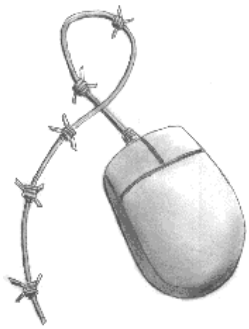
Participating With Safety Briefing no. 1

Introducing Information Security



Written by Paul Mobbs for the
Association for Progressive Communications, March 2002.

Introduction

Using computers is a complex business. To use them properly you must learn not only how to use the functions of the word processor or database that you rely on; you also need to learn how to organise your computer and the information it contains in order to protect against the *accidental loss* of information.

It is also important to prepare your computer, your information and your premises, for the possibility of *deliberate external damage,* which could be caused by computer viruses, interception, monitoring or physical raids by the state or other forces which oppose your work.

This briefing is the first in a series about information security. It should be read in conjunction with the other briefings in this series, which concentrate on the practical aspects of security. They cover:

- Backing up information
- Passwords and access controls
- Using encryption and digital signatures
- Computer viruses
- Using the Internet securely
- Counter surveillance

This briefing outlines the main points you need to consider when addressing the security of your computers and systems. The other briefings look in more detail at features mentioned here. Much of what this briefing discusses is theoretical. It cannot be proscribed, because it is dependent upon the needs and circumstances of the individual. Although the content of the briefing may seem daunting, it is worthwhile reading the material as it provides the context for the use of other briefings as part of a system of security rather than a piecemeal system of protection.

The need for security

Information Security (also known as *IT Security*, or *Infosec*) is the theory and practice of using computers and information systems in order to:

- Prevent accidental loss or damage to information and computer systems by people using them;
- Develop and set up the systems to ensure as much reliability and security as possible - that means protecting your equipment, preventing viruses, hardware failures, etc.;
- Prevent others (i.e. hackers/crackers and other people interested in influencing what you're doing)

© APC and Paul Mobbs, 2002 - released under the GNU Public License

causing accidental or deliberate loss or damage to your data and equipment.

The above list of potential threats to security is in decreasing order of probability.

The objectives of good security

The ingredients of a good information security plan to control and/or enable the sensitivity, security, access and performance of your data and systems:

- Information must be controlled according to its sensitivity - this requires you to decide what security certain information requires, and to classify information in terms of its sensitivity or irreplaceability;
- Security barriers must prevent unauthorised access or alteration of data - you should combine physical barriers (such as locks) with programmable barriers (set up as part of computer programs or the computer's operating system);
- People must be able to access the information they need to use - this requires that people understand how the system of access works on the computer or information system, and that they have the relevant access codes/keys;
- Your computers, and the procedures people use relating to them, must perform effectively in order to meet the needs of users. You must work out what tasks you need your system to perform for you and what levels of security you require, and then develop systems that meet these criteria.

How to approach information security

The best way to approach the problem is to develop *systems* and *cycles*:

- Systems are the methods by which information is secured - for example organising information on the computer so that it is easier to find or back up;
- Cycles are periods of time over which information security is reviewed - so for example you could have cycles for changing passwords or backing up data on a regular basis.

Security is a process, not a product. You cannot buy security and install it. It is a collection of different measures, tailored to your own needs, methods and ways of working.

Assessing the risks

The most common everyday risks you are likely to face are, in order of probability:

- user errors (accidentally deleting files/damaging storage media)
- problems with software (especially Windows)
- deliberate damage (viruses, motivated damage)
- equipment failure
- theft
- power surges, flood and fire.

There will also be risks that apply only to you, as a result of the type of work you undertake, or because of the location your equipment.

© APC and Paul Mobbs, 2002 - released under the GNU Public License

When organising your information, systems and equipment you need to consider what risks you face and how you can plan for contingencies as a result:

- Consider various 'what if' scenarios: How might your data be lost, compromised or damaged?
- For each scenario you can think of, consider -
  - the risk of that series of events happening;
  - what technical means you could use to recover or protect data or information, and thereby reduce the risk;
  - the consequences of taking those actions (you could address the risk posed by fire, for example, by keeping copies of information in another location, but you would then have to find a way of protecting those copies from other risks such as theft).
- For each of your solutions, weigh the risk against the cost or difficulty of the technical solution and decide whether it's worth the time, money and effort. For example, if you have put a copy of a file on the Internet, or distributed it to many other people, you do not need to give it the same level of protection as your own local files.
- Keep it simple - introduce systems and cycles to deal with each risk one-by-one. If you try to tackle everything at once, the task may seem overwhelming. You may find that taking steps to prevent one risk will often solve the problems created by another. For example, you may wish to guard against theft, but find that the same procedures can also guard against intervention by the state or others who oppose your work.

Looking after your information

In industry, 75% of information loss or system damage is caused by staff error, rather than by external forces (such as hacker/crackers or viruses). Analyse your own information security skills, and identify where you need additional training or resources in order take steps to deal with those needs.

Get organised

From filing cabinets to floppy disks, looking after information is all about how you organise your data. You need to make sure it is:

- Accessible - You need to find things when you need them - that doesn't necessarily mean adopting strict structures, but it does mean you, and those needing access to your data, need to know where things are;
- Quantifiable - You need to have a good idea what you have in order to tell if anything goes missing following a burglary or a raid - would notice any tampering with your computers or filing systems, is all your software properly registered in case someone checks, or are you aware of the content of the paper and digital information you hold and whether it contains information that could be considered unlawful?;
- Transparent - In the event of you or key people in a network being detained or taken out of circulation, by illness or some other more deliberate action, other people need to be able to access and make sense of your data to continue your work;
- Recoverable - You need to be able to easily reconstitute data if it gets damaged - that means making sure you only have 'useful' information on your files, and a minimal amount of useless or superfluous data that complicates the process of reorganising your information.

© APC and Paul Mobbs, 2002 - released under the GNU Public License

Developing and organising a good information system is a process of learning, and experimenting with different ideas until you find a system that works for you and those you work with. Learn from your mistakes.

Security barriers

As noted earlier, you need to set up barriers so that people cannot get hold of your information unless you want them to.

Paper-based information is fairly easy to protect because it is bulky; you would notice if it went missing. Electronic information is more difficult to control because it is easily copied; someone could break into your office with a laptop, transfer your information onto their system, and you would be none the wiser as to what they had taken.

A word of caution - if your system is too well indexed, or too well classified in files and boxes or directories, then it's easier for people to locate sensitive information within your filing system. Therefore it's a good idea to have a few gaps and illogical filing practices that those using the information are familiar with, in order to make sure your files are not completely open to everyone.

Protecting your information

There are various ways in which your information can be compromised (in increasing order of severity):

- Infiltration - people work their way into your office on a pretence, or as part of the group of people you work with, in order to gain access to your information;
- Burglary - people gain access to take your computer or information (either copying, damaging or destroying);
- Raids - the state uses its powers to gain access to your premises and computer and take away your information (see discussion below);
- Arson - the most quick and effective way to prevent activists working, is to simply incinerate their equipment and information to prevent them working effectively in the future.

Guarding against the first two is fairly simple - basic access barriers and security measures will prevent access, and if loss does occur, you can swiftly replace it.

Guarding against raids and arson is more difficult, and ultimately futile. Guarding against arson can be expensive, and is most effectively solved by keeping copies of important information and files in another location. To be effective in the immediate aftermath of an attack or raid, you must also ensure you can always beg or borrow access to a compatible computer.

State Intervention

Guarding against action by the state presents a different set of problems. The purpose of access barriers is to increase the amount of time taken to gain access to your information. Those seeking covert access will be deterred by good access barriers because of the additional time taken to circumvent the protection you have installed. When the state acts officially it does not have this problem. It can act openly. It can employ staff and specialists tools to help gain access. It also has complete legal rights to prevent any efforts by you

© APC and Paul Mobbs, 2002 - released under the GNU Public License

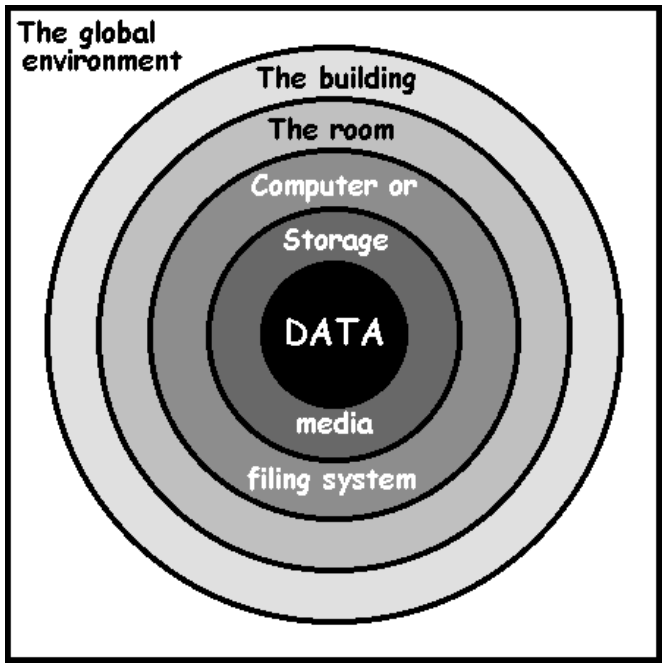
stop or frustrate their attempts to gain access.

No matter what physical security you have in place the officers of the state will forcibly enter your premises and destroy or remove computer equipment if they believe you have information concealed there. Even then, if they are not happy, they will take those people they believe have the information and hold or interrogate them until they turn it over. The greatest risks are usually presented when you have the best security - those people who hold the password to systems or encryption keys, or who know of the location of backed up data, will be under the most pressure to reveal what they know.

Although access barriers do not provide effective protection from action by the state, they can provide valuable time to allow you to take other action. For example, calling legal support or other organisation who can provide assistance. If you have good physical security, you might also have time to encrypt sensitive databases, or back up your current work off the computer in case the computer is taken away.

The best defence against raids by the state is to have many copies of your valued information held amongst a number of people. In the event of a raid they can circulate copies and publicise the work of those who have been subject to state action, according to the instructions you give them.

Security barriers



Security is all about protection layered in depth through the provision of barriers to access. You must build different layers of protection - *like the layers of an onion* - around important equipment and information. You need to protect access to:

- The building or premises where your equipment and/or files are located;
- The room where your equipment and/or files are located;
- The hardware of your computer(s);
- The operating system installed on your computer(s), and any boxes or cabinets where paper information is stored;
- Your files and data (including paper information).

Another important issue are services, such as power and Internet or network connections, that penetrate through the layers. These too must be secured if you are to have effective security. In particular, network or Internet connections should use firewalls to prevent access remotely over a network. You should also consider the other ways by which security can be covertly breached and try and minimise the potential for their use (see the briefing 7 on *Living Under Surveillance*).

Level 1: Securing your premises

Securing your building is a matter of common sense. If you lost your keys, could you get into your office? If you can find a way in, it is likely that somebody else could.
You will first need to consider the three types of intrusion you can expect:

© APC and Paul Mobbs, 2002 - released under the GNU Public License

- Opportunist burglars only want your equipment, not the data it contains. Good door and window locks are usually enough to prevent them gaining access. Opportunist burglars have no strong motivation to enter your property specifically- they will choose any empty, easily accessible property. Good external security will deter them.
- Targeted burglaries (where someone is trying to get into your premises because of who you are and what you do) are a different matter. However good your external security is, these burglars will try to get through it. Your defence must be to protect the items they are likely to be looking for.
- Access by the state or police cannot be prevented, but can be made more difficult. If they can't get in with your co-operation, they'll force their way in. If you try and hide things in the building, they will quite happily rip the building apart to find them. There's no hiding from a search warrant, so there's no point in trying - all they'll do is make an even bigger mess of the office.

Planning for a 'catastrophic' raid or burglary

As part of the assessment of risks, it is important to consider the 'what ifs...' for common events. Two significant problems are raids by the state, or motivated attacks or burglaries that seek to remove or destroy your data and equipment.

In the event of a raid you should have identified procedures to: call or inform other persons or organisation you work with; obtain legal support, if possible immediately, in order to lessen the damage or impacts of the raid; and activate a network of friends or supporters who can immediately begin fighting your cause whilst you are in the middle of having to deal with the circumstances of the raid, and perhaps the detention that might immediately follow.

Classifying information as 'general', 'irreplaceable' or 'sensitive' allows you to provide appropriate protection with minimum effort. If the information was appropriately classified, backed-up off-site according to its importance, and protected according to its sensitivity, the loss of the information should not prove a major obstacle. So long as sensitive data was encrypted, and the passwords for encryption were not disclosed, you may assume that the information has not been disclosed (but you may not be able to rely on this if someone who knows the passwords was pressured to disclose them).

What is important is ensuring you can recover and start again. For this reason you should try and arrange with someone to have access to another computer that your backed-up information will be compatible with. You should also make sure that, if the original copies and licenses for your software were taken or destroyed, that you can obtain copies of the licenses from the manufacturer, and access to copies of the software, to reinstall when you get another computer of your own.

Finally, either after a burglary or raid, you should change all passwords - for computers, Internet access or email. You should also generate a new set of encryption keys with a new password (but keep the old ones - you'll have to decrypt sensitive data that has been backed-up, and then re-encrypt with the new password).

When looking at physical security measures, consider the following points:

- Doors - Using a dead-lock will prevent people from opening the door from the inside without a key, making it more difficult to remove equipment.

© APC and Paul Mobbs, 2002 - released under the GNU Public License

You can only strengthen doors so far. They only need to be strong enough to prevent someone prising them open with a crowbar or kicking them in with a boot. If they are too strong, the fire brigade won't be able to get in if your building is on fire.

- Windows - Use key locks to secure window frames (professional burglars carry a variety of the spanners and pins used to open standard security locks). Burglars are often unwilling to break glass because it's risky climbing through the broken glass on the frame. Preventing them from opening the frame after they have broken the window will be a deterrent.

Toughened glass can help prevent access, but it can also trap you inside during a fire. If you put bars on a window which may be a means of escape in an emergency, make sure the frame that the bars are attached to is hinged and can be opened quickly.

- Walls - It's as easier to smash a weak wall than a strong door. Many newer buildings do not have solid internal walls, just boarded partitions. If you need really good security, you may need to consider the likelihood of someone gaining access from another part of the building.
- Roof spaces - If you share roof spaces with adjoining buildings you should fit locks to prevent access that way.

Roof and ceiling spaces are good locations for listening/surveillance devices because they provide space for equipment, and they have power supplies running through them. Tell-tale signs of interference from a roof or ceiling space are small holes on the ceiling, or unexplained damage/repair to the paint work. You should restrict people's ability to access roof spaces in general.

Level 2: Securing The Room

You can secure a house or office up to a point, but not so far that it may prevent emergency services getting in when you <u>really</u> need assistance. Once you have done what you can to make your building secure you should then consider the room, or rooms, where you keep sensitive information.

There are a few basic things you can do:

- Locks on any means of entry to the room - this may be windows and/or doors.
- Use cupboards and lockers to store material, and bolt them to the wall or floor to stop them being removed.
- Vital equipment can also be bolted to shelves or workbenches, providing they too are fixed to the wall or floor. You can get brackets or metal cages for computers, thereby ensuring that important systems can be fixed to floors or shelves.
- Although alarm systems for a whole building can be expensive, you can secure a room using simple systems that detect motion within a space, without the need for a lot of wiring.

Level 3: Your Computer Hardware

Computer hardware (the physical components of your system) usually comes with a number of features that make it more difficult (although not impossible) for unauthorised people to use a computer system. These features are a mixture of physical and 'firmware' (programmable hardware) locks:

- Most computers have a facility for a password to be entered before the computer boots up. The

© APC and Paul Mobbs, 2002 - released under the GNU Public License

password is held in an area of memory inside the computers circuits, but it is only secure if the person cannot get access to the inside of the computer. If the computers case is opened and the battery inside disconnected, the password will be cleared from memory after one hour and anyone will be able to boot up the computer.

Some (but not all) computers have 'back doors' installed in the computer's firmware. They allow the police, security consultants, etc., to gain access to the system with a secret password unique to each type of computer system. If in doubt ask the manufacturer before buying the system.

- Keyboard locks are small key-activated locks on the front of a computer which disconnect the keyboard from the computer system, making it unusable.

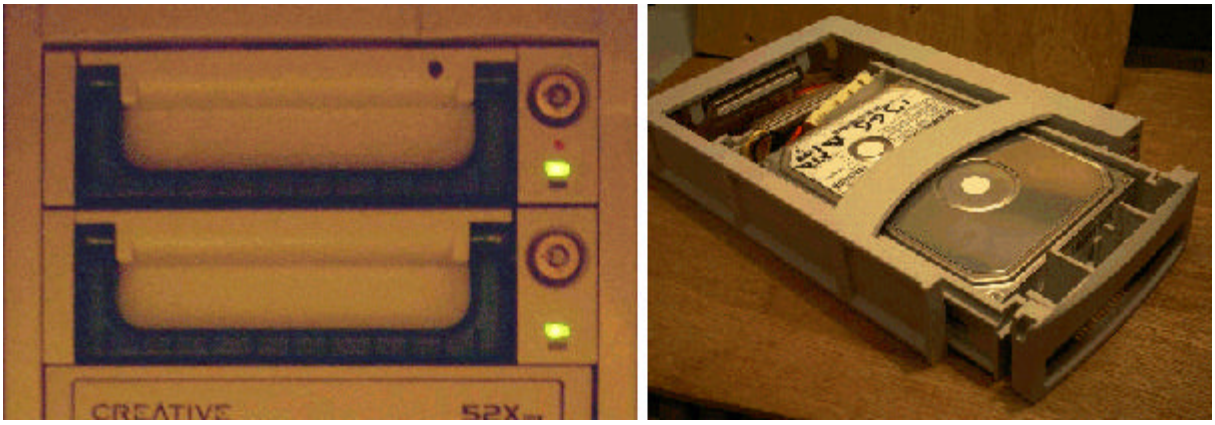
Keyboard locks are easily forced, or can be manually bypassed if someone gains access to the inside of a computer's case - they are therefore no guarantee of restricting access.

- Floppy disk drive locks are flat pads inserted into the floppy disk drive (like a normal floppy disk). Most require a key to fix into place and to remove. If someone tries to remove the lock it will damage the disk drive, making it unusable.

The aim of a floppy disk drive lock is to prevent the removal of data from the system, but they can be easily overcome - for example, by simply replacing the floppy disk drive.

- A removable hard drive rack and caddy allows for the entire hard disk of the computer to be easily removed and locked away for safe keeping, or taken away from the office altogether. This is the most secure option for computer systems. If the hard disk, containing all the data on the system, is removed, there is no possible way to access it.

Hard drives can be easily removed by unwanted visitors, so get disk racks with key locks to hold the hard drive caddy in place.



Left -Removable hard drives, with key locks, installed in a computer.
Right -a hard disk rack and caddy, with the hard disk installed, before installation in a computer

- Lockable cases are included on some computers. They prevent access to the inner workings of the computer system, but the locks are often of low quality and can be easily forced. However, you can buy high-tensile steel locks that clamp the case together. Some of these also double up as frames (or small cages with a high-strength lock on the front) that lock the computer to a desk, floor or other surface. They are good anti-theft devices because not only do they prevent removal of the

© APC and Paul Mobbs, 2002 - released under the GNU Public License

computer, and they also prevent people getting at the expensive and easily portable components inside the case.

How far you need to go in securing your hardware will very much depend upon the type of threats you are guarding against:

- Opportunist theft - Locking your equipment to a desk or to a work surface is the most secure option. With a little more difficulty and a little less security, you can also secure by fixing screws from inside the case, through the base, into the work surface below.
- Targeted theft - If someone is after your data, they can circumvent any hardware security features, with the exception of removable hard drives. To protect your data, install a removable hard drive, and remove the hard drive to another, more secure location at the end of the working day.

Hardware, in particular the monitor (the display screen) gives off strong radio waves. These can be picked up using special equipment; just a few hundred metres from where you are using your computer, someone can reassemble an image of what you have on your screen at any time (the military code name for this type of system is 'tempest').

If you are concerned that the material being displayed on your system is so sensitive that you cannot risk any disclosure, you should pay for an extremely expensive *'shielded' monitor*. This has a metal mesh running inside the case, and the glass screen is interlaced with fine wires, to prevent the emissions of radio waves. The easier option is to use a laptop computer, which is far less liable to give off large amounts of radio waves from the display screen.

Level 4: Your Operating System

How you make your operating system secure will very much depend upon the threats that you are likely to face. If you want to secure against *opportunistic damage or theft*, operating systems do not provide a great deal of additional protection. If you want to protect against *theft of or damage to data*, the operating system is very important.

Windows (the most popular desktop operating system in the world) has next to no security at the operating system level:

- User accounts can be easily bypassed
- Once access to the system is gained, all areas of the system are open to the reading and writing of data.
- Some versions of Windows, such as NT, have better security and segregation of parts of the system between different users. But the Windows operating system is notoriously fickle when it comes to security, and most of these security features can be bypassed.
- Because Windows does not prevent users of the system from having access to files and programs that make the operating system function, it can be easily damaged or corrupted by mistake.
- Windows programs, in particular the Microsoft Outlook email program, are highly susceptible to computer viruses.

The best form of security available at the operating system layer is *encryption* of the hard disk.

If you use *Windows* you should be aware that:

- The disk encryption that comes with the later versions of the operating system is not very secure, and can be easily 'cracked' by the police or security consultants.
- It is possible to get programs to encrypt portions of the hard disk on Windows systems, but they

© APC and Paul Mobbs, 2002 - released under the GNU Public License

are not totally secure; there are always areas of the disk where your data may be backed up in an unencrypted form, and so available to anyone with the knowledge of how to interrogate the hard disk.

- Hard disk encryption uses a lot of processing power, and therefore should only be used on more powerful computers; it will significantly decrease performance speeds on slower computers.

A simple and effective way of protecting your system when computers are running is to use a screen saver with password protection:

- If you leave your computer, and are delayed for longer than you expect, the screen saver will start up after a few minutes and prevent others viewing your work, removing data or corrupting the contents of your computer.
- If you are working on something sensitive, and want to leave the computer, you can run the screen saver to lock out access.
- If you leave to answer the door, and it happens to be a raid, the screen saver can lock up the computer to prevent access. This requires a short screen saver time limit to be effective - no more then three to four minutes.

Screen savers are not wholly foolproof. There are ways to circumvent them, although it would take professional assistance to do so.

Level 5: Protecting Your Data at Program Level

Most program-level security uses passwords to prevent access to word processed or database files.

The password protection systems available with most mainstream office programs are completely insecure. They work by simply refusing access to the file; because they do not encrypt the contents of a file they still allow the raw data to be read by anyone who knows how.

Other systems work by 'hashing' the data. This is a very weak, low-level form of encryption that is easily cracked. You can find programs available over the Internet that enable you to do this.

The main form of program-level security is the use of *secure encryption programs*, such as PGP, to encrypt files (see the briefing on *Using Encryption and Digital Signatures*).

You should not rely on encryption for total security. When editing data, your computer uses areas of the hard disk for *temporary files*. These files are not fully erased from the hard disk when you close the file you're editing, and so for some days afterwards, parts of the file you were editing will be available to anyone who knows how to access the raw data stored on the hard disk.

The only certain safeguard against this is to *encrypt your hard disk at the operating system level*.

A less reliable option is to use a program that *scrambles* or *overwrites* all unused areas of your hard disk with random data and so completely erases any temporary files. If you use this sort of program, you must remember to run it on a *regular* basis, otherwise you will jeopardise your security.

The other essential aspect of program-level security is maintaining the system and protecting against computer viruses. There is a variety of specific programs available to help you do this:

- Use clean-up tools for your hard disk, to repair or remove corrupted data from the system. This will make your system faster and more reliable, but also helps security. When files are deleted they are not really deleted -they are just removed from the index of files on the disk.

© APC and Paul Mobbs, 2002 - released under the GNU Public License

- You can get programs that shred files by overwriting them with random data.
- Remove damaged files (by using utilities like Scandisk for Windows), and reorganise the files on the disk in a more logical order (by using utilities like Defrag for Windows). This will make it harder for intruders to access files you have deleted or any temporary files created when you edit data.
- Use an anti-virus program for systems that are susceptible to viruses. This is primarily those using the Windows operating system and Microsoft-based Internet and email software.

Anti-virus software is no failsafe guarantee of protection. New viruses arise all the time, so if you use anti-virus software be prepared to pay for regular updates.

The majority of computer viruses target Windows, and are initiated through Microsoft's Outlook email program. You can improve security by using an alternative to Outlook for email, or even using an alternative operating system that provides a higher level of security, such Apple Macintosh or the Linux operating system for PCs.

- Encryption programs often have other useful functions contained within them. Some have shred functions that completely erase data from the disk (see above). Others have scrambling functions that overwrite all unused areas of a disk to remove deleted files and any temporary files created by the operating system (see above).
- Most programs have a setting enabling you to automatically save and back up copies of files that you are working on at regular intervals. This is a good way of guaranteeing against the loss of information if your computer crashes whilst you are working, or if you accidentally delete a large quantity of data and cannot 'undo' the operation to put it back. Creating back-up copies also means that the older version of the file can still be accessed. This can be useful if you accidentally edit the wrong file, delete data or a main file and cannot recover it.

Persistence

Paper records are easy to destroy. They can be shredded or pulped, or sensitive sections can be blocked out with indelible ink. But computer data can be more difficult to deal with:

Computers store large quantities of information very effectively. As we discussed above, even when files are deleted the data remains on the disk unless you take steps to 'shred' the file. The 'persistence' of this data can prove incriminating to those whose work attracts the displeasure of the state. Persistence also presents a risk to personal privacy. The persistence of information, therefore, may jeopardise your security.

- Problems of persistence arise particularly where you back up information to write-once disks, such as write-only CDs (CD-Rs). These cannot be erased. Instead they must be carefully destroyed (the best way to destroy a CD-R disk is to break or cut it with a guillotine into four or more pieces).
- Other backing-up media, such as tapes or large capacity disks, should also be disposed of very carefully at the end of their working lives.

Often we dispose of backing-up media because they have failed to work. But even though the media may have failed, experts can still recover data from the undamaged or uncorrupted areas of the media. For this reason failed media should be physically damaged to render them completely unreadable before disposal.

- If you have a hard disk that has failed, magnetic erasure is not reliable. The most secure erasure option is to unscrew the steel case that protects the hard disk and then split the hard disk's plater into quarters using a chisel or other heavy-duty cutting tool.

© APC and Paul Mobbs, 2002 - released under the GNU Public License

- CD-ROMs should be cut or sawn into thin strips (some heavy-duty paper shredders will do this).
- Tapes should be removed from their cassette, the spool of tape then cut in half, and the small strips of tape then randomly dispersed in other refuse.
- Floppy disks can also be a problem because people have a tendency to send each other floppies containing files without giving any thought to what was held on the disk previously. If the data held previously was not fully erased by using a shredding program, or by conducting a full re-formatting of the disk's file system, the information will still be on the disk. It can be read by anyone with the required skills and computer software.
- You should also pay careful attention to the disposal of computer systems and components when they reach the end of their lives. Hard disks will not only contain highly sensitive and personal information; they may also be the means by which you protect the security of other information you hold, such as passwords or encryption keys. Merely deleting files from the disk is not enough.

Before disposing of any computer, thoroughly erase the hard disk by using a file-shredding program. Otherwise, replace the hard disk with a new one.

Email and the Internet

The use of *email and the Internet* to send data also presents problems of persistence. Depending on the requirements imposed by law, some Internet Service Providers will store some or all or the data you move over the Internet. Therefore not only may the *text* of the messages you send be available, but perhaps the *files* you attach. The only solution to this is to send sensitive information using *encrypted* messages or files.

Even so, the fact that you have sent information across the 'Net will always generate *communications data*. Communications data is the description of your information transactions on the Internet - dates, times, addresses and the quantity of information passed. Communications data is increasingly being used as a means of covert surveillance by states and security services.

Going beyond passive security - counter-surveillance

Securing the space where you work is the first objective. If anyone can walk in and use your computers and other equipment, you have no security. But after that you should consider developing systems that actively seek to avoid the potential for the surveillance of your activities.

The first thing to concentrate on is the security of the computer itself. As well as securing the operating the operating system, described at length earlier, you should take steps to secure the hardware. Some computers have locks on the case. Those that do not can be secured by fitting some sort of lock to the case.

An option to secure not only computer cases but any type of cased equipment it to provide a 'seal' on the screw or bolts. Take a very fine brush, and a pot of model-makers enamel paint with the colour chosen at random, and paint a small line over the minute gap between the head of the screw and the case of the enclosure (but do not paint over the head of the screw!). Then, if the screws are ever undone, the paint will split and the tampering will be obvious. The reason for choosing a random colour is that any attempt to redo the paint seal will be foiled unless they can match your colour.

You should assume that all mechanical locks can be picked by professional surveillance operatives. Therefore do not assume that good locks will secure your working area. Instead seek to secure the

© APC and Paul Mobbs, 2002 - released under the GNU Public License

workplace 'in depth' so that even if access is gained to the working area, access to information can still be frustrated. There are various options to do this:

- Ensure that you have good quality locks. On internal rooms the locks are usually of a lower quality. You can improve security by using higher quality locks on internal doors.
- By having a locked area within the space where sensitive material is kept you make it harder to access your sensitive material. If this too can contain cupboards or storage spaces with high quality locks that will help too.
- An alarm system on the doors or windows can provide good security. But some sort of motion-detection is a far better means to provide an alert if someone attempts to access an area. Also, whilst alarm systems are expensive, motion detectors provide a cheap means, within minimal need for wiring and alteration of the fabric of the building, to cover a large area.

Those who wish to access your information will, if required, smash their way in. But the object of good space security is to make covert access harder, as well as preventing general theft. Covert access is more of a problem because it does not provide you with a warning that someone has attempted to make an entry. Good security around your workplace should primarily be aimed at highlighting any access attempts. Having detected them you can step-up your security.

If there are any attempts to access your workplace you should always conduct a thorough search of the area. Your first goal should be to check that all your computers are intact. Then you should check that you data back-ups and installation disks are intact and uncorrupted. If you find that the computer has been tampered with to gain access, you should assume that the computer may have been uploaded with a virus or other rogue program. You should disconnect it from any networks before booting the system, take off any data files that cannot carry viruses, and then wipe and reinstall the system.

After dealing with the immediate problems of any attempt to access your work space, you should then systematically check all your communications equipment. The cases of telephones and other communications equipment can be secured using a small line of paint on the screws that secure the case, as described above. This will show any attempts to open them up. But you should also check for any damage to the walls, ceiling or floor of the room, or for any attempts to mask damage with paint. This may give away attempts to install some sort of surveillance device. You should also check the mains power sockets as these provide both a space and a power supply for surveillance devices.

If you have access to the equipment, you might also sweep the area for radio transmitters. But unless you have professional sweeping equipment, this is likely to only pick up the low-tech/amateur style listening devices.

Counter-surveillance is difficult to described in a general way. This is because, unlike general computer security, it is highly specific to the location and layout of the areas/equipment that need to be protected. There is further information provided on this issue in briefing no.7 - Living Under Surveillance.

© APC and Paul Mobbs, 2002 - released under the GNU Public License

Free Documentation License:

Copyright © 2001, 2002 Association for Progressive Communications (APC) and Paul Mobbs. Further contributions, editing and translation by Karen Banks, Michael de Beer, Roman Chumuch, Jim Holland, Marek Hudema, Pavel Prokopenko and Pep Turro. The project to develop this series of briefings was managed by the Association for Progressive Communications, and funded by OSI.

Permission is granted to copy, distribute and/or modify this document under the terms of the GNU Free Documentation License, Version 1.1or any later version (see http://www.gnu.org/copyleft/fdl.html for a copy of the license).

Please note that the title of the briefing, and the 'free documentation license' section are protected as 'invariant sections and should not be modified.
For more information about the Participating With Safety project, or if you have questions about the briefings, contact secdocs@apc.org