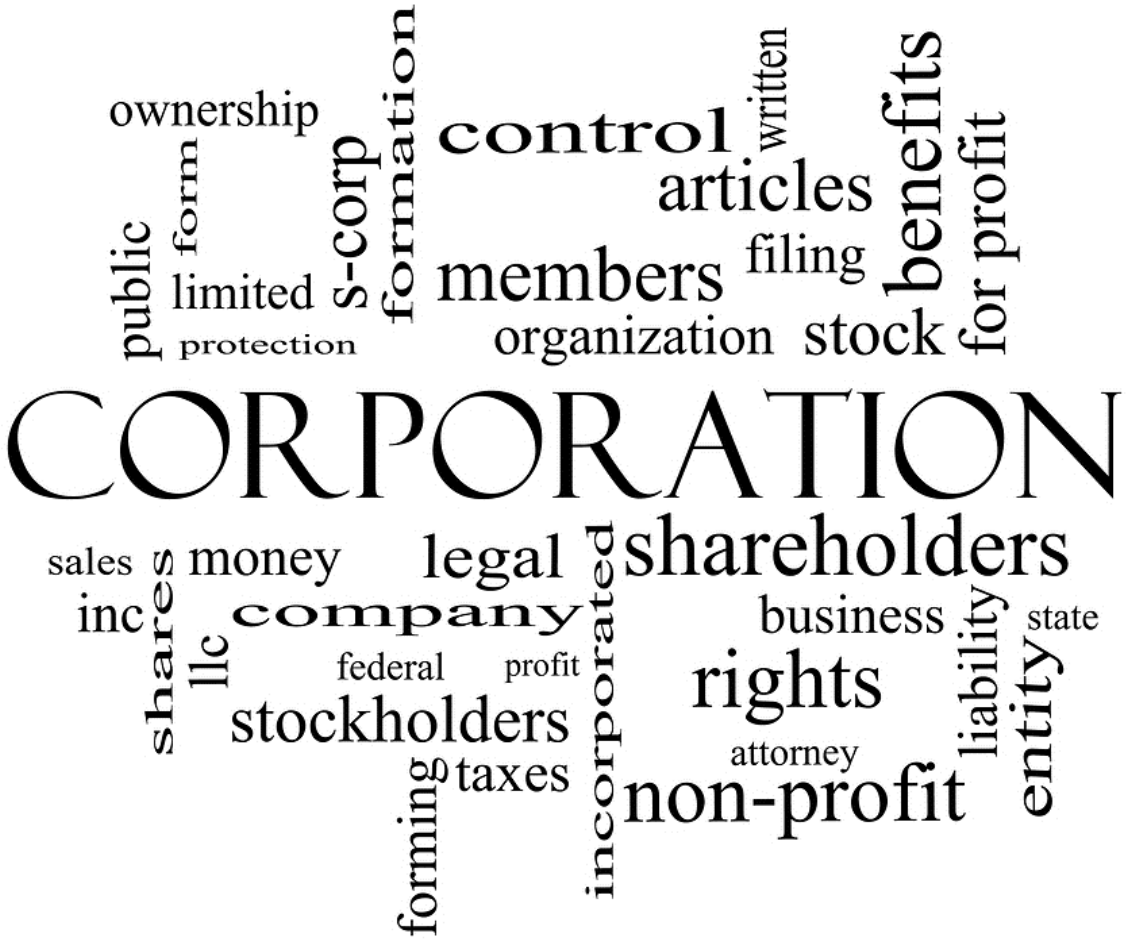
The Legal Practice Guide to Cyber ~~Security~~ Crime



Copyright

© R & I ICT Consulting Services Pty Ltd.
Free downloads - www.smesecurityframework.com.au

By Roger Smith
CEO and manager R & I ICT Consulting Services
SME Security Framework Mini Guide Downloads

LinkedIn profile: http:// au.linkedin.com/in/smesecurity

PLEASE FORWARD TO OTHERS
This is a FREE Guide. You are welcome to forward this guide or the webpage link http://smesecurityframework.com.au/cybersecurity-mini-guides/ to your clients and contacts.

For Publishers: please feel free to use the content in this guide for publishing in magazines, newsletters, etc. Please do not change the substance of the content. Simply cite the author, publication title and website.
The abbreviated content in this document is taken in part from a number of publications by this author including the book "The CEO's Guide to Cyber Security".

© R & I ICT Consulting Services Pty Ltd.
Free downloads - www.smesecurityframework.com.au

All rights reserved.
R & I ICT Consulting Services .com.au
PO Box 368
Kippax ACT 2615
AUSTRALIA

Keep in touch! For new articles and guides
Email: sales@rniconsulting.com.au
Downloads: www. rniconsulting.com.au

Twitter: Follow @smesecurity

Linkedin: Connect at http:// au.linkedin.com/in/smesecurity

Google+: connect at https:// gplus.to/smesecurity

Subscribe: Free subscription at www.rniconsulting.com.au/newsletter

NOTE: The information in this guide is of a general nature only. When making decisions about your business it is strongly recommended that you seek qualified advice tailored to your particular needs and business situation

Contents

We may all look back on the last five years as the only the beginning as the increase in cybercrime became more noticeable. Along with everything else there have been a number of high profile data breaches involving more major corporations and online services. Attacks on Facebook, Apple, Twitter, Adobe, the New York Times and Lexis Nexus to name just a few.

There are millions of other business entities and individuals who experienced breaches this year as well, alone either directly on their own computers and systems or indirectly where there was a data breach involving information about them was stored with a third-party. Everybody needs to take notice of the issue of cybercrime but law practices more importantly.

Legal practices are a very appealing target for Cyber Criminals.

Cyber Criminals target Legal Practices for 3 reasons:

- They have a large amount of sensitive and confidential information that can be very valuable to the right people.
- They have large sums of money in their bank accounts and have access to trust accounts with even more. And
- They have a large amount of anecdotal information that is kept on everything to do with cases

Information on cybercrime tools and techniques are widely available online. This makes it easy for even non-technical people to undertake malicious cyber activity, but make no mistake that while rank amateurs may launch attacks on any legal practice, industrial espionage on high-value targets like legal practices can involve the most skilled hackers in the world including potentially foreign governments.

Cyber criminals will use every tool at their disposal to attack legal practices. They will send SPAM and Phishing attacks via email, they will try to install malware or create backdoors on your computers, servers, tablets and smart phones, they will use social engineering to gain access to your business secrets and they will look for weaknesses and misconfigured security configurations to exploit. They will exploit them in order to access the firm's network in very devious ways. They will even try to trick your staff into helping them. It is quite possible they would target you individually, including attacking your home computer and mobile device and hacking into your office systems.

Cybercrime is “a real and present danger” for any organisation but it is more noticeable that legal practices are a prime target. All legal practices should understand cybercrime risks and what they are exposed to. They need to do a risk analysis and take steps to reduce the likelihood that they will experience a data breach at the hands of a cyber-criminal.

HOW PREPARED ARE YOU?

There are a number of questions that you need to ask within your practice that will define how prepared you really are to a cyber-attack.

- Are all passwords that allow access to your digital environment complicated and unique?
- Would it be possible for your staff be duped with a Phishing message?
- Would everyone within your business understand what to do if one of your servers or if your cloud-based systems were hacked?
- Is your end point protection software the most current version and is it kept updated at all time?
- Could you tell if a computer was infected with malware?
- Are your computer security settings adequate?
- Is there a backdoor into your network, into your website or into your cloud storage system?
- Would critical business and case information be compromised if a firm's laptop or smart phone was lost or stolen?
- How would your organisation manage a major data theft by an ex-employee? and
- Is your home computer safe and secure to the same level as the corporate network?

The biggest problems we face today for any business is ensuring we protect other people's information, our own Intellectual Property and our lively hood.

The preferred attack weapon of the cyber criminal - Malicious software (Malware)

One of the most common and easiest used systems of attack that the cyber criminals have is malware.

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

- Record keystrokes to capture usernames, passwords, account numbers and other personal information
- Create backdoors that allow hackers to access your computer or network without your knowledge by bypassing normal authentication and security protocols
- Disable your security settings and end point protection security so that more malware can be installed or the malware that is there will undetected
- Use your computer to hack into other computers on your network and on the internet
- Take control of individual programmes or even entire computers and servers

- Use your computer to send email messages to people in your address book who will in turn become infected through clicking on the links and attachments in those messages
- Use your computer to send spam to thousands of people usually with the intent of infecting them
- Steal data from your computer
- Alter, delete, hide or encrypt files and data
- Display unwanted pop-up windows in your internet browsers that will slow your computer and / or network and prevent access to your data
- Contaminate the firm's website and install "drive by malware" on your site

How Malware gets around

Malware employs a number of mechanisms for self-replication. To infest a computer, phone or tablet normally, not always, requires some kind of deliberate action by a user to infect their computer.

You can become infected with malware by doing any or all of the following things:

- Opening an infected email attachment
- Visiting an infected website, in some cases you don't have to click on a link to trigger a download
- Clicking on a link on a website, in an email, in an instant message or on social media post
- Plugging in an infected USB stick or external hard drive into your computer
- Download free programs and applications to your computer, your tablet or smart phone
- Installing a toolbar or other add-on to your browser

What does Malware look like?

Some types of malware, for instance worms, can spread on their own without user actions

There are a number of common types of malware. Malware is classified by how it propagates or what it does.

- Viruses are by far the most common type of malware and something like 40,000 of them are being created every day.
- Worms are one of the most common types of malware. The difference between a worm and a virus is that a worm doesn't need anybody to activate it's attack profile.
- Trojans are named from the wooden horse in Greek mythology and is used to allow something (an application) to deliver something (malware) inside another person's network.

Drive by Malware

Ever been to a website – in most cases you are looking for the newest news on the latest celebrity stuff up, where the web site has asked you to update flash / java.

The pop up looks exactly like the real version. It will have all of the correct information about installing the application update but when you click yes it will install malware on your computer or smart device.

This is drive-by Malware

- Spyware usually comes in the form of a free download. They can however, be installed automatically. Most of the time spyware is actually coupled with other downloads
- Root kits Once malware is installed on the system it will try to stay hidden. This is achieved through a root kit, hiding the malicious code within the operating system and in some cases the actual hardware code to remain hidden.
- Scareware is just plain annoying. Usually deployed from a website as “your computer is infected click this link to fix”. Clicking the link installs any manner of Malware.
- Ransomware is the newest attack system for the cyber criminals and like scareware has a pop up. The difference is the pop up comes from the malware already installed on your computer. Ransomeware usually encrypts all of the information on the hard drive and you have to pay to get the decryption key.
- Botnets are created by viruses worms and Trojans and are usually what in the industry called zombie computers. These infected computers and smart devices are capable of sending out large amounts of data from your computer without your knowledge

Malware is not the only problem, don’t forget the insider threat

Cybercrime dangers can also originate inside your network, inside your practice, as well. Many people assume that the biggest cyber dangers come from outside of a law practice. Statistics actually show that the majority of incidents involving the destruction or loss of data and information are perpetrated by current, soon-to-be dismissed or recently dismissed employees.

Few know more about your firm systems than employees. Many are in positions to cause major damage, in particular your IT staff, your employees with advanced technical knowledge and outside technical support people.

HOW TO PROTECT THE PRACTICE

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 scams or thefts. Cyber criminals are considered resourceful. Cyber criminals have considerable resources and expertise and can cause significant damage to their targets.

Cyber criminals significant specifically target law practices as they have funds in their trust accounts, client data that is often very valuable and more importantly information that can be bought and sold. All legal practices need 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 and digitally related dangers.

It all starts with support from senior management.

Any and all effort to tackle cybercrime must start at the top. Senior partners and management of all legal practices must be advocates of cyber security, support the implementation of appropriate practices and policies and allocate sufficient resources to address cybercrime exposure.

There are some quick fixes that can help make your office and systems more secure. All law firms will need to spend more time and money to protect themselves from cybercrime. This may include upgrading and installing new technology, training staff and managing how tasks are done. Your legal practice should also put some thought into how a cyber-breach, a loss of client data or hacking of a firm server would be handled.

You may need expert Help

Your legal practice 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. You will need support and you may need expert help, you need to ensure you know where to get it. Beyond the very practical issue of wanting to avoid being the victim of cybercrime you have to remember that when using technologies, lawyers and paralegals must meet their professional obligation that as outlined in the legal statutes of the country.

These rules are in place to ensure you have a reasonable understanding of the technology used in your practice or you have access to someone who has such understandings. It is not likely that a sole practitioner or a partner in a small or medium practices will have someone on staff who has the technical expertise to properly address all relevant cyber security issues.

One of the biggest dangers here is that people just don't realise what they don't know when it comes to cybercrime dangers and how to prevent them. We encourage firms to seek appropriate helpful knowledgeable experts when required to identify vulnerabilities. All legal practices may want to consider engaging an outside expert to do a formal security assessment.

Staff Education and Internet use policies

Staff education and “digital” use policies are just as important as any other component of your protective framework, and address many cybercrime dangers involving a human element. Cyber criminals continually create situations, at the basic level through a malware infection, in which legal staff are unintentionally or unwittingly used to facilitate cybercrime as they go about their normal business.

Educating staff to help prevent this and recognise and avoid cybercrime dangers is a critical part of reducing cybercrime risk. Increased awareness is one of the best solutions that you can deploy within your practice.

You need to have a written policy that establishes guidelines and requirements governing the acceptable use of all firm technology resources. This can also help reduce cybercrime exposure. All policies 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.

The policy should also cover some basics and clearly state that technology resources provided by the firm including Internet and email access are for legitimate firm use. Staff should understand they have an obligation to the practice to use the resources properly and appropriately.

Policies should also ensure that the confidentially of the practice as well as client information is protected at all times. These policies should also indicate that the firm retains the right to monitor any and all electronic communications and use the Internet to ensure the integrity of the system.

Cyber Security Dangers you need to be aware of

There are a number of cybercrime dangers you need to address within your legal practice. These include:

1. Avoiding the dangers of email
2. Lock down all browsers and avoid surfing dangers
3. Avoid infections with antivirus and anti-malware software
4. Lock things up by using passwords properly
5. Administrators should not have email accounts attached to administrator accounts.
6. Address security vulnerabilities by installing operating systems and program updates
7. Keep the bad guys out with firewalls on your Internet connection
8. Always change your default password settings on your systems
9. Lockdown and protect your data wherever it is
10. Scrub confidential client information on discarded equipment
11. Be safe when using remote access, VPN and wireless
12. Secure mobile device data when it is on the device
13. Harden your wireless connection and use public Wi-Fi with extreme caution
14. Be careful after putting your practices data in the cloud
15. Inside people can be the most dangerous
16. Backup always, a backup will save your practice after a cybercrime incident.

YOU MUST ADDRESS ALL OF THE DANGERS

Don't be tempted to ignore any of the dangers listed above and below or skip and scrimp on the steps suggested. Remember your data and systems are only as safe as the weakest link in your security plan.

When you leave on your vacation you always lock your doors and windows in the house and you make sure the neighbours or family are picking up your mail. You know that any lapse in this regime could mean that your house is broken into and all of your treasures are stolen.

In a cybercrime environment you have to protect yourself. There is a requirement for a physical barrier, but most of your protection is in these following areas.

1. Avoid the dangers of email

Email is the main and primary communication tool for all legal professionals. It allowed virtually instant sharing of information and documents between lawyers and their clients. Email is also one of the most dangerous tools in a modern legal practice. Infected attachments, SPAM and Phishing attacks delivered by email make it easy for cyber criminals to deliver malware and breach a law firm's security.

It is essential that you educate everybody on staff about these dangers and the steps they should take to use email safely.

a. Be wary of attachments

Email attachments are regularly used to share documents within a practice as well as with clients, other practices and other members of the legal system. They are also used by the cyber criminals to deliver malware to anyone and everyone. If you're not expecting it and you don't know what it is, don't open it.

b. Use spam filters to avoid annoying and dangerous spam

During the course of the day most users of email will receive one or two unsolicited email. This is email that is unwanted, advertising or offensive in nature. An external email filter is designed to remove 99.9% of this SPAM and ensure a clean feed of email to your email server. Cloud based providers also supply this level of protection.

SPAM is not only annoying but it is also dangerous. Once again Cyber criminals use SPAM to deliver malicious code to unsuspecting users. SPAM can be filtered with the use of most end point protection software. This may also incorporate a listing system – black list – known SPAM and Malicious sites and white list all mail from your contacts (even these are not always safe)

c. Don't be fooled by phishing

Phishing is one of the main uses of SPAM. Phishing is a targeted attack on an individual designed pleasingly to get the user to follow the link by clicking on it in an email. It uses emails from Banks, Government departments or large enterprises to entice people to go to the next level.

There is a further derivative of phishing and that is called spear phishing. It's more dangerous than normal phishing as it is used to target an individual or a group of individuals within an organisation. Spear phishing is used once the criminals have discovered everything they can about an individual. Cyber criminals will start with company pages on Facebook, LinkedIn and in some cases twitter. They will use that information to work out a business hierarchy and profile and work out where people are in the business. They will then investigate their targeted people to get as much information about those people as possible.

This information is then turned into a very sophisticated attack on the individual or group of individuals. For instance: a targeted attack on the accounting people within the practice could include invitations to accounting seminars, information on accounting practices, changes to accounting rules. They are all designed for the criminal to get to the next step, being inside the network undiscovered.

Always remember Email is a broadcast medium. It can be sent around the world in seconds and can be forwarded onto anyone.

2. Lock down all browsers and avoid surfing dangers

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

Teaching your staff the following surfing don'ts will help you reduce cyber related surfing risks and reduce the likelihood of malware infection through your browser of choice.

- Don't complete online transactions involving account information pass words credit card numbers and other personal information unless you are on a secure connection as indicated by the HTTPS Symbol
- Don't visit unknown websites and also check site security when following a google search.
- Don't use file sharing sites and services unless you are familiar with I know the people you are sharing files with.
- Don't download software, Music, videos or celebrity notoriety from sites unless they are reputable and trusted sites.
- Don't download new apps from the app stores (Google and ITunes) without reading the reviews and checking the number of people who have downloaded the application.
- Don't click on okay, yes or anything else in the browser pop-up. These pop-up windows can change settings within your browser, lower your security settings and install malware.

Run an antivirus or anti-malware program that runs in the background and scans for these dangers

If you are doing online banking for your truck firm trust or general accounts it is critical that you ensure all security risks are addressed

Beware the dangers of social media

Most people are comfortable sharing a great deal of personal information on Facebook, Twitter, Instagram and other social media networks with family and friends. You should keep in mind that

cyber criminals could use the same information to assist them in personally identifying individuals within the organisation and targeting them.

3. Lock down your browser.

Many programs can automatically and secretly install themselves while you are browsing the internet. Although most require some level of human intervention – a click on OK for instance. These are called a drive-by downloads. Drive-by malware occurs when an infected website runs a script or active X controls that change your browser's system and installs the malware onto your system.

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 settings or privacy settings when choosing from different levels of security. Browser security settings can provide greater protection but they may also prevent some websites from running properly. All browsers have configuration setting and all browsers should be locked down to allow or prevent the following.

- Prevent pop-ups from loading
- disable JavaScript
- don't accept third-party cookies
- remove cookies on exit
- Clear history at close and exit
- disable active X controls
- enable automatic updates

There are also various browser plug-ins and add-ins that can be used to increase browser security and warn you about suspicious activities.

Pharming

Pharming is another common trick used to perpetrate scams. Pharming takes you to a malicious or illegitimate website by redirecting a legitimate website address, even if the website address is entered correctly. The fake website is intended to convince you that it is real 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 unwittingly give your personal information to someone with malicious intent.

4. Avoid infections with antivirus and and anti-malware software

Good behaviour alone will not protect you from malware infections. You must run software that will prevent and/or detect infections on your computer. You may need to consider it for tablets and smart phones as well.

What makes the difference between an antivirus and anti-malware software is subtle and in some cases there is no difference. Malware is a broad term used to describe many different types of malicious code including viruses, Trojans, worms, spyware and other threats.

Your best protection for computers, servers, tablets, laptops and phones is to use an end point protection system that looks for viruses as well as malware.

Windows options

Windows computers are prone to infection so you must run anti-malware software on all of them, we recommend Forticlient. Forticlient is a free download from fortinet.com, this software will protect Windows XP, Windows Vista, Windows 7, Windows 8 and also offers good real-time anti-malware protection to android and apple systems.

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

The two most widely used anti-virus programs are Nortons / Symantec antivirus and McAfee. For an antivirus system expect to pay between $40 and $150 per computer to buy the software and as an annual fee for virus signature files and updates.

Until recently it was generally felt it was not necessary to run anti-malware software on Apple computers as the Mac OS architecture prevents infections and there is no real malware threats targeting Macs. To protect against potential malware threats consider clam AV or forticlient for Mac OSx computers.

Tablets and smart phones are, in general, more likely to get malware infections, so you may need to run anti-malware of applications on them for greater protection.

As no one anti-virus and anti-malware application will catch everything, you may want to consider using more than one anti-malware tool to better protect yourself. Install one system that scans for as much as possible and that runs all the time in the background. This will protect you from attacks as you surf the Web and checks applications, open files and monitors your daily activities. Install another anti-malware tool on another system for instance on the firewall, proxy server or the main server.

Installing anti-malware software updates is critical

Installing anti-malware software is only the start. You also need to regularly update your virus definitions with a signature file. Anti-malware programs use the information in these files to recognise virus infections when they occur. There are 40,000 new viruses and malware being created every day so you need to make sure that your anti-malware and antivirus software is updated regularly. Most anti-malware programs can be configured to download updates automatically.

Staff can help you spot malware infections

Sometimes anti-malware software will not detected that an infection has occurred. While malware can be on a computer and never give any intent of its presence. In many cases there are supple clues that a computer is infected with malware. Teach your staff to recognise these symptoms. This will aid in early detection of an infection.

5. Lock things up by using passwords correctly

Like any set of keys, computer passwords are keys that unlock your computer, your mobile device and how you access all your internal data. Because of the Internet we all have more passwords than we can remember. This makes us lazy. We all use easy to remember passwords or in some cases we don't use them at all.

Cyber criminals know and target bad password habits. They are one of the weakest links within any organisation and for this reason it is critical that all lawyers and staff in a law office use passwords properly.

There are a number of ways to create complicated passwords. Here are 3 ways to create a complicated password to use as a base:

- Use a phrase – I hate passwords, then change it so that it does not look like I hate passwords (1_hate Passwords). You can write it down and no one will understand it.
- Use a phrase and use a component of the phrase – I play golf every Saturday with Paul becomes IPGESWP. This can become 1pG3Sw P. Once again you can write the phrase down and no one is the wiser.
- Use 2 unrelated words and a number – Tree56 Lamb.

There is also a need to create unique passwords for different sites on the internet. Add something to the base password – bank name – (ANZ-1_hate Passwords), Gmail –(1pG3Sw P Goo), or Paypal – (Tree56 Lamb_pay)

In all passwords try to use a combination of letters and capitals, numbers, symbols and if possible try to use a space as this confuses most of the systems that try to brute force your password.

6. Addressing security vulnerabilities by installing the latest operating system and program updates.

There are millions of lines of computer code in operating systems and programs that run on modern computers, tablets and smart phones. 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 do with these different devices. Inside all these settings and features cyber criminals look for exploits. An exploit is a particular setting or feature or sequence of commands that will cause an unintentional or an unanticipated behaviour to occur within a computer. Some exploits create security vulnerabilities because cyber criminals can use them to open a backdoor into your computer and your network. This can allow malware to run or do other damaging things to your computer. New exploits are discovered on a weekly or even daily basis for most applications and operating systems.

Updates.

When an exploit is discovered software c 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 version of operating systems and programs.

To keep your computer 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 more prone to security vulnerabilities.

This is not because the Microsoft products are all that vulnerable but it is because it is the most used system on the planet. Cyber Criminals will target the system because there are so many people using it. While not as targeted as Microsoft products Apple products should be update regularly as well.

Don't forget to update the other non-Microsoft or non-Apple software running on your device systems like Adobe, Java, Flash and other embedded systems. These should be updated as much as possible as well.

Automatic updates

Both Windows and Apple operating systems and applications have an automatic update feature that automatically notifies you when updates are available for your device. Once this feature is activated the device will periodically check for updates. Available updates will be downloaded and depending on how you configured the system they will be installed with or without your knowledge.

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

When you're connected to the Internet the Internet is connected to you. For computers to transmit data back and forth over the Internet they have to develop lines of communication. These communications works through a system of ports and applications of a certain type communicate through these ports. HTTP or web traffic use port 80 and that port is required on each computer or device.

The problem with this system is that all computers on the Internet can then see one another. These ports allow cyber criminals to access the data on the computer or even take control of the computer itself.

Regardless of how you connect your office to the Internet, your computer system must be protected by a firewall. A firewall watches these ports and will warn you and prevent unauthorised communications. In addition to this, the newer affordable firewall products have an application firewall feature that will investigate all of the allowed traffic and make sure that it is the information it is supposed to be.

Firewalls come in two varieties software and hardware. Software firewalls are set up usually to protect a single computer and are adequate for personal or small firm use. Hardware firewall are usually used to protect entire network of computers. High-speed modems generally include a basic firewall.

A firewall should also be used to protect the internet from an internal Malware attack. Most modern firewalls have the ability to check and secure outbound ports. Restricting email to servers and restricting the type of information being transmitted to the internet the firewall will also protect your practice from being put on Internet based black lists. By only allowing the correct information to be processed means that a malware infection will not be able to go outside the network and infect other systems as well as not being able to access their command and control centres.

8. Change and reset default systems

All equipment, whether it is hardware or software coming from manufacturer usually has a basic or default setting that allows you to access the system and set it up. These generic usernames and default settings have to be changed as soon as possible in a production environment. Every computer operating system program and every piece of hardware of certain contains these default settings.

The problem with these default settings is that they are common knowledge. A Google search can reveal the default passwords for any device that has been produced. Default usernames and passwords are another attack vector for cyber criminals to attack your systems. In some cases they already know the username, they only then have to try to decipher the password.

You can make your system safer by changing the following default settings on any new system:

- admin account names
- server names
- work groups

- standard working ports from the Internet
- Standard share names.

Lock down and protect your data wherever it is

In the old days all you had to worry about was a single folder that held all the documents for a particular matter. This folder could be secured in the safe or a filing cabinet. Today, your complete practice which is existing in electronic form can fit onto a device no bigger than your little finger.

To make sure that this information cannot be removed and stolen it is recommended that the critical components of your business are encrypted both at rest – where it is stored and when in motion – when it is being used or manipulated. This ensures that information critical to your business will not make it out to the internet wild and if it does it is very hard to decode.

9. Physical security

Likely whenever we leave our home, we locked everything down so that people cannot get in and steal stuff.

All electronic equipment based inside your office needs to be physically secured. This ensures that intruders and insiders cannot physically access any of the systems that your business uses. Securing the physical environment means that intruders and insiders will not be able to remove financial data, usernames and passwords, intellectual property, and / or allow them to create a backdoor into your business.

By restricting access to the physical environment of hardware like servers, switches, Routers and all other systems, intruders cannot gain access through the most basic level of the systems. There are a number of things that can be done to restrict this access further.

Access to devices on start-up

In most cases a start-up password is a component that can be deployed to protect the physical system from illegal physical access. In addition to a start-up password all critical data should be encrypted, if the information is deemed critical to your legal practice. This will ensure that if an intruder does gain physical access to the equipment, for instance the equipment is stolen, then the information that is contained on that system is very hard to decipher.

Screensavers

As part of your internal security policies, all users should be required to have a password on their screensaver so that when the equipment is left unattended and not locked that it will lock automatically and require a password to unlock. This can be forced at the policy level if using Microsoft Server products.

Network access

One of the primary reasons that people use a network is so that all information within the network can be easily accessed from all components and users of that network. To ensure that all information is compartmentalise, most network and server systems have a system of permissions and shares.

Permissions are used to restrict access to non-essential personnel and work on the need-to-know principle. If users and staff do not have a requirement to see particular case files or pertinent information about clients they should not have access to that information.

10. Getting rid of equipment

All physical equipment has a life-cycle, servers have a life-cycle of anywhere between three and five years, workstations have a cycle of 2 to 4 years, and tablets and phones have a life-cycle of about two years. All this equipment may have residual information stored on hard drives and flash drives. This information needs to be removed so that cyber criminals or normal criminals do not have access to that information.

Recycling equipment and donating to not-for-profit organisations needs to be done in such a way that this information is removed from all systems. This can be done with a defence grade scrubbing software. If the equipment is not being donated then a simple hammer will suffice, it is however recommended that the hard drives be scrubbed first.

In addition to physical equipment, items like CDs, floppy disks, DVDs, USB storage devices and external hard drives need also to be destroyed correctly. Anything that is leaving your practice should be electronically encrypted, to ensure that in the case of a loss that this information cannot be readily used or read.

11. Remote access and using public computers

The wonders of today's technology allows anyone to access information from any device from anywhere that is connected to the Internet. This creates additional problems in protecting your intellectual property within your practice.

Remote access creates problems of its own. Not only is your network required to be accessed through Internet ports that have to be secured, all information going between the device and the storage location has to be encrypted.

There are a number of strategies that a practice can incorporate that will allow for a secure capability within the practice to access data externally. Securing the practice may require a high degree of technical knowledge and advice from a computer expert, but here is a list of the basics that need to be in place:

- Use firewall and security software to keep out unwanted connections
- Only give remote access to people who really need to use it
- Restrict the type of data that can be accessed remotely
- Make sure that all connections come from systems that are secure and
- Constantly monitor firewalls and server logs for unwanted and unusual activity

You can also secure remote access by doing the following:

- Ensure the newest version of remote access client is used at all times
- Restrict access to services and functions that is only required for staff to carry out their roles
- Ensure all connections require complex passwords

- Ensure all passwords are changed regularly
- Do not allow users to use systems that automatically log on to the main network
- If possible, use token-based authentication
- Create a remote access policy that clearly defines who can use, what is required by users, to access your system remotely.
- Always remove users as soon as they leave.

12. Using public computers and public access wireless

Public computers in libraries, Internet cafes, airports and other locations are an extreme security risk. It is recommended that sensitive critical client information not be allowed to be accessed from public computers.

In addition to public computers the use of free public access Wi-Fi is also something that needs to be controlled and managed correctly. Free Wi-Fi that does not require a password, should never be used when connecting to your network. These systems do not require a password, all information that is travelling between the device and the main network is in plain text and can be read by anybody with the right equipment.

13. Securing your mobile devices

Lost, stolen, misplaced or broken laptops, tablets and smart phones can also be a large security hole within your organisation. The reason is that large amounts of confidential or sensitive data and information can be contained within them and they are easily lost and misplaced.

Some easy ways of preventing the loss and theft of your mobile devices are:

- Never leave them unattended in a public place, particularly in vehicles.
- Use a non-standard bag that does not have known suppliers names plastered all over them.
- Laptops when in the office, should be tied down with cable locks.

In addition to the devices being highly portable, the information that is contained in them also needs to be locked down and secured. Your main systems should be built to ensure that no critical intellectual property is contained on the device unless it is securely encrypted.

In today's world, bring your own device (BYOD) and allowing staff to use their own equipment in the work place is seen as a way for a business to save money on technology. In the event that this equipment and any equipment supplied by the organisation is lost or stolen a remote wipe capability is as part of your remote access policy.

Internal wireless Bluetooth and a VPN connections

If you are using Wi-Fi within your organisation then there are a number of components of the Wi-Fi system that needs to be set up correctly. Once again this can be done with the right technical advice but the following is a list of things that will make it more secure:

- Use WPA or WPA 2 to encrypt all information. Never use WEP.
- Turn off the SS ID broadcasting

- Disable guest networks
- Use a Wi-Fi device that creates the wireless network on a separate network to your main network.
- Turn on MAC address filtering so only approved devices can connect to the wifi.
- Change the default access points name and password
- Disable remote administration

All Wi-Fi access to your business network, should be done once connected to the Wi-Fi through a normal VPN connection. This ensures that there is a second level of protection within your wireless network and the main organisations network.

Bluetooth also has a number of vulnerabilities. For all devices that use Bluetooth, most come from the manufacturers in mode 1, this needs to be changed as soon as possible to ensure that unsavoury people cannot connect to the blue tooth connection on that device.

14. The cloud

The cloud is the newest catchphrase of business, in most cases the cloud offers access to information in a controlled environment. The cloud is paying for your computer requirements like a utility. A monthly fee based on your usage and requirements is all that is needed. High end technological systems are no longer required within the business.

In most cases, most organisations are already using cloud components. Whether they are breaching your internal policies or not, there will be some users within your organisation who will have access to systems like drop box, Cubby and other file storage locations. These systems allow information to be transferred between the internal network and any device that the user has access to. Your critical intellectual property is no longer under your control when this happens.

Cloud computing offers many benefits to a legal practice. There is a vast array of services, software and applications that can assist with just about every task within a modern legal practice.

The perceived problem with the cloud is that placing your clients and all your practice information in the hands of a third party raises issues of security, privacy, compliance and risk management. The cloud is as safe and secure as your normal network on the condition that your policies and procedures ensure that all critical information is secure at all times. All legal practices should do their due diligence prior to making a decision about moving information to the cloud.

15. The insider threat

The staff within your organisation can be greatest asset as well as being your largest security threat. In most situations, to do their job, they need access to information that is critical to your practice. Many of the larger security breaches in modern times have been done by people in a position of power within the organisation, prior to moving, being fired or resigning.

We are not just talking about Cyber Security. In most cases a fraud or theft will be done well before a cybercrime component comes into the business. The insider threat is also a culture and resilience business practice. Theft and fraud usually only occur when the staff do not believe that they are being treated fairly or paid correctly. In larger organisations and legal firms, it is recommended that in the process of due diligence that an enquire to http://www.thewhitehourereport.com.au be made. This will also ensure the building of a great business culture.

In addition, it is critical when hiring people for your practice that you are diligent and look at all components of their background. You need to talk to referees and to check their backgrounds. During the interview process always look for red flags that contradict their personality compared to their resume. In some positions a police check and credit check may be required to check for financial viability within applicants.

When people are leaving your organisation, regardless of how they are leaving, always ensure that the protection of your systems is paramount. In all cases make sure that information that is critical to your organisation is no longer on bring your own device systems. Also ensure that all company equipment is returned prior to leaving.

It is recommended that no matter the condition or situation that someone is leaving the firm that on the first indication that they are leaving that they be terminated as soon as possible. This will ensure that they do not have the chance to remove critical business information from your system prior to leaving.

16. Backup your data

Every organisation has a large amount of information pertaining to their business practices and intellectual property. This information is critical to the practices viability as a practice. This information needs to be protected at all times.

To ensure your business will survive a catastrophic failure of any system including a cybercrime attack your data needs to be backed up to a safe location. To ensure the viability of a business after a system failure this backup should also be located off site in a separate geographical location.

A backup system that does the following is probably your best protection:

- Continuous incremental backups of critical information to an on-site location. This can be done in 15 minute incremental is thus allowing the practice to only lose 30 minutes worth of information if a catastrophic failure happens.
- This continuous incremental backup system should also allow for the capability of the system to be virtualised in the event of a failure.
- An off-site backup of all critical information should also be done as regularly as every 12 hours.

The protection created by backing up your data, is only as good as the recovery process itself. All backup systems should be tested regularly to ensure that information can be recovered as soon as possible.

Conclusion

In conclusion, cybercrime and cyber security is real and as a legal practice you need to make sure that it is in front of mind with everyone in your organisation. We encourage all legal practice's to take protecting their practices from digital attack seriously and take appropriate steps to reduce exposure to all relevant cyber risks. I hope this mini guide will help you:

- get a couple of quick fix is in place
- See where extra is needed and
- Create a risk assessment plan for the practice

This will allow you to see what the situation is and how you can improve it, in most cases further time, money and work will be necessary. This is worth the investment as a cyber-incident will be very costly and an interruption to your organisations business capability, your financial wellbeing and your intellectual property can have a significant impact on the bottom line. Interruptions associated with a cyber-crime can destroy a firm.

I hope you have found this mini guide helpful in shedding some light on the dangers of the digital world in relation to your legal practice.

At the start we stated that this mini guide purpose is to provide this information. I hope that, what we have provided will help you to make an informed decision on Cyber Security and your legal practises' risk to cybercrime.

Below you will find information on how to request a Cyber Security Assessment. This is of course provided for free with no obligation and no expectations on our part. I want to be clear that this is not a bait and switch trick to get you to buy something. My reputation for running an honest and trustworthy managed security service business is something I hold very dear. I would never jeopardise that in any way.

So why are we offering something like this for free?

Two reasons

We are simply offering this service as a risk-free, get to know us offer to clients who we haven't had the pleasure of doing business with. Again our goal is to allow you to make an informed and confident decision and we offer this service as one way we can help you better evaluate our service. To this end it will allow us to determine if you we can even help you in your cyber security requirements.

By conducting this assessment it will enable us to perform a small service for you and give you a risk-free way of determining whether or not we are the right company for you, without risking your money.

Free Cyber Security and Cyber Crime protection assessment.

We would like to offer you a free Cyber Security and Cyber Crime protection assessment and cost analysis. This assessor assessment has three parts.

- **Cost analysis and inventory**. Our first step is to look at what your current network consists of in hardware, licensing, data and applications. We compile an IT cost assessment to reveal your total spend on IT including Internet connectivity, support and other sometimes invisible costs. Most business owners have never really looked at their entire IT costs this way and often this report alone is an eye-opener. Why we do this is because our goal is to find ways we can significantly improve your internal security without additional costs while also simplifying and improving your workflow

- **Health check.** We will avoid perform a 23 point audit on your entire network. We are looking for potential problems, security loopholes, spyware and other hidden problems that you might not yet know about. Often we find faulty backups, out of date antivirus software, faulty firewalls, missing security patches any if the left unaddressed could end up costing you more in new hardware, support, business downtime and money and

- **Cyber Security and Cyber Crime protection assessment.** After really looked at this the above areas we then look at how you and your employees work and share information and see what applications or processes need to have increased security around them and how it can be

deployed with minimal cost and time before moving onto the larger changes that maybe needed.

When completed we will give you a Cyber Security Assessment action pack that shows you how we can improve your cyber security and digital crime prevention processes. This type of assessment will give you some good information on the security and health of your computer network.

How to request your Cyber Security Assessment

Roger Smith
CEO R & I ICT Consulting Services Pty Ltd
PO Box 368 Kippax ACT 2615
02 62580056
Roger.smith@rniconsulting.com.au
www.rniconsulting.com.au, www.smesecurityframework.com.au, www.cybersecuritytraining.com.au

How to request your FREE Cyber Security Assessment

Roger Smith
CEO R & I ICT Consulting Services Pty Ltd
PO Box 368 Kippax ACT 2615
02 62580056
Roger.smith@rniconsulting.com.au
www.rniconsulting.com.au, www.smesecurityframework.com.au, www.cybersecuritytraining.com.au