Computer/Network Security Checklist

Security in the law office context is more than just a locked door and secure file cabinet. Computers and the internet are now an essential component of most, if not all law practices today. Advances with respect to technology have dramatically transformed the way that lawyers handle their clients' confidential information and conduct the practice of law. These developments have created tremendous opportunities to deliver legal services in new and innovative ways, as well as created additional challenges and risks for lawyers as they strive to fulfill their ethical and legal duties to protect their clients' information.

While most lawyers should not attempt to be their own IT department, they do need to educate themselves to the point that they can properly instruct and screen their IT support. This involves understanding your equipment, how it can be secured physically, how it connects to the outside world, and what steps you need to be taking to manage that interaction.

To properly protect yourself and your information, you first need to understand the various threats that you face, and then design a system of defense.

- ✓ **IDENTIFY THE THREATS**:

  - **Theft or physical loss of equipment** - What would you do if your laptop was stolen? Is there confidential client information stored on that machine, or is it only used to access data located back at your office? Is your information password protected? How strong is your password? What if all the computers in your office were stolen? Would you be able to recover that information? And would anyone else be able to access it?

    Whether targeted or random, portable electronic devices make ideal targets for thieves. There are examples in Alberta every year where lawyers computers, both desktop and laptop, are stolen. These thefts are from law offices, lawyers' vehicles, or from homes. This same threat can applies to external hard drives, flash drives, photocopier hard drives, and mobile devices such as smart phones, iPad and tablets. The more portable something is, the more important it is to ensure that the data is secured.

  - **External hackers** – How can you prevent unauthorized access to your office systems over the internet? Do you understand the risks of using public computers or public Wi-Fi connections? Do you know how to harden your own wireless and Bluetooth connections?

    When developing a strategy to protecting yourself from external threats, think of the types of data that you have and where and how you access it to identify potential vulnerabilities (client files, email, voicemail, network configurations, cloud services) and then consider the technical solution to address your vulnerability. This will likely require a combination of software programs to secure your systems as well as specific equipment.

Return to Top

It is not enough to simply set up the system - ongoing maintenance and monitoring is essential.

- Do you know if there have been any unauthorized attempts?
- Or what your employees are doing with your systems?
- Do you have anyone using software to remotely monitor your system's health - from servers, to desktops, tablets and mobile devices?
  Are you able to lock, wipe, and GPS monitor your tablets, phones, and other devices?

- **Internal breaches** – the actions of the humans in your office, whether inadvertent or deliberate, also presents a threat to law office security. It is critical to educate yourself and your staff about the various potential threats. Understand the dangers of email – one of the most common ways that external hackers deliver malicious programs. Emails may come with links to harmful sites, contain infected attachments, or be part of a Phishing scheme seeking to gain access to your account information and passwords.

  The best system in the world will not work if it isn't used properly. The human component of any security strategy must not be overlooked:

  - Always install software updates (Microsoft, virus scanners, etc.);
  - Conduct regular system back-ups and store these back-ups in a location other than a computer that is hooked up to the internet or a network and periodically test your back-ups to ensure that you are able to recover data if necessary;
  - Use a firewall/security suite to stop people from remotely accessing a computer or network;
  - Implement policies on internet, email, dropbox, and social media use and develop internal controls and TRAINING to ensure that everyone is following the correct procedures.

✓ **DESIGN YOUR DEFENSE**

Consider the following when developing your own cybersecurity strategy.

- **Surge Protection**
  - Uninterrupted power supply

- **Firewall**: the "firewall" is the gatekeeper on your internet connection – screening the incoming and outgoing communications from your computer. Information goes in and out of your computer through access points or ports. These ports are open and accessible to any other computers on the internet. The firewall watches these openings and prevents and warns you about unauthorized access. There are two different kinds of firewalls – hardware and software.

Return to Top

- Hardware (usually for protecting your entire network)
  - D-link
  - Linksys
  - Netgear
  - Cisco (for larger networks)

- Software
  - (built in on newer Windows and Mac OS – enable them)
  - TrendMicro Titanium Maximum Security (www.trendmicro.ca)
  - ZoneAlarm (www.zoneAlarm.com)

- Test for security vulnerabilities – ShieldsUP! (www.arc.com)

- **Antispam**: use filters to help catch unwanted and unsolicited commercial emails and prevent these from reaching your email inbox.

  - Postini/Google
  - Norton Antivirus (www.norton.com)
  - SpamNet (www.cloudmark.com)
  - www.fightspam.gc.ca for more information about Canada's anti-spam legislation

- **Anti-virus/anti-malware/anti-spyware**: Malware – short for malicious software - refers to any programs designed to gain access to computers, compromise or interrupt regular computer operations, or gather sensitive information such as passwords or valuable account information. Viruses and Spyware are just specific examples of Malware. (See "Common types of malware" attached)

  - Microsoft Security Essentials
  - Windows Defender
  - Norton AntiVirus (Norton.com)
  - McAfee VirusScan Enterprise (mcafee.com)
  - Bitdefender QuickScan
  - Trend Micro
  - Mac – yes even Mac is vulnerable

- **Encryption** - the process of encoding information so that the content, if accessed by unauthorized users, is not in a form that is not understandable. There are both hardware and software-based encryption methods and it is important to think about encrypting any devices that you use to store data – not just desktop computers, but laptops, external hard drives, flash drives, and mobile devices. Enabling encryption can be as simple as enabling the password feature on any device – or enabling password protection on an individual document. (For information on considerations for dealing with encryption in the context of cloud technologies refer to the 2013 LSBC Practice Resource Cloud computing due diligence guidelines)

Return to Top

- BitLocker (Microsoft's built-in full disk encryption feature included in many versions of Windows)
- SecuriKey Pro (laptop protection for PC and Mac)
- Symantec Drive Encryption
- Flash drives – use only encrypted eg. Defender Basic or IronKey
- Turn on passwords or enable content protection on mobile devices

- **Password assistance**

  - Password managers: LastPass, 1Password, Password Box – programs to help you remember all those passwords
  - Password checker: www.howsecureismypassword.net
  - Password generator: www.speedypassword.com

- **Back-up, back-up, back-up!** Redundancy and security in this regard is key.
  - Full system back-ups using rotating external hard drives or multiple servers
  - Offsite backup to Canadian Cloud data centres
    - There is no specific prohibition on using off-site options. Lawyers store paper files off-site all the time and that is fine, as long as reasonable precautions are taken. The location and level of protection that has been employed only becomes an issue if there is a breach in security and data is compromised. If you are sending data out of your office electronically, it must be encrypted.

    - When considering different storage providers, ask:
      - How does the provider secure my data (do they back up their servers and where are those servers located)?
      - How long has this particular company been around, and are they likely to still be in existence if I need to access my data?
      - If the company fails, how can I recover my data?
      - What is the method of encryption used, and does anyone other than me have the access key?

      Consider a company that is reliable, and is using only Canadian servers to store data. The decision and the responsibility is up to individual lawyers and their level of comfort with risk. When data is stored using servers located outside of Canada, legislation in other countries may give foreign governments the right to examine or intercept confidential and privileged client data.

Return to Top

The Law Society of British Columbia has produced good information on the risks of Cloud computing with due diligence guidelines: (http://www.lawsociety.bc.ca/docs/practice/resources/guidelines-cloud.pdf), and a Cloud computing checklist: (https://www.lawsociety.bc.ca/docs/practice/resources/checklist-cloud.pdf)

- Offsite backup using secure hard drive rotation

- **Office security protocols for online activities**: develop policies and training for safely using the internet

  - Internet use policy – develop a policy that sets out guidelines for dealing with online transactions, restrictions on website visits, file sharing sites, download or installation of software, apps or browser add-ons etc.

  - Email use policy – dealing with recommended procedures for dealing with various activities such as forwarding sensitive emails, identification of suspicious communications, the use of "reply all", or how email communications should be stored.
  - Social media policy – set out guidelines for use of such social media sites as Facebook, Twitter, Instagram, and LinkedIn, how these sites can be accessed, and what information is appropriate to share.

This material was originally developed by Jocelyn Frazer for the LESA Law and Practice Update, November 2014.

Return to Top