with it. If you connect to a Wi-Fi network without giving a password, you are on an unsecured and unencrypted connection. On an unencrypted or "open" wireless network, anyone in your proximity can intercept your data and see where you are surfing (except if you are on an https website). Using an unencrypted connection to check the news or a flight status might be acceptable, but keep in mind that performing other activities is akin to using your speakerphone in the middle of a crowd.

Even worse, hackers will create fake Wi-Fi hotspots in public places to trick unwitting Wi-Fi users. "Free Starbucks Wi-Fi" may not be the legitimate Starbucks network. Connecting to a fake network puts your data in the hands of a hacker.

And don't equate subscription (paid-for) Wi-Fi Internet with secure browsing. It may be no more secure than open Wi-Fi.

To be avoid these dangers, it is best avoid using public Wi-Fi hotspots altogether. Get a device that has mobile cellular capability, tether to your smartphone, or use a mobile Wi-Fi hotspot. This is a small Wi-Fi router you carry around that has mobile cellular functionality. It gives you a personal and private Wi-Fi cloud you can configure to securely connect your other devices to.

If you are going to use public Wi-Fi, here are some steps you can take to connect your device as securely as possible:

- If your firm has a Virtual Private Network or VPN, use it. This will encrypt your data and make it harder for it to be intercepted.
- Never connect without using a password (this means you are on an unencrypted network) and avoid using Wi-Fi that uses WEP encryption as it can easily be cracked. Use networks that have WPA, WPA2 (WPA2 is better) or 802.1x wireless encryption.
- Enable the firewall and run updated antivirus software on your device.
- Turn file, printer and other device sharing off.
- Disable auto-connecting so network connections always happen with your express permission.
- Confirm the network name in your location before you connect (i.e., avoid the Starbucks imposter).
- Use sites that have "https" in the address bar as they will encrypt data traffic (See "The S in https means you are on a safe and secure connection" on page 14).
- "http" sites transfer data in plain text and should be avoided as a hacker can easily read the data transmissions. You could use browser extensions or plugins to create https connections on http sites.
- Follow the best practices for safe and secure passwords (see page 30).

By taking these steps you can reduce your Wi-Fi risks, but you should save sensitive tasks like online banking for when you are on a network you know is safe and secure.

13 Be careful about putting your firm data in the cloud

Almost everyone has data in the cloud, although many people may not realize it. If you are using Gmail or another free email service, iTunes, Facebook, LinkedIn or other social media tools, Dropbox, or doing online banking, your data is in the cloud. The "cloud" is the very large number of computers that are all connected and sharing information with each other across the Internet. If you create or post information that ends up outside your office, you are most likely in the cloud.

Cloud computing offers many benefits to lawyers. There is a vast selection of services, software and applications that can assist with just about every task in a modern law office, in many cases allowing those tasks to be accomplished more efficiently and quickly. Many of these services permit remote access, thereby allowing lawyers and staff to work from anywhere with full access to all documents and information for a matter. Using these services is usually economical as they can significantly reduce hardware and software maintenance costs and capital outlays. Storing data with suitable cloud service providers will likely mean that it is more secure and better backed up than it might be in a typical law office.

However, placing your client or firm data in the hands of third parties raises issues of security, privacy, regulatory compliance, and risk management, among others. Firms should have a process in place to ensure due diligence is performed and all risks and benefits are considered before any firm data is moved to the cloud. The evolving

standard from U.S. ethics rules and opinions seems to be that lawyers must make reasonable efforts to ensure any data they place in the cloud is reasonably secure. Contracts with any third party that is in possession of confidential client information should deal with relevant security and ethical issues, including having specific provisions that require all information is properly stored and secured to prevent inappropriate access.

The Law Society of British Columbia has a "Cloud Computing Checklist" that will assist firms in identifying the issues that should be considered when performing the due diligence on a cloud provider. When considering your options, keep in mind that a cloud product or service designed for lawyers may have been developed with the professional, ethical and privacy requirements of lawyers in mind.

Inside people can be the most dangerous

14

People inside your office have the greatest knowledge of your systems and where the important data is located. Many of the largest and most damaging cyber breaches have been caused by rogue or soon-to-be-departing employees. You should take steps to reduce the likelihood that a cyber breach will be caused by someone inside your office.

When hiring a new employee, make sure you are diligent. Carefully check their background and speak to references. Look for any red flags on an application letter or résumé, and watch for issues during the interview process. Watch for someone who is withholding relevant information, or who has falsified information on the application. Assess the overall integrity and trustworthiness of the candidate. Consider doing police and credit checks (after obtaining consent) as persons in financial difficulty may be under pressure and become tempted to steal your firm's financial or information resources. Doing all these things can help you avoid hiring an employee who could be a problem.

When any employee leaves your firm, regardless of whether they are leaving of their own accord or are being terminated, ensure that your systems are protected. Keep a log of any mobile devices held by your staff (e.g., laptops, smartphones, USB drives, etc.) and ensure that they are recovered immediately upon termination. Immediately close all points of access to your office and computer systems, including keys and access cards, login accounts and passwords, email accounts, and – in particular – remote access facilities. If you discharge an employee who has access to critical company data, let them go without warning (you may have to give them a payment in lieu of notice), and don't allow them any access to a computer after termination.

There are literally dozens of steps you should complete systematically to make sure all points of access for departed employees are closed down. See the practicePRO website for a detailed "Employee departure checklist".

If you have given vendors, IT consultants, contract or temp staff access to your systems or networks, remember to change system passwords and revoke access rights when they have finished their work.

Be careful of the dangers of BYOD and family computers

15

In many firms, it is common for lawyers to use personal smartphones or tablets for work purposes. This is often referred to as "Bring Your Own Device" or "BYOD." Lawyers or staff may also work at home and even access the office network from a personal home computer. Both of these practices raise significant cyber risks.

BYOD

Permitting staff to use their own smartphones or tablets makes great practical sense. They already own and are comfortable with the devices so the firm does not have to incur the cost of buying them or paying for wireless plans. However, if these devices connect to the office Wi-Fi or network, or if they are used to create documents that will be sent to the office, they can potentially deliver a malware infection to the office network.

Family computers

Young people have a very high exposure to malware as they are more likely to engage in many of the most dangerous online activities, including using social media, downloading programs, and file sharing. As a result, it is far more likely that any device children or teenagers are using is infected with malware. This is a concern because using a compromised computer for remote access to your office can bypass the firewall and other security mechanisms, potentially delivering a malware infection to the heart of your network.

To be absolutely safe, avoid using a home computer or other device for work purposes if it is used by others. Where a home computer is being used for work purposes, the steps outlined in this article must be followed to protect the office network and systems from cyber risks. Creating separate user accounts will make things more secure, but a better alternative is to have two partitions on your home computer. This essentially means there are two complete sets of software on the computer: one that only you would use, and one that others in the house would use.

Where a home computer or other BYOD device is being used for work purposes, the steps outlined in this article must be followed to protect the office network and systems from cyber risks. Staff education is key for reducing the risks associated with the use of personal equipment. Technology use policies should be in place to ensure all necessary steps are taken to address relevant cyber risks. See the practicePRO Technology Use Policies Resource page for sample BYOD and remote access policies.

A backup could save your practice after a cybercrime incident

16

Every law firm has huge amounts of irreplaceable data on its servers, desktop computers, laptops, tablets and smartphones. A cybercrime incident such as a malware infection or the hacking of firm systems could result in the destruction or loss of firm data. Having a current and full backup of all firm data will be essential for recovering from such an incident with the least possible interruption to a firm's operations. And beyond any concern about a cybercrime incident, every law firm should have a current full backup of firm data as part of its disaster recovery plan.

When keeping past copies of backups, consider that firm systems could have an undetected malware infection for a considerable period. If you have an undetected infection, you may have to go back in time to get a backup that is clean or has uncorrupted data. For this reason, you may want to keep a series of past backups (e.g., daily for last week, end of week for last month, end of month for last 3 months, quarterly, etc.) so that you can do a complete and clean restoration of your data.

There are many options for doing data backups, including using a dedicated backup system, external hard drives or other portable media, or the cloud. Apple users can easily set up an automatic backup with Time Machine.

QUICK FIX

Our "Data backup options and best practices" article, available on the practicePRO website, can help ensure you have a current and full backup of all the data in your office.

Conclusion

Cybercrime is a real and present danger to you and your firm. LawPRO strongly encourages Ontario lawyers to take this danger seriously and to take appropriate steps to reduce exposures to all relevant cyber risks. The "quick fixes" highlighted in the feature articles in this issue of *LawPRO Magazine* will get you off to a good start with minimal cost and effort. At many firms, further time and work will be necessary. This extra effort is worth the investment as, at the very least, a cybercrime incident will be a costly and significant interruption to your firm's business. And in a worst-case scenario, the financial and business interruption associated with a cyber breach could destroy your firm. ■

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

Thanks to David Reid, CIO at LawPRO, and Mike Seto, of Mike Seto Professional Corporation for their invaluable assistance.

Resources

Cyber security resources

Get Cyber Safe Guide for Small and Medium Businesses from Government of Canada: Practical information and guidance for firms on cyber security risks and how to avoid them. There are other helpful resources and checklists on the GetCyberSafe.gc.ca website.

Cyber Security Self-Assessment Guidance Checklist: A self-assessment template of cyber-security practices from OSFI that would be suitable for larger firms.

Cyber Security Resources for Teachers page on Media Smarts website: Various information and tips sheets for consumer and personal cyber-safety.

StaySafeOnline.org: Good general information and resources for staying safe while online.

Microsoft Safety and Security Center page: General information on cyber-security.

PCThreat.com: Comprehensive list of malware threats, tips on how to spot them and commentary on how to clean up if you are infected.

Snopes.com – The Urban Legends page: A website that lists common email scams and hoaxes.

ICSPA Canada Cyber Crime Study: Statistics and background information about cybercrime.

Managing Cyber Security as a Business Risk: Cyber Insurance in the Digital Age Report: A report by the Ponemon Institute that contains an overview of cyber dangers.

Security Resources page on SANS.org: Extensive security information and resources on the site of this research and education organization.

Note: Live Links for these resources are available in the electronic version of this issue.

General technology resources

Technology page on practicePRO website: Large collection of article on the use of technology in the practice of law.

Technology books published by American Bar Association's Law Practice Division: Large collection of books on many technology topics. Many of these books are available in the practicePRO Lending Library (practicepro.ca/library).

Law Society of Upper Canada's Technology Practice Management Guideline: General guide on use of technology in a law practice.