Security advice from the Technology Committee – May 2013

The Technology Committee has reviewed and updated all documents in relation to its advice on computer security which is outlined in the Technology Committee Security Advice document. All previous documents have either been replaced and/or updated and links to these are in the revised edition. Computer security is becoming more important for the legal practice, particularly as the profession is now doing significant business over the internet. It is important for Solicitors to be familiar with computer security and apply the appropriate measures to secure their systems.

Physical Security

Your computer needs to be protected against damage, loss and theft.

Physical security is an underestimated and often overlooked aspect of securing your computer and its data. Physical safeguards protect information assets from a variety of threats, including damage, loss, and theft. From power surges to unauthorized visitors, be aware of the possible physical threats against your information and equipment, and plan to protect yourself from them.

It is important to lock a computer workstation with a password protected screen saver when a computer is left unattended during the day. It is desirable also to use a password-protected screen saver that activates after say 20 minutes of inactivity.

When you leave for the day, close all files and applications and log off (but remembering to leave on the server or computer, as the case may be, so it can be properly backed up automatically at night.

If using a laptop secure it with a lock and use an inconspicuous case when travelling.

If you have written down any passwords store them in a secure location, out of view from others. Never attach passwords onto your computer or other exposed surface.

Keep disks, CDs or DVDs containing sensitive information in locked drawers.

Passwords & Access

Passwords are the first line of defence against a cyber attack. A password should be a combination of upper and lowercase letters numbers and characters and should never be simply a word that can be found in a dictionary. It is recommended that you use different passwords for different sites.

If a password is eight characters or less, attackers can easily break it. They have tools and look-up tables to crack short or commonly used passwords. You can check online for a Microsoft password security checker aid here.

Never share your user IDs and passwords with anyone and do not allow anyone to use your computer or leave it unattended for any period of time while logged on.

Issues arise when a staff member leaves. The firm's policy and procedure should include immediate revocation of network user rights. The user password on that account should be changed but the account should be kept for administration access in case needed. There should be a review of all documents on that account and a review of documents which might have been saved on the local PC. The firm should ensure that anything relevant is assigned to the appropriate client files. A firm should also keep under review for exposure of the firm under other electronic headings e.g. social media use, personal emails to office address, browsing history etc.

The firm administrator should retain access to all accounts on the network at all times and conduct a periodic audit as to the use of the equipment and software. Checks should be conducted to ensure that the software legally belong to firm and not to any employee.

Firms should remember to make use of password protection apps for smartphones. Most have some encryption and it must be better to have that minimum instead of just adding passwords to the phone contacts list.

Windows & MS Office Updates should be set to automatically download and install critical updates and Windows should be configured so as to show all file extensions.

Setting up Windows Update is simple: just go to the Microsoft Download centre.

If you have already automatic updating turned on, Windows Update in Control Panel will open and show your update status. If it is not yet turned to automatic you will be guided through the steps to do so. After that, all the latest security and performance improvements will be installed on your PC quickly and reliably.

When you turn on automatic updating, most updates will download and install without you having to do anything. But sometimes Windows Update will need your input during an installation. In this case, you will see an alert in the notification area at the far right of the taskbar—be sure to click it. If you don't respond to a Windows Update alert, your PC might be missing an important download.

If you operate a server then you can configure Windows Update so that updates are downloaded once to the server and are then deployed automatically from the server.

It is recommended that you use automatic updating if you do not have the expertise or resources to review updates manually. If automatic updating is not in place then it is critical that you check for updates at frequent intervals. Some providers of computer maintenance services will remotely monitor and deploy updates on your systems to ensure that the working of your system and software will not be adversely affected and to filter out un-necessary updates.

It is important to note that Windows Update only refers to Microsoft software. It is also important that you update other software which you might be using including Adobe Flash Player, Adobe Acrobat Reader, web-browsers, Java and anti-virus software. Most malicious software attacks come through websites and target commonly used software such as video playing software and browsers.

It is recommended that windows be configured so as to show all file extensions. This is a good security precaution because, for example, if your system is hiding file extensions, then when you get a file attachment called "MyDog.JPG.VBS", your email program will show the attachment as "MyDog.JPG" which leads you to believe that the attachment is simply a picture of someone's dog. But in reality, the attachment is a VB script (a program that can do whatever the virus writer wants it to if you double-click on it)

How to do it?

Windows XP

1. In Windows Explorer, choose Tools > Folder Options.
2. Click the View tab in the Folder Options dialog box.
3. In Advanced Settings, select Show Hidden Files And Folders.
4. Deselect Hide Extensions For Known File Types.
5. Click OK.

Windows 7

1. Select Start > Control Panel.
2. In the Control Panel dialog, double-click Appearance And Personalization.
3. In the Appearance And Personalization dialog box, double-click Folder Options, or click Show Hidden Files And Folders under Folder Options.
4. In the Folder Options dialog, ensure that Show Hidden Files And Folders is selected.
5. Click OK.

Anti Virus Software is essential

You must ensure that you have Anti Virus, Anti Spyware, Firewall and Internet Security software installed, running and automatically updating. Without it, not alone do you leave yourself open to the potential destruction of valuable data on your System but by failing to abide proper protection, you may also be deemed negligent and open to claims by your client base.

Purchase from a reputable supplier. There are many off the shelf packages They are often intended as personal programs for use on one PC without mission critical data and are not suitable for business purposed. Usually, if you are operating a network of computers, you will have bought them from a single supplier. That should be the first point of contact for the purchase of Anti-Virus Software. That supplier will make recommendations for recognized industry-standard business applications. The supplier himself should be Microsoft certified a Microsoft reseller (where you are using Microsoft Software) or in the alternative have the appropriate qualifications for the type of Operating System you propose using. Those qualifications ensure that the software to be supplied should integrate properly with the operating system and word processing, e-mail programs that you are using.

Purchase a recognized product – there are a handful of strong names in the supply of Anti-Virus Software. These companies have extensive websites and relationships with the major suppliers of operating systems (Microsoft, Oracle, Sun Systems, Apple etc.) Anything less is dangerous. If you use a reputable supplier they will have access to the appropriate programs.

Ensure that a full system virus scan is scheduled to take place regularly and automatically.

The above stands to reason and must be a generally known precaution but its implementation is another matter.

It has also been found that a large percentage of all virus and malware infections are a direct result of failing to update five specific software packages: Java Runtime Engine, Adobe Acrobat/Reader, Adobe Flash, Microsoft Internet Explorer and Windows Help and Support.

The message is simple, ensure you have anti-virus systems installed, updated and working. Do regular full system scans and also remember to apply available updates to all programs running on your computer

E-mail Security

Take precautions; watch out for spam, spoofs and phishing. Spoofs, spam, and phishing are terms every e-mail or IM user should know about.

Attackers may “phish” for personal information by asking for passwords or account numbers through a spoofed (counterfeit) e-mail/IM message or Web site that appears to come from a trusted source.

Spam (junk e-mail) and spam (junk IM messages) not only clutter inboxes with annoying sales pitches but are frequently part of illegal scams to steal money as well as identities.

- Never provide passwords, PINs, or other sensitive information via e-mail or IM.
- Be suspicious of “urgent” requests to click links, or provide account information.
- Most users get infected by clicking unexpected or suspicious links in e-mail, IM messages or on questionable Web sites. Think before you click!
- E-mail attacks are common, so never open unexpected attachments.
- Never respond to spam, even to unsubscribe. Filter it within Outlook.
- Never open chain e-mail claiming to contain virus fixes, patches or warnings.
- Avoid clicking on links embedded in emails. If you receive an email from your financial institution regarding account information or logins navigate to their site using your browser. Anyone with access to the stolen database can easily see that your email address is connected to a particular bank to make things look more credible.
- Watch out for “deals”. People shop on the Internet for bargains and receive emails almost daily for some type of money saving deal. Watch out for suspect money saving offers that take you to malicious websites or cloned sites.
- Keep up with your malware scans. You may never see it coming but clicking on a link or opening a file from a spammer may infect your computer with malware that will steal from you at a later date.
- Be smart with your personal information. Don’t simply trust a company that emails you asking for important information (remember they will play on your sense of urgency).
- If you think that an email request is legitimate, call the company and update the information over the phone.

Take your time when opening emails. Don't be in a rush and don't go through the motions when reading your mail messages. Remember that attackers know all to well that when we get into a routine, we get careless and that is when they will try to strike. You can access the Committee's guidance note on the Subject of Proprietary Secure Email – Secure for whom here.

Internet Security

Be careful of the websites you visit and the dangers associated with the downloading of “free” software.

Most users know that clicking e-mail or Web links can be dangerous but what is not as well known is that you can get infected just by visiting a Web page.

Ensure that browser software is kept up to date and note that the likes of Norton Internet Security will give an indication in the search results list as to whether a site has been checked and found to appear safe.

Free toolbars accompanying “free” software are a common ruse for spyware, adware or other malware. Some fake toolbars imitate legitimate ones to fool users. But even legitimate toolbars can have security holes and be vulnerable to hijacking or other attacks.

Use “settings” to prevent access to undesirable and time wasting sites.

Portable devices, tablets and smartphones need encryption, passwords and physical security precautions

Laptops and portable devices are an easy target for thieves. If your portable device is stolen, or if someone gains access to your files while your back is turned, your company information and your personal and financial data can be accessed.

Avoid using bags that make it obvious that you're carrying a portable device. Instead, try carrying your laptop of tablet in something more common such as an ordinary rucksack. Never keep your passwords in your laptop bag.

If someone should get your portable device and gain access to your files, encryption can give you another layer of protection. With the Windows operating system, you can choose to encrypt files and folders.

Possible threats for mobile devices include:

- Loss of the physical device.
- Loss, compromise, or erasure of data on the device.
- Unauthorized use of the device.
- Unauthorized access to network service and data.

Keep your device with you. Always take your device on the plane rather than checking it with your luggage. It's easy to lose luggage and with it your data. In a car keep your laptop out of sight in the boot when not in use.

Keep your mind and your eye on your device. When you go through airport security, don't lose sight of your bag. Hold your bag until the person in front of you has gone through the screening process. Many bags look alike, and yours can easily be mistaken in exiting the security process.

If you need to leave your laptop in a room or at your desk, use a security cable to securely attach it to a heavy chair, table, or desk. The cable makes it more difficult for someone to steal it. There are also programs and devices that will report the location of a stolen laptop, table or smartphone. These work when the portable device connects to the Internet and can report the exact physical location and can allow you to disable the device remotely.

Affix your name and contact info to the laptop Security experts advise that you affix your name and contact information, along with a promise of a "Reward if lost or stolen - no questions asked” it can help recover the item.

If a laptop is lost or stolen you should immediately change your network password to help prevent unauthorised access to corporate servers, report the loss to the Gardai and to your company's IT people. If client data was on the laptop report the event to the Data Protection Commissioner.

BYOD

Bring Your Own Device is an increasing concern and requires security precautions. With 6 billion global mobile subscribers and over 35 billion apps downloaded to portable devices, one begins to wonder how secure this situation is for businesses.

People are seeking the freedom to work on the device of their choice. This situation has been described as turning an organization's network security into Swiss cheese, where holes are opening up from devices everywhere.

What previously seemed secure meets vulnerability challenges.

Staff are accessing critical corporate data via unprotected means such as public WIFI and utilizing simple passwords. In addition, an increasing number of people are accessing their employers' business applications using their personal devices.

This new world requires new security precautions.

Mobile device management (MDM) systems allow administrators to configure devices and perform remote operations, up to an including wiping a device. MDM systems can typically enforce password policies, restrict access to app stores, and deploy network management settings to devices.

Asset management features can help track the version of operating system running on mobile devices as well as produce software inventories. This information can be especially helpful for software license management. If corporate licensed software is installed on personal you need to keep an accurate inventory of those deployments so that when an employee leaves the company you can use this data to remove corporate licensed software on the employee's personally owned devices.

Among the aspects you need to consider are:

- Who owns the device?
- Who manages it?
- How is it secured?
- Who will replace it if it is lost or stolen?

You need to enforce the same controls in terms of passwords, anti virus precautions and encryption as applies to office owned devices.

Your device management policy should specify what types of operations will be performed on employee-owned devices, e.g. provisioning and configuration, and operations that could be performed, such as wiping a lost or stolen device. In respect of the latter it is to be borne in mind that the device will also contain information which is the property of the employee.

Outline in your terms of employment and as clearly as possible under what conditions those additional operations will be performed and how they may impact employee's personal data on the device.

Backups are essential for the security of your data

It is imperative to have reliable backups for any computer system. In the event of a system failure, or if a document is deleted by accident, the backups will be used to rebuild the system or retrieve the document.

Hacked or infected computers are taken off the network until they're safe. They may suffer partial or total data loss and threat removal often requires reformatting your hard drive. You could lose all your data—unless you have a backup. When was your last backup? To prevent any future loss, make backups regularly.

Backups - in addition to the regular main file backup, take a full IMAGE of your server once per month. Hold that off site. That ensures you can quickly get up again instead if having to wait for a full restore to copy over. Images on external drives can be plugged into the server and have you back and running within 30 minutes whereas the main restore might take several hrs to copy over. External drives now and imaging software have fallen dramatically in price.

If you are the victim of a security incident, the only guaranteed way to repair your computer is to erase and re-install your whole machine.

System Restore stores the state of the computer in a series of stages known as "restore points." You can manually create a restore point at any point in time to save the state at that point, or restore to any of the saved restore points. Sometimes software, like a Windows service pack, will create a restore point on its own before running.

The restore point of the computer does not contain every file on the computer, but it includes the parts that affect the configuration of the system and the contents of some key directories.

If you know that the system state at a particular restore point is safe, then it is safe to restore to it to that point. There are many times when this would be the case. For instance, if you download a program and run it and suddenly your system is infected with adware, you can go to a restore point prior to the point you installed the adware and know that it is clean. Restoring may not completely remove the attack, but it should disable it from running and make it easier to remove manually or by software.

WIFI – take care when accessing WIFI at an external location

Wireless (Wi-Fi) hot spots, are changing the way people work. These wireless local area networks provide high-speed Internet connections in public locations and at home. You can access them with a wireless-ready mobile PC, tablet or smartphone or any other mobile device equipped with a wireless card.

There are Hot spots everywhere, including coffee shops, restaurants, libraries, bookstores, airports, trains, and hotel lobbies. There are paid services as well as free public connections. Many places will inform you that they have a hot spot for wireless Internet use and will tell you how to access it, including providing you with a password, if necessary.

Public hot spots all have one thing in common—they are open networks that are vulnerable to security breaches. Because they do not encrypt data, your passwords, email messages, and other information can be visible to hackers. That means it's up to you to be aware of wireless hot spot security and to protect the data on your PC or mobile device.

Disable your Wi-Fi adapter when you're not at home or at work, it's a good idea to turn off your laptop or notebook's Wi-Fi capability when you're not using it. Otherwise your computer might connect to a malicious hot spot without your realizing it. Some laptops have a Wi-Fi hardware button you can use to disable your Wi-Fi adapter. Otherwise you can disable your Wi-Fi adapter using your operating system.

It is not always possible to choose your connection type, but Internet security is critical. When you can, opt for wireless networks that require a network security key or have some other form of security, such as a certificate. The information sent over these networks is encrypted, and encryption can help protect your computer from unauthorized access. For example, instead of using a public hot spot with no encryption, use a virtual private network (VPN).

Disable file and printer sharing. File and printer sharing is a feature that enables other computers on a network to access resources on your computer. When you are using your mobile PC in a hot spot, it's best to disable file and printer sharing—when it's enabled, it leaves your computer vulnerable to hackers. Remember, though, to turn this feature back on when you return to the office

If you're working with extremely sensitive data, it might be worth taking it off your portable computer altogether. Instead, save it on a corporate network share or on a password-protected site, such as Sky Drive or Drop Box

Sensitive Data and Cookies

Sensitive Data needs to be securely protected. If you save sensitive data (personal, financial, health, etc.), it may be at risk if your computer is compromised, lost, or stolen. Proper disposal of electronically stored data is important to ensure the privacy and security of sensitive user information. Deleting data from storage media (CDs, hard drives, USB keys, tapes, etc.) does not permanently destroy the information. Computers and media must be properly sanitized before disposal to prevent unauthorized retrieval and use of information. Sanitization permanently destroys all data stored on electronic storage media.

Examples of sensitive data that must be encrypted include:

- Personally identifiable information maintained for business (Social Security numbers, credit cards, etc.).
- Identified client data, medical records, etc.
- Any data that a user feels would cause substantial damage if exposed to the public

The E-Privacy Directive (2009/136/EC) was transposed into law in Ireland with the enactment of the European Communities (Electronic Communications Networks and Services) (Privacy and Electronic Communications) Regulations 2011, which took effect on 1 July 2011. Regulation 5(3) deals, among other things, with the storage and retrieval of information on 'terminal equipment', most commonly a computer user's browser.

Modern browsers have different mechanisms of data storage on a visitor's machine, the most common method being via the use of 'cookies'.

A cookie is a small file on the computer's hard drive that stores pieces of text. A browser can set and collect information from this text file when a visitor enters a website. A cookie might report back to the originating website details of when you last visited their site, or the number of times you visited, or details of your browser's history.

Many law firms facilitate the implementation of cookies on their websites when using the Google Analytics system of tracking visitors to their home page. Social media widgets also are known to set cookies. The 2011 regulations require that consent to the placing of cookies should be obtained and that a website should offer "clear and comprehensive information" in connection with the information being collected.

The 2011 regulations do not specify that prior consent needs to be obtained. Therefore, we would recommend that, if your website uses cookies, you should, at a minimum:

- Include a link to your privacy policy on all pages,
- Explain in that policy document how and why you use cookies, stating, for example, that the firm uses cookies to count visitors to your website (if that is the case),
- Detail how, if a visitor chooses to accept cookies, they also have the ability to later delete cookies that they have accepted. For example, in Internet Explorer 9, cookies can be deleted by selecting 'internet options' and, under the 'general' tab, selecting the heading 'browsing history' and then selecting the 'delete' button. Finally, tick the 'cookie option' and click 'delete'.

You can access the Society's practice note on the use of cookies here.

Shared & Public Computers & Internet Cafes

Involve risks to the security of your identity and data

There are a number of risks involved when using shared computers, public computers and wireless networks at places like libraries, Internet cafes, airports, and copy shops.

The network may be poorly secured and easily exploitable by hackers and thieves--one of whom may be sitting right next to you, looking over your shoulder, and stealing your information.

A hacker may even be the one running the free wireless signal you've lucked upon, grabbing all of your information as fast as you can send it.

The use of shared and public computers and wireless hotspots is ill-advised if you are working with sensitive information of any kind.

Some common risks associated with using shared & public computers and Internet cafes are:

- Web Browsers often record (or cache) your browsing history in cookies, enabling companies and individuals to track your surfing habits and possibly access your online accounts you've logged into after you have looked off
- Keyloggers may be installed that track your keystrokes in order to access your passwords and user IDs
- Spyware and Web browsers may record (or cache) your log in information, browsing history or documents in cookies, enabling other individuals to view the websites you visited or documents you printed.
- The free wireless network you're connected to may be run by a hacker
- Thieves literally looking over your shoulder to steal personal and sensitive information.

Guidelines for using a shared or public computer:

- Log off any online sessions.
- Delete browser cache/temp files.
- Never use the “remember” or “store passwords” for online web sites.
- Never leave your computer unattended while logged into any online web sites.

Cloud Services and Cloud Storage

The popularity of cloud services is on the increase.

Cloud services may offer convenience and economic benefits but they are subject to risks of their own which must be born in mind.

There are issues of security and client confidentiality which must be considered. Questions that arise are:

- Who is in control of the data?
- How reliable is the company providing the service?
- Where is the data stored?
- How is it secured and encrypted
- What are the provisions for backup and restore?

You can access guidance notes from the Committee by clicking on the subject of Cloud Computing by clicking any of the following links:

- Get Off My Cloud - Gazette July 2012
- Head in Clouds' – Gazette December 2010
- Securing Client Information is Key - Gazette Aug/Sep 2008

Disposal of computer equipment requires the greatest case and data should be cleared completely.

Selling or giving away an old computer or hard drive is something we all do at one time or another. Whether it's getting a few dollars on eBay, or taking the tax deduction by giving it to a school or charity, it feels good to clear out that old machine. However, are you also giving away personal and financial information that could be used for identity theft? Even if you don't run your business or do your banking on your PC, it collects information such as ISP passwords, names, addresses and phone numbers, or personal e-mail that, in the wrong hands, could be used maliciously. So what do you do? – Have the computer professionally cleaned.

You can access the Society's notes and guidelines on the retention or destruction of files here.

Written policies should exist in relation to computer use.

You should set out your information on security practices in a written policy. The policy should reflect solicitors' professional and legal obligations. You should supplement this with implementation procedures. You should monitor these and review them at least annually. The policy should include reference to email and internet use and the use of systems for private communications as well as the required procedures and precautions in respect of mobile and BYOD devices

Guidance relating to Computer Servicing

Specific confidentiality risks arise when access must be given to individuals, other than staff, to carry out maintenance, upgrades or servicing of hardware and software in an office. Measures to safeguard and secure client information and data could include the following:-

- Dealing only with reputable suppliers and service providers.
- Putting all maintenance and service agreements in writing and having them signed by both parties.
- Including confidentiality clauses in all maintenance and service agreements. (See below).
- Nominating one person as a liaison person with any service provider.
- Having individual engineers sign in and out and sign personal guarantees.
- Requiring written authorisation for downloads of data from systems, for example, onto CD-ROMS or floppy disks.
- Requiring written authorisation for the removal of any hardware from a PC or network server from the premises. In particular this should include memory boards and other storage devices.
- Where any item is to be disposed of, this should be done under supervision, ensuring that any data or information which may be carried on these memory

devices cannot be retrieved.

- Requiring that printouts or hard copies of electronic information or data held by maintenance service providers are disposed of when they are no longer necessary for use.

- Remote access should only take place where there is prior written authorisation from the firm.

Confidentiality Agreements

Where a confidentiality agreement is being entered into with a service provider, it should ideally contain the following clauses:-

- No disclosure of information except as permitted.

- No copying of information except as permitted.

- No use of information except as permitted.

- Recording of the number and whereabouts of copies made.

- Measures to be taken to avoid inadvertent disclosures.

- Immediate notification to the solicitor where there is any inadvertent disclosure or unauthorised access to the information.

- Delivery or destruction on demand of copies of information and notes or records made and deletion of these from any computer or other electronic system(s) on which they have been stored.

- A specific list of persons to whom information may be disclosed.

- Third party recipients to keep information confidential.

- A clear statement as to when the maintenance or service contract will end and arrangements for the return of all material which may be held on behalf of the solicitor at the time the contract is terminated.

You can access the Committee's guidance notes on the subject of allowing External Access to your system here.

Outsourcing of Document Production

You can access the Committee's guidance notes on the subject of Outsourcing of Document Production here.