6 Beyond the essentials

How far are you prepared to go to protect your devices, your family and yourself in cyberspace? The list of good practices can get very long and it forces all of us to make choices. Every one of the measures in this section will require you to consider its pros and cons, the amount of time effort that they'll require and the value they will return to you.

Figure 16: The proverbial tip of the iceberg

6.1 Inventory of your devices

What is this?

A typical inventory in 2013 would include one or more of the following (and a few more items)

- Home computer (desktop or laptop), including operating system and pre-installed software
- Other home computers, laptops or notebooks, including operating system and pre-installed software
- Tablet computers, including operating system and pre-installed software
- Smartphones (corporate and personal), including operating system and pre-installed software
- Other software, licensed as well as shareware and freeware
- Backup and other storage devices (disks, USB memory, DVD and data CDs, other)
- Connection and account(s) with an Internet Service Provider
- Wireless and other connectivity devices (home network, routers or switches, etc.)
- Warranties, maintenance contracts, support telephone numbers, etc
- Passwords and password-related devices (e.g. tokens, cards or password generators)

Why is this an issue?

Simply because it is the only way to have records to report details such as serial numbers, date of purchase, software license numbers and other information you may need to report loss or damage to the police, insurance company, internet service providers and other parties with which you may need to communicate.

What you should do about it

Many items of the equipment and software you own have basic information about them in electronic form, such as serial numbers, product ID and software version. The software packaging or the order confirmation if bought online often includes a Product Key necessary to activate it. You may have many items that do not have such data, for example USB memory devices – it would be however prudent to keep track of them to, at least, be conscious if one or more is lost.

While it may laborious, either a word processing, spreadsheet or database package can be used to build a comprehensive list that is easy to keep updated. The following parameters should be recorded:

- Hardware: Make, model, serial number, date of purchase, length of warranty
- Software: Name and purpose, version, product ID or serial number, date of purchase
- Services: Name and purpose, access codes and passwords (these should not be in clear text!)
- Networking: Provider, terms of contract, access codes and passwords (these should also not be in clear text!)

There are several programs, many included with your devices software or available as downloads that simplify this task. Given the wider range of devices, operating systems and utilities each owner has to look for the most appropriate tools for each environment. A search engine can help…

6.2 Crapware, craplets and Scareware

What is this?

Pre-installed software (in a computer, tablet or smartphone) is referred to by the device vendors as "bundled". Buyers tend to think of such software as "crapware" because some of it reduces customer choice – for example pre-installed anti-virus software which may be difficult and time-consuming to remove, or "craplets," software that the device manufacturer was paid by a software company to include. Craplets are of dubious value to the buyer, such as evaluation copies of products or outdated games.

Scareware is the name given by security writers to software sold on questionable ethics by causing anxiety or fear to insufficiently informed owners of devices. They do so by displaying warnings of malicious software infections that must be immediately removed by downloading (and paying for) their software. Alternatively, the message suggests that a particular product could greatly enhance performance – such as registry optimisers or cleaners.

Why is this an issue?

- It may be bad for you
- It limits the buyer's choice
- It makes it difficult to install an alternative product (e.g. anti-virus products)
- It consumes computing resources
- It may contain malicious software to capture and report sensitive data
- It is limited to the computer on which is was installed
- It has a limited period of validity, after which it must be purchased
- It does not come with the media necessary to re-install it should this become necessary
- It is difficult (sometimes impossible) to remove

What you should do about it

Crapware and Craplets:

- Identify the inventory of software pre-installed in the device
- Look for any Uninstall options that any software you don't wish to keep may have
- If not found, use a search engine for guidelines on "how to uninstall XXXX" from a "CCC", where XXXX is the software in question and CCC is the make and model of your device
- Remove anything that you don't wish to keep.

Scareware:

Advertisements for scareware will appear on your screen when you are online. Some will tell you that you have a major and urgent problem sometimes giving you a "free" diagnostic. Buying their product is always the answer. Many of these products will do nothing and may introduce malicious software to your device. Others, such as Registry management software may cause your computer to malfunction. Should you feel that your computer needs attention and you have no access to expert advice, start by using your search engine to look for product reviews (see also the section on "downloads").

6.3 Inventory of all your accounts

What is this?

If your device(s) may be shared at some time or another, you should take steps to control what others can access and do with them. Creating individual accounts does this. These specify what others may do without compromising your personal data.

Even if you do not share your devices it is good practice to keep your login identities and passwords to online services secret to avoid others – unknown and unknowable – from impersonating you and conducting financial transactions, abusing your social networks, writing blogs, etc.

Why is this an issue?

It is likely that, like the majority of people these days, your devices are used for accessing subscription material, bank accounts, assorted bookings and reservations, electronic mail, blogs, social networks and more.

If you are a regular use of Web-based services it is likely that you will be required to have a login identity and, typically, a password. As these may be numerous, it creates a dilemma: make it easy for yourself by using the same login identity and password for all of these accounts or, like physical keys to open locks, have a different one for every account.

The latter is a more secure option but it requires you to have an excellent memory or write them down. If you write them down, this inventory must be kept away from anyone who may misuse it or abuse it.

What you should do about it

The first step consists of identifying and listing all the login identities and passwords you have and what they are used for. While the number of login identities need not be large – many online services use your electronic mail address as your login identity. Your choice is whether to use your "real" name or a made-up identity (e.g. Retired.Auditor@….). However, passwords should be different for each service.

Having established the list, it should be protected by, for example, storing it in encrypted form, password protected and/or in a data vault.

Ensure you have also left your log-on credentials with a trusted/loved person. You never know what uncertainties life will confront you with and they may need to access your system in the event of an emergency.

6.4 Lost your smartphone or your computer?

What is this?

The popularity, affordability and usefulness of electronic devices in the hands of a large population implies that either due to oversight, distraction or any other human weakness, devices get lost, misplaced or forgotten. Many of these devices, particularly the very recent and/or fashionable become objects of desire and therefore, get stolen. They also get left behind in airport security checkpoints, restaurant tables and almost any other place. You may be lucky. More often than not, this is not the case.

Why is this an issue?

If the device cannot be recovered, obviously there is the cost of replacing the device. However, and more importantly, the device may contain personal and/or corporate information, including stored passwords to network connections, electronic mail, bank accounts, etc. that could be abused or misused by a third party.

What you should do about it

There is no shortage of options for each type of device (i.e. computer, tablet, smartphone). If the lost device has been provided by the business in which you work, they should be the first to be informed.

If you have lost a computer or tablet, the second step below may help you. If it doesn't, don't hope for much. If the device is your telephone or smartphone you should try the following steps first:

- Call your phone and listen for it to ring or vibrate. If someone else has it, they may answer it
- Do a thorough visual search (if you did not hear it maybe because the battery is flat) and retrace your steps
- Send a test message offering a reward for its return
- Contact your service provider and report the loss
- Report it to your insurance company (if you have such insurance)

You can help yourself by installing software that helps you trace the location of your lost device and, just as importantly, protect the data in your device. Other sections in this book give some more details.

> Expect the worst and you will never be disappointed.

6.5 Tracking software for electronic devices

What is this?

Given that electronic devices, particularly new models, are small and lightweight, they are easy to misplace and steal. Trustworthy sources report that in the U.S. alone, there are up to 2 million laptops stolen every year and as many as 600,000 are left behind at airport security points and lounges. Similar numbers are reported for stolen and lost mobile phones.

Why is this an issue?

Numerous studies conducted by serious researchers indicate that at least half of the lost or stolen devices contain confidential company information and the majority of the devices do not have measures to protect such information.

Besides, if the devices are yours, it does not feel good to misplace them, have them stolen and not being able to do much about it.

What you should do about it

Mobile phones and tablets

First thing to do is to note your phone's IMEI, MEID or ESN number (it's on a sticker under the battery), Which one of these numbers applies to your device depends on its manufacturer and model. The police and your network provider will ask for it when the phone is lost.

The mobile phone GPS tracking facility can be used to locate it and most network providers offer a tracking service (for a fee). There are several tracking applications (Apps) to choose from. You may consider using them if you have given cellphones to your children.

A search engine query on "cellphone tracking software" or "cellphone tracking services" will give you several options to explore.

Laptops

There is an adequate selection of laptop tracking software (fee-based) that you need to install and subsequently activate when the device goes missing. If and when the laptop is turned on and connected to the Internet, it can be located and you can provide this information to a law enforcement agency.

A search engine query on "laptop tracking software" will give you several options to explore.

6.6 Remotely wipe the contents of your lost device

What is this?

If someone else has you device and it is not protected by a good password or PIN, whoever now has it will have access your contacts, text messages, stored documents and everything else that you may have in it. If password protected, this may not be too difficult to break.

The best way to ensure the confidentiality of all the data in a mobile device is to remotely wipe it.

Why is this an issue?

Simply because your data is yours and nobody else's business – the belief that "I have nothing to hide" is no excuse to allow others access to your data, particularly if it includes details of your bank accounts, friends' telephone numbers and personal messages, as you lose control of how they may be misused or abused.

What you should do about it

Many devices, particularly smartphones may include the facility for remote wiping and there are many software products and Apps that perform this function. Several of them are included in the software that allows a missing device to be tracked.

A word of caution: if the data in the missing device has not been backed up, remote wiping will leave you without any trace of this data – would you like to lose the only copy of your baby's first words or steps?

Search engine query "remote wiping of (product name and model)".

6.7 Encryption and digital signatures

What is this?

Encryption and digital signatures use mathematical processes for somewhat different purposes. Both have been in use for many years.

Encryption (also called cryptography) is intended to transform a document (usually text) into a format that cannot be read without having the right tool (a "key").

Digital signatures use similar tools to ensure either (or both) that the originator of the document is the person who "signed" it and that the document has not been modified after it has been signed.

Why is this an issue?

As activities migrate to cyberspace, it has become essential to protect the confidentiality of valuable and sensitive data, i.e. the ability to read such data is restricted to a limited number of authorized individuals.

Similarly, it has become important to be able to demonstrate that the data's integrity, i.e. that the data has not been modified by an unauthorized third party.

What you should do about it

A private individual (as against a corporate entity) should consider several different situations:

a) The encryption of some or all the documents in a computer or smartphone so that, should the device be stolen or lost, the personal information in the device is not readable by the new "owner". While an expert having the knowledge, tools and time can break such encryption a casual thief or finder will most likely give up
b) The use of encryption in everyday activities, such as electronic mail is good to ensure the privacy of such communications. However, given that it has been reported that there are surveillance mechanisms that track electronic communications, the use of encryption – totally legal – draws attention to the parties to such exchanges. As a result, it is prudent to remember that electronic mail is essentially the same as sending a machine-readable postcard and you would not put the details of your credit card on a postcard, would you?
c) The use of digital signatures is advisable when there is a risk of dispute about the authenticity and/or accuracy of a document or transaction

If you need to provide sensitive information such as a credit card number to someone you really trust, instead of encryption you could apply the technique described in 4.8 on condition you use words other than the ones you use to encode your PINs.

Finding encryption and digital signature tools is relatively easy. Your favourite search engine should be your best friend

6.8 Geo-tagging

What is this?

Geolocation is the ability to identify the position in the world of a specific item or device using a variety of techniques including Global Positioning by Satellite (GPS) and Internet Protocol (IP) address location.

Geotagging is a feature increasingly available in electronic devices such as photographic cameras, notably those in a smart phone that records the location where the photograph was taken.

Why is this an issue?

It may or may not be an issues, depending on your cultural attitude about being tracked.

On the positive side, being able to track a person by locating a geolocation-enabled device is a valuable feature in situations such as finding a misplaced or stolen device, or in a Search and Rescue operation. If you are a parent and you give such a device to your children, you'll have the ability to find out where they are should they not answer their phone. Geolocation and geotagging can also be valuable in forensic investigations.

On the negative side, to what extent do you want your physical location to be known by others – not just friends but also potential stalkers and others with malicious intent?

What you should do about it

Make a choice that is appropriate to your circumstances, recognizing that being "invisible" and "anonymous" is gradually becoming harder.

6.9 Legislation you should know about

What is this?

A big enough topic to justify a fat book. This is not the intention of this Section, which is to make you aware that there are many areas of activity that are covered by legislation and it is sensible to avoid breaking the law.

Among the many areas covered (in different ways in different jurisdictions) are:

- Intellectual property – copyright and copy protection for digital media
- Software licenses (did you read your End User License Agreements (EULA) and understand it?)
- Unauthorised access, data privacy, dissemination of spam and other "computer misuse"
- Data retention
- Use (and particularly export) of encryption
- Computer evidence and digital forensics
- National security (e.g. the USA Patriot Act of 2001)

Why is this an issue?

Because "ignorance of the law is no excuse".

What you should do about it

Be curious about this and using a search engine or online encyclopaedia to find out more about those areas of the law that are relevant to you.

6.10 Jailbreaking or rooting your devices

What is this?

Jailbreaking is a term associated with a specific series of products manufactured by Apple using the iOS operating system (iPhone and iPad amongst them). These devices come with several restrictions imposed by their design, notably that applications (apps) need to be downloaded (some are free) from Apple's App Store. The security design of these devices ensures such apps run in a confined and controlled environment (a sandbox). Other restrictions apply to the use of the device only with a contract carrier that the end user cannot change as well as the customisation of the device beyond the parameters set by the vendor.

Rooting applies to devices using the Android operating system and is about allowing the user of the device to have access to privileged functions such as modifying or deleting system files as well as removing apps pre-installed by the vendor or carrier.

Why is this an issue?

Apart from invalidating the device's warranty both jailbreaking and rooting introduce new security vulnerabilities – by jailbreaking the device, you allow apps from sources other than Apple and that may not quality assurance and/or contain malware to run. As such applications would not run in the sandbox provided by iOS, they can corrupt the device and allow the malware to access personally identifiable information.

Jailbreaking is not supported by Apple and there are many articles about its risks and disadvantages.

Rooting, however, is permitted and reflects the open source software history of this software. The real issue is one of knowledge and responsibility. The statement that Genius has limits but Stupidity does not applies.

What you should about it

If you are a good hacker, you may have many reasons for exploring and exploiting both.

If you are a knowledgeable and experienced person with expertise in information technologies, you should already know that some things are best left alone and that any actions you take should have a genuine valid reason.

If you are not, and just read an article in an enthusiasts magazine – good luck to you because that's what you are going to need.