IT Guide

TECHNOLOGY MANAGEMENT AND SECURITY FOR LAWYERS AND THEIR TEAMS

Does your use of information technology (IT) comply with your obligations in terms of lawyer-client privilege?

Is your IT management as efficient as it should be?

IN OTHER WORDS… CAN YOU PASS THE TEST?

Barreau du Québec

NOTICE TO USERS

This guide contains advice and recommendations on the application of the rules to which Barreau members are already subject.

Although the guide is updated regularly, please note that only the online version, available at **guideTI.barreau.qc.ca**, should be considered the current, up-to-date version.

Although the contents of this guide are not binding and do not preclude the use of other tools, disciplinary or legal authorities and bodies may find inspiration here in assessing the conduct of a Barreau member.

We thank the experts who volunteered to draft this guide; however, its contents are the sole responsibility of the Barreau. The Barreau du Québec makes no warranty regarding the computer hardware and software mentioned here, or the references or proposed solutions in the guide. Please note that the “24 questions to evaluate your IT use” questionnaire is completely anonymous, and your answers cannot be used to identify you to the Barreau’s professional inspection team.

guideTI.barreau.qc.ca

24 QUESTIONS TO EVALUATE YOUR USE OF INFORMATION TECHNOLOGY

Answer the questions below to the best of your knowledge.

If you answered **NO** or **DON'T KNOW**, ***please read the IT GUIDE online.***

Go to **guideTI.barreau.qc.ca** to find the information you will need to answer the questions in this test.

	At your firm or organization	Yes	NO	Don't know	Follow the guide!
1	Have you implemented security measures to protect your computer network? If the answer is yes, is there a policy on IT use that documents your security measures?	○ ○	○ ○	○ ○	Networking
2	Does every user use a username and password to login on their computer?	○	○	○	• The password • Networking
3	If the answer is yes, is there a rule that the password must: • be changed at least every 30 days? • Include at least 10 characters with at least one upper-case and one lower-case letter, a number and a symbol?	○ ○	○ ○	○ ○	The password
4	Are work sessions automatically locked with a login screen and password when a workstation is idle for up to 3 minutes?	○	○	○	Networking
5	Is your network protected by a regularly updated firewall?	○	○	○	Networking
6	Is every workstation protected by an automatically updated antivirus program?	○	○	○	Networking
7	Are your software programs (e.g. Word, Explorer) and operating systems (e.g. Windows, Mac OS) automatically updated?	○	○	○	Networking
8	If you have a wireless network (WiFi): • Have you changed the default administrator code on the wireless router (access point where computers connect) • Have you changed the default password on the wireless router? • Have you set up an encryption method for data transiting the wireless network? • Have you configured the wireless router so it only accepts communications from the computers in your network? • Have you blocked the public broadcasting of your wireless network name?	○ ○ ○ ○ ○	○ ○ ○ ○ ○	○ ○ ○ ○ ○	Networking
9	Is data saved by users on a laptop, tablet or portable device (USB key, external hard drive, etc.) encrypted?	○	○	○	Networking
10	Are your employees allowed to work with their personal electronic devices? If the answer is yes, do you have a policy to ensure the security of these devices and manage risks?	○ ○	○ ○	○ ○	Personal devices

At your firm or organization		Yes	NO	Don’t know	Follow the guide!
11	Do users working from home have a VPN (Virtual Private Network) connection to protect their work sessions?	○	○	○	Networking
12	When your employees use smartphones: • Do they need to authenticate with a secure password (see question 3) to access their content? • Has the automatic login screen been configured? • Has data encryption been configured?	○ ○ ○	○ ○ ○	○ ○ ○	• Cellphones • Encryption
13	Are Bluetooth connections configured so they’re not available by default and are secured when in use?	○	○	○	Cellphones
14	Is access to electronic documents and email on your network reserved solely for those involved?	○	○	○	Electronic communications
15	Are communications with your clients password-protected or on a closed secured network with the client or encrypted?	○	○	○	Electronic communications
16	Have you implemented a method for organizing documents on your computers and your email as per the *Regulation respecting accounting and standards of professional practice of advocates*?	○	○	○	• Electronic communications • Organizing documents
17	Have you implemented a method for managing backup copies of data saved on your network? (computers, servers, smartphones etc.)?	○	○	○	Backup copies
18	Did you know that some documents contain hidden confidential data that can be sent without your knowledge (e.g. comments or Track Changes) and are you taking steps to prevent this?	○	○	○	Metadata
19	Do you have computer security procedures to manage employee departures (delete user account, access to confidential documents, cellphone accounts, etc.)?	○	○	○	When an employee leaves
20	Are your agreements with suppliers (e.g. technicians, hosting service, cloud computing) in compliance with your ethical obligations (confidentiality, etc.)?	○	○	○	• Agreement with suppliers • Cloud computing
21	Have your offices and computer equipment been secured?	○	○	○	Securing rooms and equipment
22	Do you have a procedure for the secure disposal or recycling of computer equipment?	○	○	○	Disposal and recycling
23	Are you managing security alerts, e.g. for backup copies or attempted intrusions in your systems?	○	○	○	Managing alerts
24	Do you have a business continuity plan in case of a disaster?	○	○	○	Backup copies

Introduction

IT security is generally designed to achieve the following objectives:

- Ensuring the confidentiality of data (making information unintelligible to anyone apart from authorized individuals);
- Ensuring the integrity of data (making sure that data has not been altered accidentally or intentionally in the process of communication);
- Ensuring the availability of data (providing access to services or resources).

The use of information technologies (IT) is of particular interest to lawyers in their professional practice from several viewpoints, but primarily as regards professional secrecy and duty of competence. This guide is designed to assist lawyers in fulfilling their ethical obligations.

Since IT security requires a global approach, this guide will explore several levels of intervention, such as:

- **Security of telecommunications** (network technologies, servers, access networks, etc.)
- **Security of material infrastructures (**secure spaces, public places, common spaces within the company, personal workstations, etc.)
- **Users' awareness** (staff training, consistent internal procedures and policies on security, etc.)

The advice and recommendations in this guide have not been specifically encoded in legislation or regulations for the practice of the legal profession (including the *Code of Professional Conduct of Lawyers*). This guide can therefore be considered a description of best practices and/or practices that are generally recognized at the time of its last updating.

That being said, please bear in mind as well that even in the absence of a specific standard established by legislation or regulation, the disciplinary council does possess exclusive residual jurisdiction under sections 59.2[1] and 152[2] of the *Professional Code* for deciding whether or not an act or omission constitutes a derogatory act.

[1] Section 59.2: No professional may engage in an act derogatory to the honour or dignity of his profession or to the discipline of the members of the order (…).

[2] Section 152**:** The disciplinary council shall decide to the exclusion of any court, in first instance, whether the respondent is guilty of an offence referred to in section 116.

Where there is no provision in this Code, the Act constituting the order of which the respondent is a member or a regulation or by-law under this Code or that Act which applies in the particular circumstances, the disciplinary council shall decide to the exclusion of any court

(1) whether the act with which the respondent is charged is derogatory to the honour or dignity of the profession or to the discipline of the members of the order, (…).

Professional secrecy

By the very nature of the tasks and responsibilities they carry out in their professional practice, members of the Barreau du Québec are required to collect confidential information from their clients[3] that will be analyzed, used, communicated, kept and eventually destroyed, in order to provide legal services of the highest quality.

By "confidential information", we mean information that is subject to contractual or legal constraints (which is not intended to circulate freely) and which the person in charge of the information (who holds the obligation of confidentiality) is required to protect. This includes, among other things, personal information, commercial or industrial secrets, information protected by professional secrecy and litigation privilege.

In addition to legislation designed to protect the confidential nature of such information[4], the Supreme Court of Canada has made lawyers' professional secrecy a basic rule and fundamental principle of our justice system[5].

Lawyers who use information technology (IT) are required to take all necessary precautions to prevent the occurrence of any glitches in professional secrecy. In that regard[6], section 34 of the *Act to establish a legal framework for information technology*[7] reads as follows:

> "34. Where the information contained in a document is declared by law to be confidential, confidentiality must be protected by means appropriate to the mode of transmission, including on a communication network.
>
> Documentation explaining the agreed mode of transmission, including the means used to protect the confidentiality of the transmitted document, must be available for production as evidence."

In so doing, lawyers are responsible for acting in a prudent and diligent manner. This is only possible insofar as they take the time to obtain sufficient information on the ITs used, the risks inherent in using those technologies, and methods or solutions for preventing or reducing those risks.

[3] This is a fundamental criterion in deciding on the advisability of setting up a professional order – *Professional Code*, sec. 25(5).

[4] *Charter of Human Rights and Freedoms,* sec. 9, *Professional Code*, sec. 60.4, *Act respecting the Barreau du Québec*, sec. 131(1), *Code of Professional Conduct of Lawyers,* sec. 60 and ff. and *Regulation respecting accounting and standards of professional practice of advocates,* sec.17.

[5] See *Lavallée, Rackel & Heintz* v. *Canada (Attorney General); White, Ottenheimer & Baker* v. *Canada (Attorney General)*; *R.* v. *Fink*, [2002] 3 S.C.R. 209. *R.* v. *Brown*, [2002] 2 S.C.R. 185; *Maranda* v. *Richer*, [2003] 3 S.C.R. 193; *Foster Wheeler Power Co.* v. *Société intermunicipale de gestion et d'élimination des déchets (SIGED) Inc.*, [2004] 1 S.C.R. 456.

[6] In addition, section 60.4 of the *Professional Code* states as follows: "***Confidential information***. Every professional must preserve the secrecy of all confidential information that becomes known to him in the practice of his profession. […]"

[7] An Act to establish a legal framework for information technology, www2.publicationsduquebec.gouv.qc.ca/dynamicSearch/telecharge.php?type=2&file=/C_1_1/C1_1_A.html

Section 61 of the *Code of Professional Conduct of Lawyers* stipulates that: "A lawyer must take reasonable measures to ensure that every person who collaborates with him when he engages in his professional activities and, where applicable, the firm within which he engages in such activities, protects confidential information.

Similarly, when the lawyer engages in his professional activities within an organization, he must take reasonable measures to ensure that the organization provides him with the necessary means to protect confidential information"[8].

Reasonable measures should be extended to include equipment, systems and computer programs used by lawyers and members of their teams.

Duty of competence

Apart from the issue of protecting confidential information, these days understanding and knowing how to use IT constitutes one of the major components of the notion of competence[9] that lawyers are expected to demonstrate at all times while providing legal services[10]. From today's vantage point, it's hard to imagine that a lawyer could practice without a computer, word processing software, email, or Internet access, without understanding and knowing how to use electronic documentary resources – legislation, doctrine and jurisprudence[11].

Depending on the field of legal practice or a specific file, an understanding of social media may also be seen as another facet of the duty of competence[12].

[8] See also sections 5, 6 and 60 of the *Code of Professional Conduct of Lawyers*.

[9] From a professional inspection department brochure, *Faites-vous une loi de viser l'excellence* [Translation] Defining competence: A competent lawyer recognizes (...) the need to master the available means and techniques for applying his knowledge in a relevant, capable and efficient manner; the ability to use such knowledge, means and techniques to put together dossiers to document the collection of important information, available avenues, justification of professional choices, their compliance with the client's objectives and decisions, and the steps in achieving objectives.

[10] *Code of Professional Conduct of Lawyers*, sections 10, 20, 21 and 29.

[11] See D. Jaar and F. Sénécal, *Les obligations de l'avocat face aux technologies de l'information*, Développements récents en déontologie, droit professionnel et disciplinaire, Barreau du Québec, 2010. www.caij.qc.ca/doctrine/developpements_recents/323/1770/index.html.

[12] See also on this subject: *Social Media and the Lawyer's Evolving Duty of Technological Competence*, Benjamin P Cooper, *Legal Ethics*, 2014, Volume 17, Part 3, http://dx.doi.org/10.5235/1460728X.17.3.463). The new *Code of Professional Conduct of Lawyers* explicitly refers to the use of social media in section 1.

SECTION 1 COMMUNICATIONS SECURITY

One important aspect of lawyers' business management is the security of the information they handle. The circulation of that information must be properly monitored. In a paper-based world, information is tracked by physically tracking documents and locations. In an electronic world, new forms of security must also be considered.

The first section of this guide focuses on the security of computerized networks, telephony and electronic communications.

Computer network technology

Principle

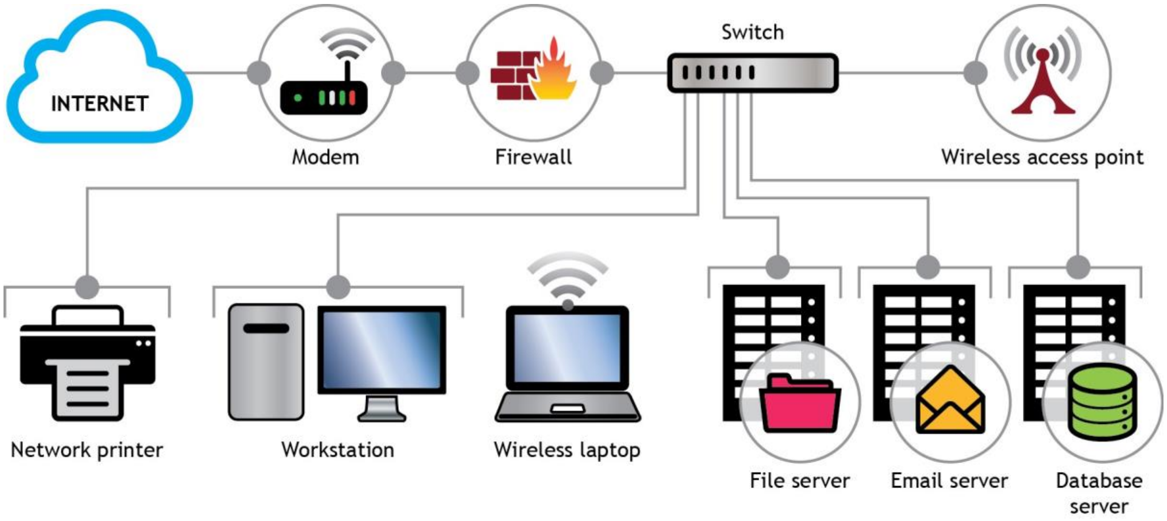
Lawyers are required to put in place a policy framework for the use of their computerized network, as well as security measures to protect the information. This policy should enable lawyers to make sure that their computer networks comply with their ethical obligations (professional secrecy, commercial and industrial secrets, personal information, etc.).

Definition

Computer network technology covers all techniques relating to the creation, maintenance and use of a computer network, which is made up of computers and peripherals, such as printers, digitizers, smartphones, tablets, servers, switches, routers and modems, which are connected – wired or wirelessly – and software.

With computer networks that connect a number of computers, users can share data. The main advantages are speed of access to information and enhanced productivity and collaboration. Data contained in computer networks is frequently of a confidential nature and so needs to be protected. In addition, data placed on a server shared by several users may not be intended to be accessible by everyone. In such cases, only those granted pre-established access rights should be able to consult the data. This can be very important when it is necessary to build a "Great Wall of China" to avoid apparent or potential conflicts of interests, or to avoid disseminating information to categories of users who have no need to be aware of this information (the principle of "need to know").

The diagram below shows a network that includes a server, workstations, a switch and a firewall.



Usefulness

Connecting computers in a network makes it possible for:

a. Resources (files, applications, material, Internet connections, etc.) to be shared;
b. Users to communicate (via email, instant messaging, etc.);
c. Various procedures to communicate (e.g. an accounting application and a billing application for phone calls), which automates tasks and reduces the risk of entry errors;
d. Accurate, up-to-date information to be found (on databases);
e. Data to be stored in a central registry.

Risks

Every computer that is connected to a network can be exposed to the outside world and fall prey to an invasion, hacking attempt or, more generally, an attack on the integrity of the computer system and the data it contains.

The threat is even greater for a computer that is permanently connected to the Internet, which is increasingly the case. To find out whether your computer is permanently connected to the Internet, on a PC, look on the lower right of your screen to find the little lines that show the network or cable symbol. On a Mac, look for the symbol on the top at the right.

These days, with wireless networks, smartphones (e.g. iPhone, Android, BlackBerry, etc.), distance connections and Bluetooth wireless devices, sensitive data is increasingly exposed and vulnerable to the risks of unauthorized access and disclosure from outside the physical office.

It’s important to make sure that data kept on your computer network is secure. Here are some points to check:

Using passwords and disconnecting from inactive sessions

To protect information on a computer network, it’s important to protect access to all the workstations that are connected to the network. We recommend setting up a user authentication method (user code plus password) when users connect on their workstations. Most network operating systems allow this type of authentication. Passwords, which should be changed periodically (every 30 days), should contain a code with at least ten characters (or more, if the system allows). The password should include at least one capital letter, one lower-case letter, one number and one symbol.

It’s also important to disconnect or lock a workstation or inactive session to avoid a third party taking control of the workstation and gaining access to confidential data. Configuring a password on the screen after three minutes of inactivity can fill that function. A configuration that blocks the system for 15 to 30 minutes after five login attempts is also a good security measure.

Using antivirus programs with frequent updates

Antivirus programs are software programs that are designed to identify, neutralize and eliminate malware. Depending on the product, the tool may also recognize spam or spyware (worms, cookies, etc.), and prevent the installation of Trojan horse-type software, which can open a breach that will give access to a computer that is part of your network. The protection conferred by this software should go hand in hand with responsible practices, especially when opening attachments to emails that are unsolicited or come from an unknown source.

Using a firewall

A firewall is an element in a computer network, software and/or equipment that protects a computer or computer network from invasions from an outside network (notably via the Internet). The objective is to provide a secure connection and control data flow between different secure zones to let data through while following established security rules. A request coming from the Internet for access to a document will be refused, while the same request coming from a user in the same network will be accepted. This is why it’s so important to install a firewall on your network. Note that there are ways of authenticating requests from the Internet to facilitate secure telecommuting.

Be aware, however, that while some routers may include a firewall, the router itself is not a firewall! The router makes it possible for several pieces of equipment (computers, smartphones, IP phones, etc.) to share the same Internet connection. While it can be configured to allow traffic flow from the Internet or block it, that is not its primary role. Unlike the firewall, it cannot direct traffic between different secure zones.

Updating software and operating systems

Even after software programs or operating systems are put on the market, there may still be bugs that allow malicious hackers to use them to compromise your system.

Most recent software programs and operating systems come with update options[13]. If your workstation tells you an update is available, it's generally recommended that you proceed with the update. But first, make sure it won't cause your system to become vulnerable.

Word of the existence of these vulnerabilities spreads quickly. That's why it's recommended to follow the default configurations and choose the daily or regular updates suggested by the manufacturer (not including beta or pre-release versions of a software program, which could be risky).

Making wireless networks (WiFi) secure

Wireless networks have a big advantage: you can connect a computer, smartphone or tablet to the network without a physical connection (cable). When they connect, a signal allows access to the network. The signal can be captured by anyone with a WiFi device. Here are some basic security rules to follow when using wireless networks:

a. Change the administrator's code and password at the access point (where you connect) or the wireless router. The default settings, which most users never change, are the first to be tested in the event of an attempted invasion. See section 2 for further details on passwords.

b. Activate data encryption for data that travels over wireless links. We recommend using the WPA2 protocol; avoid the WEP protocol, which can quickly and easily be hacked.

c. Filter MAC (Media Access Control) addresses – the unique physical address of a network card. The access point or wireless router will only communicate with addresses that have been preconfigured by the network administrator.

d. Disable the wireless network name (SSID Broadcasting) to "hide" the wireless network from unauthorized users.

If you offer WiFi access in your waiting room, plan for guest access, which is different from what you use to gain access to your own network, in order to minimize security risks and limit access to the network. Apart from gateways that give your guests access, your passwords should not be shared.

Using mobile technology

USB keys and external hard drives rapidly replaced CDs, DVDs, diskettes and other removable devices. Smartphones (iPhone, Android, BlackBerry, etc.), which contain email, agendas, contact lists and documents, can also provide access to your network. Connections to internal networks from an Internet link (outside the company) are also increasingly common. To ensure effective security for this mass of data, which can easily be left in a restaurant or on the back seat of a taxi, you need to encrypt the data they contain.

For smartphones, it's crucial to set up password authentication and encrypt the documents on the device[14]. You also need to make sure that Bluetooth (short-range) connections between devices like

[13] In most cases, only licensed versions include these updates.

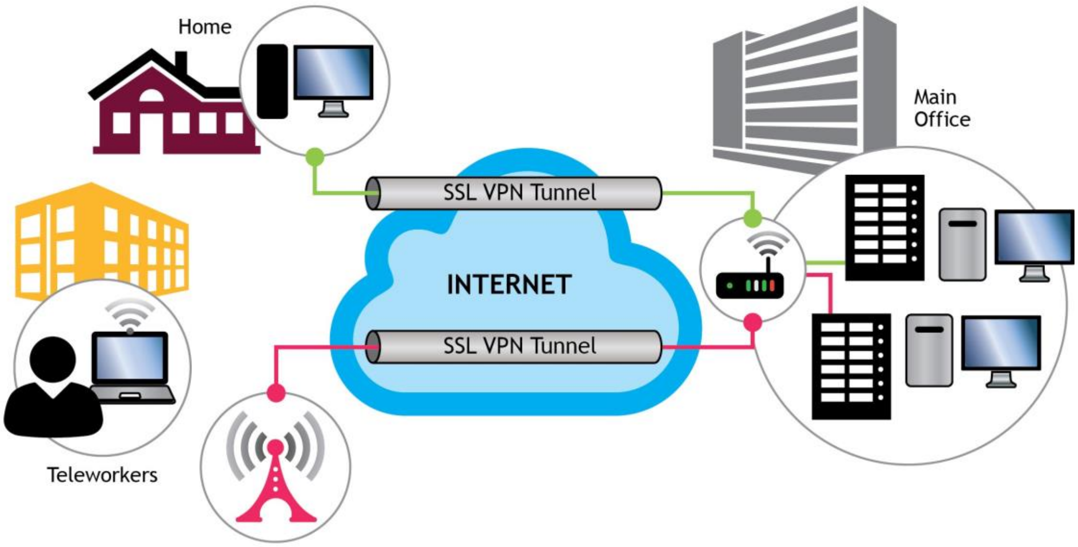
[14] For further details, see the cellular section

hands-free headsets or devices that transfer information are not available by default and are secure while in use.

When using a mobile device on a public WiFi network, make sure you're using a secure VPN (Virtual Private Network). If you are a telecommuter and you connect your work computer at home via your personal network, make sure you use a VPN connection as well.

This type of connection provides access to your company's local network over a secure Internet connection and gives you access to the resources of your local network (e.g. files, intranet, extranet) as if you were at the office.

A VPN connection provides the highest possible level of security, with encrypted tunnels and authentication technologies, protecting data that travels through the VPN from unauthorized access. This diagram shows how it works.



Resources

Antivirus programs

- McAfee
- Symantec Norton
- ESET
- Avast
- Microsoft Security Essentials (free for companies with 10 or fewer employees)
- The best free antivirus for 2016

Firewalls

- Zone Alarm
- Cisco
- Sonicwall
- WatchGuard
- Kaspersky

Updates for software and operating systems

- Microsoft Windows 10
- Microsoft Windows Update
- Apple MAC OS X
- Mac App Store
- MacUpdate Desktop 5

Adding timer and password to standby screen

- For Windows 7
- For Windows Vista
- For Mac OS X

Wireless network security

- Microsoft Technet
- Setting up wireless security on a Linksys router
- How to secure a D-Link Wireless Router

BYOD (Bring Your Own Device)

Principle

Lawyers need to put in place a policy to cover the use of personal equipment that connects to part or all of their computer network, along with security measures to protect the equipment. The policy should help lawyers to make sure that the use of a computer network complies with their ethical obligations (professional secrecy, commercial and industrial secrets, personal information, etc.).

Definition

The acronym BYOD first started to appear in technical publications in late 2011, but companies have been letting employees use their personal computers to connect to the company network over a VPN since the early 2000s, as the benefits of giving lawyers and support staff access to their files and email from home gradually became obvious, making employees more available and more productive.

With the arrival of smartphones and tablets on the market, consumers began to buy their own equipment, based on their own needs and preferences.

BYOD is equipment provided by an employee who has access to some or all of the data on the company computer network.

Usefulness

When equipment provided by employees is used:

a) The company has access at all times to some or all of the data;
b) Employees can be more mobile;
c) The company spends less on equipment acquisitions;
d) Employees get to choose the equipment they're most comfortable with and choose it carefully.

Risks

Since personal equipment is not managed by the company IT department, it can be difficult to control security for these devices. Most devices use WiFi links, which means there is a risk of clogging up and slowing down the company's connections. Here is a list of risks inherent in the use of BYOD:

a) Allowing unmonitored access to company data;
b) With several email accounts on the same device, there is a greater risk of infection from a virus;
c) With several email accounts on the same device, there is a greater risk of data loss;
d) There is no control over updates and vulnerabilities inherent in the various operating systems used;
e) There is a need to have expertise on various platforms to support users;
f) There is no control over installation of applications that could conflict with applications that are critical for the company.

Best practices

It would be practically unthinkable nowadays to prevent employees from using their own equipment and not giving them access to email, at the very least. To keep some control over data that flows over these mobile devices, we suggest putting in place some tools for the secure use of BYOD. Here is a list of tools and their useful features:

a) **Policy on personal equipment use**

This policy should establish ownership (where the company provides the equipment) and what the employee is allowed or not allowed to do with the device for personal purposes. It should also establish who owns the data that travels over the device if the device belongs to the employee. It should also determine to whom – the employee, the firm or a pro-rata division by personal/business use – monthly costs for use and bandwidth should be billed. The policy should also clearly establish security parameters (access and restrictions) for company data.

b) Tools for managing personal equipment

There are two tools for managing BYOD: EMM (Enterprise Mobility Management tools) and MDM (Mobile Device Management tools).

EMM is actually a combination of technologies, procedures and staff who know how to manage the use of BYOD and services in a business context.

MDM is an application that manages BYOD at the level of the company's computer services. With this application, operating systems can be updated remotely, device errors can be monitored and controlled, and user support can be handled remotely, as well as keeping an inventory of active terminals and consulting communications in real time. From the security standpoint, this application makes it possible to manage backups and recoveries in case a device is lost or replaced, block or delete data remotely in case a device is lost or stolen, and install applications remotely.

Resources

- The New BYOD: Best Practices for a Productive BYOD Program – Air Watch by VMWare
- Wikipedia MDM
- Wikipedia EMM

Cellular devices

Principle

All mobile phones (cell phones and smartphones) or personal digital assistants should require a password after a three-minute standby period. Content needs to be encrypted and the default name changed. Networking protocols (Bluetooth, WiFi, etc.), as well as the detectability of the device, need to be deactivated when not being used. Once activated, they need to be encrypted.

Definition

Smartphones are mobile phones coupled with personal digital assistants that offer such functionalities as an agenda, Web browsing, email and instant messaging. Additional applications can also be installed on various models. The best known phones use the iPhone OS, Android and BlackBerry platforms.

Bluetooth is a short-range radio technology designed to simplify connections between electronic devices by replacing the cables that would otherwise be needed. The Bluetooth network can interconnect computers, printers, digitizers, keyboards, mobile phones, mice, personal digital assistants, speakers, hands-free microphones, etc.

Risks

With every passing day, smartphones become more and more like computers in terms of the functionalities and capacities they offer. They contain more and more confidential data, such as personal information and commercial or industrial secrets, but most importantly, information that is covered by lawyers' professional secrecy or litigation privilege. This is why it's so crucial to protect this information under all circumstances.

Their small size makes mobile phones especially vulnerable to loss or theft, so precautions must be taken. It's important to make sure that if a device goes astray, the person whose hands it may fall into cannot gain access to the contents. The only way to do this is to protect the device with a password and encryption, with the password following the usual guidelines.

Bluetooth technology is very common for cell phones, and Quebec drivers are required to use hands-free devices. Useful as this is, it's just another weak link in the information security chain. In fact, many Bluetooth tools open a communications channel with the smartphone that is potentially insecure.

Using this technology, most mobile phones can exchange data, such as virtual business cards, calendar events, documents, and especially voices. In many cases, the Bluetooth tool synchronizes with the smartphone by getting permission to access the contents of the device. Connection is a two-step process: first, the phone and the tool detect each other's presence in order to initiate communication; next, the two devices communicate to request their respective IDs and authorize the exchange of information. An outsider could easily intrude in the exchange or even initiate the process.

Best practices

Password protection needs to be activated in the phone. This functionality is generally found in the security section of the phone settings. Here is how passwords are activated:

- → On an iPhone: Settings > Code (on an iPhone 5s or higher, activate the digital fingerprint reader: Settings > Touch ID and Code)
- → On an Android phone: Settings -> Location and security -> Lock screen (enter a code, picture or password – your choice)
- → On a BlackBerry: Settings > Security and confidentiality > Simple password or password for terminal

Standby mode reduces the device's window of vulnerability when the owner is not in control of the device. It should be set at three minutes or less. Here is how to set your standby options:

- → On an iPhone with iOS 8.x or higher: Settings > General > Auto lock
- → On an Android phone: Settings > Personal > Security > Lock screen
- → On a BlackBerry: Settings > Security and confidentiality > Password for terminal. Choose "Look terminal after" from scrolling list and choose an interval.

We also recommend deactivating the "share connection" option when not in use. This function enables a computer to use an Internet connection from a cell phone, via a cable connection, WiFi connection or Bluetooth connection. Here is an example of how to deactivate the "share connection" option:

- **On an iPhone with iOS 8.x or higher**: Settings > Share connection

Encryption, which is usually found in the same place, should be activated. You may be able to see how strong the encryption is; we suggest keeping it at the highest level. However, basic protection may be sufficient if it is 128 bits or higher.

With Bluetooth technology, to protect the information in the phone, make sure that detectability is deactivated when it is not required for communication, and encrypted and password-protected when needed for communication. This is generally the same password (mentioned above) that is used to gain "physical" access to the contents of the phone. Here is how to find the Bluetooth settings:

- **On a BlackBerry:**

  Detectability: Options > Bluetooth > Menu button > Options > Detectability > No.
  Encryption: Options > Bluetooth > Menu button > Options > Security level > High and encrypted.

- **On an iPhone with iOS 8.x or higher:**

  Detectability: Settings > General > Bluetooth > (deactivate)
  Encryption: There is currently no way to activate data encryption from the iPhone applications, but it is possible to use Hushmail to perform encryption of information on this type of device.

It's also necessary to change the default names of the phone and the Bluetooth tool. Otherwise, anyone could identify the access code and gain remote access. Here is an example of how to make this change:

- On an iPhone: The best way to prevent remote access to information on the iPhone is to deactivate the Bluetooth function when it is not required: Settings > General > Bluetooth > Close application. To change the name of the device: Settings > General > Information > Name.

- On an Android phone: Settings > About (scroll down) > press "Name of device" > Tap desired name > "OK." To change name in Bluetooth: Settings > Bluetooth, show Menu and choose "Rename device," then tap desired name and validate with "OK."
- On a BlackBerry: Options > Bluetooth > Select tool > Menu button > Properties

If you lose your cell phone, it is possible on most models to locate, lock or unlock the device, as well as delete the contents, remotely.

For further information on this option:

- On an iPhone: Before performing any of these steps, make sure you have first activated the option with the device in your hand.
- On an Android phone: Your device needs to be attached to a Google account (available free of charge);
- On a BlackBerry: BlackBerry Protect is a free application that will find a lost phone and protect the information on the phone.

Ethics and professional conduct

Lawyers must respect these practices to satisfy the obligation to protect professional secrecy[15].

Remember as well that it is illegal for a lawyer to hold a public telephone conversation with a client who has entrusted the lawyer with confidential information unless the client expressly releases the lawyer from that obligation. The obligation in such a situation is covered under section 5 of the *Regulation respecting accounting and standards of professional practice of advocates,* which reads as follows:

"The advocate shall use a consulting room or other room for meeting clients or holding conversations that are subject to professional secrecy. This consulting or other room must be closed and designed in a way that prevents the conversations of persons therein from being heard from outside the room. No other person shall have access to this room for the duration of such meetings or conversations, unless authorized by the advocate."

Resources

Security and smartphones

- Ten dangerous claims about smart phone security
- Mobile Security

[15] *Professional Code*, sec. 60.4., *Code of Professional Conduct of Lawyers*, sec. 60 and 61, *Act to establish a legal framework for information technology*, sec. 34, *Regulation respecting accounting and standards of professional practice of advocates*, sec. 17.

Bluetooth Security

- Official Bluetooth site
- Guide to Bluetooth Security
- Bluecasting
- Bluejacking (proximity marketing)
- Bluesnarfing

Electronic communications

Principle

Lawyers who communicate confidential information must protect that information in a manner appropriate to the mode of communication and the nature of the information. They should also agree with their clients on how each kind of information will be communicated and protected, and document that agreement, generally in writing.

Example

For example, a legal notice on the privatization of a public company sent by email must be encrypted to protect the notice between sending and receipt. On the other hand, a message to an adolescent who wants to have an abortion may be sent without being encrypted but should be protected in some other way and sent in a password-protected attachment, or sent to a different agreed-upon email address so that it will not be seen by the parents.

Risks

Like many other people, lawyers have no hesitation in sending highly confidential information or documents by email. However, the lawyer alone has the obligation to maintain absolute secrecy regarding the information he or she is holding for another person and has received in a professional capacity.

The use of electronic mode of communication without protective measures involves various risks: wrong recipient, deliberate misuse, interception, alterations to the message, etc. It is also important to be aware that between your outbox and the intended recipient's inbox, emails cross many servers, potentially located in other jurisdictions or countries, some of which may keep copies of emails. The same holds true for most means of electronic communication: they leave traces in many different places. These risks are inherent in the use of information technologies, but may be the subject of counter-measures to enable lawyers to fulfill their obligations.

Accidental receipt of information that may possibly be protected by professional secrecy

The accidental transmission of documents or information protected by professional secrecy[16] to a person other than the client is a problem that is occurring more and more frequently with the development of new technologies.

While errors in the delivery of physical letters were quite infrequent (wrong address or putting a letter in the wrong envelope), this type of error has become much more common with the use of instant communication methods, such as the fax machine (wrong number), and now email (wrong address, accidental cc/bcc, etc.). Electronic versions of transmitted documents may also contain information, notably in the form of metadata[17], that the sender does not wish to disclose[18].

Although jurisprudence and doctrine indicated the opposite not so very long ago, and the question remains controversial in common law, it is now recognized in civil law that inadvertent disclosure is not the equivalent of renouncing protection of professional secrecy[19], especially since the passage of section 2858 of the *Civil Code of Québec*[20] in 1994.

> [25] [Decision not available in English – Translation] In this case, considering on the one hand the Attorney General's representations that the document was inadvertently divulged to the claiming party, and on the other hand the absence of evidence of voluntary disclosure with the client's permission, the release cannot be imputed to that party nor constitute a waiver of his right to professional secrecy[21].

From a purely procedural point of view, although it resulted from an Anton Piller order, the decision of the Supreme Court of Canada in the Celanese case[22] established guidelines applicable to the problem in

[16] On this topic generally, see: M^e^ Michel Tétrault, *Le litige familial, la déontologie et l'éthique*, Cowansville, Éditions Yvon Blais, 2006, pp. 19-26, and M. Jamal and S. Lussier, *Le secret professionnel de l'avocat*, Développements récents en déontologie, droit professionnel et disciplinaire, Formation permanente du Barreau, Colloque 2008, pp. 216-217.

[17] On the ethical implications of accidental receipt of metadata in the United States, see: "Formal Opinion 2009-100 – Ethical obligations on the transmission and receipt of metadata," (July/August 2009) The Pennsylvania Lawyer.

[18] On the possible prohibition of erasing metadata in the context of "discovery" in the United States, see: "Technology traps/Ethical considerations for litigations in a 24/7 online world," (Winter 2010) 36 Litigation, p. 34, 37-38 (no. 2).

[19] See also: *Spieser* v. *Canada (Attorney General)* 2010 QCCS 3248; *Guillemette* v. *Smith*, 2009 QCCA 2190; *GeneOhm Sciences Canada Inc*. v. *Biomérieux Inc*., 2007 QCCA 290; *Lavallée, Rackel & Heintz* v. *Canada (Attorney General)*; *White, Ottenheimer & Baker* v. *Canada (Attorney General)*; *R*. v. *Fink*, [2002] 3 S.C.R. 209, par. 49; *Poulin* v. *Pratt*, [1994] R.D.J. 301 (C.A.); *G.(A.)* v. *W.(D.)*, REJB 2002-32223 (C.S.); M. Jamal and S. Lussier, *Le secret professionnel de l'avocat*, Développements récents en déontologie, droit professionnel et disciplinaire, Formation permanente du Barreau, Colloque 2008, pp. 216-217; Royer and Lavallée, *La preuve civile*, 4th ed., Cowansville, Éditions Yvon Blais, 2008, par. 1222, note 478, and Léo Ducharme, *L'administration de la preuve*, 3rd ed., Montréal, Wilson et Lafleur, 2001, pp. 117-118.

[20] *Guillemette* v. *Smith*, 2009 QCCA 2190, par. 19; *Civil Code of Québec*, sec. 2858: "The court shall, even of its own motion, reject any evidence obtained under such circumstances that fundamental rights and freedoms are violated and whose use would tend to bring the administration of justice into disrepute."

[21] *Spieser* v. *Canada (Attorney General)*, 2010 QCCS 3248.

[22] *Celanese Canada Inc*. v. *Murray Demolition Corp.*, [2006] 2 S.C.R. 189.

the case, including the fact that the party who had erroneously sent documents containing protected information should immediately:

1. be so advised;
2. be given back the erroneously transmitted documents[23];
3. be informed how closely the documents had been examined.

If this did not happen, there would be a presumption of prejudice[24], and a court could issue an order for reparations or even a declaration of incapacity[25] on the part of the attorney who received the protected information, although that incapacity would not be automatic[26].

Orders for reparations may include the withdrawal of a document accidentally produced in the Court file[27] or included among documents sent to the opposing party[28], or the documents in question being returned to the sender by the opposing party or his/her attorneys[29]. Orders may also prohibit any reference to or use of the documents[30], asking questions about them[31], requiring the production of anything resulting from the contents of said documents[32], using anything retained from the documents in interrogation (previous to or in the courtroom)[33], or revealing the contents to anyone[34].

[23] If this were not done, a court could so order; see: *Smith* v. *Bélanger et al.*, 2009 QCCS 4277 confirmed by *Guillemette* v. *Smith,* 2009 QCCA 2190.

[24] The Supreme Court of Canada, in the *Celanese* decision, applied a previous decision: "This Court's decision in *MacDonald Estate v. Martin*, [1990] 3 S.C.R. 1235, makes it clear that prejudice will be presumed to flow from an opponent's access to relevant solicitor-client confidences." *Celanese Canada Inc.* v. *Murray Demolition Corp.,* [2006] 2 S.C.R. 189.

[25] "The conflict here must be resolved on the basis that no one has the right to be represented by counsel who has had access to relevant solicitor-client confidences in circumstances where such access ought to have been anticipated and, without great difficulty, avoided and where the searching party has failed to rebut the presumption of a resulting risk of prejudice […]," *Celanese Canada Inc.* v. *Murray Demolition Corp.*, [2006] 2 S.C.R. 189 – see also par. 56-59; *Darco Archery* v. *Topo Production*, EYB 1991, 04-10-1991; *Hull* v. *Chellecourt*, 2006 QCCS 1364; on this subject, in the United States, see: Etan MARK, "Inadvertent Document Productions and the Threat of Attorney Disqualification," (November 2009) 83 Florida Bar Journal (no. 10).

[26] *Celanese Canada Inc.* v. *Murray Demolition Corp.,* [2006] 2 S.C.R. 189, par. 56; *D.L.* v. *J.G.*, AZ-50141353 (S.C.), 01-08-2002; *Chouinard* v. *Robbins*, REJB 1996-86859 (S.C.).

[27] *G.(A.)* v. *W.(D.),* REJB 2002-32223 (C.S.); *Bombardier Inc.* v. *Union Carbide Canada Inc.*, 2010 QCCS 6780.

[28] *Smith* v. *Bélanger et al.*, 2009 QCCS 4277, conclusions.

[29] *Smith* v. *Bélanger et al.*, 2009 QCCS 4277, conclusions; *Spieser* v. *Canada (Attorney General)* 2010 QCCS 3248, conclusions; *Bombardier Inc.* v. *Union Carbide Canada Inc.*, 2010 QCCS 6780.

[30] *Smith* v. *Bélanger et al.*, 2009 QCCS 4277, par.24; *Bombardier Inc.* v. *Union Carbide Canada Inc.*, 2010 QCCS 6780.

[31] *Smith* v. *Bélanger et al.*, 2009 QCCS 4277, par. 26.

[32] *Smith* v. *Bélanger et al.*, 2009 QCCS 4277, par. 24.

[33] *Smith* v. *Bélanger et al.*, 2009 QCCS 4277, par. 24 et 26.

[34] *Spieser* v. *Canada (Attorney General)* 2010 QCCS 3248, conclusions.

On the ethical front, the Superior Court has stated that the duty of confidentiality would apply to a lawyer who receives or would like to use privileged information coming from a third party who is not or never has been the lawyer's client[35].

The *Code of Professional Conduct of Lawyers* stipulates that:

> 63. A lawyer must not use confidential information with a view to obtaining a benefit for himself or for another person.
>
> 64. A lawyer must not accept a mandate if he has reason to believe that doing so entails or is likely to entail the communication or use of confidential information concerning another client.

A lawyer who receives a document, particularly from the counsel for the opposing party, that appears not to be intended for him or her or that contains information that may possibly be protected by professional secrecy,[36] should:

1. stop reading the document immediately;
2. immediately advise the colleague (even though there is no specific ethical provision to do so[37]) and find out whether the document really was intended for him or her and whether it is covered by professional secrecy or privilege;
3. upon request, destroy the document or return it to the sender without making any copies.

Given the lawyer's duties towards his or her own client, notably loyalty[38], transparency[39] and dedication to the client's case[40], we believe that the lawyer – the recipient – should advise his client of the incident and, especially if it may reasonably appear to be a matter of some debate, inform the client of the secrecy or alleged privilege, the nature of the information that is allegedly privileged, and his or her right to address the Court to dispute the alleged privilege, bearing in mind that he or she should not reveal any details of the information in question that he or she may have become aware of. In the same spirit, a lawyer who, based on the circumstances of the case, is largely or fully aware of the protected

[35] *G.(A.)* v. *W.(D.),* REJB 2002-32223 (S.C.). In this case, one of the attorneys, as frequently occurs in such situations, had inadvertently sent to the opposing attorneys documents exchanged with his client; contra: *D.L.* v. *J.G.*, AZ-50141353 (C.S.); it would likely be more appropriate, in disciplinary law, to refer to section 59.2 of the *Professional Code*, reflecting the spirit of sections 63 and 64 of the *Code of Professional Conduct of Lawyers,* the fundamental principle of our justice system, i.e. professional secrecy (see footnotes on pages 2 and 3 of the introduction to this guide), and the lawyer's role as an officer of the court, eventually concluding that a derogatory act had been perpetrated.

[36] For a review of the rules that apply in the United States, based on codes of ethics in effect in various states, studying the obligations of the lawyer as recipient at the pre-notification, notification and post-notification stages, see: "What's yours is ours: Making sense of inadvertent disclosure," (2009) 22 The Georgetown Journal of Legal Ethics, pp. 1095-1113.

[37] *Code of Professional Conduct of Lawyers*, sec. 132.

[38] *Code of Professional Conduct of Lawyers*, sec. 20, 72 sub-par. 1 par. 2° and 134 par. 6.

[39] See *Fortin* v. *Lord*, 2008 QCCDBQ 140.

[40] This is sometimes called "zealous representation"; for more on this subject, see *R.* v. *Neil*, [2002] 3 S.C.R. 631, par. 19 and the *Code of Professional Conduct* of the *Canadian Bar Association,* chapter IX, section 1.

information, should consider whether it would be appropriate for him or her to advise or represent the client who wishes to dispute the alleged privilege.

It would probably be wise for a lawyer whose client's protected information has been inadvertently transmitted to a third party to advise the client of the incident. This obligation would flow first from the fact that the secret belongs to the client and that the lawyer, who holds it in trust, is required to inform the client of any infringement or potential infringement of that secrecy[41]. As noted above, lawyers always have general responsibilities of loyalty and transparency toward their clients, as well as a duty to provide information[42].

Best practices

In cases where the client does give consent, the law of total probability may be useful when communicating confidential information. Based on that principle, information can be communicated without being protected, on the presumption that everything will be all right given the high number of emails in circulation on the Internet at any given moment and the relatively low number of people who are likely to intercept any particular email. This isn't really so far-fetched, but make sure that the client agrees in full knowledge of the risks involved in this practice and the potential consequences. However, even if a client agrees with his or her lawyer to apply the law of total probability in their communications, that does not mean the client has waived the right to professional secrecy.

In such cases, the subject line of the email should state clearly that the contents are of a privileged nature. Wording like "Confidential" or "Protected by professional secrecy" should appear in the subject line of the email, or at the very least at the top of the message.

Confidentiality notices or disclaimers added automatically at the bottom of an email are not useful in any way. First of all, they come after the confidential information in the message, so the inadvertent recipient won't see the notice in time to stop reading. These notices are generally hard to distinguish from the body of the email (even in personal correspondence), which makes them even less useful. No one really reads these notices or takes them seriously.

In most cases, documents containing confidential information should be sent in a password-protected attachment, with the password sent to the recipient by a different mode of communication or in an encrypted message.

Encryption is the ideal form of protection. Using complex mathematical algorithms, encryption substantially changes the contents of a message or the path it follows. This makes the information incomprehensible and indecipherable to all intents and purposes. The only person who can decipher the original message and read it is the recipient who has the right "key" (generally a password). Various encryption software programs are available on the market. As long as they meet current standards (256-bit algorithm, etc.), they are probably good enough to meet the criteria of section 34 of the Act to establish a legal framework for information technology.

Setting up a secure closed network with the client is of course an expensive solution that would only be considered for major clients with whom the volume of correspondence would justify the expense. This

[41] A parallel can certainly be made with the lawyer's obligation to inform a client whose file is the subject of a search warrant (see *Lavallée, Rackel & Heintz* v. *Canada (Attorney General); White, Ottenheimer & Baker* v. *Canada (Attorney General)*; *R.* v. *Fink*, [2002] 3 S.C.R. 209, par. 49), so that the client can decide whether to invoke the protection of professional secrecy.

[42] For an illustrative case, see: *Thibault* v. *Bilodeau*, 2003 CanLII 54678 (QC C.D.B.Q.); *Montbriand* v. *Desmarais*, 2009 CanLII 110 (QC C.D.B.Q.).

would clearly meet the criteria of section 34 of the Act to establish a legal framework for information technology.

Obligation to agree on a mode of transmission with the client and to document that agreement

Under the terms of the second part of section 34, it is not enough to simply protect the confidentiality of the information. In addition, "Documentation explaining the agreed mode of transmission, including the means used to protect the confidentiality of the transmitted document, must be available for production as evidence." This implies the following obligations for lawyers who plan to send confidential information via email:

- Agree with the client on what mode of transmission you intend to use (here, email), as well as how you will ensure confidentiality (e.g. encryption). We recommend that you spell out these details in the mandate confirmation letter;
- Document this agreement (on paper or electronically). The Act stipulates that there needs to be a formal agreement. Using a mandate confirmation letter would fulfill that obligation;
- Keep all documentation for production as evidence. If one day the client were to bring an action against the lawyer for failing to properly protect the confidentiality of information sent by email, the lawyer would want to be able to produce documentation establishing the client's consent to using that mode of communication and stating what protective measures were used to ensure confidentiality.

Exemptions from the obligations of section 34

Section 34 of the Act does not in and of itself impose confidentiality – it simply spells out various requirements for the transmission of documents that contain information deemed confidential under the law. The legal provision that imposes confidentiality may also provide for some exemptions.

In this case, section 9 of the (Quebec) Charter of Human Rights and Freedoms and section 131(2) of the Act respecting the Barreau du Québec stipulate that the lawyer may be relieved, even implicitly, from the obligation to respect professional secrecy regarding the client. The client may give the lawyer permission to use unsecured email for their correspondence, even for information covered by professional secrecy. However, it is preferable, and probably more appropriate, to see this as implicit authorization for using unsecured email rather than a waiver of professional secrecy by the client.

This authorization may be implicit. For example, if the client sends confidential information to the lawyer via unsecured email, it is possible to conclude, according to the circumstances, that this is implicit authorization to proceed in this way. In other words, this would mean waiving the use of protective measures means, such as encryption.

Obviously, either express authorization or a waiver would be preferable, and we recommend including a specific mention of this in the mandate confirmation letter.

Keeping emails

Since emails are documents, it is important to make sure that they are kept and managed in an appropriate manner (see Section 3, Management of electronic documents). Among other things, it's important to make sure that access to electronic documents is protected and is reserved solely for the individuals concerned (see Section 1, Communications security, and the sub-section on Passwords). Emails, like all other forms of correspondence, are part of the lawyer's files, and need to be kept (on paper or electronically) in accordance with the requirements of the Regulation respecting accounting and standards of professional practice of advocates and the Act to establish a legal framework for information technology.

Resources

Management of technology-based documents

- *Know your law: Guide respecting the management of technology-based documents*, Fondation du Barreau du Québec

Forwarding email

- Forwarding email

SECTION 2 PROTECTING ACCESS TO DATA

There are many different methods at many different levels designed to protect access to data. In the Communications security section, we discussed how to protect and configure systems in order to reduce the flow of information to what is really necessary to operate expediently.

Access to data can also be protected by an authentication process that involves, for computer systems, checking that a user really is the person he or she claims to be before granting access to systems or services. It is often said that there are three ways of identifying a person: by what the person knows, is and has[43].

Since passwords are the most commonly used means of authentication, along with encryption, we will discuss these two methods in detail below.

Passwords

Principle

Access to all documents or information of a legal nature used in professional practice should be limited by using a secure password that is changed every 30 days. This protection may also cover the computer equipment and/or software programs you use.

Definition

When a user connects to a computer system, the computer will generally ask for a username and a password to be entered before access is granted. This pairing of username/password is the key step in gaining access to the system.

Risks

Most users, believing they have no real secrets to protect and are not really vulnerable to information theft, will simply use a password they find easy to remember, such as their ID, spouse's first name, or birthday.

With password-generation tools, available on the Web free of charge, anyone can try a huge number of passwords generated by databases or at random or a combination of the two, until they find the password.

[43] Section 41 of the Act to establish a legal framework for information technology.

Every time passwords for accounts of major Web users are compromised, millions of passwords are added to the hackers' dictionaries. They have no problem identifying the most common passwords, the ones they'll test first when they mount their next cyber attack.

The longer the password, the harder it is to find – or "break," in techno-jargon. A password that's all numbers is much easier to break than a password that's all letters, and alphanumeric passwords, containing both numbers and letters, are harder still to break.

For example, a 10-digit password yields 100 million possibilities. That number may seem awfully high, but even a modestly configured computer could break it in just a few seconds. By way of comparison, a 10-letter password would be better because there are 200 billion possibilities. Even that type of password can be broken in a matter of minutes, however[44].

If devices (USB keys, phones, laptops, etc.) are lost or stolen, encryption will protect the information (see next section for further details).

Best practices

Apart from the protection passwords provide from cyber attacks, they also protect access to various systems or resources.

It's important to establish a password policy so users know they must choose a password that's really secure.

Passwords should contain at least 10 alphanumeric characters – in other words, numbers and letters, including upper-case and lower-case letters and special characters.

Passwords to avoid

- Your username
- Your surname
- Your first name or the first name of someone close to you (spouse, child, etc.)
- A word that appears in the dictionary (of any language), or worse yet, a common term like "password"
- A word spelled backwards (password-breaking tools know all about this)
- A word followed by a number, the current year or the year someone was born (e.g. "password 1999")
- The same password for several systems (this increases the risk if one of the systems is compromised)
- Any password used elsewhere, especially on social media.

Most importantly, keep your passwords confidential. If you must write them down, don't leave them lying around where others could see them.

[44] To find out how fast a password can be guessed, based on the degree of complexity (length, makeup, etc.), go to: www.lockdown.co.uk/?pg=combi

Passphrases are replacing passwords

A good system for choosing a password you will remember is to think up a “secret phrase” – for example: “I love the month of September, it’s your birthday, my love!” Turn that into numbers and letters (using the main words) and you have: **ilm09yBml!**

So now you have a password that contains at least 10 alphanumeric characters and does not appear in the dictionary – and you can remember it because it has personal meaning: **ilm09yBml!**

Invent a phrase that means something to you and follow the basic rules for using secure passwords. This type of secret phrase is more secure than an ordinary password because it’s longer, more complex and more unpredictable (which makes it harder to “break”).

Don’t replace a letter or number with a similar character, e.g. 1 and !. Password-cracking tools know all about possible substitutions of similar-looking characters, e.g. 4 and A; I, L and 1; 5 and S; 7 and T, etc.).

Recovering passwords

Many applications and software programs allow you to recover a forgotten password by answering a secret question. The answer you choose for this type of question should not be anything that is easy to find – for example, your spouse’s name, which you have probably mentioned on social media.

Alternatives to passwords

There are more and more tools out there that use biometrics (e.g. digital fingerprints or facial recognition) as a substitute for passwords. This solution does offer an interesting level of security.

Considering multi-factor authentication

Multi-factor authentication is a practice that makes a company system even more secure. We recommend that you install this type of authentication system whenever you can.

For example, an authentication system could require users to connect by entering a validation code (generated on a smartphone, for instance) in addition to their username and password.

1
123456
123456
2

Using a password manager

A password manager is a tool that helps you protect a database of passwords. This can be especially useful if you have many passwords to remember – the password for the database is the only one you have to memorize. These tools may also include a random generator for passwords, which it will remember so you don't have to. Password managers may be a cloud-based service (such as Passwordsafe) or a software program installed on a computer or even a USB key.

Make sure to follow the highest security standards when you choose the password that protects your password manager, since it's the gateway to all your other passwords.

Ethical considerations

Finally, remember that lawyers must comply with the practices discussed above to respect the duty of prudence to the client[45] and to protect professional secrecy[46]. Since it doesn't take long to break a password, it's crucial to replace passwords at least once a month, using a fresh password that hasn't been used over the previous 12 months.

Resources

- Microsoft site on creating strong passwords
- Password meter
- Password strength
- Password generator
- Password manager
- Password recovery speeds
- Password Recovery Toolkit
- How to Make Two-Factor Authentication Work for You

[45] *Code of Professional Conduct of Lawyers*, sec. 20

[46] *Professional Code*, sec. 60.4.

Encryption

Principle

Lawyers should take all reasonable measures to make sure that clients' confidential information cannot be seen or intercepted by unauthorized parties.

Definition

Encryption is a generic term that covers various techniques designed to encrypt or "scramble" messages, i.e. make them impossible to understand unless a specific action has first been taken.

Best practices

Data stored on portable devices, such as USB keys, external hard drives or iPods, can be intercepted (found or stolen), so it should be encrypted. Messages sent by email and data on smartphones should also be encrypted.

Under certain circumstances, encryption not only preserves the confidentiality of data, but also serves as a pledge of its integrity and authenticity.

Generally speaking, the more the information is exposed and/or confidential, the more crucial it is for it to be protected by encryption.

Resources

Encryption software

- Stormshield Endpoint Security (works with Windows XP, Windows Vista, Windows 7)
- PGP - Whole Disk Encryption
- Microsoft Virtual Private Network
- GNU Private Guard
- BitLocker (Microsoft)
- FileVault 2 (for Mac)

Encryption, as seen by some American bar associations:

- Encryption conniption

Security procedures for managing the departure of an employee

1. Temporarily deactivate the user account of the former employee who has left the firm (for two to four weeks) before cancelling the account once and for all.

2. Deactivate the former employee's cell phone account, voicemail and telephone extension.

3. Deactivate access to the VPN (Virtual Private Network).

4. Replace all passwords on accounts the former employee may have been using: website, banking transactions (PayPal), phone system, alarm system code, etc.

5. Archive the former employee's documents, emails, contacts, tasks and calendar.

6. Temporarily redirect the former employee's email address to the supervisor's inbox to collect all correspondence and advise correspondents that the employee has left the firm.

7. Recover all the computer equipment: that belongs to the firm: computer, laptop, tablet.

8. Remove any page or profile for the former employee from the firm's website.

9. If applicable, cancel any rights or privileges the former employee may have had as the administrator of the firm's website or corporate page on social media.

10. If applicable, cancel any administrative rights or privileges the former employee may have had in terms of managing the firm's domain name(s).

When an employee is fired, access should be suspended immediately, unless the employee is continuing to work during the period required by law. In that case, it would still be prudent to limit the employee's access (in writing) until he or she leaves the firm.

Agreements with suppliers

Beyond the world of computers, a lawyer who is looking for a place to deposit professional practice documents will obviously inquire about available security measures. It's impossible to imagine a law firm without walls, doors or locks, open to anyone at any time. Similarly, it's impossible to imagine legal documents without files and filing cabinets to prevent them from being seen by anyone who wanders in seeking information, even strangers. Moreover, a lawyer who retains the services of a supplier to do legal or factual research will of course require that the research remain confidential right from the start.

The same principles apply in a computer-based environment. Lawyers more and more often hire suppliers for various computer services (hosting, Internet access, technical support, communications, etc.). This gives the supplier access to the lawyer's computer data, which is a major problem in terms of the ethical obligations to which the lawyer is subject. Certain measures must be taken to preserve the confidentiality of the information relayed by the supplier, transmitted or made accessible to the supplier, or hosted by the supplier.

These measures include the following:

- A confidentiality agreement[47]must be signed with the supplier to fully protect confidential information. The agreement should spell out conditions for handling, data transfer, the use, storage and availability of the information, as well as access rights and ownership of the data.

- Apart from this confidentiality agreement, the service contract should include provisions covering the end of the contract or cessation of activities (voluntarily or in the event of bankruptcy or the supplier going out of business) and data transfer, and the right to audit or check data.

- Suppliers of computer equipment may have different attitudes to the requirements of their lawyer clients. A technician making repairs may well agree to sign a confidentiality agreement without negotiating the terms, while a computer system installer will want to review the terms in order to avoid any obligations regarding the result, and a supplier of Web search services will impose online conditions that are non-negotiable and provide for the reuse of data downloaded by the user in all the divisions and branches of the firm that offers that service. It is extremely important for lawyers to be vigilant, while negotiating or deciding whether to accept these agreements, that their ethical obligations be respected. In particular, when it comes to data hosting services, lawyers should check the service contract to make sure that everything is in compliance with their ethical obligations. After all, in most cases this is where the files will be stored.

- Watch out for membership contracts – ask yourself whether the confidentiality agreement meets your ethical obligations.

[47] Sec. 26, *Act to establish a legal framework for information technology.*

Cloud computing

Principle

Lawyers need to take all reasonable measures to make sure that confidential information that transits the cloud or is hosted there cannot be seen or intercepted by any unauthorized parties.

Definition

Cloud computing is an Internet-based type of computing "[…] that relies on sharing computing resources rather than having local servers or personal devices to handle applications. The goal of cloud computing is to apply traditional supercomputing, or high-performance computing power, normally used by military and research facilities, to perform tens of trillions of computations per second, in consumer-oriented applications such as financial portfolios…"[48] Cloud computing is a service, in constant evolution, dynamically adaptable and billed per use. There are various models (private internal, private external, public, community and hybrid) and service models (software as a service, platform as a service, infrastructure as a service, etc.), each with its own advantages and disadvantages.

Cloud storage models:

- **Private (internal) cloud storage:** The requested resources are installed within the client organization (e.g. client has its own servers)
- **Private (external) cloud storage:** Resources are managed outside the client organization, but in a cloud that is reserved for the client (e.g. hosting contract)
- **Public cloud storage:** Resources are offered publicly by a company (e.g. iCloud, Gmail, Google Docs, Dropbox, Outlook, Hotmail, Yahoo Mail, Microsoft Office 365, etc.)
- **Community cloud storage:** Similar to the private model; used to meet the needs of organizations that prefer to pool their resources. (The governments of Australia and the U.K. use this type of model.)
- **Hybrid cloud storage:** Generally involves a combination of two or more models (private, public and/or community) of cloud storage, depending on the specific needs of the organization.

[48] http://www.webopedia.com/quick_ref/cloud_computing_terms.asp

Service models:

- ***Software as a service* or SaaS:** Ready-to-use software, rented on demand from a supplier, accessible via the Internet (public cloud) or the organization's network (private cloud), or both at the same time (hybrid cloud). Example: Google docs.

- ***Platform as a service* or PaaS**: Ready-to-use platform, rented on demand from a supplier, accessible via the Internet (public cloud) or the organization's network (private cloud), or both at the same time (hybrid cloud). PaaS gives developers an environment for execution (operating system, equipment, network) where they can install or create their own software. Example: Facebook development tools.

- ***Infrastructure as a service* or Iaas**: Ready-to-use infrastructure, rented on demand from a supplier, accessible via the Internet, the organization's network, or both at the same time. Example: Microsoft Azure

Note: Here are three sites with definitions for technical terms related to cloud computing and other aspects of computer security. If there are any terms you're not familiar with, look them up here:

www.techterms.com

www.netlingo.com

www.computerhope.com

Examples

The types of cloud computing services most commonly used by lawyers nowadays are free Web email services like Gmail or Hotmail and free storage or file-sharing services like Dropbox or iCloud. (For a table that compares various local online storage and file-sharing services, go to: http://en.wikipedia.org/wiki/Comparison_of_file_hosting_services.)

These services store documents in the cloud so that they can be accessed from any workstation, even a tablet or smartphone (for those who have the necessary permission). However, we do not recommend the use of this type of free service, for the reasons given in the section on risks above.

As a lawyer, you must take all reasonable measures to ensure the security of your clients' information and perform your own background checks when selecting your suppliers. Have a look at the cloud computing checklist in the appendix for some suggestions.

Risks

Despite its clear advantages (especially in terms of cost and accessibility), cloud computing has some major disadvantages due to risks to the security of data hosted in or passing through the cloud. First of all, when it comes to the availability of the data, it is possible for information hosted in the cloud to become inaccessible when the servers themselves become unavailable (black-outs, maintenance, etc.).

However, that risk is generally inversely proportional to the size of the cloud, as the largest clouds will have redundancy measures in place to handle these situations.

A more important problem relates to data becoming inaccessible when it is “taken hostage” by the cloud computing supplier – for example, because the hosting fees have not been paid. It is also important to pay attention to the question of disposal of data in order to avoid ownership of data being transferred to the hosting company, either when the contract is signed, in the event of non-payment, or simply at the end of the contract. Finally, it’s important to take a close look at the time limits for data being returned at the end of the contract.

Although data appropriation clauses are rare, many cloud computer service providers (primarily “free” services) have an operating licence for hosted data, so there is a risk to the confidentiality of the data, notably in terms of data protected by professional secrecy. That risk is further aggravated by the fact that data located “in the cloud” is actually on a server, which may be located outside Quebec, in jurisdictions that do not have the same warranties for the protection of confidential data and lawyer-client privilege. For example, in the U.S., where most cloud computer services are controlled, it is possible for the state to gain access to data hosted in the cloud despite clients’ rights. Lawyer-client privilege is not actually a right accorded the same protections as in Canada, and in certain cases, this type of data has been subject to a search.

Finally, like any other service that is accessible over the Internet, cloud computer services are vulnerable to attempted access by unauthorized parties, notably if a user’s account is not protected by a sufficiently sophisticated password.

Best practices

Lawyers who wish to store confidential data in the cloud – notably data covered by professional secrecy – should give preference to clouds that consist of servers located only on Canadian soil and under the control of Canadian entities.

If such an option appears not to be available, given, for example, the desired cloud computing model, encryption of data at source is strongly recommended. Note that the documents prepared by the U.S. government and made public by Edward Snowden indicate that certain American cloud computing service providers would give encryption keys to the authorities. So it would be preferable to use a different encryption system than the system offered by the cloud storage service, although some press releases also made public by Snowden suggest that the practice is not risk-free for the same reasons (the U.S. government is able to gain access to keys). We are of the opinion that no matter what security measures are in place, hosting in another country is extremely risky from an ethical viewpoint.

It would be more prudent to adopt a solution proposed by a recognized company and avoid using entry-level services or so-called “trials,” which generally offer the attraction of free storage space (often in exchange for operating license for hosted data). It’s often best to choose paid solutions that offer warranties to protect confidential data to fulfill your ethical obligations.

As for access to data, it’s crucial to follow the advice in this guide on the use of passwords and encryption of data.

In any event, it’s important to inform clients of risks related to the chosen cloud storage model and obtain their approval, since this model cannot guarantee the protection of confidential information, including personal information and data covered by professional secrecy. As soon as client data is hosted anywhere else but the office or is replicated externally, it is preferable to inform the client.

Finally, we strongly recommend keeping a backup copy of all information hosted in the cloud to make sure that the information will still be available in the event of a power failure or a difference of opinion with the cloud storage service provider.

Resources

Jean-François DE RICO, "L'infonuagique, la protection des renseignements personnels et les droits d'accès des gouvernements," (2014) nº 6 *Technologies de l'information en bref*.

Nicolas VERMEYS, Julie M. GAUTHIER and Sarit MIZRAHI, "Étude sur les incidences juridiques de l'utilisation de l'infonuagique par le gouvernement du Québec," a study presented to the Quebec Treasury Board, 2014, available online: http://www.cyberjustice.ca/publications/etude-sur-les-incidences-juridiques-de-lutilisation-de-linfonuagique-pour-le-gouvernement-du-quebec/

Interesting articles on the subject

- Guide de l'infonuagique, Volume 3 — Considérations de contrôle et de sécurité, Architecture d'entreprise gouvernementale 3.0
- Microsoft Cloud to touch down in Canada
- HIPAA-Compliant Cloud File Services
- Comparison of file hosting services
- Cloud Storage and Client Confidentiality: A Perfect Match or Perfect Storm?
- Best Free Encryption Utility for Cloud Storage
- Top 6 Free Encryption Tools to Protect Your Data Stored in the Cloud.

Legal opinions on cloud computing from various Bar associations

- Cloud Ethics Opinions Around the U.S.

Keeping offices, rooms and equipment secure

1. Lock all doors.

2. Lock all filing cabinets.

3. Make sure that the server(s) are installed in a well ventilated, locked environment, connected to an uninterruptible power supply (UPS), at a consistent temperature of 15º C to 20º C.

4. Turn off workstations or activate the secure login screen.

5. Keep all media that contain confidential data (CD-ROMs, DVDs, external hard drives, USB keys, backup cassettes, etc.) in a protected, locked facility.

6. Encrypt confidential data on laptops and portable devices (CD-ROMs, DVDs, external hard drives, USB keys, etc.)

7. Activate the security feature on personal agendas or smartphones by setting up an unlock code (login screen with password) and encrypting the information.

Disposing of or recycling computer equipment

Servers, computers and laptops

- Delete data from hard drives by making several passes of a script (for further details, contact your technical consultant or get software that meets Canadian standard CSEC (ITSG-06)

  OR

- Destroy them physically in a shredder (for further details, contact your technical consultant or a company that specializes in information destruction and is internationally certified (National Association for Information Destruction or NAID)

Smartphones

1. Reset the phone by selecting the option to delete all data.

2. Remove the memory card or delete the information on the card.

Photocopiers and imaging equipment

1. Clear the memory on your photocopier or imaging device. These devices use a hard drive connected to the office network, which means it is accessible via the Internet.

Eco-tip

Companies that recycle old computers

There are two types of computer recycling companies: companies that recycle parts to distribute equipment to those who really need it (Third World countries, poor areas of town, spare parts) and companies that recycle the raw materials (plastic, lead, silicone). In both cases, it is better by far to have your old computers, printers and screens wind up on their shelves than in the garbage. However, you still need to follow the procedure detailed here before you hand over your computer equipment for recycling.

Here are a few recycling companies you can contact:

- RecyPro
- Reboot Canada
- MultiRecycle
- Insertech

Check this directory to find **an official drop-off point near you:**

- EPRA

SECTION 3 MANAGEMENT OF ELECTRONIC DOCUMENTS

It's hard to imagine how we could manage paper documents efficiently without using staples, file folders, filing cabinets and so on. Similarly, electronic documents need to be managed in their own way. Let's look at how to file and back up electronic documents, as well as the "metadata" that makes it possible to manage documents more precisely.

Filing documents

Principle

It's important to categorize electronic files containing documents that are part of a lawyer's files properly in order to save time, avoid the loss of documents, and make it easier to comply with the rules that govern how lawyers should keep their files and be able to show that they are properly kept.

Definition

Electronic documents created by a lawyer are saved in files. The lawyer decides what name to give each file. Files can be organized into directories and sub-directories (or "e-files") so that they can easily be found and are accessible in the same way as print documents.

Example

When an electronic document is saved for the first time, the software program generally prompts the lawyer to enter the name of the electronic file in which the document should be stored.

The lawyer can choose the directory or sub-directory in which to store the file, and can create as many directories and sub-directories as necessary to organize documents in a useful way.

Usefulness

File names

For the sake of efficiency, it makes sense to use a file name that describes the content, which will mean classifying the various elements in a file by their nature, as provided for in the rules on the keeping of files. The objective is for everything in the file – letters, decisions, procedures – to be easy to find quickly and efficiently.

A convention for naming documents should be set up to standardize presentation and facilitate searches. For instance, one such convention might include the following key elements in all file names:

Date of document_subject_name of author_ version number
2016-04-13_Ltr file_Me X_V1

Directories

It would be a good idea for lawyers to create electronic files the same way paper files used to be created – one file for each mandate the lawyer is working on.

Risks

It is perfectly possible for files to get lost on your computer! When there's a high volume of files of various kinds on a computer, it's relatively easy to lose a file if it isn't named, filed or indexed in a logical way or if it's been misfiled.

Another risk related to poor document organization involves managing access rights to the documents (see section on protecting access to data).

Best practices

When the professional inspection team visits members of the Barreau, they often remind lawyers that paper documents should ideally be organized in files in such a way that:

- correspondence is arranged in chronological order;
- procedural documents are also arranged in chronological order;
- notes in the file and research notes are kept separately; and
- a client information sheet, including information on the client, the file, and a list of important dates in the file, is included.

We recommend setting up a system with separate computer sub-directories for each client, or for each file if the client has given the lawyer several mandates. For example, set up a file called "Joe Blow" and a sub-directory called "Mandate 3."

A logical path and meaningful file name that describe the contents will generally save a lot of time spent searching for documents – leaving more time to work on the file.

We also suggest starting each document name with the date. That way, documents will automatically appear on the screen in chronological order, making searching much easier.

It is possible to improve document management and make it even more efficient. The file name, directory name and date on which the file was opened organize documents to some extent, and it's possible to add more information about the documents to make them easier to classify based on various criteria. The more sophisticated documentary software management programs use metadata from documents to refine searching and indexing, so it's possible to indicate which lawyers have worked on a file, when the file was closed, keywords, contact information for people in charge, or any other relevant information. This metadata can be captured in the same window. For example, in MS Word 2003 and more recent versions, when you look at document properties (File/Properties menu), you can access the metadata and fill in various fields.

Depending on the software used, email correspondence can be aggregated in a unique database. In that case, we suggest creating a directory in the messaging software with the name of the file in question. When the file is closed, the emails can be archived and exported, so they will all be in a single separate file that can be placed in the “physical” directory for the file.

Backup copies of documents/ Recovery plan

Principle

In addition to the file saving that is normally done so a file does not get lost when the document or software program is closed, a backup copy of all files should be made every day on a separate medium that is kept in another place so it can be recovered in case of a disaster. Backup copies should be tested on a regular basis.

Definition

Backup is an operation that involves duplicating the data in a computer system and storing it in a safe place.

This is related to two other concepts:

- Data registry, which is the operation of writing data on an information storage device, such as a hard drive, USB key, magnetic tape, etc.
- Archiving, which means registering data on a device for legal or historical purposes.

Data registry necessarily comes before making a backup, but is not really intended to be an archiving procedure. In fact, backup copies should never be used as an archiving or conservation mechanism.

Example

In the past, the *Journal du Barreau* would occasionally issue a call for colleagues to help recover files destroyed in a fire. As long as there is a backup copy, electronic documents that are destroyed can be replaced promptly with a copy that the lawyer has kept elsewhere, for example at his or her home. In this case, note that the copy of the files is subject to the same rules regarding professional secrecy. Information storage devices kept at home may, for example, be encrypted to fulfill these requirements.

Usefulness

Backup copies are most useful in helping to restore a computer system after an incident has occurred (breakdown or loss of a storage device like a hard drive, or of some or all of the data the device contains).

Backup copies may also be useful if there is a threat of ransomware, a type of malware that lets a hacker block access to data, lock a computer or encrypt data. The victim is “invited” to pay the hacker a sum of money before regaining access to the data.

Risks

Even the most advanced technology can just stop working. Even a properly protected access system can be targeted for invasion. A computer can even be stolen from a locked office, and office buildings can burn down or suffer water damage or some other disaster.

So it’s extremely important to make regular backups of your computer files, which can be used to keep your business going. The backup copy should be kept in a safe place away from the office. The most frequent problems are technical glitches with the computer you use every day, viruses, or the loss or theft of a device that contains electronic files.

Best practices

Before designing a backup system to be used by your firm, there are several questions you need to answer:

- What backup medium should we use?
- What should we back up, and when?
- How can we make sure we’re backing up our data in the best possible way?

What backup medium should we use?

Here are several solutions for backing up your data:

External hard drive

It is certainly inexpensive and practical to use an external hard drive. These devices can store large quantities of data, and some models can even be set to perform automatic backups.

USB key

USB keys are affordable and very portable, but the main disadvantage is their limited storage capacity. They are also fragile and easy to lose. For all of these reasons, they should not really be considered reliable backup devices.

Online backup

Websites that offer online data backup can be an interesting solution because the procedure is automatic and requires no intervention by the user. However, it’s important to deal with a data hosting site located in Quebec or elsewhere in Canada to avoid confidentiality problems, such as those people have encountered under the Patriot Act in the U.S. We recommend that you sign a confidentiality agreement with the supplier to make sure your confidential information is properly protected. For further details, see the section on cloud computing.

What should we back up?

The simplest method is a full backup, which means copying all the data you want to back up – recent, old, with or without changes, plus files, systems and software.

On the other hand, this method takes quite a lot of time and disk space. To save time, you may decide to do a differential backup every day of data only. A differential backup copies all the files that have been created or modified since the last complete backup.

These backups can be performed on a relatively inexpensive external hard drive. Some of these devices contain software that automatically performs a differential backup.

For data backup, we recommend using a single directory. This will make backup quite straightforward, since the program files will not be backed up during the process.

It’s a good idea to perform a full backup of data, including programs, every month or so.

How can we make sure we’re backing up our data in the best possible way?

However you choose to back up your data, you need to:

- keep the data in a different place, i.e. not the original location (don’t keep your external hard drive permanently plugged into your computer, for instance);
- use multiple backup tools, following the LOCKSS principle: *Lots of copies keep stuff safe*;
- automate backups to be performed every day;
- make sure data is encrypted.

Here is an example of how to set up automatic backups from your computer to an external hard drive and make sure your data is encrypted:

- Windows: Launch > Configuration panel > BitLocker Configuration Assistant (encryption tool included in Windows 7 Pro Edition Enterprise and Ultimate, Windows 8.1 Pro and Windows 10 Pro), then follow the steps in the Assistant. Once BitLocker is activated on the computer, just encrypt the device that contains the backup copy. If your version of Windows does not include BitLocker, you can always use another encryption software program to protect the device that contains the backup copy (see encryption section).

- Mac: From the Applications menu, choose Time Machine and slide the cursor to activate. On the left side of the Disk utility window, select the disk you would like to use for Time Machine. Choose the “Encrypt backup disk” option to encrypt your Time Machine external hard drive using FileVault 2 (OS X Lion or later version).

Metadata

Principle

Lawyers who have yet to fully master the concept of metadata should take the precaution of deleting metadata from documents sent electronically to the opposing party or anyone else, unless the documents are to be used as evidence, in which case they must remain integral documents.

Definition

"Metadata describes other data. It provides information about a certain item's content…." www.techterms.com

In other words, metadata is information relating to the context of a document. Metadata is generally embedded in electronic data and is not visible until you look at the document properties, or unless you use special software.

Example

People know about metadata but don't know they know it, since it's used every day in many software programs. For example, in Microsoft Outlook, the following fields constitute metadata: "from," "to," "cc," bcc," date sent," "date received," and even the subject line for each email. In addition, an email message generally contains a lot of information that traces the path from sender to recipient through every server.

Another example is Microsoft Word, which can show metadata using Document Properties (Office 2003 and previous versions: File > Properties; Office 2007: Office button > Prepare > Properties; Office 2013: File > Properties in column on the right). Most fields that can be found under each tab constitute metadata. The data registry date does not appear in the text, but may be used by a software program to identify the most recent version of the text.

Usefulness

The main purpose of metadata is to automate various information processing functions, such as organization, searching and categorization. Some of this information is defined and entered automatically, while other metadata may be added by the user or by information management systems when documents are registered. Some metadata tracks the history of a document, which is necessary when the time comes to demonstrate that the document has remained in its integral state.

Risks

For lawyers and for the administration of justice, metadata creates major risks that lawyers must be aware of. In fact, metadata can include confidential information, some of which is covered by professional secrecy.

For example, lawyers frequently generate documents (e.g. contracts, procedures, etc.) and forward the documents by email, asking for feedback from the client. The documents are then returned to the lawyer with certain changes, comments or annotations shown using Track Changes[49]. This type of information is frequently covered by professional secrecy or litigation privilege. After simply “hiding” the changes, the documents are often forwarded as is to the opposing party, attorneys or other parties. The other party need only have very basic technical knowledge to call up the changes, comments or annotations and see what they are.

Best practices

There are two main ways of eliminating this information – and thus eliminating the associated risks: A) using certain tools to delete the information or B) converting the file to a standard PDF.

A. Microsoft is aware of the risks and has developed a tool for inspecting and eliminating metadata, which is a default setting in Office 2007 (Office button > Prepare > Inspect document). This tool can be used to eliminate all sorts of metadata as well as other information that may be confidential.

B. With various software programs (see resource section), you can print[50] documents in PDF format. This procedures delete information that could be confidential by turning a modifiable document into a static document (i.e. one that cannot be changed).

Ethics and code of conduct

It is not only legitimate but helpful for a lawyer to be aware of metadata in documents from clients. In addition, insofar as information that cold be potentially covered by professional secrecy is identified, the lawyer needs to inform the attorney for the opposing party. It would be negligent to rely on this principle to avoid deleting metadata from documents because it could fall into the hands of other parties who do not have the ethical obligations incumbent on lawyers. We refer readers to the section on the accidental receipt of information that could possibly be protected by professional secrecy.

Resources

Explanations of metadata

- Wikipedia

Metadata inspection and deletion tools

- Microsoft

[49] N.B. Technically, tracked changes, comments, etc. do not constitute metadata; we consider them metadata here for the sake of simplicity. For further details, see the resource section.

[50] Important note: Make sure you print in PDF format, not “save as,” which certain software programs allow you to do, including Microsoft Office since the 2007 edition and Adobe Acrobat, because saving a document this way does not get rid of metadata.

- Scrubber

PDF conversion tools

- CutePDF
- PrimoPDF

Legal opinions from various bar associations on metadata

- Metadata Ethics Opinions Around the U.S.
- Legal Ethics in a Digital World (CBA Ethics and Professional Responsibility Committee)

Horror stories about metadata

- Metadatarisk.org: Content Security in the news
- Shauna Kelly: How tracked changes have made businesses and government look foolish

Monitoring and managing the computer park/Managing alerts

Principle

All computer systems should be monitored to identify, diagnose and solve technical problems before they jeopardize the security of data and the system itself.

Definition

Monitoring means the process of setting up, configuring and following up on alerts. The alerts generated by your system serve as a warning and provide an opportunity to react when a potential or real risk appears.

Usefulness

Software programs and telemonitoring services analyze responses from systems and equipment based on given parameters. These systems may, for example, be the server where the website is housed, Internet access, backup copies, etc. The responses are compared to the standards.

When system responses do not comply with the standards, alerts are generated.

The alerts may take different forms:

- messages at the bottom of the screen or when a software program opens;
- email alerts;
- warnings;
- etc.

Even if a situation does not comply with the standards and an alert is generated, that does not automatically mean that the equipment or service is defective. This is what we call "false positives."

So alerts must be managed to distinguish false positives, in other words minor alerts to keep an eye on (e.g. an alert that says a backup has not been completed when only two files have not been copied) and major alerts (e.g. about to run out of disk space, which could make the main server inoperable).

Risks

Ignore alerts at your peril. You may be tempted to deactivate alerts, but don't do it unless the alert has been confirmed as a false positive.

Here are the elements in the computer environment that should be monitored (notably in case of an electrical failure):

1. main server
2. router, firewall or access to the Internet
3. backup completion
4. antivirus

Ethics and professional conduct

Lawyers are expected to comply with the proposed practices to ensure the security of client files and protect their integrity.

Lexicon

There are many websites where you can look up detailed definitions of technical terms. We suggest that you consult the following sites, as well as Wikipedia:

www.techterms.com

www.netlingo.com

www.computerhope.com

Access management

Access management involves checking whether an entity (e.g. a person or a computer) who is requesting access to a resource is duly authorized to do so.

Antispam software

Software that uses predetermined filtering guidelines to analyze the content of emails, detect spam and move it automatically into a specific file or delete it on the email server.

Antivirus software

Security software that analyzes files and the computer memory, automatically or by request, to prevent parasite invasions or to detect and eradicate any viruses in a computer system.

Archiving (electronic)

Storage of data that must be preserved so that they can be used at a later time.

Backup

Transferring information held in memory onto a separate support medium in order to protect the information or ensure that it is secure.

Beta

A pre-release version of software that may contain bugs. Beta software is distributed to certain potential users for testing and evaluation purposes, to assess how the product works, look for programming errors, etc.

Bluetooth

Bluetooth is a standard for the short-range wireless interconnection of computers, printers, digitizers, mobile phones, keyboards, mice, personal digital assistants, speakers, hands-free microphones, etc.

BYOD (Bring Your Own Device)

An expression used to describe the way an employer allows or requires employees to use their personal electronic equipment at work.

Cloud computing

An Internet-based model that relies on interconnected remote servers, providing network access on request to a shared pool of configurable, externalized and non-locatable computer resources. Cloud computing is a service, in constant evolution, dynamically adaptable and billed per use.

Computer network

A computer network is made up of computers and peripherals, such as printers, digitizers, servers, switches, routers and modems, connected wirelessly or not via computer equipment and software.

Computer security policy

A document that sets guidelines for access to the computer network and for data flow, authorized or not, stipulating what is not allowed (e.g. visiting porn sites, using office printers for personal purposes), providing for the application of the policy and presenting part of the basic architecture of the network security environment.

Directory (sub-directory)

A table that gives the name, location, size and date of creation and revision for every file in mass storage.

Encryption/ cryptography

Cryptography is a generic term for all the techniques used to encrypt messages, i.e. make them impossible to understand without a specific action first being taken. It also makes it possible to authenticate messages, e.g. digital signatures. The preferred verb form is to encrypt.

File

A file is a mass of information that has been given a name and is kept in memory, generally in mass memory, such as a hard drive.

Firewall

A firewall is an element in a computer network, software and/or equipment that makes the network secure by allowing or denying access to certain websites or functions. The objective is to provide a secure connection and control data flow between different secure zones to let data through while following established security rules. For example, the Internet is a low security zone, and the company’s local network is a high security zone.

Malware

Malicious software is developed with the aim of harming computer systems. The best known forms of malware are viruses and worms, but there are many others.

Modem

A combined device for modulation and demodulation, for example, between the digital data of a computer and the analog signal of a telephone line.

Networking

Networking covers all the techniques related to setting up, maintaining and using a computer network.

Operating system

Often known by the initials OS, this is a global term for the central programs in a computer that serve as interface between the equipment and software applications; Windows, Linux, MAC and OS are all operating systems.

Portable device

A medium that is easy to carry (e.g. USB key, external hard drive, iPod, etc.).

Router

A router is an intermediary device in a computer network that directs traffic (data). Its function is to move data from a network interface (e.g. the company's internal network) to another interface (e.g. the Internet).

Server

A computer whose role is to answer requests transmitted by users who are networked on the server so that they can share computer resources.

Session (active/inactive)

An active session is when a computer device is communicating and performing operations to serve a user, software or another device. An inactive session is when the device is in a period of inactivity (on standby) determined by the user.

Smartphone

A smartphone is a mobile telephone that also performs the tasks of a personal digital assistant. It may also perform other functions, such as keeping an agenda or calendar, Web browsing, searching, email, instant messaging, etc. The best known smartphones use the iPhone OS, Android and BlackBerry platforms.

Switch

Network equipment that interconnects computer equipment in a local network.

Drafting and updating of the *IT Guide*

Last update: January 2016

This update of the ***IT Guide*** was made possible through the generous cooperation of members of the information technology security committee:

- M^{e} Jean L. Beauchamp
- M^{e} Jean-François De Rico
- M^{e} Maxime Fournier
- M^{e} Annick Gariépy
- M^{e} Patrick Gingras
- M^{e} Dominic Jaar, Ad. E., committee chair
- M^{e} Geneviève Lefebvre
- M^{e} Éric Lestage
- M^{e} Jean-Michel Montbriand
- M^{e} Dyane Perreault
- M^{e} François Senécal
- M^{e} Michel A. Solis
- M^{e} Benoît Trotier
- M^{e} Nicolas Vermeys
- Mr. Patrick Vicente

Appendix

Cloud computing checklist

Lawyers need to take all reasonable measures to make sure that confidential information that transits the cloud or is hosted there cannot be consulted or intercepted by any unauthorized parties. This document is intended to be used in conjunction with the IT guide, to help lawyers who want to make cloud computing part of their practice maintain high security levels.

Before you make the leap to having your data hosted or using applications that involve cloud computing, here are some important things you should know:

1. If the data you intend to send to the cloud is of a **sensitive nature**, your security requirements should be higher and the warranties provided by your supplier should be broader (for example, if your files have to do with intellectual property, national or international interest, etc.).
2. Make sure that your **liability insurance** provides sufficient coverage, i.e. that it covers damages to you and your clients for anything that could result from using cloud computing.
3. Make sure that applications (e.g. management or accounting software) in the cloud **are fully integrated** with the other systems used in your office.
4. Fill in the **checklist** (starting on page 2) with the supplier you are considering and keep the information for future reference. When negotiating with your cloud computer supplier, be just as rigorous as you are with your clients.

Once in the cloud, make sure that cloud computing is fully integrated with your management practices:

1. Always obtain **authorization in writing** from your clients (e.g. as part of your mandate) before storing their information in the cloud, and find out whether there are any particular legislative or contractual obligations that require additional precautions to be taken or prevent you from transferring information to the cloud.
2. Establish **policies for the use of cloud computing** for users in your firm and train users so that they know how to manage your data in the cloud.
3. For additional security, **encrypt your data** before sending it to the cloud so you have a higher level of protection in addition to the encryption performed by your supplier.
4. Inform any lawyer who has agreed to be your **transferee,** as per section 78 of the *Regulation respecting accounting and standards of professional practice of advocates*, of **transfer procedures** to give your transferee access to your data or applications in the cloud.

Evaluation grid for suppliers

While cloud computing has many advantages, this tool was only developed rather recently. As with many other new products and services, suppliers tend to impose conditions that limit their risks and responsibilities. You may have to be insistent with a supplier to obtain more favourable conditions than those that were initially offered. This can be difficult, but certain clauses can always be negotiated. Before you sign a contract with a supplier, make sure he or she is able to provide certain warranties that will enable you to fulfill your ethical obligations as well as protecting you in case of data loss or violation or termination of the contract. If the supplier cannot meet your requirements, at least you will have a better idea of the potential risks and of steps you can take to attenuate those risks. For example, once you are aware of the supplier's limited liability, you may have to save a copy on your local server, decide not to transfer certain sensitive documents to the cloud, or take additional measures (e.g. encryption) to ensure that your clients' confidential data remains secure.

Additional advice:

- Find out about the supplier's track record in terms of financial health and how the company has performed over time.
- Ask about total internal costs (equipment, software and accessory costs) associated with your move to the cloud computing service and analyze how the change could affect your administrative costs and bandwidth charges.
- Find out how much the supplier charges up front and on a monthly basis, how often the supplier can raise those charges while the contract is in effect, and what the ceiling is on such increases.
- Ask about the limits to the supplier's liability insurance.

DATA SECURITY
1. The supplier is a Canadian company held by Canadian interests.
2. All data, including backup copies, will remain in Canada at all times.
3. The supplier will inform the lawyer if hosting or backup of data is subcontracted to other suppliers (cloud to cloud). Subcontractors will be held to the same obligations as the principal supplier, who remains responsible for subcontractors at all times.
4. Data will be encrypted, both during transmission and at the storage site.
5. The supplier will immediately notify the lawyer of any breach in security.
6. The supplier will produce regular audit reports conducted by independent and reputable experts (e.g. with SOC 2 certification) and send the reports to the lawyer immediately.
ACCESS/ OWNERSHIP OF DATA
7. The lawyer and his/her clients remain the sole owners of data stored in the cloud.
8. The lawyer will be able to access his/her data at all times, 24 hours a day, 7 days a week (the industry standard being about 10 hours of maintenance/down time per year).
9. The supplier is equipped with an appropriate authentication and access monitoring system and keeps a register for access to information stored in the cloud.

10. The supplier’s access to the data is limited and the supplier can make only restricted use of the data. In addition, the supplier undertakes to maintain the confidentiality of information the lawyer has entrusted to the supplier.

11. The supplier will inform the lawyer of any request for access by another party to the stored information, and the lawyer will have a reasonable period of time to react.

12. The supplier cannot prevent the lawyer from having access to his or her data in the event of failure to pay charges or for any other reason.

13. In the event of data loss or cessation of activities, the supplier will give the lawyer easy and swift access to the data, and the lawyer will be able to import the data in a format that he or she is able to read and use.

14. The supplier will indemnify the lawyer in the event of data loss resulting from the use of the supplier’s service. The supplier holds sufficient liability insurance and agrees to provide the lawyer with a copy of the insurance policy.

15. The supplier will give the lawyer the support required to cooperate with inspections and investigations by the Barreau du Québec, notably to allow access to all files required by the professional order.

CONTRACT, CHANGES AND TERMINATION

16. The lawyer may terminate the contract at any time.

17. No changes can be made to the conditions for the duration of the contract unless notice in writing is sent to the lawyer prior to making such changes. This notice will be sent within a reasonable period of time so that the lawyer can refuse the changes or terminate the contract without any penalties or compensation.

18. The lawyer’s data will remain available when the service ends and the supplier warrants that he or she will offer transitional support so that the lawyer can recover his or her data. Within a reasonable period of time after the end of the contract, the lawyer’s data will be destroyed and the supplier will produce confirmation that this has been done.

19. In the event of termination of activities, the supplier will give the lawyer access to the source code (by escrow agreement or another form of agreement) so that the data can be transferred to another supplier.

20. In the event of conflict, mediation or arbitration will be the preferred methods of resolution. The contract is governed and interpreted according to the laws in effect in the province of Quebec, and the Quebec courts will have sole jurisdiction in the event of a dispute.

guideTI.barreau.qc.ca

Maison du Barreau

445 Boulevard Saint-Laurent
Montréal, Québec H2Y 3T8

Phone 514 954-3411
Toll-free 1 844 954-3411

infobarreau@barreau.qc.ca
www.barreau.qc.ca

Barreau du Québec