Data Protection and Security for Personal Computers

A manager's guide to improving the confidentiality, availability and integrity of data on Personal Computers and Local Area Networks.

By Robert Schifreen

"Ignorance is precious, for once lost it can never be regained."

Elsevier Advanced Technology
Mayfield House, 256 Banbury Road, Oxford OX2 7DH, UK

Elsevier Science Publishers Ltd
Mayfield House, 256 Banbury Road, Oxford OX2 7DH, England

Robert Schifreen
TTK Technical Publications Ltd
10 Barley Mow Passage, London W4 4PH, England

ISBN: 1 85617 163 9

Printed in the UK by Professional Book Supplies, Abingdon, Oxon

THE SMALL PRINT

The contents of this Guide are believed to be correct at the time of writing. However, the publishers can accept no responsibility for loss of, or damage to, computer data caused by errors or omissions contained in the pages that follow.

The author of this Guide makes no apology for using the word "data" as both a singular and plural form of itself. Strictly speaking, an item of information is a datum and a collection of these are known as some data. However, English is a living language and there is little to be gained by refusing to move with the times. Unfortunately, however, no adjective has yet been coined to describe someone who steals information from a PC without the permission or knowledge of the owner of the information. I have used hacker, thief and data thief interchangeably; you will no doubt have some more suggestions of your own.

Obtaining Further Advice

In a general purpose Guide such as this, it is impossible to give specific advice that will be applicable and relevant to every type of company in every area of business.

Should you wish to receive detailed information, designed to be directly relevant to your company, its methods and its areas of business, please contact TTK Technical Publications. We can provide confidential consultancy services in all areas of PC security. For details please call +44 (0) 81 995 9845 during office hours or write to TTK Ltd, 10 Barley Mow Passage, London W4 4PH.

Acknowledgements

Many thanks to Wendie, Debi, Helena, Paul, Andrew, Keith, Steve and everyone else involved in proof-reading this Guide, making it look presentable and suggesting areas for improvement. I could have managed without them all, but I'm glad I didn't have to.

This Guide was produced and formatted with WordPerfect Version 5.1 and a DES program was used to encrypt the document while it was held overnight on the PC in my office.

The Guide was backed up onto two separate floppy disks every night, one of which was kept in my car and the other at home. WordPerfect's automatic timed backup facility was used to back up the document file every 15 minutes while I was working on it, in case the PC crashed or there was a power failure. I also kept a copy of the Norton Utilities within reach, in case my hard disk developed a problem.

As it turned out, the PC never crashed, the hard disk behaved impeccably and there were no power failures. That's just the way it goes, most of the time.

FOREWORD

I should start with two admissions about the content of this Management Guide.

First, there are many security-related topics that this Guide makes no attempt to cover, except for a brief mention in passing. Because this Guide is primarily about the security of data on stand-alone PCs and local area networks (LANs), you will find little information about the hacking of large mainframe systems. If you want to read yet more amusing anecdotes about Trojan Horses, Salami Techniques and cash-dispenser frauds or yet another account of the Great Prince Philip Prestel Hack, I refer you to the many books on the subject and to the front pages of the weekly computer press.

My second admission is more personal. I was, once, a hacker. I never denied it. For a brief period in 1985, while the Court of Appeal and the House of Lords deliberated, I even had a conviction for it. However, don't think for a moment that I am some kind of modern-day super criminal with the magic ability to penetrate any computer at the touch of a button or the twist of a telephone dial. There was nothing special about the techniques I used to obtain access to computer systems that were not mine. I simply waited for people to leave doors open, then slipped inside. Having made notes on the method used, I then quietly left.

If you are worried about taking security advice from an ex-hacker, then please don't be. If my targets of old had read this Guide, my attempts at hacking would have been totally fruitless.

Several years after my arrest, I still think as a hacker thinks. I still peer under managers' desks during business meetings to look for the passwords that are frequently taped there. I still attempt to walk past receptionists to see just how long it takes before anyone questions my presence in a building. The aim of this Guide is to explain to you how a data thief thinks, so that you can protect your company's property while it's still in your possession.

I've been invited to speak at a number of seminars and conferences since my arrest, to explain what I did and how I managed to do it. Even the boards of a multi-national oil company and a high street bank approached me for general information. It was frequently indicated that, while such companies would not be keen to show me around their computer installations so that I could point out the weaknesses, an in-depth report about what I consider to be today's major computer security weaknesses would be appreciated. Hopefully, what you are about to read will fill that need.

As you will notice, the majority of the advice given here is preventative in nature; only one chapter is devoted to recovering from problems. This is deliberate; you should not need to read it if you have followed the advice in the remainder of the Guide.

Robert Schifreen
London

INTRODUCTION

Every month, it seems, a new book appears claiming, once again, to be the ultimate guide to computer security. The advice they give is usually good advice, and is well worth following. But too often, security text-books give text-book answers. One, for example, contains a section about erasing highly-sensitive data from hard disks. The suggestion is that the reader turns the hard disk unit "into small ingots, using an oxy-acetylene torch". While this method of erasure will certainly defeat even the most determined hacker, there seems little point in suggesting its use. Sales of oxy-acetylene burners to DP staff are few and far between, though I am reliably informed that at least one department of the Metropolitan Police in London uses one for just this purpose.

This Guide, therefore, takes a unique approach to giving advice on data security. It doesn't give textbook advice. Instead, it gives advice that can be practically carried out by any competent manager or his (or her) staff. Human nature, time constraints, office politics and cost factors, amongst others, have been taken into consideration. We all appreciate that forming committees, drafting plans and spending money is one way to increase security. However, these actions are not always easy to take in a company of any size. This Guide, therefore, assumes that you want practical advice that will not cost a lot of real money.

As the following pages will show, you can protect the data in your company without recourse to high-temperature welding equipment. All it takes is knowledge and inside information, which is what you are about to gain.

If you require further information about any product, or type of product, mentioned in this guide, or you wish to know whether a product is available to perform a certain security-related task, please call +44 (0)81 995 9845 (during office hours). We have a large collection of reference books and product catalogues and will gladly search them for you.

Why You Need This Guide

Of all the computer security books and awareness-packs that currently exist, few are dedicated purely to data protection on PCs. The majority cover mainframes, telephone hacking and a lot more besides. While it is true that major international conglomerates rely on one or more mainframe computer systems, almost every company has at least one PC. The ridiculously low prices of these machines, and the immense local processing power that they can bring to an employee's desk, has led to a massive increase in their use worldwide.

But stop and consider, for a moment, the security aspects of this situation in your company. Do you actually know:

- How many PCs you have?
- The whereabouts of all PCs?
- Who's using them?
- What they are being used for?
- How much unlicensed software is in use?
- How many undiscovered viruses are lurking on the machines?
- What data is being stored?
- Whether all important PCs are backed up?
- Whether the integrity of the backups has been tested?

And do you really know how many of your staff have, in the last year or so, seen a floppy disk labelled "sales figures" lying around, and thought "that looks interesting. No one will notice if I take a quick copy to look at on my machine"?

Enough data to kill off a large international company can fit on a single floppy disk. And such a disk can be copied in just a couple of minutes. Only in exceptional cases will you ever know that it has happened. It's up to you to prevent and detect such acts. The purpose of this Guide is to show you how.

Horror Stories

The world is full of amusing anecdotes about data security, most of which are told by security consultants who wish to prove to you that you need their services. My favourite concerns a company which installed and operated vending machines in the gents lavatories of around 5000 London public houses. Like most modern businesses, they used PCs to run the company. A database was used, which recorded the address of each pub containing a machine, and the dates on which the machines should be refilled and the money container emptied.

One day, the PC's hard disk crashed. No one had made any backups, and there were no printouts. The database was found to be corrupted and the PC would not allow access to it. All the company's assets were fixed to the walls of 5000 pubs, yet there was no record of where the walls were. Additionally, these machines were rapidly being filled with money, yet the company's staff could not collect it as they had no idea where it was.

At great expense, the company called in the services of a data recovery professional who managed to recover most of the database. Eventually the list of names and addresses was recovered, but not without the loss of a week's trading and the huge fee from the consultant. Needless to say, this is one company that now knows the true value of taking precautions.

Remember that the true cost of a PC is not the replacement value of the hardware, but the data that the machine contains. And that predicting a computer problem is only slightly harder than predicting the precise moment at which a light bulb will blow.

How To Read This Guide

There are many hazards that threaten the data on PCs. Malicious and accidental deletion of files. An outbreak of a virus. A hacker loose on your computers. A faulty machine. Or a set of backups that turns out to be unreadable. Each is a distinct risk and each risk should be tackled and secured separately. The press tend to consider hacking and viruses as one and the same thing. They are not; a hacker is someone who attempts to break into your computer to steal your programs or look at your data. A virus is a program that finds its way into your system and damages the data it finds.

The contents of this Guide have been split into several sections, each dealing with one aspect of security. Each section can be read separately. If you don't have any formal data security procedures in place at present, start with the section that deals with the subject which poses the greatest risk to your company and its data. Use the information in the Guide to formulate and implement a policy that deals with this threat. Only when this is up and running and most of the teething problems have been sorted out, and when you are satisfied that the newly-imposed security policy is actually going to provide real protection, should you attempt to secure another area of your business.

Certain key facts and warnings regarding PC security have been put in italics in the text, and special note should be taken of these passages as they highlight some of the most common problems.

If you feel overwhelmed by the quantity of information in this Guide and do not know where to start, acting on the passages in italics will put you well on the way to creating a far more security-aware company.

THE ULTIMATE GOAL

The national and computing press carry regular stories about computer hackers who penetrate the financial networks and manage electronically to siphon half a million pounds into a Swiss bank account. One also reads of stories involving hackers who tap into the life support machines at a hospital and wipe out a paediatric ward, or who manage to dial into NASA and turn orbiting satellites around.

There's no doubt that computer hacking does take place. However, the risk of a hack into your computers is relatively insignificant. *At least 75% of crimes which involve a computer are plain-and-simple inside jobs, involving staff who make fraudulent use of a PC or terminal.*

It is this unauthorised use of your computers that must be detected and eradicated. Don't think for a moment that you need take no action because that sort of thing doesn't go on in your organization. It's extremely likely that that sort of thing does go on, and has been going on for a long time. Just because your personnel department turns off the PC at night, and the salary files are still there in the morning, doesn't mean that no one has rummaged through the personnel manager's hard disk during the evening. And if your security system amounts to locking the door of the personnel office, this is inadequate.

Not all data thefts happen as a result of a premeditated act. The majority take place because a person sees a vulnerable PC and becomes curious about its contents. Remember: A thief is simply an honest man with an opportunity.

Your ultimate goal as a senior manager, and the goal of the person to whom you delegate the security responsibilities of your organization, is to achieve three things:

- *The confidentiality of the data held on the company's PCs.*
- *The integrity of that data.*
- *The availability of that data to those that need it and are authorised to use it.*

An effective security policy needs to take into account all three of the above points. Compromises will have to be made in order to provide a level of security that makes a fair job of keeping out intruders but does not make the information inaccessible to authorised users.

The Guide covers protection from both accidental and deliberate data loss; it is up to you to decide whether you wish to concentrate on just one of these or attack both at the same time.

1 | Where To Start

That you have purchased a copy of this Guide indicates two key things: first, you are concerned about the confidentiality, integrity and availability of the information in your organization. Second, you wish to take steps to increase the levels of protection.

So how do you go about improving the level of security? Some form of risk analysis (a.k.a. risk assessment) is called for. Professional risk analysis consultants are expensive, and the textbooks tend to teach you everything about the subject except how to go about actually doing a risk analysis for yourself. Employ a consultant by all means, but first use the following simple steps to get an overall picture of your company's current security situation and the major weaknesses that exist at present.

Analysing The Risks

Start by making sure that you have a thorough understanding of your company's business. Make sure you know:

- What the company does, and how it does it.
- What information, if any, it needs from outside.
- What information is generated by each department.
- Where data is used to make business decisions, whether the integrity of that data be proved.
- Details of your major rivals.
- The value of your company's data to your rivals.
- How and where information is processed.
- Who might want to steal or destroy your data.
- How long the company could survive without access to its data.
- What you will lose if data is lost or copied.
- Who has access to each type of data.

- How sure you are that competitors do not already have copies of crucial data.
- Do you have a disaster recovery procedure in place?
- Where is the information that is most crucial to your business?
- Whether these crucial computers are protected adequately.
- Whether all important data is backed up, and are the backups known to be intact?

This list-making task is an important one and must not be hurried. Only by drawing up detailed answers to the above questions can you begin to understand where the major risks to your company's data lie and how much effort and money need to be spent to protect that information.

Priorities

Once you know where the data processing takes place, and the type of data that is processed, decide which areas should receive your attention first. Draw up a table of all the different types of information that is available on your company's PCs, who has access to the information, and who needs access to the information.

Give serious consideration to which class of information is currently most valuable and most under-protected. The various chapters in this Guide will help you to decide which data is most under-protected, though only you can decide which is most in need of extra protection. Categories of data that should be considered as being in need of improved security include mailing lists, sales data and forecasts, personnel records and budgets. For further information, see the chapter on Access Control which starts on page 85.

Once the table is complete, and you know the categories of information which are processed, you can decide on one or two areas to work on. Do not be tempted to work across the whole organization at one time; stick to one PC, or one department, or one type of information at a time.

Monitoring Your Progress

While you are working on improving PC security in your company, keeping detailed records is important. These records should allow you to see, at a glance, the status of all ongoing work.

Most Guides of this type include a few blank pages at the back which are headed "Notes". Such pages are singularly unhelpful and none is included here.

To keep notes, rule up some sheets of paper or prepare a word processor (or spreadsheet) file. Each sheet should include space for the project name, and there should be a separate sheet (or file) for each project. Typical projects are:

- Ensure that all PCs are backed up regularly.
- Evaluate backup programs.
- Train staff to recognise viruses.

One suggested way to head up the columns on the sheet or file is:

Date	Today's date
Who	The staff member concerned
Action	The action being taken, or the action that the staff member has been asked to take
Page	A reference to the page in this Guide
Status	The current status of the action.

Ignore The Press

When deciding on where the risks to your corporate data lie, ignore everything that you read in the press and that you see and hear on television and radio.

Mass-media journalists are interested in giving news value to a story, and this is almost always done at the expense of the technical facts. It's also worth remembering that journalists are trained to take the basic facts of a story and present them in a package that anyone can understand - a television reporter would feel equally capable of interviewing a skate-boarding duck as a programmer who had just lost his life's work through a computer virus.

If stories appear in newspapers, use this as a starting point for your own research. Talk to colleagues and to end-users in the real world to discover whether there really is any truth in the story, and whether you need to be concerned.

It's worth bearing in mind that those "experts" who are quoted in newspaper reports and on television news programmes often have an axe to grind. When a virus outbreak occurs, or when hackers penetrate a government network, it's normally the suppliers of anti-virus or access control software who are interviewed. It is clearly in their interests to make the problem seem worse than it really is.

2 | Security And The PC

This Guide is concerned primarily with the protection of data on PCs. The following chapter presents a non-technical introduction to the constituent parts of an IBM-compatible PC, with special emphasis on the security risks associated with each component. Not all of the components listed here will be present in your company's PCs. For example, laptop computers have the CPU box, screen and keyboard in one unit rather than as three separate parts. Also, you may not have tape streamers or modems installed on all or any computers.

This section also includes coverage of operating system software. While not strictly a component of a PC, the machine is unusable without such a program and each operating system poses its own security threats.

One rule applies to every part of a PC, and that's the way that it should be physically treated. Modern computers contain complex electronics which are far from unbreakable. There is no harm in taking a PC from one end of the country to the other in the back of a car, but treat it with at least the same amount of protection as you would a fine bone-china dinner service. If you drive over a hump in the road, it's easy to peer cautiously at the back seat to ensure that all the china is still intact. The same jolt may corrupt a small part of a file on a hard disk, or may loosen a chip just enough to introduce an intermittent memory fault in the machine. Such accidents are far harder to spot than a plate which can now be shared among your dinner guests along with the cake it was designed to hold.

The CPU Box

PCs normally have three main parts, namely the screen, the keyboard and the CPU box. The CPU box (central processing unit) holds the disk drives and all the electronics that actually make the machine work. This is the box that normally sits on the desk or under the monitor.

Ensure that the CPU box is placed on a stable surface so that it can't rock. Cleaners frequently treat floor-standing computer CPU boxes in the same way as they treat filing cabinets, and will think nothing of ramming the sharp end of a vacuum cleaner into them every morning. Don't

assume that your particular cleaners know all about computers. Cleaners get ill, just like the rest of us, and it may be that strangers will occasionally be assigned to your particular department.

Cleaners are also fairly ruthless when looking for a socket to plug in a cleaning machine or polisher. Mark clearly any electric plugs that must not be pulled out. It is not unknown for some electrical sockets to be controlled by a time switch so that lighting and heating can be turned off automatically at night and weekends, or for a socket to be wired to an 8 amp or 10 amp circuit instead of being able to provide a standard 13 amp supply. Any socket of this type must be clearly labelled to avoid problems of servers being powered down at the wrong time or of entire circuits cutting out when an employee decides to bring in a portable heater from home.

Ensure that on/off switches and reset buttons are well out of the way and that they cannot be knocked accidentally. The same goes for power cables, which can also be kicked or tangled around a foot.

To prevent machines overheating, do not place them on soft carpets if this would obstruct one or more of the machine's air ducts. Also, allow at least two inches behind the machine to ensure that the air blown out by the internal fan can make a clean getaway.

Most CPU boxes today have a lock on the front panel. This controls access to the machine by disabling the keyboard. If the key is turned while the machine is turned on, the keyboard (and, therefore, the machine) will become unusable until the computer is unlocked. If the machine is turned on while locked, a message will appear on the screen informing the user that the machine will not start up until the computer is unlocked. These locking mechanisms are a useful first line of defence but should not be relied upon to protect data. Nearly all of these front-panel locks can be hot-wired by removing the case of the CPU unit and shorting out a couple of wires with a paper clip. Even computers that are specifically advertised as being impossible to open are, in the experience of the author, easy to break into in this way.

An alternative to the front-panel lock is the password facility as found in IBM's PS/2 range of desktop PCs. These machines let you set a password, and the computer will not power up unless the correct password is entered. The password is stored (in encrypted form) in the computer's clock, because this device is permanently powered by a battery and will not, therefore, lose its contents each time the machine is turned off. However, if the clock is disconnected from the battery for a couple of hours, the password will become corrupted. The PC, sensing this, will not bother to ask the user for it when the machine is next turned on, so the machine will then be entirely open to hackers.

For the reasons just stated, *do not rely on the front-panel lock or the PS/2's password to control access to a PC. Both of these systems are easily crackable and, once cracked, the entire machine is wide open.*

Night Duty

Should PCs be turned off when not in use, or left switched on permanently? There is, as yet, no definitive research that proves which method leads to greater reliability. Some say that the most stress to electronic components is caused when they are first turned on, and that this procedure should be carried out as infrequently as possible. Others say that this is not the case.

In the absence of proven research, our recommendation is to turn off all PCs when they are not in use for more than a few hours at a time. If a PC is left on overnight, the monitor and printer should be turned off if they are not required, to save energy and to lessen the fire risk.

Maintenance Contracts

Where the continued availability of a computer is essential a third-party maintenance contract should be taken out. The more that you are prepared to pay, the faster the maintenance companies will be prepared to arrive on your doorstep in the event of a problem. In this case, fast is defined as four hours while slow means 48. Network servers should always be covered by a maintenance agreement. Whether individual PCs merit such a level of attention must be decided by the people who will suffer in the event of a computer failure. Consider buying a spare PC to keep as an emergency source of spare parts.

Never assume that a person who claims to be a PC engineer actually knows anything about the machines he will be servicing — always ask for reference sites and the names of satisfied customers. The level of service for which you are paying should be agreed in writing and should include details of what will happen if the agreed service level is not provided. For example, how will you be compensated if your server goes down and no engineer arrives for two days?

The Monitor

All PCs use a screen to display their output. Laptop and portable machines tend to use LCD displays, while desktop PCs use CRT units that resemble television sets. The quality of the image that can be displayed is known as the screen's resolution. A typical resolution is 640

x 480 x 16, which means 640 dots (pixels, or pels) horizontally and 480 vertically, each of which can be any one of 16 possible colours. This is one of the resolutions that a VGA-class screen can display.

The greatest security risk posed by any display is obviously the fact that people can see what's on the screen. Ensure that displays are positioned on desks in such a way that guests in an office or casual visitors cannot see what is displayed. Also, do not leave confidential data on the screen for longer than is necessary, even if you are present. (If you leave the PC, even for just a few seconds, clear the screen every time). If the screen has to face a window, watch out for curious people across the street who own a set of binoculars, as well as curious window cleaners.

For PCs that regularly are used to display confidential data, install a screen-saver program. These automatically blank the screen if the keyboard is not touched for a few minutes, thus protecting displayed data from passers by if a machine has been accidentally left unattended. Screen savers normally restore the display when a key is pressed, though some can be configured to ask for a password too. Don't use software that totally blanks the screen, as this makes the machine appear to be turned off and a passing cleaner in need of an electrical socket will have no qualms about unplugging the computer. Opt instead for screen savers which leave a small message on the screen asking for a key press or a password.

Make it known throughout the company that, if the security manager comes across a terminal or PC that is turned on and unattended, he will type an obscene message to the Chief Executive and leave it on the screen. Users will not want to risk anyone hearing of this message so it should act as a deterrent to leaving terminals unattended.

It's possible to read a computer screen even if it cannot actually be seen. The electronic circuits in all computers, though especially the high-voltage components in CRT displays, produce radio-frequency waves which, with the right decoder, can be picked up and reassembled into a picture by someone a couple of streets away. The decoding equipment costs little more than a good-quality stereo radio receiver. You can protect against this form of eavesdropping by ensuring that confidential data is not displayed on screens for longer periods than is necessary.

Where highly sensitive data is concerned, such as boardroom data concerning large takeovers, use laptop computers with LCD screens as these do not give out such strong radio emissions. Also, avoid using laser printers as these produce readable emissions too. There are devices which can be placed alongside sensitive computers. These give out strong interfering radio emissions which claim to obliterate the emissions from the CRT. Consultants to whom I have spoken are of the considered opinion that such add-on devices do not work, and any

machine which needs such protection should be a computer designed with this degree of security from the start rather than having it added in as an afterthought.

Protection from radio-emission eavesdropping normally goes under the name of Tempest, which is the NATO code name for the technology.

It should be noted that, while reading computer screens by radio is certainly possible, it is not one of the most popular methods employed by data thieves. Consider Tempest protection only if the future of your company (or a country's national security) depends on the utmost secrecy.

The Keyboard

The keyboard is normally the only way that data enters the PC, ie it is typed by a user.

There may be occasions when simple access control can be effected by removing the keyboard. For example, the case of a file server in a locked room which is designed to be accessed via the network but not directly. There are two problems associated with this. First, most IBM-compatible PCs use a standard keyboard and connector, so anyone can plug in a new keyboard. Second, Zenith and Dell are fairly unique in that they supply machines that can be configured to run normally without a keyboard attached; others will refuse to start if a keyboard is not plugged in and found to be working correctly.

There's little that can be done to prevent a user plugging his or her own keyboard into a machine that does not have one. Simply use the fact that the machine has no keyboard as a deterrent, and warn staff against the penalties of being found with a keyboard hidden in their jacket or handbag without good reason. A couple of PC manufacturers use non-standard keyboard connectors which could help. Some Olivetti and Epson machines fall into this category.

Keyboard eliminators are available from many electronics suppliers. These are small connectors that plug into a keyboard socket and fool the PC into believing that a keyboard is present and, therefore, allow it to boot up without error. Normally these plug into the outside of the PC, and can be removed and replaced with a real keyboard if there is a need to do so.

For more permanent protection, you can install one of these devices inside the case of the PC and disconnect the real keyboard connector.

Install a hidden switch for emergency use. If this method is used to protect a private machine such as a network server, do not publicise the fact that the server is protected in this way.

It's worth knowing that there are fundamental differences in the workings of old-style PC keyboards used by the original IBM PC and XT (normally distinguishable by having the function keys in two columns down the left hand side), and the new extended keyboards used by the AT and PS/2 (function keys in a row on the top). A keyboard made for one type of machine will not work in the other, though most modern keyboards have a small switch that allows the device to resemble either type of keyboard. The switch will often be labelled PC and AT, and will be found underneath or on the back of the keyboard itself. Although far from foolproof, you can delay the casual intruder from exploring the contents of a PC by changing the position of this switch while the computer is turned off. Most machines will refuse to boot up if this switch is in the wrong position, because it appears to the computer that there is a problem with the keyboard.

Remember that the keyboard is not the only part of a computer capable of receiving input. Serial (a.k.a. RS-232) and printer (a.k.a. Centronics, or parallel) ports can also receive data and, with the aid of a simple program, a PC can be made to accept instructions from a remote machine via its RS-232 or printer port. These instructions include, but are not limited to, sending the contents of confidential files back down the line to the remote machine. Check frequently, but at random, the cables emanating from the back of network servers, and ask at least two independent people for an explanation of any new ones that have appeared since the last check.

Dumb terminals, as used to connect to mini and mainframe computers, frequently have a serial connector so that a printer can be attached to a terminal. Any device equipped with the correct interface can be attached to this port, and data normally destined for a printer can be captured and stored by a PC. To prevent this happening, disable the RS-232 connector in the terminals of those users who do not have a printer.

Floppy Disks

From a security aspect, the floppy disk is the most vulnerable part of any computer system. Today's PCs store 1.2 megabytes (MB) of data on a 5.25" disk, or 1.44 MB on a 3.5" disk. A megabyte is around 150,000 words of text, or 50 small spreadsheet files, or a database with 5000 name and address records. *A disk can be copied in under a minute, and the computer normally keeps no record that a copy has taken place,* but see the Resource Guide (page 155) for ways of monitoring copying.

Copying

When a cassette or LP is copied, each generation sounds slightly worse than the one before it. After four or five generations, the copy becomes uncopyable. Floppy disks do not suffer from this degradation — a thousandth-generation copy will work just as well as the original.

A couple of minutes alone with a PC is all that the data thief needs in order to copy data to a floppy disk. Indeed, he doesn't even need to be alone — can you be sure that when one of your staff asks if he can take a copy of a memo, he or she is not actually copying next year's sales forecasts?

Once data has been copied to a floppy disk, the thief can take it to a safe location and examine and analyse it in his own time. He can also alter that data and replace it without the knowledge of the owner of that data.

Keep confidential data on floppy disks and lock these disks away when they are not in use. If you must keep data on a hard disk for convenience (see below for details of hard disks), then use an encryption (scrambling) system. Scrambling a data file means that, without the correct password being supplied to the unscrambling program, the data is unreadable. In this situation, the thief can gain nothing by taking a copy of a confidential file as he will be unable to crack its code. For example, the word SALARY may appear as Z74JYWQ. Only when the correct password is supplied will the thief be able to understand the contents of the scrambled file. Data encryption is discussed on page 109.

If your organization uses a lot of floppy disks, consider buying easily-identifiable disks. Disks in bright colours instead of the standard black are available from a number of sources, and many suppliers will also print your company name on the sticky label and / or the paper envelope. Having coloured disks means that "foreign" disks that have been brought into the company stand out. Employees will also be less likely to pilfer blank disks, as they are so easily identifiable.

Accidents

So far, this section has talked about preventing the deliberate stealing or copying of data via floppy disks. However, the floppy disk is also responsible for much of the accidental data loss among users of PCs.

A floppy disk can, and frequently will, fail. Even if an LP is quite heavily scratched, a listener can still recognise the music being played. If a floppy disk develops a minor scratch or mark, there's no way that the computer can decide whether the word on the disk at that point is WAGES or PAGES without access to an undamaged copy.

Such problems with floppy disks are rare, but there are certain actions that can exacerbate the problem and multiply the chances of error by a factor of 100 or more. Mishandling a floppy disk, or forgetting to keep it in its protective sleeve when not in use is an example. As is keeping a disk in a hot car, where the continual expansion and contraction will damage the surface of the disk. Window sills which receive direct sunlight or that are atop radiators can cause similar damage.

Storage

Floppy and hard disks work on the principle of magnetism. Minute areas of the disk are magnetised or demagnetised by the disk drive, and this is how data is recorded. Any magnet, or a piece of equipment which contains one, will erase a disk if the disk is placed too close to the magnet. Telephones with bells or buzzers (rather than electronic warblers) contain magnets, as do electric motors, power supplies and loudspeakers, and floppy disks should not be allowed to come within 12 inches of such devices. The same goes for old-fashioned PBX control boxes as found on office walls, as these contain transformers which have been known to damage floppy disks that have been left on top of the case.

Computer monitors contain magnets and they get very warm, too, so these should also be kept away from disks.

In theory, airport x-ray machines should not damage disks placed in suitcases. However, some machines contain powerful magnets. Where possible, request that boxes containing disks be hand-searched instead of being x-rayed. Electric trains, especially those on the London Underground, should not be used to carry your only copy of a valuable disk. Diesel-electric trains should be treated with the same respect, as the diesel engine is simply used to generate electricity to drive large motors.

When using brand new disks for the first time, or when preparing to use a disk that has been locked away for some time, check for any signs of physical damage such as stains or scratches. If a disk is beginning to give occasional errors, copy its contents to a new disk and discard the original.

If a new disk fails to format 100% correctly, discard that disk or use it only for non-essential work such as transferring files between machines. The defect could be caused by a piece of dust — if that piece of dust moves then data will definitely be lost.

5.25" Drive Types

A problem will occur when an office contains an assortment of new-style PCs and old XT-type machines, which use a mixture of 360 KB and 1.44 MB disk drives. It's normally quite safe to use a disk in more than one PC, but *if a disk is used interchangeably in an old-style and a new-style drive,*

there will quickly come a time when the disk is readable only in a new-style drive.

The solution to accidental loss of data on floppy disks is as simple as the encryption solution above. Keep backup copies of important files. In the case of information that you absolutely cannot afford to lose, keep at least two backups, and store them in separate locations. One at home, perhaps, and one at the office. Also, keep a printed copy in a secure filing cabinet if the information is not unmanageably large. Having to retype a spreadsheet is better than not having the information at all.

Alignment Problems

Floppy disk drives (both 5.25" and 3.5" varieties) frequently suffer from a problem known as misalignment. This means that the precise position and angle of the head is minutely different from the agreed standard for IBM-compatible floppy drives. In my experience, such problems are common and are likely to occur in up to 5% of installed drives. However, the problem often goes undetected because a misaligned drive will have no problems formatting, reading and writing disks that will only be used in that particular drive. The problems occur when a disk is taken from the misaligned drive to another and is discovered to be unreadable. There is no easy solution to this problem, except to prevent it happening in the first place. *The moral here is to think carefully before discarding any unwanted PC, especially if its floppy disk drive has been used to create backup disks that you will want to access in the future.*

Labels And Serial Numbers

Starting with MS-DOS Version 4.00, every disk is assigned a serial number when it is formatted. This number is displayed whenever a directory listing is taken. Do not use this number as a way of identifying a disk; the number is calculated from the date and time that the disk is formatted and it is not difficult to create a disk with any serial number desired. (A useful side effect is that you can reverse-engineer the serial number if you need to know when a disk was formatted).

If a user attempts to store data on a write-protected disk, DOS will complain. A frequent response at this stage is for the user to say "Oops, I meant to put this other disk in". He will then swap disks, and press R at the "Abort, Retry or Fail?" message. It must be stressed to all users that *under no circumstances should the Retry option be taken. Instead, the operation should be aborted by pressing A, and the operation started again. This is because of a serious bug in versions of DOS prior to 4.0, which will lead to complete corruption of the second disk.*

Disk Cleaners

Ignore any salesman who tries to convince you that floppy drives get dirty and that your data will be much safer if you buy one of his expensive drive-cleaning kits. Unless you are in the habit of using your PC on the beach or in a flour mill, disk drives are quite capable of keeping themselves clean and the experience of the professionals suggests that cleaning kits introduce far more problems than they solve or prevent.

Boot Options

A security manager should have a basic understanding of the boot-up process on a PC. This is the process where the operating system is loaded into memory. Almost all PCs start by looking for the operating system on the floppy disk in drive A. If a bootable disk is found in this drive, the operating system is loaded. If no such disk is found, the system looks to the hard disk and, if there is still no operating system, the user is asked to insert a bootable disk in drive A.

Few PCs will look to drive B, the second floppy drive, for a valid operating system program. Zenith's range of machines is one of the few exceptions.

Many companies have recently taken to swapping the cables inside any PC that has one floppy drive and one hard disk. The floppy drive can then be made to appear as drive B. The benefit of this setup is that you now have a machine which cannot be booted from a floppy disk without opening the machine. This will reduce the spread of those viruses which spread by creeping into the machine at boot time.

DISKCOPY Weaknesses

You should be aware of the security weaknesses inherent in the MS-DOS disk copying program called DISKCOPY. If a disk is copied in a single drive, DISKCOPY reads the contents of the disk into the PC's memory and then copies it out again onto another disk. Once the operation is complete, much of the information from the copied floppy disk is now in the PC's memory and will not be deleted until that memory is overwritten by another program. It is possible to load in a small program that will copy the PC's memory to a file, thus producing a copy of a lot of the information from the copied disk. Although the information recovered will not be divided into files for use directly with the application packages, it can be deciphered easily by a PC expert.

This knowledge can be useful to a thief. It can also be useful to a security

manager who suspects that a particular PC has been used to copy a floppy disk in the recent past.

The Hard Disk

The hard (or fixed) disk unit is where most data and programs on PCs are stored. The capacity of a hard disk is measured in megabytes (1 MB is 1,048,576 characters), and today's hard disk units typically store between 20 and 600 MB. Data on a hard disk must be protected if unauthorised use or accidental loss of the data is to be avoided. See the chapter on Access Control (page 85) for full details.

Floppy disks and hard disks should be subjected to the same levels of protection. For details, see the section on Floppy Disks above (page 10). Remember that a hard disk unit can fail, and it is extremely rare for a hard disk not to suffer at least one severe data loss in its lifetime. Even if the drive survives mechanical catastrophes, there is a chance of a software bug corrupting certain areas of the disk. Although backing up a hard disk takes longer than a floppy, it is an essential task that must be performed regularly. There are ways of speeding up the backup process, which are explained in the chapter on Backups that starts on page 61.

Modern hard disk units are tough enough to be installed in laptop machines and for them to withstand the occasional jostling as you walk onto a train. Further, almost all modern laptop machines will have hard disks that automatically park (ie lock in position) the head when the machine is turned off. The head is the device which actually reads data from a disk, and it moves across the disk like a stylus tracks across a record. Unless the head is locked, and locked in a position such that it bangs against an unused portion of the disk rather than an important data file, you are guaranteed to lose or corrupt data if the device receives a knock. Therefore, it's essential that hard disk units are parked before they are moved, and that the correct parking program for that particular hard disk is used. Machines that don't come with auto-parking disk units will normally be supplied with a program called PARK, HDPARK or similar.

If a PC is to be used as a network workstation, consider the use of diskless PCs for this task. As the name implies, these machines have no hard or floppy disk units at all, yet are otherwise identical to a standard PC. All software loading is performed across the network, so data and programs can be accessed easily. However, the lack of local disk units prevents the user from copying data that has been sent to him by the network.

A switch to diskless workstations is highly cost-effective where users have PCs with hard disks but the hard disks are used purely to store a

software package to allow access to the LAN. This also helps to maintain the security of LAN-based data too. See the discussion of software audits, which starts on page 104, for ways of detecting hard disks which contain few or no application packages.

If a user is performing data analysis on the network, he will need access to the data file in order to run the analysis programs. This means that the whole data file could be copied to a floppy disk and taken from the company if the workstation was equipped with a floppy disk drive. In such cases, it is advisable to use a product which encrypts the database file while it is held on the server and only decrypts it for a brief moment while the analysis is performed. A specialist dealer or distributor should have information on such products.

As an alternative to the diskless PC, there are several removable hard disk units on the market. These have the capacity of normal hard disks, but can be removed from the computer just like a floppy disk so that they may be physically locked away in a safe when access to their data is not required. There are two types of removable hard disk. In the first type, the disk and the head are both contained in the removable cartridge. The other type of cartridge contains just the disk platter and the head remains in the PC. This latter system is to be preferred, because no moving parts need to be carried around and risk being knocked. It's cheaper, too, because you only need one set of heads per computer. The most common of the platter-only type of removable hard disk is the Bernoulli system.

One common misconception about hard and floppy disks is that, once a file has been deleted from a disk, that file cannot be recovered. In fact, *a file that has been deleted with the DELETE command under MS-DOS can be recovered, completely intact, in about three seconds.* Indeed, there are several widely-available programs on the market that will do this and one is even supplied as standard with MS-DOS version 5.0 and above. While this is a useful property of the PC in the case of files that are accidentally deleted, it also poses a severe security problem.

MS-DOS divides a disk into two main areas. The first is a small area known as the directory. This contains a list of all files on the disk, plus information that allows MS-DOS to find each one. The second area contains the files themselves. When a file is deleted, MS-DOS does not wipe the entire file. Instead, it replaces the first character of the file's name in the directory with a special character that does not appear in the alphabet.

When DOS wants to create a new file and needs some space on the disk, it will re-use the space occupied by files whose directory entry starts with this special character.

It follows, therefore, that until the space is actually re-used, everything but the first letter of the file's name can be recovered. And this is exactly what can be done. As soon as the first letter has been replaced, the file magically reappears and can be copied and accessed as before.

Journalists who review PCs for computer magazines are well versed in the use of programs for recovering deleted files from hard disks. The speed at which one machine manages to find its way around the offices of the UK's leading magazines has, in the past, led to some interesting discoveries being made. Whenever you delete a file from a floppy disk before throwing it away or giving it to someone else, or whenever your company disposes of an unwanted PC, do not rely on deleted files remaining confidential. Even if the disk has been reformatted. There are programs that will thoroughly erase a disk, and these programs should always be used in favour of the DELETE command where private data is concerned. See the sections on encryption (page 109) and secure erasure (page 97) for more information.

When a disk is formatted the computer asks if you would like to assign a volume label to the disk. This is a word or phrase of up to 11 letters and/or numbers. The volume label is displayed whenever the user lists the disk's directory. Before MS-DOS will allow a hard disk to be formatted (thus erasing all the files on it), the system asks for the volume label and will refuse to format the disk unless the label is typed correctly. For this reason, all hard disks should be assigned a volume label as this offers an extra level of security in the event that the user mistypes the FORMAT command when formatting what he believes to be a floppy disk.

A hard disk that was not given a volume label when it was formatted may be assigned one at any time with the LABEL command.

Tape Streamers

A tape streamer, sometimes called a streaming tape unit, is a storage device that works like a cassette tape recorder. The tape cartridges typically hold anything upwards of 40 MB and are far cheaper than removable hard disks. However, they are far slower than hard disks, for the same reason that it's faster to locate a particular audio track on an LP or CD than on a cassette tape.

Tape cartridges are used primarily as backup devices. Although it can take half an hour to back up a 40 MB hard disk to a tape streamer, the process can be totally automatic if the cartridge is of a sufficient capacity, and the job can be performed at night while the machine is unattended.

Tape streamers are usually internal devices which fit inside a PC like a floppy disk drive, connected by a plug-in card. External plug-in units are also available, which simply plug into the printer port of any computer and no interface card is required. Such a unit can easily be shared among lots of PCs and provides a relatively quick way to back up a number of machines that are not connected to a central network.

Few tape streamers offer any security facilities, so special care should be taken to ensure that tape cartridges containing valuable backups are kept securely and can always be accounted for. Highly confidential data on a hard disk should always be kept only in encrypted form, but remember that encrypted files on a faulty backup tape will be very difficult to retrieve if a problem arises.

Tape streamers are fairly reliable devices, though there can be problems if some basic precautions are not taken. *Once you have backed up a hard disk unit to a tape streamer, never assume that the backup is now complete and that the cartridge can be filed safely away. It is quite possible that the tape itself has become jammed, or that there is a fault in the streamer unit, and that no backup has taken place.* Several incidents of this type were only discovered when a hard disk failed and the backups were required.

Always check that a tape backup has been successful by restoring the tape to another machine and checking that the restored files are readable. Do not, under any circumstances, attempt to restore to the machine that was originally backed up, because you risk replacing the contents of a healthy hard disk with the corrupted contents of the backup.

The Modem

A modem is a black box that connects a PC to a telephone line. The modem is the favourite tool of the common hacker, who is more used to penetrating computers by dialling phone numbers at random than attempting to walk into an empty office with a pocket full of blank floppy disks.

It is not the purpose of this Guide to discuss telephone hacking at length, though the modem needs to be covered briefly because many PCs are connected to one in order that the user may have legitimate access to a company mainframe or to one of the commercial on-line database systems that offer everything from press cuttings to financial reports.

It is difficult, though not impossible, for a data thief to access your PC via the modem that you have connected to it. If you do have a modem installed in your PC in order to make use of various services, ensure that passwords and associated log-on data are not kept on the PC along with

the communications program. Most communications software has the facility to dial up a service and connect you, and will even send your passwords down the line. For this to happen, you need to program your passwords into your PC, and this should never be done. Staff must always be discouraged from doing so, as any unauthorised use of a dial-up service frequently goes undetected until a bill arrives. This could give the thief three months' free use of your account or access to the company mainframe from the thief's home.

Some modems have the capability to answer the telephone as well as to make calls. With the right software installed on your PC, a hacker could dial into it and read or copy your private files. Make sure that you know how to tell whether a modem has been placed in answering mode without your permission, and how to turn off that mode. External modems normally have an indicator light labelled AA, which will glow if Auto-Answer mode is selected. Modems that fit inside PCs are harder to interrogate, but there are small utility programs that can help. Consult the modem's manufacturer if you feel that you could be at risk.

Although the risk from such acts is small, it is recommended that PCs holding confidential data that are linked to modems should be disconnected from the telephone line except when the modem is being used for authorised access to a service. Remember, too, that laptop and portable PCs used by on-the-road sales staff are often fitted with modems so that orders and sales figures may easily be exchanged between the employee and Head Office. Ensure that sales staff understand the risk that the modem poses, and that they know how to guard against confidential data from their computers being accessed by unauthorised outsiders. Where necessary, ensure that encryption software is used on the portable PCs.

If an external modem is connected to a PC, and that modem is used purely for outgoing calls, it is possible to make a small modification to the cable that links the PC to the modem. By cutting the Ring Indicator core of the cable (consult your modem manual first, though it's normally pin 22 in a standard 25-pin connector), the modem will be unable to inform the PC that the telephone is ringing. This prevents any host software granting the caller access to the computer.

Telephone lines can be tapped. If there is a BT inspection cabinet in the street near your building, ask that no documents or notices be kept inside that could indicate to an intruder which lines go into your company and where precisely they terminate. Keep internal wiring diagrams locked away. If anyone has a need to know about the location of any cabling, show them only the part of the plans that they need to see and, if possible, do not allow copies to be made.

Many companies operate bulletin boards. These consist of a PC, a modem and some special software. Users can dial into the PC to leave

messages for other people and to transfer files. Some bulletin boards are run by hobbyists for personal use, while some are run by companies in order to provide information to customers. Although the software that controls access to the bulletin board is quite sophisticated, it is still possible for hackers to break out of the confines imposed by the controlling software and to gain access to the entire hard disk on the PC being called. Therefore, never keep any confidential data on a computer that is being used as a bulletin board, or on a computer that is linked by modem or network to the computer that is running the bulletin board.

A number of security-oriented modems are now available, which automatically scramble data as it is sent down a telephone line. The key on which the scrambling is based is automatically changed by the two modems every minute or so, at random intervals, making line-tapping almost impossible. Details of secure modems are included in the Resource Guide.

When choosing a secure modem, or any other secure telecommunications device, ask the vendor what action the device takes when the quality of the telephone line drops. Some devices are known to switch to unencrypted mode if the line quality drops to a level which would make encrypted communication too slow. A hacker who knows that this is the case can easily introduce some noise into the line. As can, so it is rumoured, the telephone company itself, or even a Government security agency.

Remote Access

Software packages that provide remote access to a PC are becoming popular. To use one, you need two copies of the software and two modems. You can then call up one PC from the other, and control that remote PC just as if it were in front of you. Such software provides two major benefits:

- A worker at home can access his or her machine in the office
- Technical support staff can sort out problems with a user's PC without having to be on the premises.

The problem with such programs is obvious; if a user can dial into his office and access the machine, so can anyone else. The solution is just as simple: all remote access programs come with a password protection facility that will attempt to verify the bona fides of the caller before allowing access. Ensure that the password facility is set up (make a test call) and enabled, and that the password is changed regularly.

Some remote access software packages provide a dial-back facility. When a user calls the machine, the remote-access software will hang up

the line and then call the user at his registered number in order to re-establish the connection.

While this provides an extra level of security, it has a disadvantage in that it prevents field sales staff from accessing a remote PC from more than one site.

If the user of a remotely-accessible machine is on holiday and he has no plans to access the computer, disconnect the phone line for this period. The same goes for evenings and weekends: 24-hour access may be desirable, and the user may claim that he will get more work done, but there is a serious security risk.

There are LAN equivalents of the remote access software package, designed for use when one user on a network is receiving training or support from another. Such programs allow one station on a network to view the entire session on another station, often without the knowledge or permission of the person whose work is being monitored. Frequent checks should be made to ensure that such programs have not been installed without permission on any workstation; such checks can usually be made by a supervisor who has access to the configuration files for each workstation.

Electronic Mail

A PC equipped with a modem can be used to send electronic mail (email). This can be done through public bulletin boards, a private bulletin board or a commercial email service such as those run by BT (née British Telecom) and Mercury Communications.

If you set up a private bulletin board for use by staff or customers, set it up so that new users are asked to supply their password and, if they cannot do this, are refused access. The default on most bulletin boards is for new users to be told "You are not recognised as a user, so I'll register you now. What password would you like to use?". Disabling this method allows you to control the number of users by issuing them with passwords before they log in for the first time.

Public email services are not secure. Their sales brochures will state otherwise, but this is just not true. After all, would you run a computer system that was set up in such a way that anyone could place information on it but you could not read it? Current legislation permits BT to intercept calls if one of the parties consents; this is how obscene calls are traced. When you use an electronic mail system run by BT, BT is one of the parties and they have been known to use this fact to justify tapping calls. If this loophole fails, they will claim that calls were being monitored in

order to "improve and monitor the quality of service". Such actions are expressly permitted by the Interception of Communication Act.

If you use a commercial email service, encrypt all messages and files that you do not wish to become public property.

If possible, do not use the same email system to inform the recipient of the password. If you must, include a line such as "the password is my middle name, preceded by my car registration number" instead of "the password is ROMEO".

Fax Cards

A fax card is a plug-in device that allows a PC to send and receive fax messages. These are now available from many manufacturers and typically cost around half the price of the cheapest stand-alone fax machine.

Because a fax card lacks the ability to scan in documents, it is limited to sending files that are prepared on the computer itself. These can be text files, prepared with a word processor, or graphics prepared with any program that saves its images in a format that the fax card's software can interpret.

Most fax cards have the ability to receive faxes too, and this operation can normally be carried out while the PC is in day to day use. Incoming faxes are saved to the PC's hard disk as a graphics image and can be viewed with custom software that is supplied with the fax card. Remember that the incoming fax is a graphic image, as would be received by a standard fax machine, and not a text document.

Some fax cards are supplied with software that attempts to convert the incoming fax into a text file for use with a word processor, but such programs should never be considered 100% reliable. If the incoming fax is handwritten, unclear or proportionally spaced, recognition becomes even harder and only the most expensive dedicated character recognition packages will attempt to decipher it.

The benefit of being able to send faxes from one's desk brings with it a number of potential security loopholes.

Local Storage

Incoming faxes are saved on the PC's hard disk as a graphic image. Fax card manufacturers make great play on the fact that the image is saved in a format that can easily be read by common PC painting programs.

The ease with which a fax can be modified before being printed and handed to the recipient may prove a problem.

Unauthorised Copying

Fax messages stored on disk are easier to copy and/or conceal than printed versions. If you delegate the handling and distribution of incoming faxes to a particular person, ensure that he or she is trustworthy and make occasional covert checks by tracking the progress of a message through the system.

Identity Marks

A stand-alone fax machine usually prints the identity of the sender at the top of each page. This identity is transmitted by the sending machine, having been programmed into the device when the machine was installed. PC fax cards allow this identity to be programmed by the user at will. It is, therefore, simple to program a fax card to send messages that purport to originate from any person or organization.

Scanning

Devices for scanning handwritten text or pictures into a PC drawing package can now be obtained for less than £100. A signature, once scanned into a computer and loaded into a graphics program, can easily be incorporated into a document before it is sent via a fax card. Although this deception can also be carried out by users of stand-alone fax machines, by careful use of scissors and glue, it can lead to serious problems when coupled with the programmable sender's identity as mentioned above.

The Operating System

Almost all IBM PCs and compatibles run the MS-DOS operating system. The four major alternatives are UNIX (in one flavour or another), DR-DOS, OS/2 and Novell NetWare. This Guide is primarily concerned with machines running MS-DOS, though see the notes on DR-DOS on page 27.

As an operating system, MS-DOS is a serious security risk. *Any program has access to every part of the machine's memory and the entire hard disk drive.* Compare this with UNIX and, to a certain extent, OS/2, where programs and users are confined to their own areas of memory and disk and are not permitted to stray.

All the functionality of MS-DOS is controllable and changeable via easily-installed programs called TSRs. These get their name from the fact that they load themselves into memory through a DOS function called Terminate And Stay Resident. If a programmer doesn't like the way that MS-DOS accesses the keyboard, he can simply rewrite that part of MS-DOS. If he wants to add new commands, it's just as easy.

If a malicious programmer wished to install a new component in MS-DOS that kept a copy of all keystrokes typed, and stored this copy in a hidden file on the hard disk, such a program could be written in a couple of hours and installed on a computer in seconds. The programmer could then return after a few days and, under the guise of someone trying to help you recover some space from your hard disk, remove the hidden file for analysis. The file would contain everything that you had typed, including confidential information, passwords and so forth.

The expertise required to implement this type of MS-DOS add-in is not very great; anyone with six months' experience of assembly language can do it easily. *There are several programs that will highlight any TSR programs that have been installed in a machine, and such utilities should be used frequently by security staff.*

Disabling Commands

The MS-DOS operating system provides several commands that allow users access to data and programs. Some commands are built into the operating system and are available at all times. Examples of these commands are DIR, COPY and RENAME. DIR produces a list of all the files on a disk, while COPY and RENAME operate on files in ways which should be clear from the command's name.

Preventing access to these commands requires the use of a special utility program. Many such programs are detailed in the Resource Guide, which begins on page 155.

Some MS-DOS commands are not built into the operating system but are supplied as separate programs in their own right. Examples are XCOPY (a more sophisticated version of COPY), FORMAT (for formatting blank disks) and PRINT (for printing files). Access to these commands can, at a simple level, be restricted by deleting the program files. However, anyone with a copy of the program on a floppy disk can take it from one machine and use it on any other that is running the same version of MS-DOS. Casual prowlers can be deterred by removing unwanted DOS programs from machines but a more sophisticated access control program should be considered if a higher degree of protection is required.

DR-DOS allows passwords to be attached to files. However, this scheme is not unbreakable and should not be relied upon to protect highly confidential data. Encryption, or a professional access control package, is to be preferred.

The PATH Command

MS-DOS arranges its files into groups, and these are known as directories. The PATH command lets you specify a list of directories through which MS-DOS will search if it can't find a program. For example, if a user is in the LETTERS directory and types WP to start WordPerfect, DOS will look in the current directory (ie LETTERS) for the WP program. It won't be there, so DOS will look through all the directories mentioned in the PATH. Assuming that the WP51 directory appears in the list, DOS will be able to find WordPerfect and all will be well (WordPerfect 5.1 normally resides in a directory called WP51). If the WP51 directory doesn't appear in the PATH, DOS won't look there and the WordPerfect program won't be found. Consequently, a Bad Command or Filename error will be produced, and the user won't be able to use WordPerfect until the problem is fixed.

It's important to keep an eye on how users set up their PATH command. Among the problems that can be blamed on a PATH command are:

- The wrong version of a program is executed. This occurs because there are two versions of the program on a hard disk, and the directory containing the older one appears earlier in the PATH command than the newer one. This problem frequently occurs with programming language compilers, where an old version of the LINK utility is executed instead of the one supplied with the compiler, thus causing compilation errors.

- A hard disk contains two or more programs that perform different actions but share a similar name. For example, many applications are supplied with an INSTALL or SETUP program, and these programs are normally copied to the hard disk so that you can change the program's configuration. If this is the case on your machine, typing SETUP or INSTALL will have varying results, depending on which directory you are currently in, and the way that your PATH is arranged.

This can lead to serious problems if, for example, a user is reading a book on Microsoft Windows and is told to type SETUP in order to alter some of the settings. If the user sees a SETUP program that doesn't actually belong to Windows, he may get confused. If the SETUP program that he runs turns out to be the program which allows the PC's CMOS memory to be altered, it is very easy to get into the situation where the CMOS memory becomes corrupted and the machine refuses to boot.

Windows And Multi-tasking

Microsoft Windows is an add-on for MS-DOS that provides a PC with a graphical user interface (GUI) and the ability to run more than one program at once (multi-tasking). Although standard MS-DOS programs can be run under Windows, the product comes into its own when used with specially-written applications that take advantage of the graphical environment to provide a full menu-driven system. Such software products include the Excel spreadsheet, the Corel drawing package and the Word For Windows word processor.

There are two inherent security problems with Windows which can affect the integrity of data. First, there are known problems when certain programs are used with Windows. Utilities known to cause problems are non-Microsoft disk caches and partition managers, as well as file de-fragmenters and backup utilities. There are also incompatibilities with certain makes of PC. When installing Windows, it is important to read the documentation carefully to ensure that you do not have one of the incompatible programs or machines. Information about incompatibilities that comes to light after a batch of Windows manuals are printed is contained in a disk file called READ.ME. When the Windows installation procedure asks if you wish to view this file, it is important that you do so. Never run a file de-fragmenter or backup utility under Windows while another program is running.

The second security problem is not so easy to avoid, except by providing staff training. A novice user, sitting at a machine that he or she does not know how to use (any machine; not necessarily a computer), will typically press every button in sight in the hope of getting it to work. Similar effects are observed when this person is using a PC.

Windows makes it easy for a user to access all the features of a program, as everything is presented to him in a number of menus and these simply need to be clicked with the mouse. Typing DEL COMMAND.COM at the MS-DOS prompt is fairly hard for a novice to do by mistake but, with Windows, deleting a file is done simply by clicking a few pictures with the mouse pointer. By deleting the wrong file (COMMAND.COM is just one example) it is possible to get into a position where the PC will refuse to start up unless parts of MS-DOS are re-installed from the master disks.

Windows is widely advertised as making a PC more friendly and easier to use. *Beware of users who believe that their computer instantly becomes more tolerant of user errors once Windows has been installed.* Turning off a computer at the wrong moment can corrupt an entire hard disk; just because Windows looks friendly does not mean that this is not still the case.

As stated above, Windows adds multi-tasking capabilities to an MS-DOS PC. It is not the only program that provides multi-tasking; DESQview is

another well-known utility that does the same, although this does not provide a GUI as Windows does. Because of a limitation in MS-DOS, multi-tasking is inherently unsafe. If you are running eight programs simultaneously and one of them crashes, the other seven will all be terminated too. If one of those seven was in the process of accessing the hard disk, corruption of data could result.

Encourage Windows users to keep open only the programs that they need to use, and to shut down programs when they are no longer needed. This also applies to non-Windows word processors and spreadsheets that allow multiple files to be opened at a time — do not keep files open that are not required.

The OS/2 operating system exploits the PC hardware and provides a more rigid multi-tasking environment where this problem does not arise; if one program crashes then any others may still be accessed by the user and shut down gracefully.

DR-DOS

DR-DOS, from Digital Research, is an MS-DOS "clone" which many manufacturers choose to include with their machines instead of the Microsoft product.

Starting with version 6.0, DR-DOS is a fairly robust and stable system which provides many advantages over MS-DOS. From a security point of view, its facilities are excellent: password-controlled access to files and directories is included as standard.

There is, however, one major component of DR-DOS 6 which represents a potential data integrity risk. This is the special disk formatting program called SuperStor, which is included in the product as standard. SuperStor is a device driver which, by the use of data compression techniques, is able to double the amount of data that can be stored on a hard disk.

As information is written to a hard disk which has been set up with the SuperStor program, it is automatically compressed. When a program tries to read that data, DR-DOS de-compresses it automatically, and the program is never aware that the data was held in compressed form.

While such a utility is a boon to the user who is short of hard disk space, it is also considered to be highly dangerous by the majority of data security experts. Having information held on disk in a non-standard format means that few recovery tools will be able to access it in the case of a hard disk crash or other disaster. Also, a small number of programs are not compatible with the SuperStor system, and some users have

already reported that entire hard disks have become corrupted and unusable.

If you wish to use data compression to increase hard disk space, use a stand-alone program to compress specific files, rather than a utility which compresses an entire disk. The safest files to compress are executable program files, as these can always be re-installed from the master floppy disks in case of corruption. Check out two Shareware programs called LZEXE and PKLITE, which compress executable files in such a way that they do not need to be uncompressed before they are run. Instead, a special loader program is attached to the start of the program, so that it uncompresses directly into memory when you run it. Not only does this increase hard disk space, but it also speeds up the load time as there is less data to be retrieved from the hard disk.

Note that it's essential to keep a DR-DOS bootable floppy disk handy if you use DR-DOS with a SuperStor hard disk partition. An MS-DOS boot disk will not recognise a SuperStor partition, so an error in a CONFIG.SYS or AUTOEXEC.BAT file could render a PC non-bootable until a suitable boot disk is located.

Access Control Under DR-DOS

DR-DOS 6.0 includes an access control system which, though not uncrackable, does prevent casual intruders from discovering the contents of your PC.

The first level is login security. Here, DR-DOS sets up your system to request a password each time it's booted. The "please enter your password" screen, and the "sorry, access denied" screens are both customisable so you can easily add help messages to inform users what to do if they forget their password. This security system doesn't encrypt the data on the hard disk. It does, however, scramble various pieces of the partition table so that booting from a floppy disk will give you nothing more than an "Invalid drive" message unless you know the password.

If you use this feature, remember to keep a DR-DOS bootable floppy handy for emergencies — the partition table scrambling makes your hard drive inaccessible to MS-DOS.

The second security level works on a per-file or per-directory basis, rather than on the whole machine. This is managed by the PASSWORD command. For example, PASSWORD WP.EXE /R:BUTTER adds the password BUTTER to the WP.EXE file. Typing WP from the command line will result in an Invalid Password message. Type WP;BUTTER loads the program as normal.

There are two levels to the PASSWORD command - you can control read access, write access or both.

PASSWORD operates on entire directories, if you wish, and you can use wildcards when setting up access control. However, protecting my entire WP51 directory prevented WordPerfect from loading properly — it kept asking for disk 2 to be inserted into drive A. Protecting just WP.EXE solved the problem.

PASSWORD-level protection can be bypassed by booting from an MS-DOS disk, by the way, so it's useless unless you have the boot-level security installed too.

The LOCK command locks the keyboard and clears the screen, and requires entry of the boot-up password in order to regain control of the system.

3 What Motivates A Hacker?

An appreciation of what motivates someone to steal data from your company is essential if you intend to help prevent theft from your own PCs. Someone who is about to steal data from you will normally have one of five thoughts going through his mind.

- "This is a wonderful opportunity that I can't afford to miss."
- "This will serve the company right for what it's done to me."
- "No one will miss it. I'm only curious."
- "This information must be worth a fortune."
- "I wonder if the security system is all it's cracked up to be."

Opportunity

The concept of an opportunity that presents itself to a person who is normally honest is, in my experience, the most common and the most dangerous motivating factor. Imagine the case where an employee has reason to visit the personnel office to collect some forms. One of the assistants in the office hands him the forms, and also hands him a floppy disk. "Can you do me a favour and put this in Duncan's pigeonhole on your way up?", asks the personnel assistant. The disk is labelled "Proposed salary review and redundancy plan".

The temptation for the employee to make a surreptitious copy of the disk on his own PC before delivering it to Duncan is overwhelming. Human nature being what it is, even the most honest person will seriously consider taking that copy. If there is any doubt in the person's mind as to whether he should copy the data, he'll probably make a copy of it anyway, but decide not to actually look at the information until he's thought about the consequences.

It's important to ensure that such easy opportunities for data theft never arise. A thief, as has already been said, is only an honest man with

opportunity. And once an honest man has discovered just how easy it is to become a thief, and how simple it is to steal valuable information with almost no possibility of detection, he will set his sights on higher things. If you're lucky, he'll start stealing notepads, paper clips and highlighter pens. If you're not, he'll look for yet more floppy disks.

Revenge

Someone who, in his opinion, has suffered at the hands of your company will often be tempted to seek revenge. Few of us would go as far as to commit arson, or steal data to sell to a competitor, but deleting a couple of disks "accidentally" will be just enough to cause minor irritation. Unfortunately, in many cases, it's possible for the loss of a couple of disks to lead to severe problems for the company that suffers the loss.

An organization, or a department within an organization, must never be in the position that a major catastrophe would result from the loss of the contents of a single computer and/or its contents. Ensure that:

- *Backups of all important information exist.*
- *These backups are kept in a secure location.*
- *The backups are complete and are known to be intact.*
- *Backups are re-taken whenever important data changes significantly.*
- *Staff know how to restore data from backups.*

Procedures for implementing an efficient backup strategy are discussed on page 68.

Note that revenge can take many forms. Deleting or copying data is one. Another is to make a phone call to FAST (the Federation Against Software Theft). This organization concerns itself with investigating (and prosecuting) companies suspected of using unlicensed copies of software. *Staff at FAST are known to regularly receive tip-offs from disgruntled employees.*

Curiosity

Everyone in your company is curious about how the organization works. Let's face it - if they weren't of the inquisitive type, that enjoyed finding out facts and learning new things, you would not have employed them in the first place.

In addition, those who contribute most to the daily total of inter-office gossip gain instant respect from their colleagues.

Curiosity must never be allowed to turn into dishonesty, and it is the responsibility of a good manager to ensure that this never happens. If junior staff are to handle floppy disks containing confidential information, label the disks "Backup program" or "miscellaneous printer drivers" or something similarly uninspiring to the would-be sneak. Don't leave the labels blank, as this will arouse suspicion. Equally, don't hint at the importance of the contents by saying "take these totally worthless disks to Duncan but be very careful with them".

Greed

Most data thefts are as a result of curiosity or revenge but never forget that there are greedy, jealous people within and outside your company who will regard your confidential data as hard currency.

Care must be taken to avoid private data, either on disk or printed out, leaving the building except in the hands of those authorised and trusted to have it. *Unless there is a good reason for an employee to take confidential data outside the building, such as keeping a backup at home, he must not be allowed to do so.* That someone is taking some work home to finish off in his own time is not a good reason — suggest that he takes some less-confidential work home and uses his time in the office to work on the confidential matters.

Any confidential documents that leave the building in staff hands, for use at home or at a client's site, should be signed for and numbered in a way that will allow each copy to be identified should it later turn up in unauthorised hands. Where multiple copies of a sensitive document are distributed, such as a proposal or specification for a new product, each copy should be marked with individual identifiers so that leaked copies may be traced. A missing comma here, an extra semi colon there and so on. Do not divulge the existence of these markings; use the presence of the serial numbers to imply that the documents are not protected in any other way.

Special care must be taken when an employee resigns or is dismissed, especially if he was privy to confidential matters. This subject is discussed more fully in a later chapter.

The Challenge

There are always people who regard security systems as a challenge. In one way, these people need not be feared because it is unlikely that they will actually steal or corrupt data once they have managed to get their hands on it. The thrill of being able to breach the security is sufficient.

However, such people should be considered a threat because they will be immediately attracted to any computer which is known to have a particularly stringent security policy attached to it. A mountaineer would rather climb Everest than a hill in the local park. In the same way, this sort of computer cracker would rather attempt to read the personnel data on the MD's computer than the stationery orders held on a secretary's machine.

Protecting information from those who seek personal improvement by accessing it is not easy. If you're going to keep adding more protection layers, and publicise the fact that you are doing so, then it's essential that these layers should be as tough as possible. It won't take long for the hacker to realise that this machine is not worth attacking.

However you protect the most private PCs, ensure that every employee knows the consequences of being caught attempting to hack them. If you do actually catch someone then ensure that he or she is given the punishment that he was expecting. If the deal was that hacks mean instant dismissal, then do it, even if it means you lose a key member of staff. If you don't, then word will spread that the contract clauses aren't worth the paper they're written on, and yet more staff will take up the challenge. Also, "John did it last year but he never got fired" is a valid defence in an unfair dismissal tribunal.

4 Tricks That Hackers Use

Hackers are cunning, resourceful and quick-witted and will stop at almost nothing to get their hands on your data. There are lots of tricks that they use to con you or your staff into allowing them access to information that they should not have. All the tricks below have been carried out by data thieves of my acquaintance and none was detected by the victim until it was too late.

Straight Past Reception

Hacking into mainframes is all about telephones. Getting data from PCs usually means that the hacker must gain physical access to the machine. In the vast majority of companies, this is easier than it sounds.

The simplest way to gain access to a PC in an office (especially an open plan office) is simply to walk in off the street, straight past the reception area, and sit down at the PC. (If it's lunchtime, the hacker will roll up his sleeves and carry a sandwich under his arm. After all, who else but an employee would turn up in shirt sleeves carrying a sandwich?). Those security consultants who have used this method have invariably succeeded without being questioned. Those that are questioned by alert receptionists show a business card and then walk through. Remember that a single business card must never be accepted as proof of identity. A caller with a wallet full of the same business card is frequently who he claims to be; this is not the case with someone whose wallet contains many people's cards.

Another way of getting around stubborn receptionists is to arrive for an impromptu appointment. A favourite trick of one British security consultant is to explain, toolbox in hand, that the company upstairs has reported some interference on their network and would you mind if we eliminated your floor as the source of the problem? Once inside, the consultant then proceeds to remove the covers from a number of cable junction boxes and places his business card in each one. A few days later, he calls the managing director and suggests that the company needs some security consultancy. The question "Tell me why we need security consultancy" is usually answered with "have a look in your network cable junction boxes, then call me back".

All of the above situations can be prevented by issuing some basic training to all staff, *especially those at reception.* If staff are not comfortable having to deny access to what may turn out to be the chief executive on a flying visit from the US, suggest they say "Sorry sir, I've been told that I have to check you out first" rather than "Sorry, I'll have to check you out first".

The reception area staff should be issued with an incident log, to record all suspicious events. This log should be studied daily by a security-aware manager in the search for evolving trends. The events which warrant an entry in the log must be clearly defined, and should include:

- All visitors who wish to see a named member of staff but who do not have an appointment.
- Any visitor who seems hesitant or nervous on arrival.
- Any staff member removing equipment from the building.

Reception staff must also ensure that the staff signing-in book always contains an up-to-date record of who is in the building, plus arrival and departure times. Not only is this record of use in emergencies, it can also help track down unauthorised out-of-hours use of PCs when cross-referenced with the log produced by a program such as the HISTORY utility described in the Resource Guide.

Inventory Log

Staff at reception, or at the gate house if appropriate, should maintain a log of all equipment and disks taken into the building by staff. In cases where total security is required, this may involve the searching of brief cases and handbags.

A recent document from the Department of Trade and Industry reports the case of an employee who was stopped by his employer's security guards when attempting to leave the office with a floppy disk. Because he had not declared the disk when he had arrived for work that morning, the guard examined the disk and it was discovered to contain highly confidential information that was destined for a competitor.

A major weakness in the company's security procedures was then discovered. Had the employee carried a blank disk (any disk) into the office that morning, and declared it to the security staff on arrival, he would probably not have been caught attempting to leave the premises with a disk full of data.

Keystroke Traps

A detective sergeant in the Metropolitan Police once sought my advice on how to protect his computers. The machine was on his desk and, he assured me, no one ever used it or entered his office without permission. Knowing that his office was in one of London's most secure police stations, I decided not to attempt to impress him with the "how to get past the receptionist" routine. Instead I put to him a simple scenario.

In this scenario, I have been out with him for lunch or an evening drink. We get talking about computers and, it is discovered, he's partial to the occasional computer game. I just happen to have about my person the latest version of a very popular game and I'd be willing to show it to him on his office computer. He takes me back to his office and I put my disk into his machine.

This scenario can lead to one of two possible methods of extracting data from the computer. The first goes something like this.

We power up the machine and start playing the game. After half an hour or so, we get bored and decide to call it a night. I suggest that, before we go, I show him a list of the files on my floppy disk to reassure him that there's no virus on the disk; just a copy of the game and nothing else. We then go our separate ways.

The hack has now been perpetrated. The game that I was demonstrating had been specially altered in a way that any competent programmer could do. While it was playing, it was also copying all the spreadsheet files and/or word processor documents onto the floppy disk. Once all the files had been copied, they were deleted from the floppy disk. Having reassured the machine's owner that the floppy disk was devoid of all information apart from the game, I then return to my office and use a commercial utility program to undelete the spreadsheet and document files.

The second scenario is this. In the couple of seconds before the game actually starts playing, the disk installs a specially-written program in the computer. Again, this is the sort of program that any programmer could write or obtain. The program hooks itself into the MS-DOS operating system and watches every key that the policeman presses. The program is installed in such a way that it cannot be detected or removed, and every key press that it sees is saved in a file on the machine's hard disk. As if to make the hacker's job even easier, MS-DOS allows the creation of files that do not show up in a directory listing, ie will not appear when the machine's user asks for a list of files that currently exist.

A few days later, I return to the policeman's office with yet another new version of the game. While it is playing, it is also moving the hidden file

from the hard disk to the floppy disk. I now have a complete log of everything that was typed on that machine in the last few days. This includes data that was typed into spreadsheet and word processing programs, as well as any passwords that may have been entered to achieve access to networks or mainframes.

"Err, you don't actually tell people this, do you?" said the Detective Sergeant.

Documentation

Ignorance of the inner workings of a computer system is a useful defence against hackers and efforts should be made to control access to system manuals and documentation. A data entry clerk who is entering figures into an accounts package should not be given access to the entire manual - there is no need for the particular staff member to know everything that the package is capable of doing.

Instead, create a series of Fact Sheets that explains everything that the staff member requires to be able to do his or her job, but no more. These sheets can be written by the Support department or can simply be photocopied from the manuals. (Bear in mind that copying more than a handful of pages from a software manual is probably prohibited by the licence agreement.)

It should be remembered, however, that most software and hardware companies will supply extra manuals to any person with a telephone and credit card. This includes complex mainframes, where even the system programming manuals can be obtained this way. This is one more reason why the list of all available commands on a network or mainframe should never be made available to users, as inquisitive users will then be tempted to acquire a manual in order to find out how all the commands are used. It is also a reason why possession of manuals should not be regarded as proof of purchase of a software package.

Where pure data-entry tasks are being performed, consider having the data entered into a standard text editor, word processor or simple database application and then instructing the accounts package to read transactions from the text file instead of from the keyboard. In this way, data entry staff can be totally excluded from the entire accounting software.

Where this is not possible, use the accounts package's password facilities to ensure that clerks cannot gain access to balance sheets or other confidential information, and that no unauthorised personnel can enter or amend prices or delivery addresses.

File Names

The most obvious clue to the contents of a file on a PC is the file's name. Under all versions of MS-DOS, files have names of 11 characters, split into two words of eight and three characters. Where possible, don't choose file names that give away the contents of the file. For example, keep staff names, salaries and addresses in files called STAFF1, STAFF2 and STAFF3. Such names are fairly easy to remember and are far more innocuous than STAFNAME, SALARIES and STAFFADR. Try to avoid common file names with only minor differences, especially in the three-character extension, as MS-DOS makes it easy to copy groups of files in a single step. By default, the Lotus 1-2-3 spreadsheet adds a "WK1" or "WK3" extension to all files it creates, which means that all the Lotus spreadsheets in one hard disk directory can be copied to a floppy disk with just a single command.

Classification codes should also be considered when you are thinking about how to name files. Unless there is a real need to do so, do not allow staff to assign codes such as "unclassified", "classified", "secret", "confidential" and "top secret" to files. Hackers like to collect and amass information that they are not supposed to have, and if two hackers are in competition with each other then a way of judging the winner is required. This is easy when the company whose data is being stolen is kind enough to allocate different numbers of points to each file according to the secrecy of the information it contains. If you must differentiate between public files and those of a sensitive nature, use as few codes as possible and restrict their use to senior staff. In addition, grant a file "classified" status only in extreme cases; *if staff get into the habit of calling every file "classified" then the value of such a description rapidly depreciates.*

Refuse Areas

It's often easier to check through a data file by reading over a printout instead of staring at a screen. Hackers know this and will frequently raid the contents of your rubbish bins for interesting information. If sensitive information is regularly printed out and then thrown away rather than filed, invest in a shredding machine. Alternatively, dedicate one rubbish bin on each floor for confidential waste and ensure that its contents are burned regularly.

One-time carbon (rather than nylon) printer and typewriter ribbons contain a readable image of every character that has been printed. They should be disposed of carefully (or kept locked away if they are not yet exhausted) if they have been used to print confidential information.

5 The Manager's First Tasks

That you have bought a copy of this Guide indicates that you intend to take seriously the security, availability and integrity of corporate information held on PCs. As the preceding and following chapters show, there are dozens of major risks to your data, and it is clearly impossible to plug all these holes overnight. As the person who has been charged with implementing, or who has volunteered to implement a company security policy, there are many major steps that you should take first. Some of these steps actually lead to greater security, while some simply lay down ground rules and pave the way for obtaining the co-operation of others in the company. All are essential, and each step mentioned in this chapter should be performed before any other action is taken.

Senior Management Commitment

Any attempt to change a long-standing corporate attitude needs the involvement and co-operation of managers at the highest level. Wherever possible, consultation with the main Board should be sought. This gives the whole process an air of authority and will help to compel staff to comply with the terms of the corporate security policy that you are about to implement. Remember that you are about to draft a series of new company rules and that those above you in the company hierarchy are just as likely to break these rules as those below you. Without the involvement of the Board you will find it impossible to suggest to a senior manager or director that the way he stores sales forecasts on his PC is inherently insecure and a major threat to the company. However, unless you are in a position to do something about this then your attempts to improve corporate security are doomed from the start.

The recommended time to seek involvement from the Board is when the security plan has been drafted but not yet formally announced to the whole organisation; let the senior managers comment on, and amend if they wish, the draft as this will help both the Board and yourself to form a good working relationship.

Convincing The Board

It should be possible, in a single presentation session, to explain the benefits of your security policy to the senior management. Some of the key points to bear in mind when planning the presentation are as follows:

- Open by explaining why a formal security policy is required, and contrast this with the current methods (if any) of dealing with security threats, viruses and so on.
- Ensure that the presenters are technically qualified to answer any questions which the Board may ask.
- Back up the presentation with statistics. How many of the company's PCs are currently backed up? Are those backups known to be reliable? How many staff claim that they could recognise a virus?
- Sprinkle the presentation with horror stories about companies which have suffered or been bankrupted by security-related problems which could have been avoided.
- Explain clearly the benefits that the new security policy will bring.
- Show how little the drafting and implementation policy will cost, and how little disruption it will produce.
- Show how the senior managers will benefit.
- Explain that only essential measures will be taken - no clauses will be included in the policy without good reason.

How To Inform Staff

Having gained approval from the Board, make a formal announcement to all staff that security is about to become an important consideration throughout the company. Whether the memo is signed by you or a Board member depends on how you wish to portray your role and is a decision that you must make for yourself.

The memo (for it must be a written announcement) should make clear:

- That security is now a major issue.
- That a security policy is being prepared and anyone wishing to be involved in its drafting should contact you.
- That the drafting of the policy has full Board approval.

- That such a policy is urgently needed, by citing recent examples of poor data control if any are known.
- When the policy will come into effect.
- That the penalties for ignoring it will be severe.
- That its adoption by all staff will greatly benefit the company.
- How staff can formally air objections to any aspect of the policy or its implementation.

Set Targets

Set yourself targets, and devise a set of measurements to ensure that you will be able to recognise when the targets have been met.

Possible targets to set could include:

- Ensuring an 80% awareness of the potential damage that viruses can cause, within four months.
- Ensuring that all PCs have been subjected to a software audit within three months.
- Removing all unauthorised software from PCs within six months.

Motivating Staff

Motivating staff to think about PC security is all about convincing them of the benefits. At all times, try to promote "what's in it for them". Psychologists have proved that someone is more likely to change their behaviour because of the perceived results.

Consider setting up an awards system as an incentive. For example, ask that all departments submit a quarterly report that explains what steps have been taken to improve PC security, and award a prize for the best.

A Sample Data Security And Integrity Policy

The detail of your data security and integrity policy must be tailored to your own company, and its content will be largely determined by the results of the survey that a previous chapter of the Guide recommended that you carry out. Some general points that should normally be in-

cluded in every PC security policy are listed below and may be used as the basis of your own policy document.

The clauses below are written in a form that can be directly copied to your own policy document. Text in square brackets indicates information for the compiler of the policy which should not be publicised.

It's essential that clauses covering computer misuse be incorporated into employee contracts. Sacking an employee for breach of contract is easier than sacking for "misconduct".

The Personal Computer

If you are issued with, or given access to, a PC, it must be treated with care. While the monitor and keyboard may be repositioned for comfort, the system box itself must not be moved within the building or taken off the premises without permission. Under no circumstances should the cover be removed and circuit boards added or removed without prior authorisation from the Support department.

Home computers owned by staff may not be brought into the office.

PCs should be turned off at night unless there is good reason not to. Remember to turn off printers, monitors and other attached devices.

If you use a company PC at home, you must take steps to ensure that it is not used by other members of your household for unauthorised purposes.

If you use a laptop PC, do not rely on the "restart" feature which allows the machine to be turned off while an application is active. This feature can lead to data loss if the machine's batteries run low. Ensure instead that all applications are shut down and that you return to the DOS prompt before turning off the machine or leaving it unattended for more than a few minutes.

Software Packages

Your PC will be installed with one or more software packages when it is set up for you. These programs will be the ones that you have requested or that you will need in order to perform the tasks for which your PC was purchased. You must not copy the software from your PC to any other PC within the company, and you may not take a copy of any software outside the company. If you do this, you and the company will be committing a criminal offence and will be liable to prosecution for theft. Computer manuals may not be photocopied, for similar reasons.

Programs from outside sources must not be used on your PC. This includes programs that you have bought, been given, or downloaded from a bulletin board or online system, and applies equally to copies as well as original shrink-wrapped disks. As has been widely publicised recently, there have been outbreaks of computer viruses in the past. Only by following the "no software from outside" rule can we keep this company free from virus attack.

[Virus Guard, part of Dr Solomon's Anti Virus Toolkit, includes a facility to allow only diskettes which have been individually authorised to be used on one or more specified PCs. Details can be found in the Resource Guide].

Screen Displays

Do not leave confidential information displayed on screen for longer than is necessary, and certainly not while you are away from your desk. The PC Support department has a screen-saver program which will automatically blank the screen if information is being displayed and no key has been pressed for a few minutes. The screen is unblanked by pressing a key and entering a password. Contact the Support department if you would like a copy of this program to be purchased for you.

Encryption Of Confidential Data

You have been supplied with a data encryption (scrambling) program and a fact sheet that explains how to scramble a file. Please ensure that all confidential files held on your hard disk are held in scrambled form, and that you do not choose easily-guessable passwords for scrambled files. If any of your staff need to know the password for your scrambled files, ensure that those files to which your staff do not need access are protected by separate passwords.

[Where staff members or departments routinely keep confidential data files on hard disks, an access-control program which automatically scrambles all files should be used. See the chapter on Access Control (page 85) for details.]

Backups

You must keep backup copies of all crucial files. Your PC has been installed with a backup program and you should have received a fact sheet that explains how to make backups. Backups must be made every week, without fail, and the backup disks handed to PC Support for storage in the fireproof safe. Backup disks should be in boxes labelled with your name, extension number, department and the date.

[The Support department should be instructed to maintain accurate logs of all backup disks held, and should produce regular reports to show the frequency that each PC was backed up.]

Contact the PC Support department if you require access to your backup disks in the event of loss or corruption of one or more files.

Backup disks may not be taken out of the building.

[Where staff are linked to a network, it is worthwhile using a backup program that automatically backs up all workstations to the file server at regular intervals. The file server Support department can then back up the server itself.]

[For more information on backups, see the chapters on backup (page 61) and networks (page 135) later in this Guide.]

Removal Of Company Data

You may not take home information that relates directly to the activities of the company without permission from your Head of Department. This includes printouts and floppy disks.

If you use a company-supplied laptop computer for access to data while out on site, the machine must not be left unattended in a car unless it is positioned out of sight. Do not leave more programs and information on a portable computer than is necessary, especially if you share a laptop computer with another member of staff. Never program passwords into the computer.

Formatting Disks

All floppy disks that are for your own use must be labelled with your name and department. This may be done by writing the information on a sticky label and then placing it on the disk. Also use the Volume Label feature of MS-DOS to record the details on the disk when it is formatted. This information is required as a safety feature to monitor the spread of a virus in case of a company infection; it is not designed to control the number of blank disks that an employee uses.

Refuse Disposal

Highly confidential printouts must be shredded before disposal. If this is not possible, tear printout sheets into four quarters before disposal

and throw two sections into one rubbish bin and the remaining sections into another.

Anti-Virus Precautions

Do not use floppy disks in your PC unless and until they have been scanned for viruses.

Do not lend floppy disks to anyone. If you must do, then scan the disk after they are returned to you.

If you receive a disk from someone, scan it for viruses or ask the PC Support department to scan it for you.

Do not leave floppy disks in your drive once you have finished with them. Always check that the floppy drives are empty before turning on a PC.

If you accidentally turn on a PC with a disk in the drive, do not follow the on-screen advice to remove the disk and press a key. Instead, turn off the PC, remove the disk and then turn it back on again.

Reporting Procedures

Please report all instances or suspicions of data loss to the PC Support department so that action can be taken to stop the problem spreading. A virus introduced into one machine can often be eradicated with the use of special software if the problem is detected in time. If you suspect that any employee is treating confidential company information in a way that could be harmful to the company, or if you suspect that a virus may be present in one or more computers, this should be made known. If you do not wish to incriminate yourself, please consider leaving an anonymous report with a member of the PC Support group so that the problem can be investigated and cleared up with the minimum of disruption.

Use Of Passwords

[See page 86 for details of passwords which should not be permitted.]

Enforcing Penalties

Having publicised the data security policy, explain the penalties. Remember that there is the potential for instances of loss of company data

to be treated by the Police as theft or criminal damage; such a situation is not to be taken lightly.

There are two golden rules about penalties. First, they must be severe yet fair. Second, they must be seen to be carried out.

One way of implementing a severe yet fair penalty is with a system of points, rather like those collected by speeding motorists. An employee can be given between one and four points, depending on the severity of the situation, and dismissal for gross misconduct should follow after four points. It follows that it is possible for an employee to be dismissed for committing a single offence, such as attempting to pass client lists to a trade rival.

If you adopt such a system, consider weighting the number of points in accordance with seniority. For example, DP staff who lose data through carelessness should be more severely penalised than data entry clerks, as the DP staff member should have known better.

It is essential that penalties are seen to be carried out. If this does not happen, then an employee who stumbles across an unguarded floppy disk labelled "Payroll backup" will not think twice about taking a quick look. "Janet in accounts got caught playing games on her PC last week but nothing was done about it, so there's no reason why anything will happen if I take a quick copy of this disk".

The fact that a blind eye has previously been turned to similar offences is a valid defence against dismissal by an employee.

There is, of course, a serious problem when implementing the two golden rules mentioned above. An employee who discovers that his after-hours gaming on the computer has introduced a virus will not wish to inform anyone. By the time that the situation is detected, the cost of the clean-up operation could have escalated by a factor of 100. If a system of anonymous reporting is in place, then it may be that the problem can be detected early and the culprit can be promised immunity from disciplinary action if he co-operates by explaining where the infected disk came from and which other PCs in the company may be infected. For this reason, such a system is highly recommended but immunity must be granted only in special cases and must not be unduly publicised.

Handling Dismissals And Resignations

If you are forced to dismiss someone for misuse or mistreatment of data, ensure that they are escorted off the premises immediately. Many sys-

tems programmers of my acquaintance have admitted to leaving "back door" traps in programs so that they could bring the system to its knees in the case of a dispute. Avoid all possibility of such a trap being detonated by ensuring that the culprit is not around to set it off. Traps that are automatically set off if the system detects that the employee is no longer around (a logic-bomb placed in a payroll package, for example) are harder to detect.

Make sure that all passwords to systems that the ex-employee used are changed, including encryption passwords on PCs and log-in passwords on mainframes and networks, and change them again after a couple of weeks in case he or she still has sympathetic friends on the inside.

It is common for a sacking to be accompanied by a glowing reference in order to soften the blow. *Under no circumstances should you ever give a reference to anyone who has been sacked for data misuse.* The chance to pass the miscreant over to your rival may be tempting, but *you open yourself to the possibility of legal action if he commits the same crime against his new employer* and you are found to have known about his criminal tendencies yet not to have disclosed them.

In the case of a resignation rather than a dismissal, the rules about changing passwords still apply. You should also consider allowing the employee to leave almost immediately instead of working out a period of notice. Any staff member with access to data such as sales records, client lists and so on should not be allowed to remain at his desk for more than a few hours after resignation, and should be warned that legal action will be taken if current clients are found to start favouring the resigner's new employer.

It is common for an employee to be given a friendly farewell chat with his manager when he announces his resignation. Use this interview to find out whether there are any major grievances among the remaining staff. Also, ask why the employee has decided to resign and always find out how long ago the decision was taken. If the period since the resignation was planned coincides with the employee spending an unexpectedly long time at the photocopier or near a disk copying machine, it may be worth asking some questions.

Contingency Planning

If it does not already exist, a contingency plan must be worked out and tested as soon as possible. As a bare minimum, the plan should cover backups, virus outbreaks and hardware failure. Until you or your security manager can provide answers to the following questions, your company's data is at risk:

- If the LAN server were to be stolen this evening, would the thieves be able to access its data? Do you have the serial number, so that the police can notify you if it is found?
- Is there a recent backup? If so, how recent? Do you have a copy of the software to restore the backup? Has the integrity of the backup been tested?
- Have you ever performed a complete backup and restore for test purposes?
- If a virus is suspected this afternoon, do staff know what to do? Do they know who to report the incident to? Could you trace the source of the virus?
- Could you find out which other computers might have been infected?
- Have you ever conducted a virus drill, where you or your security manager have monitored the effects of planting a fake virus on one or more PCs?

6 If You Suspect A Security Breach

If you suspect, or if you receive a report of, a security breach there are many actions that can be taken. The precise form of this action will depend on the desired outcome: do you want to clean up and preserve your data (in which case, see also the chapter on insurance) or simply catch the offender at all costs?

There are many ways of catching the suspect. The obvious ones are 24-hour guards or the installation of closed-circuit video cameras and recording equipment. The problem here is that the perpetrator will realise that he is close to being caught and will probably decide that further acts would be too risky to carry out. That the misuse of company computers is stopped may be satisfactory for you, and you may consider taking no further action once the cameras or guards have been installed. However, the suspected employee will probably still be itching to get his fingers on your information and will quickly turn his attention to a part of the company that is less well protected.

The only way to stop this is to detect the culprit at an early stage. If a demand for a name produces no results, the following uses of technology may provide enough information on the patterns of computer misuse to give a clue as to the misuser.

Installing Telephone Logs

Most modern telephone switchboards have a logging facility that will keep records of all calls made. For each call, the number dialled is noted, plus the duration of the call and the extension from which it was made. Check the log alongside the staff signing-in book and look for calls made by staff who are known not to have been on the premises at the time. This will tell you who is deliberately making calls from another person's extension.

The programmable facilities on modern switchboards are often accessed via a password that must be typed in on the switchboard console itself. Ensure that

the default password that was installed when the switchboard was delivered has been changed, to prevent unauthorised use of the commands that turn off the logging facility.

Using Network Analysers

A network analyser is a program that is run from the Supervisor's workstation and allows the supervisor to "spy on" any other user. The supervisor is able to view on his screen an exact copy of the subject's screen, without the knowledge or consent of the subject. Your network supplier will be able to provide details of such programs, which are normally used for training and fault-finding purposes.

Keyboard Recorders

See the Resource Guide (page 155) for details of programs that can record all keystrokes typed on a PC or network terminal. It is possible to install such a program on a number of machines without the users' permission. Such programs record all commands typed, along with the time and date. Such logs can help you detect unauthorised out-of-hours use of PCs or users copying files that they are not permitted to copy.

It goes without saying that any employee installing such a recorder without good reason should be considered for instant dismissal, unless it can be proved that the program was not installed as an attempt to discover users' passwords.

Command recorders such as HISTORY (see the Resource Guide on page 155) can note the time and date that a command is typed, and the command itself, but not the name of the person who typed it. There are two ways to help put a name to the command. First, consult the signing-in book that the reception desk staff should be forcing all staff to fill in correctly. This may help you narrow down the list of suspects. Another possibility is to write or buy an attractive piece of software such as a game, and to place this on or near a PC in a place where it can be found by the intruder. The actual game that you install is not important, so long as it is one that asks the user to enter his name for inclusion on the high-score table. You may just be lucky.

If Files Are Being Deleted

If someone appears to be deleting files from a PC or a LAN without

permissions, there are three ways to prevent this happening and to help catch the culprit.

Delete Tracking

The Delete Tracking program, as supplied with MS-DOS 5.0, allows deleted files to be undeleted. This utility also records the date and time that the deletion took place, which may help to catch the person who deleted the file.

To install the delete tracker, type MIRROR /Tx, where x is the letter of the drive to track. Once this is installed (preferably in AUTOEXEC.BAT), typing UNDELETE /LIST will show all deleted files that can be recovered, along with the date and time of their last amendment and of their deletion.

Rewriting The DEL Command

If your network server has sufficient spare capacity, it is a fairly trivial task to set up user's PCs such that, when the user deletes a file, it is actually copied to the server rather than being deleted altogether. This task should be easily performed by any competent DOS technical support person or programmer; the steps involved are as follows:

1. On the server, create a directory called DELETED. We'll assume that the server is drive G: in this example.

Now, on each user's machine, do the following:

2. Patch COMMAND.COM and look for the table of resident command names. Change DEL to, say, DQL.

3. Create a batch file called DEL.BAT, and place this in the user's PATH. The batch file should consist of:
   ```
   COPY %1 G:\DELETED
   DQL %1
   ```

It is now the network supervisor's task to monitor the DELETED directory and to purge files when the need arises.

If this system is adopted, it is well worth adding a PKZIP to the batch file, to compress files before they are copied to the server. If this slows things down too much for the user, then the PKZIP command can be used on the contents of G:\DELETED directly, on a regular basis.

Involving The Police

The threat of having the Police called in to investigate unauthorised PC use or software piracy is a useful deterrent, and is well worth including in staff contracts and in the corporate data security policy. In practice, though, the Police are often unable to assist once they have been called in. Few police forces in the UK have sufficient staff with the skills to investigate computer crime. Those that do, tend to spend their time on secondment to the Home Office, touring the country to train other officers. This is known to be the case in the UK, and is probably repeated throughout Europe.

7 | Employing A Security Manager

Where a company is largely dependent for survival upon the information contained in its computers, it is essential to employ a full-time security specialist. Not only does this buy you experience and knowledge, but it means that security is clearly the responsibility of one named person. This may be seen simply as an easy way to provide a scapegoat in the event of a disaster, but it also means that staff who are worried about security know that there is someone to whom they can turn for advice.

The position of security manager should be a high-profile, highly paid post reporting to the most senior person possible. This is the only way to ensure that the company realises the importance that is placed on data security.

The Ideal Qualifications

According to recent studies by major management consultancy firms, the average computer security manager employed in a UK company has been in the business of computer security for just 8 months. This is because most UK management posts are awarded in recognition of long service rather than knowledge or experience. While this brings loyalty to the job, it rarely brings sufficient expertise and some training should be given as soon as possible.

The person whom you will charge with maintaining PC security must have thorough knowledge of both computers and security. A lack of real management experience is far from desirable, but a lack of technical or security experience is far more serious.

If you decide to recruit from outside the company, do not give away too much information to any candidate except the one who is eventually successful. By all means explain the sort of information that the company uses, but not where it is stored or details of where the current security loopholes are known to be. This caution can work in your favour, though. A standard interview question in your repertoire, when poach-

ing staff from other companies, should be to ask the candidate where he considers the major loopholes in his present employer's systems lie.

Ask for references from previous employers, and make sure that these are taken up. Write to each previous employer and ask specifically whether the candidate was involved in any incident that might lead to doubt as to his or her honesty or integrity.

Ask to see all examination certificates, including university degrees, that the candidate claims to have, and check their bona fides with the relevant examination board or university.

During all interviews, ensure that one or more members of your technical staff are present so that you can talk to the candidate on a technical level. When briefing the successful candidate, and at all subsequent meetings, never give the impression that you, as his boss, know nothing about the work he does. Saying "I really don't understand what you do; it's all gobbledygook to me" is effectively admitting that there is little chance of the security manager being caught if he chooses to abuse the authority and responsibility that he has been given.

Interview Psychology

This Guide does not pretend to be a general-purpose management handbook and we will not dwell extensively on staff matters. However, the psychology of interviewing is crucial when recruiting staff who will be trusted with sensitive information. For this reason, it is worth mentioning here, if only so that you may realise its importance and invest in a book or some training that covers the subject in more depth.

The four key qualities that you are seeking in a security manager are technical knowledge, security experience, honesty and loyalty. While the first two of these can (and must) be measured with standard testing techniques, gauging loyalty and honesty can only be done with carefully-constructed questions and tests. Some possible ways of testing loyalty and honesty are detailed below.

- During the course of the interview, let slip some confidential information about your company, ie the one with whom the candidate is applying for work. Naturally, the information should be fake! For example, mention that the research labs had a virus infection last year, and that some valuable data was lost. Or that you know for a fact that there are dozens of copies or pirated software in use throughout the sales department. Make it clear that such information is private and must not be disclosed, even to other staff within the company.

Having planted the information carefully during the interview, tell the candidate that the first part of the interview is now over and that he must now talk to the personnel manager. The personnel manager (or whoever you choose to pose as the personnel manager) should attempt to coax the candidate into parting with the confidential information that he has been given. For example, the personnel manager can bring into the conversation the fact that one of the candidate's duties will be virus protection. "It would be a disaster if a virus hit our company. Nothing has happened yet, and I hope it never will." Or "If you are looking for pirated software, which department do you normally start with?".

- There is another way to try to persuade the candidate to part with the so-called confidential information that he has been given. Inform the candidate that you need to test his communications skills.

  "Put yourself six months in the future. Pretend that you have been working here as security manager for six months, and you come across an advert from IBM. IBM is seeking a security manager with six months' experience, and they're offering twice the salary that we're paying you. Write a letter to IBM, applying for the job and explaining why you think you are qualified for it."

  Leave the candidate alone for 20 minutes to write the letter. Even at this stage the candidate should be showing signs of loyalty to you, a potential employer. Read his letter, looking for instances where he has given away confidential information. For example, "I am experienced in all sorts of disaster recovery procedures" is acceptable. "I helped recover my managing director's spreadsheets when a disk was stolen from his car" is not.

- Before the interview place a closed folder on the desk, away from windows and draughts, and mark it clearly but discreetly as "private and confidential". Place a hair, a grain of sugar or a similar item on the cover in such a way that it will fall off if the folder is opened. During the interview, make your excuses and leave the room for a few minutes.

The Security Manager's Duties

The security manager that is ultimately employed must be given a written job description so that he knows exactly where his responsibilities lie. He must also be told precisely the extent of his jurisdiction, including how far he is permitted to go in the pursuit of employees suspected of breaking the rules. You may like to consider some of the following points for inclusion in such a job description:

Monitoring

You should not spend more than 60% of an average working week in your office. Instead, you should be making regular unannounced visits to computers and users around the company, ensuring that all is in order and that staff are aware of your existence.

Policy Implementation

You should draw up a company-wide data security policy and plan for its implementation and policing. You must also ensure that procedures are in place for testing adherence by staff to the policy. For example, you should regularly check that staff are not keeping passwords written down and that access codes are not being shared. Occasional random checks should be discreetly made to ensure that sensitive and valuable data is secure and backed up.

Responsibility And Jurisdiction

You have full responsibility for all data security matters. In instances where the security of the company has been known to have been compromised, you must report the incident to your superior. Where problems are detected early enough that they can be cleared up, you may wish to co-operate with staff to ensure that the problem is eradicated in return for agreeing not to report the incident to a higher authority.

[Although this is far from ideal, from a management textbook point of view, it leads to far better security than forcing all security breaches discovered by the security manager to be disclosed, as no security manager will voluntarily put his job on the line by documenting all the loopholes in the policy that he was charged with implementing policing.]

Data Protection Act Compliance

It is your duty to ensure that the data processing carried out by the company is in compliance with the Data Protection Act and any other relevant legislation currently in force.

Recruitment

Where necessary, the security manager may need to employ further security staff. Other senior managers of the company must be involved in this process, to prevent the security manager building up a team whose aims may not always be in the best interest of the company.

Remember that one of the most effective deterrents against theft is the concept of dual control, where sensitive tasks are carried out by two people even though one would normally suffice. High street banks, for example, always ensure that no one person has access to both the front door keys and the strong room combination. Also, the person who takes in a transaction over the counter is not allowed within 20 feet of the computer terminal where that transaction is actually entered into the accounting system. *If a security manager is given free reign over whom he employs, much of the benefit of dual control can be lost.*

8 Backup

Backup is the most important and effective form of protection from accidental and deliberate loss of data. Although there are many software utilities that claim to be able to un-erase disks or recover data from broken computers, such software is no substitute for having an intact, up-to-date copy of the data held in a secure location.

The most common problem that will ever afflict a computer is user error. Users who accidentally delete files or type incorrect values into accounting packages are far more common than floppy disks being rendered useless by a stray magnetic field. For this reason, taking regular backups is the biggest single improvement that you can make to corporate information security.

Backup software consists of two main parts, normally known as backup and restore. Backup is the process of making a copy of all or part of a (normally hard) disk. Restoring is the process of extracting the data from the backup in the case of loss of the original copy of that data.

It's crucial to bear in mind that, in all probability, every PC will suffer at least one serious fault during its period of use. This is the case whether you buy a well-known brand or a back street clone for 20% of the price charged by major manufacturers.

Even manufacturers freely admit that every PC will fail during its lifetime. Hard disk units typically have an MTBF (mean time between failures) rating of around 20,000 hours. Assuming that a file server is switched on for 365 days per year, 24 hours a day, that works out to an average of one hard disk failure every 2.2 years. If the controller card has a similar MTBF, then one or the other will fail every 13 months or so.

The hard disk and its associated controller card, as well as the power supply, are the components of a PC that are most likely to fail. Each of these components, when it does fail, will almost certainly result in the permanent loss of some or all of the information on the PC or server.

Full And Incremental Backups

All but the most unsophisticated of backup programs provide facilities for either a full or an incremental backup. A full backup is just as the name implies; every file on a disk, or every file in a specified set is backed up. An incremental backup is quicker. It backs up only those files from the specified set that have been altered since the last full backup was made. Perform a full backup wherever possible, and use incremental backups sparingly. Although MS-DOS includes a facility that lets a backup program determine whether a file has changed since it was last backed up, this feature is not foolproof and represents yet one more source of potential problems.

Backup Media

There are many types of media onto which backups can be made. These are detailed below, along with recommendations for which type of media should be used for specific purposes.

Another Part Of The Same Hard Disk

It is fairly common for a user to back up one part of a hard disk onto another part of the same hard disk. Sometimes this is done by using a feature of MS-DOS that allows one physical hard disk to be "partitioned" into two or more drives. Each drive appears to be a separate unit, and can be referenced by its own letter, but is actually part of one physical hard disk.

Such a system is permissible for very short term (one day or less) backups. For example, if a user wishes to keep a copy of a spreadsheet while performing some experiments on another copy of the same file. For any other purpose, such a backup method is asking for trouble. If the hard disk unit develops a fault, both the original data and the backups will be lost. The same situation will arise if the hard disk controller card becomes faulty, or if an error is introduced into the partition table. This is the part of the disk that MS-DOS uses to work out where one partitioned drive ends and the next one begins.

There are also programs called low-level formatters which can delete all the information on an entire hard disk, even if it has been partitioned into many drives. Such programs should not be made available to users; they are normally used only by engineers but are supplied as standard with many of today's PCs.

Another Hard Disk In The Same Machine

Where a machine has two physical hard disk units, there is a temptation to use the second unit as a backup. This has the advantage that the whole operation is very quick and can be performed while the machine is unattended. However, both hard disks are usually operated by the same controller card which, in the case of a controller fault, can lead to corruption on both drives.

A business acquaintance of mine, who makes a living restoring data from damaged disks, frequently tells the story of the man whose PC had two hard disks, one of which was used as backup. One night, the PC was stolen.

Floppy Disks

Floppy disks are the most frequently used backup media on PCs. They are cheap and widely available and very (though not 100%) reliable. There are many commercial software packages for backing up a PC's hard disk, or parts of it, onto floppy disks. Many of the programs offer built-in compression features to reduce the number of floppy disks required, though such features should not be used when backing up critically important data as this makes the information much harder to recover manually in the event of problems.

Tape Cartridges

A tape streamer is a device rather like a domestic cassette recorder that will back up a PC onto one or more tape cartridges. These cartridges can only be used as backup media and not as a substitute for hard or floppy disks for day-to-day use, because of the comparatively long time taken to locate a particular file.

A tape cartridge typically holds between 20 and 500 MB of information, which means that all but the largest hard disks can be backed up onto a single cartridge. Tape streamers are available as internal units that fit into PCs, or as external devices that can be plugged into several PCs in turn. Tape cartridges are the standard way of delivering UNIX-based application packages and operating systems, so tape streamers are often fitted as standard into PCs that will be running a version of the UNIX operating system instead of the more common MS-DOS.

Tape streamers are supplied with proprietary software, though many commercial backup packages designed for use with floppy disks will also work with the market-leading tape streamers.

The Network Server

PCs connected to a LAN can be backed up quickly and efficiently by copying all the data from the PCs' hard disks to the network on a regular basis. The network file server can then be backed up to a tape streamer or optical disk by the network support staff. This method is very convenient, though the risk posed by loss of the network server or its backup is severe. For this reason, great care must be taken, and at least two backups of the file server should always be made and thoroughly tested.

The main disadvantage with backup to a LAN is that the performance of the network will slow down rapidly as several users choose to back up their PCs at the same time. Avoid implementing a rule that says all employees must back up their machines to the network every Friday afternoon, or the system will grind to a halt. Instead, the network supervisor should set up all workstations so that they automatically back themselves up to the server at various times during the week. Some machines will obviously need to be backed up more frequently than others, depending on the way in which the machines are used.

If you use a standard MS-DOS COPY or XCOPY command to back up workstations to the server, ensure that regular checks are made on the server's hard disk capacity. Several companies have discovered non-existent backups, which happened because a user blindly copied his entire hard disk to the network server without checking that there was space on the server to receive all the information.

For more network-specific backup information, see page 135.

The Corporate Mainframe

PCs connected to a corporate mainframe or minicomputer may be backed up to that machine in a similar way to those machines connected to a LAN. However, storage space on mainframes is comparatively expensive.

Optical And WORM Drives

Optical and WORM drives are among the most recent backup media to reach the market and offer lots of significant improvements over other media. The greatest benefit is the storage capacity.

An optical disk looks similar to an audio CD but needs a special machine to access it. You can read from and write to an optical disk, just like a floppy disk, but the capacity is around the 600 megabyte mark. That's 500 times the capacity of a high-density 1.2 megabyte floppy disk.

Also available are WORM drives, which are similar to optical disks except that data written to a WORM drive cannot be erased. Once a WORM disk fills up, therefore, it provides a permanent record that is useful for audit trails of financial data where tampering must be easily detectable.

Digital Audio Tape

DAT is the technology which provides CD-quality sound on domestic Hi-Fi equipment, using special digital cassette tapes and a special player. DAT recorders can also be adapted to be used as computer backup equipment, offering capacities of up to 1.3 gigabytes (GB), or 13,000 MB on a single cassette which can easily be slipped into a shirt pocket. Such technology is far from commonplace at the moment, but will undoubtedly spread in the coming years.

Bernoulli Drives

The high capacity and easy transportability of Bernoulli cartridges make them useful for backup data. See page 16 for details of the Bernoulli principle.

Choosing A Backup Program

If you are backing up your PCs to anything but floppy disks, you are limited in your choice of backup software. Normally, the backup device will be supplied with custom software. Only when the backup medium is the floppy disk do you really have a choice of software package, though some of these floppy-disk backup programs can drive the more well-known tape streamers.

MS-DOS is supplied with a backup utility as standard. The utility is actually two separate programs known as BACKUP and RESTORE. As backup programs go, these are unfriendly, slow and cumbersome and should never be used except in emergencies. There is also a known bug with some versions of BACKUP and RESTORE as shipped with Amstrad PCs, such that the RESTORE program claims that the backup floppy disks created by BACKUP are empty when in reality they are not.

When choosing a backup program, speed, flexibility, ease-of-use and reliability are the main criteria by which such programs should be judged. Whichever package you decide to use, stick to the same program throughout the whole organisation. Mistakes which occur because a user

thought he was using one package when in fact he was using another cannot be tolerated with backup operations.

Speed

The speed at which a backup is made is crucial, as staff will be unwilling to perform regular backups if the process takes an unacceptable length of time. To speed up the process, most of today's commercial backup programs (but not MS-DOS's BACKUP and RESTORE) use a technique known as data compression. This compresses the data before backing it up, which normally saves time by demanding fewer disk swaps by the user. Needless to say, the technique saves disks too.

The recommendation of this Guide is that data compression should not be used for critical data backups, as the data will be extremely difficult to recover from the floppy disk in the event of a fault with RESTORE and a consultant having to attempt a manual recovery with the use of special software tools.

Speeding Up Backups

One way to speed up the backup process is to back up only a user's data files, and to leave application programs to be restored from the master disks in case of emergency. A well-structured hard disk, with all programs in separate directories, and with no data files in program directories, makes this easy to set up.

However, remember that some files contained in a program directory are actually data files and should be backed up regularly in order to avoid the need for much tedious work in the case of their loss. Such files include:

- All .INI and .GRP files which are in the Windows 3.0 directories.
- CONFIG.SYS and AUTOEXEC.BAT files from the root directory.
- All .SET files from a WordPerfect program directory.
- Setup information used by memory managers, hard disk managers, data caches etc.

These files contain users' preferences and other settings, and their contents often mature over many months of use. The loss of these files can often be disastrous and, therefore, they should be backed up frequently.

Flexibility

Sometimes you will wish to backup the entire contents of one or more

hard disks. Sometimes, however, you will only wish to backup important files or those that have recently changed. Most modern backup programs include such facilities. You can set up various backup profiles, each of which contains a list of files, directories and/or disks, and any of these profiles can be used to automate a backup process. Different users on a network can often be assigned their own profiles, to backup only their own directories and/or the shared areas to which they have access.

The methods used by various programs to define and manage these profiles varies greatly, and it is well worth trying at least two packages in the search for a standard package to use within the company.

For audit and security purposes, backup packages normally produce a log file that records the date that each file is backed up. *Make sure that this file contains all the information that you will require, and remember to copy it to a floppy disk once the backup has been created.*

Ease Of Use

Some backup programs are easier to use than others. Configuring the program for a number of users, all of whom wish to backup different parts of a hard disk, can sometimes be difficult and tedious. Ensure that the package you choose makes this task relatively painless, and that it is easy to make permanent or temporary adjustments to the list of profiles.

Reliability

You should never assume that it will always be possible for a set of backup disks to be restored without error in the case of data loss. I hear stories every week of users who suddenly lose the contents of a hard disk and have to dig out an old set of 30 backup disks, only to find that many are unreadable.

Some points to check are:

- *Ensure that the RESTORE part of your backup package will let you skip unreadable disks, rather than abandoning the entire operation.*
- *Make sure that the BACKUP program also includes a VERIFY option to read back the contents of a backup disk immediately after it has been created and to compare it with the contents of the hard disk that has been backed up.*
- Some backup programs attempt to push the PC's hardware to its limits in order to achieve a faster backup speed. These programming tricks may not work on all PCs. Ensure that the BACKUP program

allows such quirks (often referred to in manuals as direct DMA access) to be turned off by the user.

- Some backup programs format the floppy disks to their own standard, rather than the normal MS-DOS arrangement. This means that the backup disks are readable only by the backup and restore programs and not by a data recovery expert with special DOS-based software to help you recover your data in the event of a problem. For this reason, do not use any backup program that cannot create standard DOS-format floppy disks.
- *Test a new backup program by backing up to two different types of media (floppy disks and, if available, a tape streamer) and then attempting to restore the backup.*
- Never buy the first release of a new backup program. Let someone else find the bugs.

Formulating A Backup Strategy

If you do not have a backup strategy in place, ensure that one is defined as soon as possible and that staff know the penalties for not adhering to it.

Backup To Mass Storage Device

Where backup is to a mass storage device such as an internal tape streamer, network server or mainframe, the process is simple enough to be performed in full on a regular basis. In such instances, a full backup of the machine can be performed overnight or during a lunch hour. The backup should be checked by the network supervisor, support engineer or staff member to ensure that it is complete and properly readable. The only way to do this is to attempt to restore it onto another machine.

If a tape streamer is being used, it is essential that a re-tension operation be performed prior to each backup. This involves running the tape all the way to the end of the cartridge and then back again. If this is not done, the possibility of a failure increases greatly.

Backup To Floppy Disks

Where the backup medium is a set of floppy disks, some more thought must be put into the formulation of a backup strategy. There is little point is making a general rule that all staff must backup their entire hard disk every two days, as anyone with a large hard disk containing what is considered to be expendable files will not be willing to do this.

All modern commercial backup programs have the ability to backup files on a directory-by-directory basis. Therefore, the most efficient way to organise backups is to ensure that users keep all important files in one or more directories, and that only these important directories are backed up regularly. The remainder of the machine, containing application programs and other replaceable files, need only be backed up much less frequently.

When neglecting to back up directories that contain application programs, bear in mind that the setup and configuration files for certain applications may have taken a long time to tune properly and may contain many weeks' of work. For example configuring Microsoft Windows to run correctly on a machine, and setting up the various screen groups and .PIF files to run applications correctly, is a never-ending process. These setup files are stored in the same directory as the Windows programs and the backup program should be instructed to include these files in the regular backup process.

When buying floppy disks for backup, do not skimp on costs and do not use a disk more than once.

Motivating Staff To Take Backups

The best way to motivate staff to take regular backups is to convince them of the benefits. The benefits to staff of taking backups include:

- A security precaution in case they accidentally delete data.
- Protection against computer failure.
- They will not be sacked in the case of loss of sensitive data.

An excellent way of ensuring that staff take backups is to use the "fire drill" method as thought to be used by many UK Government offices. This involves placing notices in all offices that say:

At 11am on the first Wednesday of every month there will be a fire drill, and you will be required to evacuate the building in accordance with the standard regulations.

During the evacuation, members of the PC Support department will visit a number of offices and will, at random, delete certain key files from PCs. The files will be deleted in such a way as to make recovery via standard UNDELETE utilities impossible. Copies of the deleted files will be taken, and will be stored by the security manager for a period of one week.

It is essential that you ensure your PC is properly backed up before the fire drill

takes place. Disciplinary action will be taken against any employee who finds need to ask the security manager for a replacement copy of one or more files.

Note: If scheduling a weekly backup, do it on Thursdays rather than Fridays, to lessen the risk of being caught by a "Friday the 13th" virus and not having up-to-date backups available.

Verifying Backups

It is not safe to assume that, once you have made a backup, the set of disks or cartridges on your desk now contains a copy of the files that you backed up. For example, there have been many cases in the past of a tape streamer whose motor had broken. This means that the tape never moved in the cartridge, and all the information during the backup was recorded over and over again on the same inch of tape.

There is only one guaranteed safe way to verify that a backup is complete and intact, and that is to attempt to restore it. This operation should always be done when using a particular backup program on a particular PC for the first time, and should be done every half-dozen backups thereafter. Where highly sensitive data is involved, the test restore should be performed every time.

When testing a restore, never restore to the same machine that was backed up; use a separate machine. Otherwise, if the backup disks are corrupted, you will replace the only good copy of the data with a corrupt copy.

When restoring a backup for test purposes, you should check file lengths and totals as a bare minimum. Ensure that the number of files restored is the same as the number backed up, and that the length of each restored file is correct. I know of at least one case where a new backup program was tested and, despite the backup going smoothly and the "verify" option producing no problems, the restore process produced six fewer files than had been backed up.

Storing Backups

Unless some simple common-sense rules are followed, it's all too easy to ruin a set of backup disks or cartridges. Worse still, you may only discover that the backup is unusable when you really need it.

Rules to be followed, in order of importance, are:

- *Never store backup disks or tapes near the machine that has been backed up.*

Backing up a PC onto a box of disks and then storing the disks in a desk drawer is just asking for trouble from leaking radiators, burst pipes, thieves and so on. If the company has no fixed policy for backup storage, and no fire safe, take the disks home or leave them in the car. If disks are left in a car, though, keep them out of direct sunlight or they will warp.

- *When you back up a PC to floppy disks, keep a bootable operating system disk in the box of backup disks, along with a disk containing a copy of the RESTORE program.* Many companies have run into problems when a broken hard disk was found to have held the only copy of the program that would restore the data from the backup disks.

- *If backing up to tape, keep a copy of the tape-reading software on a separate machine and on a floppy disk.* I know of at least two companies who lost a hard disk but were unable to restore from tape as the only copy of the tape-reading software had been on the hard disk. There was a delay of three days before a new copy of the software could be obtained.

- *There is little point in putting the copy of the tape-reading software on the tape itself.* According to security consultants, however, this is a fairly widespread practice by users who fail to think ahead.

- When backing up a PC, obtain a program that will print out the information stored in the machine's CMOS memory and keep this printout with the backups. Among the crucial information stored in CMOS memory is what's known as the hard disk type. This is a number between one and 1000 that represents the characteristics of the hard disk and if the CMOS memory gets corrupted or erased, the hard disk cannot be used until the number is replaced in the CMOS memory.

The following BASIC program will interrogate CMOS memory and report the drive type number of the hard disk installed as drive C. If you do not know the type of the drive in a machine, run this program and ensure that a note of the drive type is kept somewhere safe. The program will run under the GWBASIC interpreter, or any Microsoft BASIC compiler including the QBASIC product supplied with MS-DOS versions 5.0 and above. For completeness, the program will also report the type of floppy drives installed as drives A and B.

```
100 CLS
110 PRINT"Read CMOS and display hard and floppy"
120 PRINT"disk type numbers."
130 PRINT
140 PRINT
150 OUT 112,18
160 PRINT "Hard disk C type is";
170 DC = INP(113)
```

```
180 DC = DC AND 240
190 DC = DC / 16
200 IF DC  15 THEN PRINT DC
210 IF DC = 15 THEN OUT 112,25:PRINT INP(113)
220 REM Now look at floppy drives
230 OUT 112,16
240 FD = INP(113)
250 DRIVEA = FD AND 240
260 PRINT"Drive A is ";
270 IF DRIVEA = 0 THEN PRINT"Not installed"
280 IF DRIVEA = 16 THEN PRINT"Double sided"
290 IF DRIVEA = 32 THEN PRINT"1.2 MB 5.25"
300 IF DRIVEA = 48 THEN PRINT"720 KB 3.5"
310 IF DRIVEA = 64 THEN PRINT"1.44 MB 3.5"
320 DRIVEB = FD AND 15
330 PRINT"Drive B is ";
340 IF DRIVEB = 0 THEN PRINT"Not installed"
350 IF DRIVEB = 1 THEN PRINT"Double sided"
360 IF DRIVEB = 2 THEN PRINT"1.2 MB 5.25"
370 IF DRIVEB = 3 THEN PRINT"720 KB 3.5"
380 IF DRIVEB = 4 THEN PRINT"1.44 MB 3.5"
```

- *Invest in a fire safe for the secure storage of backup media and other important software. The safe must be kept locked at all times and never left unlocked for more than a few seconds; if there is a fire, no one is going to think to check it.*

- When buying a fire safe, ensure that it is watertight too. There are numerous stories of companies who bought fireproof safes, the contents of which were destroyed by a flood. If a disk is accidentally soaked by cold water, it is usually possible to recover it; see the Troubleshooting chapter which starts on page 129.

- Portable fire safes are good protection against fire when only 50 or so disks are involved, but keep the portable safe in a larger safe to prevent theft.

- If you do not have a suitable site for storing backups, or if the backups take up too much space, there are companies in what's known as the security archive business who will store the material for you in their own secure buildings. However, no one is going to be as concerned for your data as you are, and the general advice is not to use security archive companies unless there is a pressing need to do so. A better alternative, when there is only a few tapes, is to keep them in a safety deposit box at your local back.

- Backups, especially large sets or those that contain a backup of a LAN server, should be accompanied by full documentation that lists the full pathname of each file (eg C:\PAYROLL\1991\SALES.WK1)

and, wherever possible, a brief description of the files in each directory and the name of their creators.

Before Restoring

In the event that you need to restore lost data from a set of backup disks or tapes, there are several actions that should be taken first. If you make a mistake at this stage, it is very easy to lose the backup in the same way as you lost the original data. *Before using a RESTORE program, read the notes in the Troubleshooting chapter which starts on page 129.*

9 | Viruses

An infection by a computer virus is potentially one of the most dangerous incidents that can afflict a computer user or a department that uses PCs. If not handled correctly, vast amounts of damage can be done. The threat from viruses is real, yet the possibility of damage can be totally eliminated by a little thought and planning.

What Is A Virus?

A virus is a computer program that has the ability to copy itself. A program that does not have this property is not a virus. A program that claims to be a spreadsheet but actually reformats your hard disk is not, therefore, a virus; it is what's known as a Trojan Horse. This is still dangerous to your data, and should not be ignored, but such a program is easier to remove as it is simpler to trace the other computers which contain a copy of the trojan horse than it is to track a virus.

The ability of a program to copy itself is not, of course, dangerous. All that you end up with is a program which spreads to all the computers in your company. The reason that a virus is dangerous is that many of them will deliberately damage your computer by, for example, deleting or corrupting files.

It is the combination of the ability to copy itself, and the ability to damage your data in unpredictable ways, that makes a virus so dangerous.

Who Writes Them?

Viruses, like spreadsheets and word processors, are written by programmers. Viruses don't simply appear by accident, they are written by people. The reasons why people write viruses can be found in psychology textbooks; our only concern here is to help you detect and destroy viruses and to clean up after them.

How Many Viruses Are There?

There are currently known to be at least 1000 known viruses in circulation.

What makes one virus different from another? In many cases, hardly anything at all. Someone simply takes an existing virus and makes a minor change to it. Sometimes, though, totally new viruses appear. For example, as soon as one company releases a program designed to search for viruses and erase them, the virus writers try to decipher the program and designs a virus which will be immune to the particular detection system used.

How Does One Catch A Virus?

Almost without exception, viruses are caught from floppy disks. The UK press has recently led the PC-using public to believe that dial-up bulletin boards are the main source of viruses. In the experience of many researchers to whom I have spoken, this is not the case. The availability of modems to staff who use PCs is less than 10% yet almost every PC user has access to a machine with one or more floppy disk drives.

How Viruses Spread

An example of how a virus can spread goes something like this:

1. Alan, the Sales Manager, has a problem with his PC's floppy disk drive. He shows it to the PC Support department, who decide that the machine should be returned to the dealer for repair.

2. The machine is taken to the repair shop. While repairing the machine, the engineers notice that the machine contains some interesting games programs so they decide to take a copy for themselves. This is common practice among many computer dealers in this country, and is one reason why you must never send a PC for repair that contains confidential information.

3. In return, the engineer copies a new game called MINIGOLF to Alan's computer.

Unknown to the engineer, the MINIGOLF program has been infected with a virus for the last few weeks. The virus is now on the machine, in the MINIGOLF program.

4. The dealer returns the PC to the sales manager, who starts using it normally. The dealer explains that he thought Alan might like a golf program, which has been copied to the PC ready for use.

5. Alan runs the MINIGOLF program. The virus has attached itself to the start of the program so that, before the game starts, the virus springs into action. It first loads itself into the PC's memory. This memory-resident program will now keep watch on every program that Alan runs. The virus will attach itself to any program that is not already infected. An infected program will then act in a similar way to the MINIGOLF program.

   Having loaded itself into memory to look for other programs to infect, the virus also does something else. It looks at the computer's built-in clock/calendar. If the date is Friday the 13th, the virus picks a file at random from the hard disk and deletes it. If the date is not Friday 13th, no damage is done, but the virus is still there.

6. Later that day, Alan runs a program called FILEBOOK to update his accounts. The virus attaches itself to the start of the FILEBOOK program in the same way that it attached to MINIGOLF.

7. The next day, Alan's secretary needs to copy the FILEBOOK program onto her machine from Alan's hard disk. She copies it to a floppy disk, and then onto her hard disk. She runs FILEBOOK on her machine, and the virus at the start of FILEBOOK performs the same actions on her machine as MINIGOLF did on Alan's.

We now have two machines that are infected, each of which will suffer random damage when the date is Friday 13th. Any program copied from one of these two machines will infect another computer, at which point there will be three infected machines. Before long, all the PCs in the company have the virus. What is more, every floppy disk in the company may contain a file that carries the virus at its start in the same way as MINIGOLF and FILEBOOK do. And what about the floppy disks that the company has given to clients?

Common Ways That Viruses Spread

Once a virus finds its way into an organisation, it can spread very quickly as staff share disks and computers amongst themselves. But how does a virus find its way into a company in the first place? There are many possible ways that this can happen, and just some of them are listed below. These represent ways in which real UK companies have been infected with a virus in recent months:

- In December 1991 a computer games magazine included a free floppy disk on its cover. Some 20,000 copies of the disk were sent to newsagents all over the country, and over half of these had been sold before it was discovered that a virus was present on the disk. It is thought that the virus infected the master disk when it was being prepared in Germany by the magazine's owners, and was not detected by the UK-based duplicators.

  If you must use a program which has been distributed on the front of a magazine, wait until 2 weeks after publication. Then call the magazine's offices and, if no problems have been reported, use the program.

- In January 1992, Novell sent out a set of NetWare maintenance utilities to all Certified NetWare Engineers. The 5.25" version of the disk contained a virus. Luckily, the virus was more of an inconvenience than a disaster, as it causes computers to hang rather than to lose data. However, Novell's credibility suffered a serious setback.

- In 1990, at least one major supplier of shrink-wrapped software for the Apple Macintosh inadvertently supplied its customers with a virus. Yet again, the source of the infection was never traced.

- In 1991, someone deliberately added a virus to a well-known Shareware program and released it onto a number of dial-up bulletin boards. The infected version was announced as being a new version of a popular program, which encouraged many users to download and run it.

How To Detect A Virus

There are lots of software products on the market which will scan the programs on your hard disk, and the memory in the machine, looking for viruses. These programs contain small harmless extracts (around 16 bytes) from every known virus, and they look through the machine for occurrences of these 16-byte signatures. *It is strongly recommended that you install one of these programs on all machines, and use it regularly.*

Because new viruses appear so often, the more reputable producers of virus scanning software also promise to send you updates every couple of months that include extracts from recently-discovered viruses. Some will even send these by fax, for you to key into the program using a special utility program that is also supplied.

Not all viruses check the date and delete files on Friday 13th. Some are less dangerous, and simply alter the screen display. Some of the ways in which you or a user can detect a virus are:

- *The lengths of files increase after they are executed.* The increase in length is the virus code which has attached itself to the start of the file. Sometimes the virus is sophisticated enough to intercept the DIR command and to give the impression that the length has not changed, so do not assume that a file which does not appear to change its length is clear of all viruses.
- A number of "bad sectors" appear on the hard disk, and utilities such as the Norton Disk Doctor report their presence. MS-DOS marks sectors as bad when a disk is formatted, so that these areas of the disk are not used. Viruses which need space to store their code often mark good sectors as bad, thus providing a place to store code which DOS will not use.
- Characters are erased from the screen at random.
- *Characters drop down the screen like a snowstorm.*
- Political and/or obscene messages appear on screen.
- Your PC magically types words into your word processing documents, often in response to your typing certain "trigger" words such as the names of world leaders.
- A PC is booted from a DOS disk, but the machine claims that the disk is not bootable and you should insert another. *At this point, do not insert another disk; the virus is in control* and will copy itself to the new disk. Turn off the machine instead, boot from a known clean disk, then seek assistance.
- *The speed of the PC decreases, partly because the virus is busy looking for programs to infect and partly because the virus has deliberately slowed down the machine.*
- The PC accesses the hard disk when you are not expecting it to.
- Files, or their names, become corrupted.
- The disk's volume label changes.

Some of the messages produced by viruses are only seen when the machine is first booted. With the "Stoned" virus in particular, the mess-

age appears at the top of the screen and informs you that your PC is now stoned. It also displays a slogan asking for the possession of marijuana to be legalised. Such messages often go unnoticed, as users tend to put a CLS (clear screen) command in their AUTOEXEC.BAT file, which has the effect of clearing the screen as soon as the PC has booted.

Proprietary menu systems also tend to hide messages produced by viruses. If you use such a menu system to help users load programs, or to limit the number of programs they can use, ensure that machines are checked regularly for viruses.

Ensure that all users are aware of the ways that a virus makes its presence known, and that everyone knows what to do if they suspect an outbreak. If the presence of a virus is discovered, it is far better to co-operate with the person who may have unwittingly introduced it to the company via a brought-in game, rather than sacking them on the spot. Only this way can you gain an insight into how far the virus may have spread.

What Is Not A Virus?

Over 90% of the calls that virus experts receive from worried PC users turn out to be false alarms. This is because there are many cases where a PC does something unexpected and the user assumes that, because it hasn't happened before, a virus must now be present.

Of course, if you are in any doubt then it's always advisable to seek an expert opinion if you suspect a virus attack. However, there are some instances where the perceived problem is actually harmless and no action need be taken. Examples of these situations include:

- Repeated "Bad command or filename" message when trying to run a program, where there were no problems in the past. This often happens because the PATH setting has been changed, so MS-DOS no longer knows where to look for the program. Also, it can happen if the user is not logged onto the correct drive.

- Appearance of hidden files. Some programs create a number of small, hidden files. The Norton Antivirus program, for example, creates one 77-byte hidden file for every executable file on a hard disk. This hidden file contains a checksum, and is used to detect changes made to a program by a virus.

  Although these hidden files are harmless, they each take up large amounts of hard disk space. Even though the files are 77 bytes long, they take up between 512 bytes and 4096 bytes according to the size

of the hard disk and the version of DOS in use. This is because of the way that MS-DOS organises the layout of a hard disk.

- The sudden change in size of the SETVER.EXE file, which is one of the files supplied with MS-DOS 5.0. This program records its data in its own .EXE file. Many virus detectors assume that the only time an .EXE file is altered is by a virus. This is not always the case. Using PKLITE, LZEXE or any other program which shrinks an .EXE file without renaming it may also lead a virus detector to jump to the wrong conclusion.

How To Protect Against Viruses

There is only one foolproof way to protect against loss of data from a virus attack, and that is to take regular backups. Some of the virus-detector programs also attempt to remove the virus from files but such techniques should not be trusted. *The only safe way to remove a virus is to format the hard disk and then to restore its entire contents from backups.* You must first make sure, of course, that the backup disks are free from infection.

It is worth subscribing to a virus information service which will fax you news of new viruses as they are discovered. You will also receive information of new virus detectors as they are released. Such subscription services are detailed in the Resource Guide.

As has been mentioned earlier, in the sample data security policy, you must control carefully the traffic of floppy disks into and out of the company.

Assign one PC as a place for testing new disks for viruses. All new software, even that which is bought in shrink-wrapped packages from a reputable source, should be loaded first onto this machine and subjected to a scan for viruses. Ensure that the machine is booted from a known clean DOS disk, as this will prevent a virus from intercepting the scanner and fooling the scanner into giving a clean bill of health to an infected disk. If possible, use two scanning programs to lessen the chance of a particular virus being missed. If you do use two programs, ensure that you use two different types. See below for a discussion of the different types of virus scanning packages.

All software disks, especially new versions of DOS, should be write-protected as soon as they are unwrapped and before they are used for the first time. With copies of DOS, this is the only way to ensure that you will be able to find a copy that is known to be virus-free when you need one, as nothing can get past a write-protected disk unless the hardware in the machine has deliberately been tampered with. To write-protect a 5.25" disk, cover up the notch in

the side with a sticky label. Don't use transparent or translucent sticky tape, as some write-protect mechanisms use a light beam which can pass through transparent tape. Write-protecting a 3.5" disk is achieved by sliding the black plastic tab so that the hole is open rather than closed.

How To Choose A Virus Detector

There are four ways in which virus detectors work, and many examples of programs that use each of the four methods. To keep your PCs safe from viruses you should use a cryptographic checksummer and also a scanner.

Cryptographic Checksummer

This program examines all the programs on a hard disk and constructs a unique signature for each one. On a regular basis, you run another part of the program to compare the programs with the signatures. If a program is found not to match its signature, this indicates that the program file has been altered and suggests the presence of a virus.

Before opting for such a program, check with the vendor that the checksums are calculated and stored in a secure way so that no virus could tamper with them.

Scanner

The scanner, as described above, scans each program file on a hard disk and looks for patterns which are known to appear in a number of known viruses. Scanners are faster than cryptographic checksummers, as they use intelligence to decide which parts of which files need checking.

Problems With Scanners

A scanner will only detect viruses that it knows about.

Ensure, when choosing a scanner, that it will work successfully with hard disks that have been compressed with a real-time compression utility such as SuperStor or Stacker. Scanners often access hard disks directly, instead of going through the official MS-DOS channels, which may render them unreliable when used with compressed drives.

Remember, too, that a scanner will not detect a virus in an archive file that has been compressed with a program such as PKZIP, LHA or ARJ. You should un-archive such files before scanning them.

File Size Checkers

This program records the length of each program file, then alerts you whenever the length is found to have changed. Not all viruses change the length of a file, and those that do find it easy to fool this type of detector. For this reason, this type of program should not be used.

Hard Disk Monitors

This type of program monitors the hard disk, and alerts you whenever a program attempts to store information on parts of the hard disk that are normally accessed only by viruses. Users of this type of program report regular false alarms which lead to a sense of complacency, after which the alerts tend to be ignored. This type of program should not, therefore, be used as part of an anti-virus policy.

In The Event Of An Infection

If you discover or suspect that your company's computers are infected by a virus, the advice is to call in an expert. Do not attempt to remove the virus yourself unless you are certain that you, or someone in your company, knows the process involved.

The whole process of removing a virus, finding its origins and ensuring that all traces of it have been removed is a non-trivial task. There is a handful of experts in the UK who have developed special software tools for removing viruses, and hardware devices for checking floppy disks at the rate of one every 10 seconds.

Remember that *if a virus finds its way into your company, the future of your organization may depend on successfully removing it and upon ensuring that your backup disks do not become contaminated.* Therefore, it always makes sense to call in an expert. See the Resource Guide (page 155) for a list of some known experts.

10 | Access Control

To prevent (and to help detect) unauthorised access to a PC, some form of access control is required. Remember that not all unauthorised access involves the deleting or copying of data - some hackers simply browse around the system. Unless you have access controls in place, such acts will be almost impossible to prevent or detect.

There are two fundamental ways of controlling access to a PC. The first is some form of physical control, such as locking the machine in a closed room and/or posting a security guard on 24-hour duty. The second way is to make the machine physically available but for the PC itself to control who is allowed to access it. This is achieved by special software and/or add-in cards which ask a user to identify himself. If the user is unable to do this, the machine refuses to grant access. If the user correctly identifies himself, the machine grants access to the parts of the machine that the user is entitled to see but not to any other areas.

The physical methods of access control have been covered in more detail elsewhere in this Guide and will be touched upon only briefly here. This chapter is primarily concerned with the subject of automatic access control by the computer itself, using software and hardware products. Details of actual products are not listed here; see the Resource Guide (page 155).

There are one or two PCs on the market at present which have built-in access control that requires a password in order to use the machine. Also, all data on the hard disk is encrypted when it is written to add a further level of protection. I know of only one simple way round such protection, and that is simply to swap the "secure" PC with one that has no protection. You then add some simple software to the imposter PC to make it appear protected, ie make it ask for a password when the user turns it on and save the password in a hidden file. There are many cases where this simple act is all that would be required to steal information. An example would be if the supposedly secure machine is only used as a place to which senior staff copy spreadsheet files for safekeeping.

Proof Of Identity

Almost all computer-based access control systems rely on a password to identify users. Each password is associated with a particular user and, if someone types in John's password, the computer assumes that the person must indeed be John and should be granted access to John's files.

The password is an inherently insecure system for identifying people. Users frequently swap passwords, or write them down in obvious places. Passwords are rarely changed by users unless they are told to do so.

If you run a password-protected computer, the security of the system can be tightened by ensuring that staff obey the following rules. Enforcement of the rules should ideally be performed by the host computer, though if this is not possible a strict warning from a manager will have to suffice.

- *Passwords must be changed every two weeks.*
- *Passwords must not be less than six characters in length.*
- *Wherever possible, a password should consist of two unrelated words separated by a non-alphabetic character. For example, CARROT&WIRE or CHOKE=BREAD.* Alternatively, use the initial letters of phrases or sentences. TBONTBTITQ is one example, unless the hacker is familiar with Shakespeare's Hamlet.
- Do not re-use a password that has already been used in the last 12 months.
- When changing a password, the new one should not rely on the old one. Using APRILFOOL for a password during April and MAYDAY during May, for example, should be discouraged. I once cracked a high-level account on a computer system; I knew that the first part of the two-level password was LIVE, and discovered that the second part was WIRE.
- Passwords must not consist of plain english words which would be found in a dictionary. This is especially important in UNIX systems.
- *Do not use your name, or any information about yourself, as a password.* This includes your address, your spouse's name, details about your car and your address.
- Do not use the following as passwords: FRED, SECRET, PASSWORD, LETMEIN, ACCESS, GUEST, HELP, MANAGER, SECURITY, SESAME, DEMO.
- When choosing a password ensure that it is pronounceable, even if

it is not a valid English word. This makes it easier to remember, and lessens the need to write it down.

- The host computer should reject a password that is in a format which appears to be a car registration number or telephone number. For example, a seven-character password consisting of a letter, three digits and three letters is almost certainly a car registration.
- *A password should never be used on more than one system.* This is especially important if staff have home computers that are used for calling free-access bulletin boards. Those who operate bulletin boards have access to the passwords of all users on that bulletin board, so these passwords should never be used on other computers.
- The mother's maiden name is rapidly becoming used as a standard piece of information for validation purposes. It is one of the questions on the application form for an account with a well-known UK bank, and is used as part of the authentication process if you call the bank and ask for certain actions to be taken on your behalf. For this reason, mothers' maiden names should not be used as passwords.
- Groups of staff in a department should not choose passwords that are related, eg HORSE, DONKEY, SHEEP, GOAT.
- Don't discuss passwords, or any other confidential matter, during a conversation when one person is using a mobile telephone. These devices are totally insecure, and anyone with a suitable radio receiver can listen in to conversations. Such receivers are available in many high-street stores.

The machine-generated password is often used. Here, the computer system generates a new password for each user every couple of weeks. The generated passwords are designed to be unguessable. Unfortunately, they are frequently so forgettable (and unpronounceable) that staff have to write them down.

Better Than Passwords

Authentication is the process of proving that someone is, or is not, who they claim to be. The three fundamental ways by which a computer can recognise a person are by:

- Something the person knows (eg a password).
- Something the person owns (eg a physical key or card).
- Something about the person (eg a signature or fingerprint).

The major flaw in a password-based authentication system is that it relies on only the first of these. Ideally, where strict security is required, all

three methods should be used. A number of products are available that provide a sophisticated authentication system; details are in the Resource Guide.

Where cost or other factors prohibit any authentication devices other than passwords, consider the use of one-time password systems. A user is given a one-time password generator, which consists of a small device that generates a 7-digit (or so) number each time it is used. This number is then used as a password. The password generator uses special routines to generate the numbers, and these routines are known only to the generator and the host software. Each password is unique, and the system automatically ensures that no password is used more than once and that each password is valid. Additionally, the host computer is capable of ensuring that the password generator has not been used more times than it should have been.

Controlling Information

Access control on PCs can do one of two things. First, when a PC has only one authorised user, the package can use passwords and encryption techniques to ensure that only the authorised user has access to the data and programs held on the machine.

Second, where more than one person is using the machine, the access control package segregates programs and data so that a user may only see and use the files that the package wishes him to see. Again, the protection is by passwords and encryption.

Software Solutions

Access control packages that work as described above come in two varieties, namely hardware- and software-based products.

Software-based packages typically work as follows. If the package is protecting access to an entire computer, the program usually tampers with one or more items of control information on the hard disk to make it unrecognisable to MS-DOS. Whenever the user attempts to access the hard disk, DOS will claim that the disk drive does not exist.

To un-tamper, a program must be run each time the computer is turned on, and this program requires a password before it will operate.

Access control programs that work in this way have one major flaw; it is possible

to write programs that can access data on a disk even if the control information has been tampered with. Common disk-fixing programs such as the Norton Utilities use this method. To get around this, the access control packages also usually have an optional encryption facility which will automatically keep everything on the hard disk in encrypted form. *If you use such a package, ensure that the encryption is always turned on or the package is next to useless.*

Where a software-based access control package is providing protection at the file level, similar methods are employed except that the program will recognise more than one password. Only one user will be given permission to add new users to the system and to specify which parts of the machine may be accessed by the holder of each password. Needless to say, the password controlling access to this supervisory level must be carefully guarded and changed regularly.

About Encryption

There are many ways of encrypting data. One of the best is known as DES, or the Data Encryption Standard. Some access control packages use DES while some companies prefer to invent their own system. The beauty of DES is that the method is publicly available (it is published in quite a few books) yet it is uncrackable without the help of thousands of years of computing time. Home grown encryption methods used by the vendors of access control packages usually rely for their security on the fact that the company will keep the algorithm secret. This is unacceptable, and you should never use any encryption system except DES, RSA or another similar method.

When deciding whether or not to use encryption, the simplest rule is to consider the difference between public and private channels of communication. If you prepare something on a disk, then pass it directly to a colleague, that is a private channel. If you pass a document over a network to which only you and he have access, that too is a private channel. But if the transaction uses non-private channels at any point in the journey, encryption should be used. Public channels include publicly-available telephone lines, PCs in unguarded offices and so on.

Hardware Solutions

The problem with access control packages that use software-only techniques is that the system can always be cracked with some other software. If there's a program in place that always encrypts data as it is sent to the hard disk, then another program can be written that stops the encryptor from working.

Although a PC protected by a software-based access control program that has all its encryption facilities turned on is far more secure than having no protection at all, the system is not unbreakable. For total protection you must use a hardware-based method, though even these methods will fail if they are not used properly by staff.

At the centre of the hardware solution is an add-in card that plugs into the computer. This takes control of the machine as soon as it is turned on, and asks for a password to be supplied. If the correct password is given, access is granted, otherwise it is not.

Encryption and decryption are handled by the card, which cannot be tampered with by software. Also, the encryption system used varies slightly with each and every card, ensuring that a stolen hard disk cannot be deciphered using another card to which the thief knows the password. DES encryption performed by hardware is more secure than encryption performed with software. One reason is because the key, or password, can be stored on the card in a special kind of chip that is designed to disintegrate if attempts are made to physically remove it in order to read the password. The password cannot be extracted from the chip purely by software, as there is no physical connection between the chip and the computer's memory so it is impossible to write a program that could access the chip.

Hardware-based access control systems also include physical access tokens. These act like passwords, but are physical devices which must be inserted into a special connector all the time that the machine is in use. If the device is not inserted, or if the device does not match the password with which it is associated, access will be denied.

The plastic tokens often take the form of keys, conveniently punched for the user to keep on his key ring. If your staff use such tokens, warn them of the danger of lending their car to a colleague, as this will allow the colleague to use the token if it is on the same key ring. Of course, a password will be needed too, but a surprisingly large number of PC users are quite free with their passwords "because the plastic token is quite secure enough on its own."

While software-based access control packages cost in the region of £60 per machine, the hardware solution typically multiplies the cost tenfold. The advice of this Guide would be to use software-based access control, or to consider a PC with hardware-based access control built in. A few machines of this type exist, and are detailed in the Resource Guide.

Doing It Yourself

A little control is better than none at all. By this token, it is worth

attempting some form of access control yourself if there is none in place at present.

It is relatively simple to write a small program whose name is placed in the AUTOEXEC.BAT file so that it is run every time the machine is switched on. The program should ask for a password and, if the correct one is supplied, the machine continues operation. If the password is not supplied, the machine locks up.

Such a program should not be considered as remotely secure. It will, however, deter casual intruders with little technical knowledge of a PC.

Protecting Files with ATTRIB

The ATTRIB command, which is part of MS-DOS, allows you to set the attributes of a file or a directory. Each MS-DOS file and directory has 4 attributes, namely Read-Only, Hidden, Archive and System. These are known as R, H, A and S. The ATTRIB command allows you to set and remove attributes from a file or directory. However, it was not until MS-DOS version 5.0 that ATTRIB allowed access to all 4 attributes - users of previous versions of DOS will have to rely on a third-party utility such as XTREE to gain access to attributes other than R and A.

The attributes assigned to a file or directory affect the file or directory as follows:

Read-only A file with a Read-only attribute cannot be edited or deleted. Attempting to delete a read-only file will generate an Access Denied error message. This is a useful form of elementary protection, though only an ATTRIB -R *.* command is required to remove the Read-only attribute from all files in a directory.

Hidden A file with a Hidden attribute can be accessed as any other file, but its name will not appear in directory listings. This attribute can also be applied to entire directories, including programs and data files. A user can still access a hidden file, but only if he knows its name. Or, if he has access to a utility which lists the name of all hidden files on a disk. ATTRIB will, unfortunately, do this.

Archive The Archive attribute is normally set by backup programs, to record a note that the file has been backed up. MS-DOS clears this attribute whenever a file changes, so that backup programs can detect

the change and back up the file again. This type of backup, where only changed files are backed up, is known as an incremental backup. For access control purposes, the Archive attribute serves no useful function.

System — System files, ie those with their System attribute set, are regarded by MS-DOS as being part of the MS-DOS operating system itself. For security purposes, the System attribute serves no useful function.

What To Control?

What aspects of a PC should be subjected to access control? There are three categories: data, programs and facilities. Where data is concerned, access is normally controlled for reasons of confidentiality. In the case of programs, control is needed for two reasons: first, where that program could aid in breaking security systems or allowing access to data; second, where incorrect use of that program could result in loss of or damage to information stored on the PC.

Facilities which should be controlled include communications ports and printers; remember that keyboards and screens are not the only routes by which information can enter and leave a computer.

Data And Information

Data to which access should be controlled includes:

- Word processing documents such as memos and letters.
- Sales figures and forecasts.
- Costings.
- Marketing plans.
- Personnel files which include names, salaries and levels of qualifications.
- R&D plans and reports.
- Reports from consultants into the workings of the company.
- Mailing lists, especially customers.
- New artwork for adverts detailing unannounced products.

- Internal phone directories (where appropriate).
- Floor plans and cabling layouts.

Hacker-friendly Software

Programs which can aid in helping users to gain unauthorised access to PCs include:

- Debuggers such as the MS-DOS DEBUG utility can alter program files and bypass software-based access control systems when encryption is not used.
- Disk-examination utilities such as the Norton Utilities or PC Tools allow access to parts of hard disks that MS-DOS cannot usually access. Access control systems that store unencrypted passwords in such hidden places are, therefore, useless.
- Disk utilities which can recover files that have been deleted and disks that have been formatted.
- Low-level formatters which can destroy all partitions on a hard disk.
- The MS-DOS ATTRIB command can re-instate hidden files and directories.
- Communications programs that allow passwords to be stored and transmitted automatically. Storing passwords for automatic transmission should be prohibited. If you are designing an access control system for a mini, network or mainframe, consider adding a facility that will reject passwords that appear to have been typed too quickly or where the delay between each character is identical. This will prevent users from transmitting stored passwords.
- Keyboard enhancers that have the ability to record keystrokes.
- Disk-based English dictionaries and word lists for use when trying to decipher passwords that are only ever held in encrypted form.
- Any software package, especially accountancy software, where the factory-supplied password has not been changed.

Potentially Dangerous Software

There are certain programs whose use should be restricted because, used carelessly, damage to information could result. Such programs include:

- Disk utilities which allow direct manipulation of a disk's File Allocation Table and directory information.
- File defragmenters, which can cause loss of information if not used

in accordance with the instructions. Few file defragmenters are reliable when run under a multi-tasking system such as Windows.

- Disk caches set aside a large area of memory as a buffer in order to speed up disk access. Delayed-write caches, which keep disk-bound data in memory and only write it to disk when the memory is full, should be avoided at all costs as a machine crash will prevent changed data from being written to disk.

- ANSI.SYS is a device driver supplied with MS-DOS. Unless required by a specific program, ANSI.SYS should not be used as it allows rogue programs to redefine keys on the keyboard. For example, the Return key can be redefined to a command which deletes all document files or formats the hard disk.

- DOSKEY, the command line editor supplied with MS-DOS 5.0, allows redefinition of all MS-DOS commands and should, therefore, be used with caution. For example, it allows DIR to be changed to DEL. If users wish for a utility that allows previous commands to be recalled, a number of less dangerous alternatives are listed in the Resource Guide.

- FORMAT will delete an entire hard or floppy disk, and should not be used on hard disks without good reason. It is worth renaming the FORMAT program to F0RMAT (change the O to a zero), to help prevent accidental misuse.

- MS-DOS 5.0 includes an UNFORMAT command which will recover data from a formatted disk. The FORMAT /U command will format a disk in such a way that UNFORMAT will not work on that disk.

- CHKDSK /F will attempt to recover data that is contained in "lost clusters". Lost clusters are formed when a machine crash or a program bug causes loss of synchronisation between the information stored on a disk and the data stored in the directory. Careless use of the CHKDSK command can result in lost files, and the CHKDSK program should be abandoned in favour of a commercial disk-repair utility package.

- RECOVER, a utility supplied with all versions of MS-DOS, attempts to recover as much information as it can from a physically damaged disk. The name of this utility, and the misleading information in most MS-DOS books and manuals, has led to the belief that it will restore accidentally deleted files. When used incorrectly, RECOVER can cause irreparable damage to a healthy disk and should, therefore, be removed from all PCs.

- If a hard disk head parking utility is used, ensure that the program is designed for use with the particular hard drive. Using a parking utility on the wrong drive can damage the disk by dropping the head

onto what the program thinks is a safe parking zone on the outer edge of the disk but is actually an area containing data.

- Versions of MS-DOS prior to 4.00 were unable to cope with hard disks larger than 32 MB in capacity. DOS 4.00 raised this limit to 512 MB and version 5.0 raised it to 2 GB or 2000 MB. There is no longer any need to use special non-standard disk partitioning software to handle large drives, and such utilities should be avoided as they are often incompatible with modern programs such as Windows.
- SETVER, supplied with MS-DOS version 5.0, allows DOS to mislead an application program as to the version of DOS that is currently running. This facility should be used with care, as programs often treat hard disks in different ways according to the version of DOS that they think they are running.

11 | Secure Erasure

Secure erasure of information held on PCs is a key to retaining the confidentiality of that data. Every senior manager knows that unwanted printouts of customer lists, budgets or salary charts must be shredded. Few, though, realise the ease with which such information, when deleted from a PC with the DELETE command, may be retrieved.

This Guide covers the subject of secure erasure in many places. However, for completeness, it is well worth repeating the most important points again. These are as follows, and should be made clear to all senior staff who work with confidential data.

- A file on a PC which is deleted with the DELETE command can be quickly and easily recovered by any user who has access to an UNDELETE command. This is because, when a file is "deleted", all that happens is that the name of the file is removed from the disk's directory - the data is still intact and several programs are available which will locate it. Utility packages such as PC Tools and the Norton Utilities include an UNDELETE program, as does MS-DOS 5.0 and DR-DOS 6.0. To delete a file in such a way that it cannot be recovered, use a program such as WIPEFILE (supplied with the Norton Utilities) to completely remove all traces of deleted files from a disk.

- Even the FORMAT command is not save from reversal by a data hacker. MS-DOS 5.0 is now supplied with an UNFORMAT program which makes a good job of recovering data from a hard or floppy disk that has been formatted. If using MS-DOS 5.0, use the new FORMAT /U command to format a disk in such a way that the UNFORMAT command will not work.

- Be especially careful when disposing of PCs, or sending PCs to be serviced. Ensure that all data is removed from the hard disk. Using DELETE or FORMAT is not sufficient; use a commercial secure erasure program too.

- Many programs create temporary files during their operation. These files frequently hold copies of, or extracts from, the user's data files. Ensure that all temporary files are deleted by applications and, where necessary, that a secure erasure program is used on these files. Temporary files often, but not always, can be identified by the .TMP extension.

- Multi-tasking programs and task switchers such as Windows, DESQview and the DR-DOS TaskMAX utility, create swap files which consist of copies of the entire memory of a PC, including an application and all its open data files. Ensure that these swap files are deleted completely whenever confidential data has been processed.

12 | Preventing Hardware Theft

So far, this Guide has talked mainly about preventing the loss of information from PCs. Today's PC is a highly compact product - even powerful network servers can be carried by one person and put in the back of a car. For this reason, it is worth giving some thought to the protection of whole computers rather than just the information they contain. *Remember that, although you can insure against the loss of a PC, you may never receive sufficient compensation to cover the loss of all the data on a network server which, it turns out, has not been backed up for six weeks.*

Marking The Components

Mark all PCs with your company name and an identification number. This helps to prevent theft and also aids in the auditing process (see below). Use strong adhesive labels, or burn a mark into a machine's plastic case with a soldering iron. Record all serial numbers, otherwise there is no chance of stolen equipment being returned to you if it is found.

All add-in cards should also be marked with serial numbers. Hard disk controllers, graphics cards and other cards that were supplied as part of the machine may be ignored, but extras such as memory expansions, modems and network adaptors should be recorded. All peripherals, such as monitors and printers, should be similarly identified, and a database kept so that a monitor, its computer and the add-in cards can all be proved to belong together.

Preventing Removal Of Equipment

No equipment should be taken off company premises without authorisation, and that authorisation should take the form of a docket signed by a senior manager. Make staff aware of the procedures, and offer a reward for anyone who reports equipment being taken off the premises without a docket. You can help deter thieves by putting up notices

warning that anyone taking equipment from the building is liable to be asked to produce a docket.

Ensure that security and reception staff know when computers are due to be removed from the premises, by keeping them informed of all dockets that are issued. If a staff member is seen taking equipment off the premises, details should be recorded in the reception desk's daily incident log.

Ensure that any paperwork concerning equipment purchases is not left lying around; an anonymous box that has been lying around unopened for a few days becomes more stealable if attached to an invoice for £1000.

Hardware Audits

A hardware audit involves reconciling the invoices for purchased hardware with the equipment that is actually in use in the company. The aim is to ensure that all hardware that has been purchased is still on the premises, and that it is being used. Many companies have found a hardware audit a very useful way of cutting down on expenditure by discovering computers and peripherals that they didn't know they had, or that had been assigned to staff who had never used them.

A hardware audit is a useful extra level of detail in a Fixed Asset Register, which will prove invaluable to company accountants.

There is no need to employ a specialist to carry out a hardware audit; it can be done by any competent member of staff who can recognise the various parts of a computer and who is able intelligently to talk to users about how and when they use PCs.

Labelling Hardware

Each piece of PC hardware, including add-in cards and all peripherals, should be assigned a unique company serial number when it is installed. Ensure that the numbers are kept securely in a database. Remember to tell visiting engineers to inform the database holder if any numbered component is moved, removed or replaced, so that the database can be kept up to date.

13 | Controlling Software Piracy

From a legal point of view, knowing which software packages are installed on corporate PCs is essential. Without such knowledge, the company and its directors are open to prosecution if unlicensed software is found and no steps were taken to detect or remove it. In the worst case, a company suspected of possessing pirated software can find itself the subject of an Anton Piller raid. This involves an unannounced police raid on the company premises, and the immediate searching for evidence. Computers containing unlicensed software will almost certainly be taken away, as will any backup disks and other media which are suspected. It is unlikely that any of this will be returned until after the police investigations are completed, by which time the company may well have been bankrupted by the loss of its crucial business data.

Software houses go to various lengths to detect unauthorised copies. For example, if a software company regularly receives support calls from 20 people at company X, but it is known that company X has purchased only 3 copies, it is not uncommon for the software company in question to call company X and ask for a cheque by return of post. This has happened in the UK on more than one occasion.

Why Software Gets Pirated

There are a number of reasons why unlicensed (ie pirated) software finds its way into an organisation. Knowing the reasons will help you to plan your campaign for eliminating it from your company.

Economics

The cost factor is a major cause of software piracy. Business software packages such as spreadsheets, word processors and databases typically cost around £500 in one-off quantities, which is a considerable amount for a small company or an individual to bear.

Convenience

The easiest way to get hold of a software package is to take a copy from a friend or colleague. Where it is important that a package be obtained quickly (perhaps because it is needed in order to complete some urgent work), this is especially important to remember.

You can help to reduce piracy by ensuring that internal software purchasing arrangements do not cause unnecessary delay - if a manager has an urgent forecast to complete and has ordered a copy of Lotus 1-2-3, the standard 30-day delay will be unacceptable and it is a fair bet that a pirated copy will be acquired.

There will occasionally be instances where copying of software is difficult to avoid. If a copy of a program is needed urgently (ie, within half an hour so that an unexpected visitor can do some work), and a program has to be copied in a way that contravenes the licence agreement, ensure that the paperwork for ordering an extra copy is started immediately. Few software companies will object to this procedure - if you suspect that they might, telephone the marketing department and ask permission. Explain to all staff involved, that the extra copy has been made with the permission of the software vendor and that an extra copy has been ordered.

Evaluation

The number of software packages on the market increases daily, and deciding which one is right for a particular project is no easy task. Ensure that those whose job includes software evaluation are given adequate budgets to buy or rent evaluation copies. You must avoid situations where:

- Some software is not included in an evaluation because no budget is available.
- A pirated copy of a software package is acquired in order to include it in an evaluation.

Ignorance

Ignorance can often lead to piracy. For example, staff may not realise that copying software constitutes theft. Also, staff may not be aware of the extent of a licensing agreement, and will produce 50 copies when in fact permission has only been granted for 40 copies to be made.

Network managers must check that all software installed on a network

is correctly licensed. A product for which you have 50 licences should not be installed on a LAN which would allow 70 simultaneous users.

Where a software audit shows that a user has, on a stand-alone PC, a copy of a software package that is also installed on the company network, you should remove the single copy. In most cases, you can use this single copy to increase the number of simultaneous users permitted to use the package on the network, and this represents a far more efficient way of working.

Documentation

Business software packages are complex, and documentation is essential. Printed manuals typically come to between 500 and 1000 pages.

To keep costs down and to make their software easier to use, many software companies now include copies of the documentation on disk. This is usually accessible via a "Help" key. Having the manual available on screen provides a number of advantages to the user, not least of which is the fact that the computer can rapidly search the manual for a specific piece of information.

Of course, the presence of on-line documentation removes one of the earliest forms of copy protection from software. There is no longer any need for the user to possess any printed documentation at all. In the few cases where no on-screen help is available, a local bookshop will usually provide a solution.

Care of Master Disks

When software packages are purchased for use within the company, ensure that the master floppy disks are kept safely under lock and key. This helps to prevent piracy, and also ensures that you are able to re-install the software in case of deletion or corruption of the installed version. You will also often need access to the master disks when installing, or applying for, upgrades from the vendor.

Note that much of today's software is supplied in what's known as "dual media" form. This means that the program is supplied on both 5¼" and 3¼" disks. This is to make it easy to install, and does not mean that you own two separate licences. Ensure that only one set of disks is installed, and keep the other for emergency use.

The Software Audit

The concept of a software audit is relatively new. The end result of the process is a database containing details of every PC in the company, and the software that is installed on it. Further information can also be recorded, too. Having such a database is invaluable, for a number of reasons. These include:

- A technical support person can instantly look up the configuration of a particular machine if its user is reporting a problem.
- Management can use the database to check whether the number of copies of a program installed on the company's PCs exceeds the number of licences or copies that have been purchased.
- Some software companies offer discounts for multiple purchases of programs. It is often up to the purchaser to indicate how many copies have been purchased to date, in order to qualify for cumulative discount rates or site licence agreements. Your audit database will provide this proof, and also alert you to the fact that you should approach software companies and ask for discounts.
- Retrieving software that is no longer used, or that was assigned to ex-employees, becomes easy. Such a practice can save large amounts of money. Some companies even offer financial incentives to staff who return unwanted software that has been issued to them.

A number of automatic software audit programs are available, which will record details of the software that is found on a machine and merge this into a central database. Alternatively, the process can be done by hand. If there is a desire to produce a comprehensive software audit database, the information to be included for each machine should be as follows. The information should be recorded in three databases, known as the Recognised Files database, the Computer database and the Permissions database. The structures of these files are detailed below. Although there are many software auditing packages in existence, some of which are detailed in the Resource Guide, few currently come close to providing the functionality detailed here. For details of those that do, see the Resource Guide (page 155).

The Recognised Files Database

A list of filenames, and the application programs they represent. For example, any computer containing a file called WP.EXE can be assumed to contain a copy of WordPerfect.

This database should contain the following fields:

Field Name:	**Description:**
FILENAME	11-character name of the recognised file. Eg, WP.EXE.
APPLICATION	Name of the application, eg WordPerfect v5.1.
TYPE	Type of software. Suggested types: C - Normal commercial application. I - Internally developed application. D - Demonstration copy. E - Evaluation copy. P - Public domain. S - Shareware. G - Game
LICENCES	Number of licences owned by a company for this program.
DIRECTORY	Optional directory name. Automatic audit programs can use this information to help determine if the file is a true instance of the application it claims to be, by checking the name of the directory in which the file is contained.
MAXDATE	Latest permissible date for which the file represents a copy of the application.
MINDATE	See above.
MAXTIME	See above.
MINTIME	See above.
MAXLENGTH	See above.
MINLENGTH	See above.

The Computer Database

For each PC, the following information should be recorded:

- The name, length, date, time and attributes of every file on the hard disk(s).
- The contents of the machine's AUTOEXEC.BAT file.
- The contents of the machine's CONFIG.SYS file.
- The date and time that the audit took place.

- The number of hard and floppy drives detected.
- The amount of free space on each hard drive.
- The type (hard, floppy, high density, low density) of all drives.
- The capacity of all drives.
- The volume labels of all hard drives.
- The name of the machine's regular user.
- The manufacturer of the PC.
- The PC's model number/name.
- The physical location in the company.
- The department.
- The site/building.
- The manager's name.
- The user's telephone extension number.
- The manager's telephone extension number.
- The PC's serial number.
- The name, manufacturer, model, serial number and port of each peripheral.
- The company serial number of the machine, if assigned.
- The CPU type. 8088, 8086, 80186, 80286, 80386, 80486.
- The amount of base RAM, in KB.
- The amount of extended memory installed, in KB.
- The amount of expanded memory installed, in KB.
- The video type. CGA, EGA, VGA, MDA, HERCULES, XGA, OTHER.
- Is a maths co-processor installed?
- The DOS version number.
- The type of mouse installed, if any.
- The number of serial ports.
- The number of parallel ports.
- The contents of the machine's CMOS memory.

The Permissions Database

For each file in the Recognised Files database, a cross reference should be kept to explicitly specify any users or departments which should or should not own a copy of the file.

Field name:	Description:
Usertype	Indicates whether user is a named person or a department.
User	The name of the user or department.
Ownership	Y if user is expected to own a copy of the file, or N if the user should not.
Filename	The name of the file.

Generating Software Audit Reports

When you have the database of recognised applications, and the database containing information about each PC in your organisation, you can then produce some highly useful reports. For example:

- AUTOEXEC.BAT/CONFIG.SYS analysis
  - List AUTOEXEC.BAT
  - List CONFIG.SYS
  - Search AUTOEXEC.BAT
  - Search CONFIG.SYS
- TECHNICAL SPECS
  - List technical details
  - List of machines, by CPU
- HARDWARE INVENTORY
  - Details of machines
- OWNERSHIPS
  - List of machines, by user name
  - List of machines, by manager
  - List of machines, by department
  - List of machines, by site
  - List of machines, by manufacturer
  - List of machines, by model
- FILE SEARCH
  - Search for recognised file or application
  - Search for duplicate files
  - List number of copies of each file in the company
  - Directory trees of specified machines

- PERMISSIONS
  List deviations from permissions list
- RECOGNISED FILES/APPLICATIONS
  Search for recognised application name
  List owners of recognised files/applications
- AUDIT INFO
  List of all audit files on record
  Compare two audit files
  Export audit data to text file
  Export Recognised Files data to text file

Detecting Pirated Software

If your organization uses some form of automatic problem-tracking software for its internal support and help-desk departments, the logs from the software should be monitored on a regular basis. Watch out for users requesting support for software which they are not supposed to have.

Occasional inspections of machines are useful, especially where specific staff members or entire departments have a history of acquiring unauthorised software. When performing an inspection, ask for proof of ownership of all applications installed on the machines under scrutiny. Master floppy disks, or original receipts, are acceptable forms of proof. Manuals, even original ones that are clearly not photocopied, are not - it's easy for anyone to order extra copies of manuals.

Do not install a photocopier in a place where it can be operated without the user being seen by either desk-based workers or staff walking past.

14 | Encryption

If backup is the only foolproof way to prevent accidental loss of data, then encryption provides the same level of protection against deliberate abuse of information.

The beauty of an encrypted file is that there is no need to keep it physically protected; you can even send out copies to your trade rivals if you wish. This is because an encrypted file is scrambled and will be completely unintelligible without the password.

Encryption routines are always based around a password. The password is used by the routine when scrambling the file, and the decryptor needs the password in order to restore the file to readability.

It follows, of course, that passwords for encrypted files must be carefully guarded (if you must write it down, disguise it as a phone number in your diary, and don't use the same password more often than is necessary).

Choosing An Encryptor

There are many programs that provide file encryption, some of which are mentioned in the Resource Guide. Before you use or buy an encryption package, though, you should be aware of three points:

- Utility packages such as the Norton Utilities are advertised as including a DES-based file encryption program. However, there are complex export regulations involved with sending DES programs out of the US and consequently you will find that *UK versions of some utility packages do not include the encryption program.* Either import a US version personally, or find a package that does include the encryptor.
- Some application programs claim to provide built-in encryption and/or password protection on their data files. Lotus Agenda is one such program. However the current version (2.0) of this program does not scramble the data at all so *the information is fully visible if the Agenda data file is examined with a text editor* from MS-DOS.
- Don't use the built-in encryption facility in your favourite software

package. At least one company specialises in producing programs which can recover the passwords from such protected files. See the Resource Guide for details.

See the Resource Guide for details of encryption products, plus a review of a hard disk controller which provides automatic encryption.

DES And RSA

As illustrated by the second point above, it is always wise to use a specialist file encryptor rather than the built-in facilities of an application package.

There are many encryptors about, and a wide variety of encryption algorithms. The algorithm is the formula by which the text plus the password are turned into the scrambled text.

Some algorithms rely on secrecy for their security, ie the company that developed the algorithm vows not to reveal how it works. *Such algorithms are secure only until one person has cracked it, after which every document protected with that system becomes vulnerable. Such algorithms should, therefore, be avoided.*

The two most secure publicly-available encryption algorithms currently in existence are known as DES and RSA. DES is the Data Encryption Standard, designed by IBM and used by governments and defence establishments worldwide. RSA is named after its inventors, Rivest, Shamir and Adleman.

Both are published algorithms. That is, you can go out and buy a book that will tell you exactly how the algorithm works and how to go about encrypting a file. They are secure because no one has yet proved them crackable. It is currently estimated that it would take the world's most powerful computer hundreds of years to reverse the encryption process.

Note that *the "crackability" of an encrypted file does not depend on the length of the password; it depends solely on the encryption algorithm used. A file protected with DES and using a two-character password is safer than the same file protected with a weaker algorithm and a 50-character password.*

To show how encryption systems can be secure even when the algorithm is known, consider the following. Two prime numbers 17 and 19, when multiplied together, give 323. Because 17 and 19 are prime, there are no two other numbers that have a product of 323. Given 323 as a starting point, deducing 17 and 19 is difficult. If 17 and 19 were replaced with two prime numbers, each of which were 150 digits long, the reverse-en-

gineering would be impossible. Yet that is the only way to find the combination to an RSA-encrypted file.

Whenever possible, DES or RSA encryption should always be used when scrambling is required. On a modern PC, the process is fast if not instant, and the security offered is total. If an extra level of security is required you can even scramble the encrypted file again, using a different password.

Remnants

Having scrambled a file, ensure that all traces of the unscrambled version are removed. If a file has been copied to or from floppy disk, or edited with a word processor, remember that the data will exist somewhere in the PC's memory until it is overwritten by loading a suitably large program. It will also exist in a temporary file, or swap, file, on disk, if a task-switching or multi-tasking system such as DESQview or Windows has been used. Also, if the unencrypted file was stored on disk and then subsequently erased, the data will still be recoverable by an UNDELETE utility program. The solution here is to use a program that overwrites with random data the parts of a hard disk containing pieces of erased files. The Norton Utilities is just one package that will do this.

Problems And Caveats

- Watch out for problems when using non-standard encryption techniques when you are using more than one type of microcomputer. If you regularly transfer data between PCs and Apple Macintosh machines, for example, you may find that the Apple computers won't run the decryption program and are, therefore, unable to read information created on the PC. This is especially important where Macs and PCs are connected together on a network. The DES and RSA methods are available in PC and Macintosh versions, so there should be no problems if either of these is used.

- Some encryption programs are menu-driven, while some are operated from the command line. A DES program to encrypt a file called TESTFILE using the password OCTOPUS may take the form "ENCRYPT TESTFILE OCTOPUS". *Never use programs that force passwords to be included on a command line* like this, because many PCs have command-recall programs that allow previous commands to be recalled and edited using the up-arrow key. In this case, a passer-by could press the up-arrow key, note the password that has been used, then clear the screen to cover his tracks.

- The same goes for application programs which include encryption. If you must use built-in encryption facilities, don't quote the password on the command line when loading a protected spreadsheet to work on; wait for the program to ask you. This will take a little longer, but avoids the password being stored in the command-recall area.
- Never rely on the built-in password feature of an application program, unless the program uses DES or RSA encryption. See the Resource Guide for details of at least one program which claims to be able to recover passwords from protected WordPerfect, Lotus 1-2-3, Paradox and Excel files.

ZIP, ARC, LZH And Other Archive Programs

File archiving utilities are much used by computer enthusiasts and software vendors. Such utilities do two things: they pack lots of files into one file to ease the copying process, and they compress the data to (in a typical case) around 60% of its original size. In some cases, data compression can reduce a file to 10% of the original especially where database files are concerned.

A complementary unpacking program is used to split up the archive into its component pieces and to uncompress the data.

Archive files can be identified by their extensions. Common archive extensions are ZIP, ARC, LZH, ZOO, PAK and ARJ. Although archive files are unintelligible if examined, this is because the data has been compressed rather than encrypted. No password is normally needed to run the uncompressor and return the data to normality. *You should not, therefore, consider an archive file as any more secure than one which has not been archived.*

Some archiving programs do include encryption as standard and will then prompt the user for a password before the file is uncompressed. However, archivers designed for the non-US market tend to lack this feature. Luckily, the best file archive programs are available as public domain software or Shareware, and can be downloaded direct from the USA if you have a modem and access to a US-based bulletin board. See under Software in the Resource Guide for a definition of Public Domain and Shareware.

Because of recent publicity that links the spread of viruses with software downloaded via modems, many archiving programs now include built-in cryptographic checksummers (see the chapter on Viruses (page 75) for details) which will detect any changes in an archive. Such a facility can also be used as a security feature when archive files are stored within a company for backup purposes.

15 | Security For Applications Packages

Application software packages warrant less protection than the data files that they create. After all, if you lose your only copy of the Lotus 1-2-3 spreadsheet you can send a motorcycle messenger to a local software dealer and have a new copy in just a couple of hours. The spreadsheet files containing your sales forecasts cannot be recovered so easily. There are, however, a few reasons why you do need to protect application packages. These include:

- *It is the responsibility of the company to ensure that software is not copied except in accordance with the licence agreement.* If a staff member takes a copy of Lotus 1-2-3 to use at home, both the staff member and the company's directors may be liable for prosecution. Even worse, the software supplier may withdraw your licence to use that application, which leaves you with lots of spreadsheet data but no software under which to manipulate it.

  Note that, although many software packages are now supplied on both 3.5" and 5.25" disks, the licence agreement usually states that you are authorised to use only one of the copies. Installing the other copy on another machine is classed as piracy unless you have paid for both copies.

- Software that has been specially written or adapted for you may be difficult to replace quickly.
- Some applications, such as hard disk performance adjusters, should not be used by unauthorised staff as careless operation could damage company data.
- It is not unknown for a disgruntled ex-employee to notify the legal authorities of his previous employer's use of unauthorised copies of commercial software packages.

Traceability

It's easy to add a degree of traceability to a software package and many

software vendors do just this. This makes it easy to determine its origin, and also deters thieves in the first place. Such procedures also help you detect illicit copies of software that are being used in your organisation.

When installing a new software package for the first time, the program will often ask for the name of the company and/or the user. Although the program does not allow you to leave these data fields empty, users often put fictitious names here. Ensure that all software is installed by a trustworthy staff member and that, as a minimum, the company name is correctly stated. This name will then be displayed each time the software is used, which is one of the most effective deterrents against theft.

Copy Protection

Most software packages, especially in the PC market, can be copied simply by copying the master disks. There are techniques that software vendors can use in order to stop you, as a customer, doing this. Obviously, protecting software from illicit copying means increased sales for the software companies. Or, at the very least, their software will be used only by people who are willing to pay for it. Unfortunately, the methods used to protect disks against copying often cause great inconvenience for the legitimate purchaser.

The "protection" described above, embedding the purchaser's name in the program, is simple, effective and not inconvenient for any party. There is no reason why you should not use software packages that employ such protection techniques.

However, there are several other protection methods. *You should always try to avoid using software that uses these methods if at all possible, as the protection mechanism is just one more potential source of problems.* In almost all cases, there are non-protected software packages that will do the same job as a protected program. In a few cases, though, especially with high-cost, low-volume vertical market packages in highly specialised areas, you have no option but to go ahead and use software which has protection built in.

The two most popular (with the software vendors) ways of protecting software packages are described in the following sections, along with details on how and where problems can arise if you use protected programs.

The Dongle

A dongle is a physical device approximately the size of a conventional box of matches. It plugs into the back of a PC, usually into the printer socket. The existing printer cable then plugs into the dongle, and the printer will continue to work as normal.

The dongle contains a special chip and some proprietary software. It is possible for a computer program to send a command to the dongle, effectively saying "are you there?".

Such a command is included in a protected program. So, when the program starts up, it interrogates the dongle. If the dongle is found, the program carries on as normal. If the dongle is not detected, the program refuses to run.

On the face of it, a dongle-based protection system seems pretty harmless. Master disks can be safely copied for backup purposes as required, yet no more than one copy of the software can be used at a time because the dongle is a sealed circuit and no user would be able to copy it.

However, dongled software can potentially cause serious problems. *If a dongle is lost, stolen or broken, you will find yourself with large amounts of information that cannot be accessed.* In the case of a whole operating system that is protected by a dongle, as is the case with at least one multi-user operating system, you could find yourself in the situation where a dozen people are locked out of the system for days while you persuade the software vendor that you are entitled to a new dongle.

Dongles can also cause problems if a computer is pushed too far back against a wall. The pressure on the dongle stresses the PC's motherboard and faults can develop.

Protected Disks

A dongle is a hardware-based protection device. However, software-based protection systems exist too. A program protected by a software device will normally consist of a disk that cannot be copied by normal means. If you copy the disk with the MS-DOS command DISKCOPY, you'll find that the program detects that it is running on a copied disk and will refuse to run.

Programs on non-copyable disks make special provisions to allow you to install them to a hard disk. This is normally done with a special INSTALL program which only allows you to copy the program onto one computer. At this point, the floppy disk becomes unusable and will refuse to run. If you want to move the installed program to another

computer, you need to run a special UNINSTALL program to put the software back on the floppy disk and then run the INSTALL routine again to copy the system to another computer.

Software protected in this way is very sensitive to the way you use your PC. For example, one software-based protection system works because, when you copy the program to your hard disk, it automatically makes a note of exactly where on your disk it has been copied to. Whenever you run the program, it checks that the program file is still where it is supposed to be. If it is not, the protection system assumes that the protected program must have been copied to another hard disk and so refuses to run. However, many disk utility programs are available that speed up your PC by moving files around on the disk. Not all such utilities are aware that protected programs should not be moved, and you end up with a program that will not run from your hard disk, and an unusable floppy disk.

Yet another problem with protected software comes if your PC's hard disk becomes corrupted. Often the only solution is to erase the entire hard disk, and then restore everything from backups. But protected programs cannot be backed up, and it may take days before a replacement disk can be obtained.

Comparing Serial Numbers

If you have two or more Novell network servers connected together, the first thing that the NetWare operating system does is to compare the serial numbers of the copies of NetWare on each machine. If a match is found, the system manager is informed that he is using an illegal copy of NetWare.

Other programs also use this form of protection. Teleclone, a package that allows one PC to access another via a modem, is supplied with a unique serial number embedded in each copy of the program. One copy of Teleclone will refuse to talk to another copy which bears the same serial number.

Cracking Copy Protection

Almost all copy protection systems can be circumvented. Therefore, if you find yourself in a situation where the unavailability of a protected program is causing problems, do not assume that all is lost.

I do not intend to go into detail about how to break through copy

protection schemes, but a few words to illustrate the possibilities are in order.

The key to breaking a dongle-protected program is to locate the part of the program that interrogates the dongle and bypass it. A competent programmer with access to standard debugging programs could accomplish this in anything from one to 10 days; it all depends on how well the programmer managed to hide the part of the program that interrogates the dongle.

Copy-protected disks can also be broken. One way to protect a disk is to write a program that will deliberately create non-standard areas on a floppy disk. When a user attempts to copy that disk, MS-DOS will come across the non-standard areas and claim that the disk contains errors and is, therefore, uncopyable. A program that knows about the non-standard areas, though, would be able to access the disk as normal. Now, although the standard DISKCOPY command is unable to untangle the non-standard areas on the disk, there are plenty of programs that can. Such programs, often known as bit-copiers, will copy a wide variety of protected disks.

Software that relies on serial numbers to provide protection can be cracked in the same way that dongle schemes can be broken. It simply comes down to a case of how well the programmer has managed to hide the part of the program that actually performs the comparison between the two serial numbers.

16 | Insurance

If you are unlucky enough to suffer data loss in any form, there are two pieces of paper to which you can turn for some sort of relief. One piece of paper is the Computer Misuse Act, or another similar piece of legislation which may enable you to get your revenge on the perpetrator of the computer misuse. The other piece of paper is an insurance policy which covers you and your organization for just this type of emergency.

Insurance against computer abuse is not cheap, but can often mean the difference between life and death for a company. Using the law to prosecute a hacker may well bring a smile to your face when you see the hacker imprisoned or fined, but it won't bring back your data or compensate you for its loss. An insurance policy, on the other hand, could mean that you are back in business quickly. Without your data or computers, perhaps, but with sufficient compensation to allow you to cope.

Specialist Policies

A number of major insurers offer specialist computer insurance. Such policies start at the "theft of computers" end of the scale, and go all the way up to those which really understand the value of corporate data to your business, even though that data is not a tangible piece of equipment.

When choosing a policy, it pays to take advice from at least two specialists. The job of an insurance company is to avoid paying out money wherever it can, so remember to read the small print very carefully. Before you take out a policy, ask for a copy of the terms and conditions and discuss them with a solicitor or your company's legal department.

What To Look For In A Policy

There is no end to the get-out clauses which insurance companies will include in policies. If you come across one which you consider unfair, and an insurance company is using it to avoid paying out, consult a copy

of the Unfair Contract Terms Act. If you can persuade a court to agree, you may be able to have the clause declared null and void.

Some of the clauses that you should watch for in policies designed to protect against computer misuse are as follows:

- Are you covered for data loss if your staff forget to take backups, or if the backups are useless because no one checked them?
- Are specific perils such as fire or flood excluded?
- Are you covered for water damage caused by fire brigade hoses and/or your own sprinkler system?
- Are you covered for data or computer loss caused by negligence by your staff and by visitors?
- Are you covered for loss of earnings, as well as the replacement or the machines and re-keying of the data?
- Are you covered for employing the services of a data recovery expert?
- Must damaged hardware be shipped to the manufacturer for repair, or will the policy pay for on-site repair? If hardware must be transported, are the transport costs covered?
- Does the policy allow you to hire equipment while yours is being repaired?
- Are you covered for transferring data from backups onto new hardware, whether that hardware is on short-term hire or for permanent use? What if the new machine is not the same as the old one, and data and/or programs need converting?
- Does the policy cover the cost of investigating why the disaster happened?
- Does the policy cover the cost of putting into place procedures to prevent a re-occurrence of the disaster?
- Are you covered for the carrying out of loss prevention and damage limitation acts?
- Are you covered for debris removal and the cleaning up of the computer room?
- Do you have to wait for approval before repairs can go ahead, or can you get started immediately? If you need approval, is this the case for all amounts or only where the cost exceeds a certain limit?
- Is the refilling of fire extinguishers covered?

- Will you be inconvenienced by the demands made? For example, do you have to lock all PCs away in a strong room every night in order to qualify for theft cover? Do you have to install expensive alarm systems or security guards?
- Is the loss of, or damage to, dongles insured? You may find that software companies will refuse to replace stolen dongles. The same applies to master floppy disks, especially copy-protected ones, as these normally represent your only proof of legitimate ownership.
- What is the situation regarding power cuts? Damage caused by accidental or deliberate breaks in power are often not covered, but severe data corruption can be caused if a PC's power supply is cut off at the wrong time.
- Are you covered for damage caused by the connection of "unapproved" hardware to computers? For example, what happens if a user connects a modem which has not been approved by the BABT?
- Note that it is normal practice for no cover to be available until 48 hours after a policy has been taken out.
- It is also normal practice that no cover is available for the failure of a major component until after a 30-day "settling down" period. For example, if you install a new LAN server you cannot claim compensation if it crashes on the first day.
- Can claims only be made when actual material damage has taken place? What happens if a hacker changes passwords so that no invoices can be sent to clients? Although no actual damage has been done, this situation could cost the company dearly.
- Some insurance policies will refuse to pay out until the perpetrator of the crime has been identified. Does this conflict with your company policy of agreeing anonymity for hackers in return for co-operation?
- Does the policy explicitly exclude damage caused by a virus, or a suspected virus?

17 | Software Development

Programmers and software developers are often considered as being outside the normal company data security arrangements. It is often assumed that a programmer needs unrestricted access to a machine and all its data in order to do his job. This is not always the case.

There are unlikely to be any users more capable of removing data from your computers than programmers or software developers. Although there will be times when development staff need unrestricted access to computers, such access should not be given unless there is a proven need for it.

If you employ programmers on short term contracts, strict supervision should be undertaken as you cannot rely on company loyalty to protect your property.

Much of the information already given in this Guide applies to software development staff as well as less privileged users. There are, though, many security-related points which apply solely to programming staff and these are detailed below.

Chinese Walls

A programmer is, in computer security terms, an extremely powerful person. Unless properly controlled, he has access to confidential data and he also has the wherewithal to read or amend that data.

Financial institutions use the "chinese wall" method to help avoid problems here. Any programmer working on the software that helps to run the bank has to test his work on dummy data instead of real customer balances. Staff who work with live data do not have access to the programs that can manipulate that data. Achieving this level of segregation is difficult but possible. As a minimum, the two categories of staff should be in different physical locations; ideally in separate buildings and definitely not in the same office.

There should never be any need to let a programmer near live data. All programming should be performed on development computers using

copies of live data files. When data is copied from live systems to development machines, ensure that security-related information is not copied. For example, password files and audit logs must not be copied as the programmers can then reverse-engineer the password files in the comfort of their development environment and use this information to gain access to the live system.

Protecting Source Code

Programmers frequently fail to appreciate the security aspects of their work. They will leave confidential printouts taped to walls. They will leave debugging trace output files in public areas on a network server that can be accessed by any user. They will use system manager-level passwords to perform mundane tasks because one day they may need supervisor-level access and there's no point in remembering two sets of passwords.

You or the security manager must ensure that none of these acts is allowed to take place.

Software Houses

If your company's core business is the development of software for commercial sale, or of your department produces bespoke software for internal corporate use, the protection of source code is paramount. The source code represents a huge investment, and the consequences of its loss are enormous.

For example, the source code for your sales system allows your competitors to see exactly how your business is operated.

Ensure that access control systems and encryption are used on all PCs which hold source code.

Backups

Software developers are nocturnal creatures by habit. Given the choice, many would prefer to work from 4pm to 3am instead of standard office hours. If the building is not open during these times, developers will frequently take work home. This work can be programs to finish on a machine at home, or printouts to read through. It is up to you to decide how much of a risk such actions pose, and to impose restrictions on the type of work that can be taken home.

The rules regarding backups must be made to apply to software devel-

opment staff as well as other employees. Ensure that development machines are backed up regularly.

Backing up executable programs is useless and unnecessary. Instead, back up the source code plus the relevant compilers, documentation and operating system.

Some backups are more valuable to a data thief than others. Backups of source code are often priceless, especially where the source code for an entire project is available on a single DAT cartridge or removeable hard disk. Backups of important projects should be encrypted, or physically protected, or both.

Programmers' Tricks

Programmers, especially contract programmers, have a whole arsenal of techniques to protect themselves in case contractual problems arise. Such problems include "unfair" dismissal, or non-payment. These techniques can all loosely be described as preparation for blackmail and it is wise for an employer to know about them beforehand so that action can be taken to prevent them being used. There are three main tricks that are used, namely logic bombs, back doors and deliberate errors.

Logic Bombs

A logic bomb is a section of a program designed to cause damage, and which is triggered by a certain event. For example, someone writing a payroll system for your company may include a logic bomb that wipes out the entire computer if the programmer's name is ever deleted from the payroll. If the programmer resigns, he will de-activate the logic bomb. If he is sacked, he will suggest that it may be in your interest to reconsider the decision to dismiss him.

Bear in mind at all times that it is human nature to build defences against potential problems whenever the opportunity arises. Ensure, therefore, that all software development staff are aware that their work will be regularly scrutinized by other staff, and offer a large financial incentive to those other staff to encourage them to uncover logic bombs.

Back Doors

A back door is a way into a program that is created by the programmer. For example, imagine the case of a programmer designing some access control software for your PCs. The software system would normally

consist of two parts; the program itself, and the (encrypted) file holding the passwords. Whenever a user wishes to gain access to the computer, the program checks the password file to authenticate the user.

One possible back door would be that the designer of the system adds a facility to the program such that if a user called "BAMBI" attempts to log in with a password of "DEER", that user is automatically given top-level access whether or not an entry for "BAMBI" appears in the password file. Attempting to lock out the programmer by deleting his entry from the password file once the system is written will be ineffective.

As with the logic bomb, the only way to detect such back doors is to ensure that programmers document their work thoroughly, and that the code and the documentation are checked regularly.

Consultancy

If you employ a contract programmer for a year, and you then discover problems with the program two months after the programmer has departed, it is highly likely that you will decide to re-employ the original programmer to fix the problems. The programmer knows this, and it is not unknown for a programmer deliberately to introduce time-delayed problems which he knows will lead to further work.

A variation on this scam is for programmers to deliberately introduce delays into a system so that, under heavy load, it will work intolerably slowly. When called in at a later date to try to speed up the system, the programmer simply spends three months pretending to work on the system, then takes just a couple of minutes to remove the delay and presents the client with a large invoice. The client gratefully pays for what he considers to be a job well done.

Once again, careful checking and daily vigilance is the best way to stop such practices.

Resignations And Dismissals

If you part company with a member of your software development staff, ensure that all privileged access to computer systems is immediately withdrawn. Check, too, that the ex-staff member does not have any hardware, software or confidential data at home by consulting the logs that should have been made when any equipment or data was taken off the premises.

All top-level supervisor passwords on all systems to which the person may have had access should be changed. Don't forget keypad combinations on doors leading to restricted areas.

Copyright Considerations

The law surrounding copyright is complex and the author of this Guide is not qualified to give detailed legal advice. However, copyright with respect to software development can throw up some very important considerations:

- The copyright in a computer program normally rests with the author of that program. There are exceptions to this, especially where work is carried out on behalf of an employer, but copyright law is a very grey area. It is essential, therefore, that all software developers should sign a contract that assigns the copyright of their work to you, along with the copyright to all documentation, research and other supporting material.
- Under UK copyright law, someone who is contracted to amend or update a copyrighted computer program becomes a part-owner of the modified program. Maintenance programmers be asked to sign copyright waivers to avoid this situation.

18 | Troubleshooting

While most of this guide has been concerned with prevention, there comes a time when it is necessary to talk about cures. If a problem arises, you should find sufficient information here to enable you to work on a solution. If you find that a great deal of work is needed, the Resource Guide lists many books, software products and experts who are skilled in sorting out problems related to data security.

The remainder of this chapter is divided into small sections, each of which is designed to help you overcome one particular problem. These sections provide enough information to get you started on curing the problem. However, where rapid or complete recovery is crucial it is highly recommended that you seek advice from a professional before you or your staff tackle the job.

A File Has Been Accidentally Deleted

Stop. Do not do anything until you have read what follows, or you will almost certainly destroy any possibility of recovering the file.

Because of the way that MS-DOS handles files, a file that has accidentally been deleted can be easily and quickly recovered if no data has been written to the disk since the file was accidentally deleted. If data has been written to the disk, recovery may still be possible but more effort may be involved.

MS-DOS version 5.0 and above includes an UNDELETE utility which will undelete files subject to the warning above. If this program is not available, a number of third party utilities are available which will do a similar job. The Norton Utilities is just one example.

If a file has been accidentally deleted from your hard disk, remember not to copy the recovery program to that disk as you will almost certainly damage your chances of recovering the file intact.

Consult an MS-DOS manual or the documentation accompanying the recovery utility for details of how to use the program. If you need to search for, or buy, a recovery utility, ensure that the disk containing the

deleted file is not touched in the meantime. Remember that some applications create files on a disk even when you do not tell them to, to use as temporary storage, and these files can render deleted files unrecoverable.

A Disk Has Been Accidentally Formatted

A hard or floppy disk that has been inadvertently formatted can normally be recovered. The same rules about undeleting files apply to unformatting disks - no operation should be carried out on the formatted disk until the correct utility program has been used, or the disk may become unrecoverable.

There is an UNFORMAT program supplied with MS-DOS version 5.0 and above, and a similar program is included with the Norton Utilities package. These programs consist of two individual programs. The first is a program that you should always keep loaded into your computer. It keeps a record of the arrangement of the files on your disk. The second program is the UNFORMAT utility itself, which reconstructs your hard disk by using the information saved by the first program.

So long as you have been using the information recorder, the second program will almost always be able to reconstruct a formatted disk. If you have not been using the recorder, the disk can usually still be unformatted but you will find that many of the recovered files will be corrupted or incomplete.

If you have a copy of MS-DOS 5.0 or any other UNFORMAT utility, check that the recording program (called MIRROR) is installed, and ensure that it remains active at all times.

If UNDELETE or UNFORMAT programs are unable to fix the disk or the file, see the Resource Guide for details of companies that provide a data recovery service. Data recovery companies use special software tools and can retrieve all or part of a disk even if it has been severely physically damaged or if files have long since been erased and overwritten. Such companies usually work on a "no fix-no fee" basis. The price charged in the case of a successful recovery will depend on the amount of work involved and, often, the value to you of the data recovered.

A Hard Disk Becomes Corrupted

Sometimes a hard disk becomes corrupted. Usually this is because an errant program has attempted to write data to the wrong part of a disk,

or a program has crashed while MS-DOS was in the process of updating a disk's directory.

Another cause of problem is a hard disk crash, where the disk drive's head touches the disk surface itself (under normal circumstances it floats a couple of microns above the surface).

A common symptom of a corrupted hard disk is a jumbled directory listing, consisting of corrupted file names and file lengths that are many hundreds of times larger than the values expected.

If you have a recent backup, the best solution is to format the hard disk and to restore from backups. Before doing this, use a machine that is known to be healthy in order to make a copy of the backup disks. Then restore from the copies. This way, you avoid the possibility that the backup disks will be corrupted by the faulty hard disk controller that may have corrupted the hard disk in the first place.

If the corruption problem goes away following the restoration from backups, then the usual procedure is to consider the problem solved. If the problems persists, consult a dealer or a data recovery expert.

By all means obtain a program that diagnoses disks, such as the Norton Disk Doctor that's part of the Norton Utilities. However, unless you are certain that you understand the diagnosis, do not seek to treat the problem yourself or let the program attempt to do so.

A Floppy Disk Becomes Corrupted

The rules above apply to corrupted floppy disks too. However, corrupted floppy disks can usually be copied with a bit-copying program. If you intend to fix a corrupted floppy disk by yourself, take a copy first and work only on the copy. Remember that you only get one chance to repair a disk.

If a floppy disk fails to read, try it in a different computer as there may be a problem with a drive being out of alignment. Try the disk in the drive that originally formatted the disk, for the same reason. If this technique solves the problem, assume that there is a problem with the original drive in that it creates disks that only itself can read. This should be fixed as soon as possible.

A Protected Program Is Lost

As discussed earlier, protected software packages are guarded by software or hardware means. Hardware protection normally means a dongle, and a lost or broken dongle can only be replaced by calling the software company to obtain a new one.

It is common for a small charge to be made for supplying replacement dongles. It is also unheard of for a software company to supply a spare one for emergencies. The moral here must surely be to avoid dongled software if 100% availability of the software is sought.

If a software-protected application is accidentally deleted, or if the installed program suddenly starts claiming to be an illicit copy and refuses to run, start by finding out as much as possible about what the PC was being used for immediately before the problem appeared. Then call the manufacturer of the software. There may be a simple solution, though it is more likely that you will be asked to sign a form declaring that the copy has been lost, after which a replacement disk will be sent.

A Backup Fails To Restore

It is possible, while restoring a multi-disk backup to a hard disk, for the RESTORE program to reject one of the disks, claiming that it is not the correct disk in the sequence or that the disk is not part of the backup set at all.

Such error messages are usually followed by a prompt, asking if you'd like to retry, ignore, or abort the restoration process. Start by asking for a retry. If the error persists, remove the floppy disk from the drive, rotate the disk slightly inside its plastic sleeve, then replace it and retry again. If there is still no success, you have two choices. First, you can select Ignore, which means that the restoration will continue and the error will be ignored. You will find that any files that were stored on the bad part of the disk will not be restored, or will be corrupted or incomplete, but at least you will have a semi-successful restoration.

The second choice is to abort the backup and attempt to fix the damaged disk. It may be suffering from a physical defect that can be fixed (see below). You can try a utility program such as the Norton Disk Doctor to find the problem.

Whatever you do, remember that you only get one chance to fix the problem. If the contents of that disk are important, consult an expert before doing anything else.

A Virus Is Suspected

The chapter on viruses (see page 75) lists some of the tell-tale signs that indicate the presence of a virus. If you suspect that one of your machines is infected, get hold of an automatic virus detector as soon as possible. Turn off the machine from the main switch, then turn it on again and boot from an MS-DOS disk that is known to be clean. Having done this, run the virus detector.

If the detector locates a virus, call in someone with the requisite skills to remove the type of virus that has been detected - do not attempt to recover the machine yourself unless you know exactly what to do. The person that you call in will be able to fix the hard disk and check any floppy disks, as well as other PCs, to ensure that the infection has not spread.

If you are tempted to clear up the virus yourself, or suggest that someone in your company takes on the task, the benefit to be gained by calling in outside help cannot be overstated. Even if you do not wish to call in an outsider, consider a telephone call to one of the virus experts listed in the Resource Guide; it will almost certainly save you time and money in the long run.

A Floppy Disk Gets Wet

A disk that gets wet is not beyond repair. If the liquid is cold water, just wait for the disk to dry out thoroughly and all should be well. If the water was hot, some distortion will often result and the disk may or may not be readable once dry. It all depends on the temperature of the water.

If another substance is spilled onto a floppy disk, the disk should be carefully washed in cold water. If the protective jacket is damaged, or if the spillage is bad, a transplant may be required (see below).

A Floppy Disk Gets Scratched

If a disk won't read, check for physical scratches. Rotate the disk in its sleeve, checking carefully under a desk lamp. If the scratch is actually a piece of dirt or a hair, then it can be removed. A physical scratch means that there is little you can do; attempt to copy the disk to another and select the "ignore" option when error messages are produced. This will copy all of the readable parts of the disk, and ignore the bad parts.

This process may leave you with a data file that is partly complete but with a number of gaps. If the file is a data file produced by an application program, the application may refuse to load the file, claiming that it is damaged. In this case, you will need to call in an expert or use a low-level disk editing program to search the disk for pieces of data and manually piece them together. This is not an easy job, and is made difficult because the layout of data files used by some application programs is hard to decipher. In an emergency, most application vendors will make available their file formats to data recovery specialists. Some, though, do not, claiming that file formats are trade secrets. The advice is obvious; do not use applications from vendors who refuse to publish their file formats.

A Floppy Disk Won't Spin

If a 5.25" disk is giving problems, attempt to rotate it in its plastic sleeve with your fingers. Place two fingers in the centre hole, then move the fingers apart until the sides of the fingers are gently gripping the sides of the disk. Now try to rotate.

You should find that the disk spins freely in its sleeve. Sometimes 5.25" disks refuse to spin. This problem often occurs if a disk has been on a journey through the UK postal system in an unsuitable envelope.

To cure the problem, you'll need a sharp knife, a spare disk and a clean surface. Place a finger in the centre hole and press down on the actual disk (the part you were attempting to spin) to ensure that it is out of the way of the top of the plastic sleeve. With the knife, slice the top off the sleeve of both disks. Remove the spare disk from its sleeve and throw it away.

Without touching the disk surface, remove the unreadable disk from its sleeve and place it in the spare sleeve. It is essential that the orientation of both disks is the same, ie take care not to turn the disk over in its new sleeve.

You should now have a disk which will spin, although the sleeve has no top. This disk should now read properly; copy it to a healthy disk then throw away the open-top version.

Sometimes, brand new disks fail to spin. If the problem is not detected early enough, someone will copy a file onto an unspinnable disk and send that disk to you. If this happens, there is no point in transplanting, as the data will not have been recorded correctly in the first place.

19 | Considerations For Networks

A local area network, or LAN, is a complex setup that has a number of unique security needs. These are outlined below. The subject of backup in general is also covered in the chapter which starts on page 61.

Cabling

Although wireless LANs are slowly beginning to appear, the vast majority of LANs are currently cable-based. Every workstation must be linked to the LAN by at least one cable. Where workstations are linked together in a ring, rather than directly to the server, there are two cables.

All types of network cable can be tapped though some are harder to tap than others. If data security is paramount, fibre optic cable should be chosen as this is far more difficult to tap. It is not impossible, of course, otherwise no one could ever install a workstation on a fibre optic LAN. It does require special tools, though, whereas copper wire can be spliced with little more than a screwdriver, some sticky tape and a pair of scissors.

If extra workstation sockets are installed when the network is cabled up, ensure that the unused sockets are disabled until they are required. This can either be done with the use of software utilities running on the server, or by physically removing one or more of the wires inside the socket. Failure to do this will allow an unauthorised user to plug a PC into the network in a location that your security staff would not normally check.

Cable junctions should also be protected, and marked in such a way that security staff (and no one else) can tell at a glance how many cables should be going into a junction box. This will allow boxes to be checked quickly and regularly to ensure that wires have not been inserted or removed.

If a wireless LAN is in use, ensure that all security options are turned on. If you are considering the purchase of a wireless LAN, choose carefully

the area of coverage that you require, or that you think you will require during the lifetime of the network. If your company's secrets are going to be floating around above the city streets, it makes sense to limit the area to as few streets as possible.

If you have more than one LAN, check the interconnections carefully. Make sure that you know which LANs are connected and which are not. If care is not taken, a user with supervisor-level access on the data entry LAN could, because of a little-known interconnection, gain similar access on the network used by the company's directors and financial controller.

Detecting Cable Taps

There are two ways to detect cable taps, ie breaks in network cabling where someone has covertly connected an unauthorised workstation, data logger or other device. The first method is by physical inspection, which should be carried out regularly. This is made easier if all cabling is of a bright, highly visible colour and is always kept in the open rather than being placed in hidden ducting.

The second method involves the user of a TDR, or Time Domain Reflectometor. This device is normally used to test network cabling installations, and it works by measuring the time taken for signals to travel between segments of cable. Such a device, which is available for sale or hire from any competent network specialist, allows you to pinpoint all taps in the cabling. Assuming that all authorised taps are documented, you can then detect any unknown breaks.

Unauthorised Laptop Connections

A number of products are now available that allow a laptop PC to be connected quickly and easily to a LAN. One such product is Lap2Lan, from Dublin-based East Coast Software. This product does not require the presence of a network card in the laptop. Instead, the laptop connects to a desktop PC via the parallel printer ports. By use of some special software running on the PC and the laptop, the laptop can share the network card in the PC, so that both can log on independently.

A product such as Lap2Lan is a great time-saver for someone who uses a laptop machine while out of the office, but who occasionally needs to access the network to transfer data when he or she is back at base. However, network managers should be aware that the use of such products means that you can no longer guarantee that you know the physical location of each logged-in user. Every PC with a network card represents a point from which a laptop user can connect to the network.

Of course, a valid user name and password is required (the laptop user can't piggyback onto the desktop owner's ID), but it does mean that a hacker equipped with a laptop can find a desktop PC in a quiet office and mount an attack on your LAN without fear of being spotted.

Welcome Screens

Legal experts have expressed confusion recently over the wording of "welcome screens" on a network. It is normal, when a user powers up a workstation and connects to the network, for a message such as the following to be displayed:

```
Hello and welcome to the Acme Paper Company
Computer.
The system is up.
Today is Saturday March 21st.
Please log in.
```

The Computer Misuse Act makes it an offence for someone to gain unauthorised access to a computer system. The police are known to be concerned that a message like the one above suggests to the user that the system knows who they are, and is inviting them to log in. This, it is claimed, makes it impossible for the network owner to claim that any access is unauthorised. This has resulted in several prosecutions being abandoned, or never started at all.

The above message also identifies the name of the company. Where computers are accessed over telephone lines, this is not a good idea — legitimate callers do not need to be reminded whom they are calling.

It is recommended that your welcome screen reminds the user of the Computer Misuse Act and asks him to confirm or deny, by typing Yes or No, that he or she:

a) does not intend to contravene the Act while logged in;

b) is authorised to use the computer;

c) will access only that data which he or she is entitled to access.

Do not simply say "Entering your password at this point implies agreement to adhere to the terms of the Act", as you will be unable to prove that the user actually read the message before signing on.

Software Packages

Some application software packages are designed for use on a network while some are not. A package designed for use on a network should allow the main program to be installed on the server, with configuration files for each user kept in the users' own directories. It should also provide correct file locking so that only one user can update a file at a time, and it should ensure that sensible action is taken if a user's workstation is accidentally or deliberately removed from the network while a file is open and locked.

Take care to ensure that packages not designed for network use are not installed on the server, as problems could result if multiple users attempt to access an unlocked file.

Do not allow any new software package to be installed on the network without permission, and make it a serious disciplinary offence for this rule to be broken.

Technical Support

Any network needs looking after. Some problems will be simple ones, like network cards and cables working their way loose or the installation of a new application software package on the server. Some may be more complex, and will need an experienced hardware engineer to solve and fix correctly.

Employing network support staff can be costly and there is a growing temptation among senior DP personnel to use a third-party company to support networks. These third parties claim in the brochures that they make the support job more cost effective and that they will take away the worry of dealing with your suppliers.

In practice, senior managers who have farmed out network support tell a different story. It normally proves impossible to convey to another company that the security and availability of your network is crucial to the running of your business, and outsiders will be happy to leave until tomorrow what you consider to be urgent maintenance that must be performed within the half hour.

Claims that third-party network maintainers will take the headaches out of dealing with hardware suppliers tend to be totally without foundation. The author has heard of many instances where the situation becomes more difficult because there are now three sides to every argument instead of the original two.

Copying From The LAN

Network workstations usually take the form of IBM-compatible PCs. There are two ways to configure the loading of a software package. In the first method, the software is stored locally on the workstation's hard disk; only the data files are accessed via the network. In the second method the program itself, as well as the data, is stored on the network.

Storing programs on local hard disks is more efficient as it reduces the amount of network traffic. However, it does mean that a user can copy data from the network to his local hard disk. If the workstation has a floppy disk drive too, this information may then be taken away. Even if the workstation has only a hard disk and no floppy drive, the data may be transmitted to another PC via the serial communications port on the back of the machine.

When buying workstations and configuring a network, consider the use of PCs that have no disk drives at all. They will still be capable of running all the programs from the network (so long as they have sufficient memory), but provide added data security by removing the ability for data from the server to be copied.

Network Analysers

A network analyser is a diagnostic tool used to locate problems on a network and/or monitor traffic to ensure that it is within acceptable levels. Network analysers can be hardware or software based; the hardware variety plugs into a spare port while the software version simply runs on any workstation.

A LAN analyser will display every packet of data that travels around the network, along with details of the workstation from which the data originated. Every byte, from every user (including the server) will be displayed by the analyser as it travels around the network. This includes passwords as well as any confidential data file that a user has requested. If you use a LAN analyser, keep it securely locked away when not in use. If your support department or an outside engineer wishes to use one to diagnose a problem, ensure that no staff are carrying out sensitive work on the system during the visit. Once the analyser has been used, supervisor passwords should be changed.

Sensitive files held on servers should be encrypted so that they will be unintelligible to the user of a LAN analyser. Although most LAN operating systems send passwords around in encrypted form by default, this is, ironically, the form in which the hacker needs them as he can capture

the encrypted password and feed it into the network again at a later date in order to impersonate the owner of that password.

Note that if you are using encryption options to ensure that no plain text data is sent around the LAN, special attention should be paid to printers, as the link between a LAN server and a printer cannot be encrypted unless the printer has been modified to accept scrambled data.

The Network Manager

The most crucial person in a network installation is the network supervisor or system manager. He is the person who sets up new user accounts, allocates passwords and sets up file permissions. He is the person who decides whether a user is allowed access to particular files or directories on the system. He is the user that must be responsible for ensuring the integrity of the data and that it is safely backed up on a regular basis. Where several users are keeping their data files on a central file server rather than on local hard disks and workstations, integrity and availability of the data on the server is paramount and the system manager must be aware of the responsibility that the job entails.

File Permissions

Setting of file permissions is the most important task, from a security aspect. *Keep thorough documentation of the file permissions that have been granted, and make occasional checks to ensure that the permissions you think have been installed are the ones currently active.* Do not allow a user access to any file or directory unless there is a good reason for him being allowed such access. If a user needs access to a particular program, give read access only to lessen the chances of an unintentional outbreak of a virus on the system.

File permissions should never be granted on a basis of seniority. If there is no real need for a user to be given access to data, then such access should be denied - even if the person concerned is a member of the senior management. This rule should be placed in the corporate data security policy to avoid arguments between network staff and those who feel that their job title entitles them to full network access.

When assigning file permissions, never give a user more rights than he or she requires. Only give a user rights to a program or directory if access is required.

To prevent infection by a virus, never give any user write-permission to

directories containing executable programs. Where programs insist on keeping their setup and configuration files in the same directory as the program file itself, do not allow user access to these files.

Trojan Horses

A user on a LAN, or on a multi-user machine such as a Unix box, has total control over the files he creates. The operating system normally allows the owner of a file to assign a number of security "attributes". For example, a user can specify that one of his files can be read by anyone on the entire network, but can only be amended or deleted by himself, ie the owner of the file.

Of course, the operating system prevents all except the file's owner from changing the attributes, or privileges, assigned to a file.

However, a security-conscious system manager needs to be on the lookout for Trojan Horse programs. For example, a hacker could write a program called "Patience", which plays a game of patience but also contains a command to the operating system which says "please make all my files accessible by anyone on the system". The hacker then makes the Patience program available to anyone, and tells people (in person, or via email) that the game may be used.

Anyone who uses the Patience program will find that their files magically become available to all, including the hacker. Such a situation may never be detected, unless regular checks are made by the system manager to ensure that all users' files are correctly protected with the required attributes.

Physical Security

The physical security of a file server must be maintained at all times. Although a network operating system may provide password control and thorough auditing of usage, it is often possible to start up a file server from a floppy disk and bypass the entire network system. Unless data on the server is encrypted, this leaves every file, in every directory, visible and copyable. Even when network operating systems do not exhibit this major security flaw, it can still be possible for an intruder to gain access to the entire contents of the server via the use of specialist disk-explorer utility programs if he can get near enough to the server to insert the explorer program disk.

The OS/2 LAN Server (unless running the High Performance File System) is an example of a system whereby the entire hard disk is vulnerable

to anyone who manages to load a utility program onto the server. Novell NetWare is slightly more secure in that it uses a non-standard disk format which cannot be read by standard programs such as the Norton Utilities. You may consider that the OS/2 LAN Server situation, where diagnostic programs can be used to help recover lost data, preferable. From a security point of view, it is better to have a server that is less accessible and which is backed up frequently.

No one except the network manager should be permitted to install new software packages on the server. Anyone else who is caught attempting to do so should be dealt with severely. A program installed on the server will normally be available to all users and it is essential that you control carefully the software available to users. This is not only for security reasons, but also to ensure that you comply with the licence agreements which often forbid installation of software on a network unless a suitable number of copies or licences have been purchased.

When engineers are on site, testing the network or installing new equipment, they should not be left unattended at any time.

UNIX-based servers must be physically protected, and the master UNIX boot disks kept in a secure location at all times. *With most versions of UNIX, someone with access to the server and the boot disks can log in with root privileges* and will have access to the entire system.

A number of companies sell lockable plates that can be fixed over a floppy drive to prevent unauthorised users inserting disks. Such a device is recommended for file servers.

Securing A NetWare Console

If your network operating system is NetWare 3.x, you should include the command SECURE CONSOLE in the AUTOEXEC.NCF file. With this command installed, a user who gains physical access to the server cannot load any NLMs (NetWare Loadable Modules), exit to DOS or change the system time/date.

You should also load the MONITOR.NLM program and select the "lock file server console" option. This will force the system to request a password before any commands can be entered from the server's keyboard.

Disabling The Server Floppy Drive

You can take some simple steps to help prevent access to the floppy drive on a network server. With Novell NetWare, typing:

MAP A:=SYS:USERS\FRED

will re-map drive A (the floppy disk drive) to a directory on the server. Any attempt by a user to copy data to drive A will result in that information being copied to another part of the server instead.

Of course, the MAP DEL command gets around this security precaution by removing the effect of the MAP. To prevent users typing MAP DEL, you can patch the MAP.EXE program and change DEL to any other 3 letters. You will, though, have to patch every copy of MAP.EXE held on the server and on users' workstations.

Executable File Protection

The FLAG command on a Novell 3.x network can be used to prevent users copying programs (executable files) from the server. Typing:

FLAG PROG.EXE X

prevents the file PROG.EXE from being copied. Note that the X flag, once applied, cannot be removed. Use it with caution and remember that the loss of the ability to copy a file with an X flag also means that the file cannot be backed up.

Password Rules

Some network operating systems allow the system supervisor to set up special rules for the use of passwords. The following rules should be followed:

- If the system allows a minimum password length to be specified, set this to six characters.
- If password expiry can be set, a value of no more than 30 days should be entered. This will force each user to change their password every month.
- If the operating system includes a feature to prohibit multiple logins on one account name, ensure that this feature is enabled.
- Make it a rule that the system manager password should be used only for performing system administration tasks. Holders of the system manager password should use normal user-level passwords for all other tasks, to minimise the risk of disaster. Every network manager of my acquaintance has had a least one data loss caused by

using a password that was more powerful than the user had thought before he typed a certain command.

Backing Up The LAN

For general backup-related information, see the chapter on Backups (page 61). There are, however, certain points relevant specifically to backing up a local area network. These are discussed below.

Users

Integrity of a backup can be guaranteed only if all files on the server are closed and all users are logged out. If you are backing up a server that is linked to another network, ensure that the links are disconnected. If a user on a remote server alters part of a database while that database is being backed up, the integrity of that database will almost certainly be unreliable.

Buying Tape Streamers

When buying a tape streamer for backing up a network server, plan ahead for the level of network usage. Where possible, you should back up overnight while all users are away from their terminals. You need to ensure that your tape streamer has sufficient capacity to back up the entire server without manual intervention. Otherwise, you may arrive in the morning and find that the backup device is waiting for a tape to be changed, but that one or more users have already logged in. Once again, this is a severe threat to the integrity of the backup.

Backup Software

If you intend to back up overnight, look for backup software which will automatically back up the LAN at a predefined time, without any user intervention. Ensure that the software can automatically check that no users log in during the backup. Some backup packages also let you create special script files to customise the package. For example, you can specify different backup options according to the day of the week.

Where To Back Up From

The backup device can attach to the network in one of two places - at the server or at a workstation. For a simple network consisting of a single

server and a number of workstations, you should back up from the server.

Backing up from a workstation poses a number of security problems. First, the workstation from which the backup takes place needs to have supervisor status. For this reason, the workstation should be physically protected to prevent a passer-by aborting the backup and using the workstation to perform supervisor tasks.

There is also the issue of speed. Backing up from a workstation involves large amounts of information travelling across the network. This should not slow down the users, as there should not be any, but it is still likely to slow down the backup process.

Finally, consider costs. If your server is remote, linked to a workstation by an X.25 line or similar, you will be charged for each packet of data sent over the line. If this is the case, backing up via the server should be the only method used.

Auditing

Most network operating systems provide an automatic audit facility. This logs all unsuccessful login attempts and system usage in a file, for later analysis by the system manager. *Ensure that all audit facilities are enabled, and that the log files are protected so that they cannot be deleted by an intruder attempting to cover his tracks.* In one well-documented case, a hacker spent many nights trying to guess a password. His efforts went undetected because all records of incorrect passwords were sent to the electronic mailbox of the security manager. The hacker already knew the password to this mailbox, so was able to remove the evidence before the security manager arrived for work in the morning.

Passwords

It is difficult to persuade employees to change passwords regularly and to keep them confidential, and the security of a computer must not rely on users remembering to do this. The more security-aware network operating systems automatically impose minimum password lengths, and maximum and minimum password lifetimes. Such systems should be used if available. The latest versions of OS/2 LAN Manager and Novell NetWare allow the administrator to specify that certain users may only log in from certain workstations and at certain times of the day or week. Holders of supervisor-level passwords should always be subjected to such controls if available.

Replication And Mirroring

Where many users' data is stored on a central network file server, the risk of losing the contents of that server are greater than losing the hard disk on a single PC and steps must be taken to guarantee the integrity and availability of the server's hard disk. File Replication is one facility to look out for. This automatically copies named files, or groups of files, to a specified destination after a specified period of time. For example, it could be set up to copy all spreadsheet files to another workstation every 30 minutes to provide an automatic backup mechanism for those in the planning department who work on spreadsheet files.

Investigate hard disk mirroring too. This is based on a special hard disk controller card in the server which saves all data to two physical hard disks - one being a complete copy of the other. The second hard disk unit is automatically brought into use if the first develops a fault. Look out, too, for transparent "hot fix" features, where the network automatically copies data from one part of the hard disk to another if a fault develops in one small area of the system.

A variation on mirroring is known as duplexing, where a computer contains two hard disk controller cards as well as two separate hard disks. This adds a level of security.

Not all disk mirroring systems need two full-size hard disks. Compaq's SystemPro unit has a mechanism whereby around one third of the disk is set aside for mirroring. A clever combination of data compression and special software means that this part of the disk contains everything needed to reconstruct any piece of data if part of the disk becomes bad.

Data Striping

A variation on replication and mirroring is data striping. Here, a server is equipped with, say, 8 separate hard disks. Files are arranged in "stripes", so that each hard disk holds one eighth of the file. The benefit of such a system is that, in the event of a total hard disk failure, no more than one eighth of each file will be lost. The downside, though, is that the statistical probability of a hard disk failure in such a machine is 8 times greater than the probability of a failure in a machine with only one hard disk. For this reason, systems which employ data striping also use some form of replication or mirroring.

Data striping can drastically increase access times where large files such as databases are involved, as it is possible for two parts of the file to be accessed at the same time provided that they are located on different physical hard disks.

Uninterruptible Power Supplies

Invest in a UPS, or uninterruptible power supply. This is a battery pack that is capable of keeping a network server and some terminals running for between five and 30 minutes in the case of a mains power failure. The UPS will detect a power failure and switch itself into the circuit. At the same time it will notify the network operating system that a power failure has occurred. The network can then send messages to all users and warn them to quickly exit the program they are using, save their data and log out. When all users are logged out, the network can then be shut down safely.

Filters

Many companies supply main power filters which eliminate fluctuations in voltage and current caused when large machinery is turned on or off. File servers and PCs holding particularly sensitive data should not be placed near heavy electrical equipment and should not share a mains socket with such machinery. If such a situation is unavoidable, a power filter should be fitted. In the absence of equipment that is known to introduce surges into electrical circuits, personal experience suggests that such filters are not required.

Examples of machinery that can cause power fluctuations include any piece of equipment containing a powerful electric motor. The fan and hard disk in a PC are not considered powerful in this context, but portable air conditioners and dehumidifiers are capable of causing problems. Washing machines, upright cleaners, fridges, portable convection heaters and floor polishers can cause problems too.

Mains power in the UK is fairly "clean", especially when compared with that of the US. There are relatively few surges, spikes, unexpected voltage drops and so on. While many computer users in the US use power filters, even home workers with just a single PC, the need for such a device is not nearly so great in the UK. However, where a company-critical network is involved, the investment in a UPS and filter is tiny compared to the peace of mind they provide.

Replacing Power Supplies

Modern PCs are built to a highly modular design and the power supply is easily replaceable. If a machine goes down and the power supply is known to be the only culprit, a new unit can be purchased from any

competent dealer and simply plugged in to replace the old one. It is essential, however, to ensure that the input and output voltages and currents of the two units match. Make sure, also, that the new power supply has sufficient output cables to power all the devices fitted in the machine.

Login Security

Ensure that no actions can be taken by a user before he or she has logged in. It is not unknown for large networks to allow access to the HELP command before a login. This allows an unauthorised user access to the list of valid commands plus, frequently, the name and phone number of the person to call in case of problems. Restrict access, also, to the command that allows users to see who else is logged in, as user names can be used by the hacker as a good starting point.

Encryption

Many network operating systems have an encryption option. When this is enabled, all data sent around the network is encrypted and thus of no use to someone who has tapped a cable.

Where networks use public telephone lines, or long stretches of exposed cabling, encryption should always be used.

However, remember that any cable linking a server or workstation to a printer is very unlikely to be carrying encrypted data, so such cables should be physically protected if necessary.

20 | Current UK Legislation

Following are details of the current UK legislation that is relevant to, or that contains sections relevant to, PC data security. Copies of the relevant Acts may be obtained from HMSO, or inspected at any large public library.

Hackers don't always make good lawyers. Please bear in mind that the interpretations of the Acts detailed below are my own, and are no substitute for the advice of a good solicitor.

Data Protection Act 1984

This Act states that any company which processes personal data about individuals on a computer must register with the Data Protection Registrar. The registration must state the type of data held, and the uses to which it will be put. The holding of data not documented in the registration, or the use of that data for purposes not specified in the registration, constitutes an offence under the data protection Act.

The Act includes eight "data protection principles" to which all registered data users must adhere. These are as follows and are direct quotations from the Act.

1. The information to be contained in personal data shall be obtained, and personal data shall be processed, fairly and lawfully.

2. Personal data shall be held only for one or more specified and lawful purposes.

3. Personal data held for any purpose or purposes shall not be used or disclosed in any manner incompatible with that purpose or those purposes.

4. Personal data held for any purpose or purposes shall be adequate, relevant and not excessive in relation to that purpose or those purposes.

5. Personal data shall be accurate and, where necessary, kept up to date.

6. Personal data held for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.

7. An individual shall be entitled -

   (a) at reasonable intervals and without undue delay or expense -

      (i) to be informed by any data user whether he holds personal data of which that individual is the subject; and

      (ii) to access to any such data held by a data user; and

   (b) where appropriate, to have such data corrected or erased.

8. Appropriate security measures shall be taken against unauthorised access to, or alteration, disclosure or destruction of, personal data and against accidental loss or destruction of personal data.

Computer Misuse Act 1990

This Act makes it an offence to gain unauthorised access to a computer. The two major offences created are those under Sections 1 and 3 of the Act as follows:

- A person is guilty of an offence under Section 1 of the Act if he "causes a computer to perform any function with intent to secure access to any program or data held in any computer, and the access he intents to secure is unauthorised, and he knows at the time when he causes the computer to perform the function that that is the case".

- A person is guilty of an offence under Section 3 of the Act if he "does any act which causes an unauthorised modification of the contents of any computer, and at the time when he does the act he has the requisite intent and the requisite knowledge".

The Act came into force on the 29th of August 1990, and an offence cannot

be prosecuted under this Act unless every part of the offence was committed after this date.

In mid July 1991, the first prosecution under the Computer Misuse Act failed. The defendant was charged under Section 1 with altering a price code on his employer's computer, so that the defendant could buy goods from his employer at a reduced price. The defence lawyers argued, successfully, that the Computer Misuse Act did not allow for the hacker's computer and the hacked computer to be one and the same. This apparent loophole will almost certainly be the subject of one or more appeals. At the time of writing no decision has yet been made.

Interception Of Communication Act 1985

This Act states that a person is guilty of an offence if he "intentionally intercepts a communication in the course of its transmission by post or by means of a public telecommunication system".

Note the title of this Act. Many books and Guides refer to it, incorrectly, as the Interception of Communications Act.

There are many exceptions to this. For example, no offence is committed if "the communication is intercepted for purposes connected with the provision of postal or public telecommunication services". While this allows the Post Office and BT to monitor their own services in order to measure quality or to solve problems, it also gives these companies carte blanche to monitor customer traffic for other purposes too. This is the clause under which Telecom Gold claimed that they were permitted to read all private messages in my own personal electronic mailbox during a period in 1987; the company claimed that they were tapping my mailbox in order to monitor the level of service. When I pointed out that they were also monitoring the mailbox of a friend of mine, no explanation of the coincidence was forthcoming.

Copyright, Designs And Patents Act 1988

This Act covers the copyright of software. An offence is committed under this Act if you make unauthorised copies of a software package, whether for personal use or for sale.

Companies Act 1985

Section 722 of this Act states that company directors must take steps to keep financial accounting records on computers safe and uncorrupted, and audit trails must be in place to detect falsifications.

Police And Criminal Evidence Act 1984

This Act deals with the admissibility of computer-produced evidence. It states that computer records are acceptable as evidence only if they can be proved to be correct. The exact wording states that a document produced by a computer shall not be admissible as evidence unless it is shown:

a) that there are no reasonable grounds for believing that the statement is inaccurate because of improper use of the computer;

b) that at all material times the computer was operating properly, or if not, that any respect in which it was not operating properly or was out of operation was not such as to affect the production of the document or the accuracy of its contents.

Bearing in mind that no software application vendor or hardware manufacturer would ever be so stupid as to swear that his system was totally bug free, and that no operating system yet devised has been 100% reliable, it is clear that lawyers stand to make a large amount of money as soon as a defendant stands up in court and says to the Prosecution "prove that your computer was operating properly".

Criminal Justice Act 1988

This governs the admissibility of evidence in criminal (rather than civil) cases.

It covers the admissibility of hearsay evidence, and also deals with business documents and computer printouts.

This Act updates some parts of the Police and Criminal Evidence Act 1984.

Civil Evidence Act 1968

Covers the admissibility of evidence in civil cases, in similar detail to the way that the Criminal Justice Act 1988 covers evidence for criminal cases.

Telecommunications Act 1984

This Act is not strictly relevant to the security of stand-alone PCs. It does, however, apply where unauthorised computer access is gained by way of a telecommunications system and may, therefore, be of use where access to a PC or network is effected via a modem or other telecommunications link.

Section 42 of the Act states that "A person who dishonestly obtains a [service to which this subsection applies] with intent to avoid payment of any charge applicable to the provision of that service shall be guilty of an offence".

The maximum penalty for an offence under this section of the Act is a fine and/or two years' imprisonment.

Section 43 of the Act makes it an offence, punishable by a fine, to:

a) send, by means of a public telecommunication system, a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or

b) send by those means, for the purpose of causing annoyance, inconvenience or needless anxiety to another, a message that he knows to be false or persistently makes use for that purpose of a public telecommunication system.

Finally, section 44 of the Act makes it an offence for an employee of a telecommunications system to intentionally modify or interfere with the contents of a message, except in the course of his duty. This Section may be of use if you suspect that the operator of a commercial electronic mail service is interfering with your transmissions.

21 | Resource Guide

The products, services and books listed here are those which, in the opinion of the author, may be useful to you as a reader of this Guide. Some products have been tested extensively by myself, others less so.

For convenience, this chapter is the only place in the Guide that mentions products and services by name. This allows you to peruse the list easily, and to have all product details available in just one place. You will automatically receive updated copies of this Resource Guide every few months, free of charge.

All telephone numbers are listed in international format. If you are calling a UK number from the UK, replace +44 with 0. If you are calling a US-based number from the UK, add 010 to the start of the number.

Hardware

There are many hardware products designed with PC security in mind. Some are complete PCs with access control built in, while some are add-on access control devices. The following list is far from exhaustive, but covers just about every category of product.

Sentry Fire Safes

A range of US-made fire safes designed specifically for holding magnetic media.

Manufacturer: Sentry Group, 900 Linden Avenue, Rochester, New York 14625, USA. Telephone +1 716 381 4900.

UK distributor: Silver Lynx Products Ltd, Lynx House, 23 Roman Way, Lichfield, Staffs, WS14 9YP. Telephone +44 543 254835.

AccuCard

An add-in card for 386- and 486-based PCs. In the event of power failure, the card will back up the contents of the PC's RAM to disk. When power

is restored, the special AccuCard software will re-load the system's memory from disk, and the PC will return to precisely the state that it was in before power was lost.

According to the AccuCard brochure, it is quite safe for a user to turn off a PC at night, in the middle of an application; switching on the computer in the morning will restore it to exactly the point it was at when the power was removed.

The current retail price is £169.

AccuCard is available in the UK from Emerson Computer Power, Elgin Drive, Swindon, Wiltshire, SN2 6DX. Telephone +44 793 524121.

HOTLINE Modem

A modem designed for use when sending confidential data between two sites. The HOTLINE modems are designed to be used in pairs. They include built-in DES encryption as standard, and all information sent between a pair of modems is automatically encrypted before it is sent and then decrypted when it arrives. This ensures that no data can be accessed by tapping the telephone line.

The modems automatically change DES passwords randomly at approximately 30-second intervals, so in the unlikely event of someone being able to decipher the DES password only a small amount of data would be readable.

The manufacturer is Telequip Corporation at 18 Clinton Drive, Hollis, NH 03049, USA. Telephone +1 603 881 5616. Fax +1 603 881 5635.

Tempest Protected Laser Printer

Wenger produce one of the few laser printers that's shielded to Tempest standards, to prevent remote hackers from listening to the radio emissions generated by the machine and so deciphering the information that it is printing.

The company's current models emulate HP LaserJet II, Diablo and IBM ProPrinter machines, and PostScript is also available as an option. Prices are around twice that of non-Tempest machines.

Wenger can be contacted on +44 865 891666.

Tulip Disk Encryption Unit

Tulip is one of the few PC manufacturers which takes security seriously. Its current product list includes the Tulip Disk Encryption Unit. This is a replacement for a standard IDE hard disk controller card and provides automatic DES encryption.

The DEU can be supplied in Tulip PCs, or purchased separately for use in any IBM-compatible PC which allows the existing hard disk controller to be removed or disabled.

The card provides a password facility. The user is asked to supply the password each time the computer is turned on. The encryption key is based on a combination of this password and something known as the machine code. This is another password, decided by whoever is nominated as the system administrator. Because both the machine code and the user's password are used together to create the DES key, a stolen hard disk drive will not work with any other Tulip DEU card. Equally, a stolen DEU card will not be able to decrypt hard disks that it did not encrypt in the first place.

Because the DES encryption is performed in hardware, there is no noticeable loss of performance.

The user password is not stored anywhere on the DEU card, so it's impossible to discover it. The machine code is stored, in a PROM, but is encrypted. As is the code on the card which performs encryption, asks for passwords and so on.

On the face of it, a PC protected by a device such as Tulip's DEU would seem to be 100% secure. There are, however, some important things to note:

- A user of such a machine will receive a warning message upon power up, if someone has been trying to hack into the machine. This message appears if recent attempts at guessing a password have been unsuccessful 3 times in succession. However, the flag which tells the card to display this message is concealed in the CMOS memory of the machine, ie the clock device. This allows a hacker to cover his tracks by disconnecting the CMOS battery for a few minutes.
- Tulip claims that, in the event of a user forgetting his password or the machine code, Tulip engineers can re-program the card so that access to the hard disk may be restored. At present the method for doing this remains confidential, but it is difficult to take seriously Tulip's claim that the presence of both a password and a machine code combine to make the system more secure.

- All parts of the hard disk are encrypted, even the system tracks and the File Allocation Table. In the case of a program bug or a hardware fault causing data corruption, it will be impossible to recover the data with standard disk recovery tools such as the Norton Utilities and a standard hard disk controller because, although the data will be physically accessible, it will be totally garbled and unintelligible to the person trying to reconstruct damaged files.

  Bearing in mind that the card is designed for use by senior staff who have highly confidential data to protect, this could be a major problem.

- There is no time-delay software which locks the machine and asks for re-entry of the password if no key is pressed for a number of minutes. This means that the machine is vulnerable if an authorised user turns it on, enters the password and then walks away.

Tulip can be contacted in the UK on +44 293 562323. The DEU card costs £325.

Policeman

Policeman is an access control system for PCs. It is software and hardware based, and provides a high degree of protection.

A user who wishes to access a PC protected with Policeman must enter a password. They then need to plug a special key into a receptor that is affixed to the side of the machine. Only then can the machine be accessed, and the key must be left in the machine throughout the session or the keyboard is automatically locked.

Each user can have a separate password and key, and all unsuccessful password attempts are logged. If a user fails to enter a correct password after three attempts, a siren sounds.

The system includes full encryption, so there is nothing to be gained by a user unplugging the Policeman card from the PC. The encryption algorithm is proprietary, though, and is neither DES or RSA. Precise details are not made public.

A combination of passwords, physical keys and encryption provides the toughest access control system possible without resorting to hi-tech expensive equipment such as handwriting recognition or retina or fingerprint analysis.

Details from NMDP Ltd in Farnborough, UK, on +44 252 377437.

Triumph And TriSpan

These two products from US-based Micronyx are access control packages. Triumph is a software-only package providing encryption, access control, logs of invalid password attempts and a host of other features. TriSpan provides the same facilities but includes hardware-based protection for added security. The plug-in card provides physical key protection. The encryption used in TriSpan is based on the user's password and the specific card in use, so plugging in another TriSpan card whose password is known will not allow data to be decrypted.

Although expensive, TriSpan is the most secure protection package that I have ever used; I spent many days trying to break it but was unsuccessful. Where total security is required, this is the ultimate solution.

Micronyx Inc are at 1901 North Central Expressway, Richardson, Texas 75080. The UK arm is Micronyx UK Ltd in Milton Keynes, on +44 908 604152.

Watchdog

A plug-in card for PCs which provides a comprehensive range of data security and access facilities. These include:

- Password control on boot-up, with facilities for defining minimum password lengths and forced password changes at regular intervals.
- File protection at the directory level. Separate access rights for execute, read, write, create and delete, for each user in each directory.
- Real-time data encryption using the RSA algorithm, which encrypts all data as it is written to disk.
- Password protection for DOS and PC resources such as printers, disk drives, modems.
- Automatic over-writing of deleted files so that they cannot be recovered with utility packages.
- Audit trail facility monitors usage on a per-user level, and records the names of programs executed. Audit files are dBASE compatible.
- The ability to restrict the use of the FORMAT command.

Watchdog runs under MS-DOS or OS/2. Details from International Software Management Ltd, Dukes Court, Duke Street, Woking, Surrey, GU21 5BH, UK. Telephone +44 483 740033. Fax +44 483 740282.

Physical PC Security

Qualtec provide a range of device to physically secure a PC. The special steel brackets hook around the PC and fix it to the top or side of a desk. The PC's case does not need to be opened, so warranties are not compromised, and the PC can be easily removed with a key when internal access is required. Machines currently supported include all IBM PS/2s plus some Compaq and Zenith models.

The company also supplies special locks that can prevent access to a PC's power switch or network cabling, as well as steel ropes attached to industrial-strength adhesive pads for securing PCs to walls or shelving.

Qualtec Inc are at 47767 Warm Springs Boulevard, Fremont, California 94539. Tel +1 415 490 8911. Qualtec Europe are in Aldermaston, UK, on +44 734 810220.

Computer Guardian

A burglar alarm for a PC, on a plug-in card. A motion sensor detects movement and, if the PC is moved, the built-in battery triggers the 90 dB alarm. The product is available from Harvest Electronics.

Also available is a version of the card with built-in password protection features, which force users to enter a password when the machine is switched on. Without the correct password, the machine cannot be used.

Remote PC Link

Remote PC Link is a relatively new product that protects PCs from physical theft and unauthorised use. The product consists of a set of cables, plus a circuit box, that allows you to put the computer's keyboard and screen up to 20 metres away from the CPU box. All the CPUs in a department can therefore be locked away in a separate room. Remote PC Link is produced by Europa Security Systems and costs £164.

Software

Some of the best security-related software utilities are what are known as Public Domain or Shareware. Public Domain programs are written by enthusiasts rather than business people, and released into the public domain for free use by anyone. To acquire a copy of such a program, you simply take a copy from someone who already has it. If you cannot find

someone with a copy of the program, try a local dial-up bulletin board or a commercial online system such as Cix.

A Shareware program is also distributed by being copied. However, the author of a Shareware program requires payment, which you are obliged to send if you find that the program which you have acquired is useful and you intend to use it on a regular basis. The amount required, and the address, is normally displayed when you start the program. This is typically between $5 and $150; most Shareware comes from the US though UK-based systems such as Cix have literally thousands of Shareware programs available to subscribers.

If you have trouble locating a copy of a Shareware or Public Domain program listed here, please contact the publishers of this Guide and they will do their best to find a copy for you.

DDC

DDC stands for Disable DOS Commands and was written by Robert Schifreen. It is a Public Domain utility which allows internal MS-DOS commands to be disabled. Commands that consist of executable files, such as FORMAT and RECOVER, can be effectively disabled by removing them from the user's hard disk. Those commands built into MS-DOS cannot be disabled so easily, and include DIR, COPY, TYPE and RENAME. DDC is not foolproof, though it will deter the casual intruder. DDC is available from UK-based bulletin boards including Cix.

SPM

Serial Port Monitor. Copies all incoming data from one or more serial ports to a file on a PC's hard disk. Shareware, and available from bulletin boards or shareware libraries.

LAN Assist

A utility that allows a network supervisor to monitor other users' workstations from the supervisor screen. Often used by technical support departments to help users sort out problems (the supervisor can take control of a workstation from the supervisor's console if required). Also used by security staff to monitor users suspected of abusing the network.

LAN Assist should be available from your Novell NetWare supplier.

AccessData

AccessData, based in Orem, Utah, sells a number of programs which can recover the password from a PC data file that was saved in encrypted format by the host application.

The company produces software which can recover files that were password-protected by WordPerfect, PlanPerfect, Lotus 1-2-3, Microsoft Excel, Paradox and others. I have tried the WordPerfect/PlanPerfect flavour, and it works.

The availability of such software is worrying. AccessData's marketing material suggests that being able to recover passwords makes the password feature more useable, as there is no risk of being locked out of the files which belonged, for example, to a member of staff who has been dismissed.

AccessData has taken a little trouble to ensure that its programs are available only to authorised users. To use the program you need to know the access code, and this is printed in the manual. Locking up the manual will prevent staff using your company's own copy of the software to crack passwords, but it's no defence against someone with a file to crack and $185 to spend.

The other "security" feature is that the programs will refuse to reveal passwords which contain an underscore character. Encouraging staff to use at least one underscore character in passwords will make their protected files immune to AccessData's software, but PASSWP is not so obliging.

The advice here is clear: if you want to use passwords which can be recovered by a $185 program, use the built-in facilities of your application. If you want to protect data properly, use a third-party encryption program that uses the DES or RSA algorithms.

AccessData can be contacted on +1 801 224 6970. Fax +1 801 224 6009. UK distributor is Key Exchange, based in London, whose telephone number is +44 71 498 9005.

PASSWP

PASSWP is a Shareware program which can recover the password used to save a "protected" WordPerfect or PlanPerfect file. I have tested PASSWP with WordPerfect 5.1 and PlanPerfect 5.1 files, and it successfully recovered the password for each file in just a fraction of a second.

PASSWP is distributed on bulletin boards around the country, and should also be available from Shareware libraries.

The availability of this program is just one reason why you should never rely on software packages' built-in encryption systems for protection. If your users currently protect WordPerfect documents with the WordPerfect password feature, change to a third-party DES or RSA encryption utility if you wish to ensure that your files remain secure.

HISTORY

HISTORY is a Public Domain program by Robert Schifreen, again available from Cix and other UK bulletin boards. The program installs a command logger on a PC, which keeps a log of all commands typed at that PC, plus the time and date on which the commands are typed. The log file can then be examined at a later date to help in the detection of unauthorised use of a PC. The program is also useful to support staff who wish to find out what commands are causing problems for users.

There are solid legal reasons for recording the date on which events take place. Very little legislation is retrospective, so someone who hacked into your computer in 1989 cannot be prosecuted under the 1990 Computer Misuse Act. Being able to prove that a crime was committed after an Act achieves Royal assent can make a great difference to the success of a prosecution or civil action.

For those interested in the technical aspects, HISTORY works as follows.

It is the job of the MS-DOS command processor, COMMAND.COM, to display the DOS prompt and allow the user to type in a command. Once the command has been typed, COMMAND.COM performs the necessary action. If the command is a resident DOS command such as COPY or DEL, the appropriate task is performed by COMMAND. If no internal DOS command name matches what the user typed, COMMAND searches for a file on disk and, if it's found, that executable file is loaded and executed. If the file cannot be found, COMMAND displays a "Bad command or file name" error and the DOS prompt is displayed once more, ready for the user to type in a new command.

To perform the actual process of reading the keyboard, COMMAND calls MS-DOS function 0Ah. This reads a string of characters from the keyboard, and terminates when the user presses Return. Before calling function 0Ah, you have to set up a buffer somewhere in memory to store the characters. You use the DS and DX registers to do this. You also need to tell the function the maximum number of characters you wish to permit the user to type. After this maximum has been reached, the system will just beep after every key press until the user presses Return.

The maximum character count is placed in the first byte of the buffer whose address is specified in DS:DX. When the function returns, the number of characters that the user typed is placed in the second byte, and the actual characters appear starting at the third byte.

HISTORY is a resident program which, when it installs, takes over the handling of all Int 21h calls. From now on, all Int 21h calls (ie every MS-DOS function call) is handled by the installed HISTORY program.

HISTORY's Int 21h handler starts by checking the value of AH. If this is not 0Ah, then a function call other than get_string was requested, and HISTORY transfers execution to the original Int 21h handler that was in place before HISTORY was installed. However, if AH is 0Ah, then a get_string call was requested. In this case, HISTORY calls the original Int 21h handler to get the string but, before returning control to the caller, makes a copy of that string to a text file.

PW.SYS

This simple MS-DOS device driver is a Public Domain utility known to be available on Cix in a file called PASSWORD.ARC. When installed in a PC, the computer asks the user for a password each time the machine is started up. Unless the correct password is entered, the system hangs.

While not uncrackable, and although no encryption is built into this program, it will deter casual intruders and is far better than having no access control at all.

LHA, PKZIP, ARJ And ARC

These are all Public Domain and Shareware file archiving programs. They compress files, and merge files into one for easy distribution and backup. All are in widespread use by PC users worldwide. PKZIP provides data encryption if required, but only on versions acquired from the US. You will need to obtain a copy from a US-based bulletin board to ensure that the encryption option is present.

Be aware that PKZIP's encryption system does not scramble the names of files, but only the data that they contain. A hacker can, therefore, look through a scrambled ZIP file and clearly see the names of the scrambled files that the ZIP contains. This could pose a security problem in certain cases.

These programs are totally incompatible with each other; an archive created with one program can only be de-archived with the same program.

McAfee SCAN

SCAN, from McAfee Associates, is a Shareware virus detector. It is available from many bulletin boards in the UK, including Cix. A new version of the program is made available by its author every week or two, ensuring that it knows about the most recently discovered viruses. For this reason, it is one of the most useful virus detectors. If you are worried about the possibility of a virus creeping into the detector, the author of SCAN operates his own bulletin board in the US from where guaranteed-clean copies of the program can be obtained. Telephone +1 408 988 4004 for modem calls. For voice calls, +1 408 988 3832. Fax +1 2 408 970 9727.

Flexibak Plus

A complete Shareware backup package for PCs. Not as fast as most of the commercial offerings, but praised by its users. Available from UK bulletin boards including Cix.

PowerMenu

A Shareware menu program for PCs that allows users to select commonly-used applications from a main menu. Options not on the menu cannot be accessed. Password protection for specified menu options is supported. No encryption, so not unbreakable, but a useful deterrent. Available from UK bulletin boards including Cix.

The Norton Utilities

The most well-known of the commercial software packages providing a wide variety of PC utilities in a single product. From a security point of view, the most important utilities are UNERASE, UNFORMAT, NU and NDD. The UNERASE program recovers erased files from MS-DOS disks, while UNFORMAT recovers from an accidental format. Both programs work most reliably if the tracking (recording) file is active.

NU is the main Norton Utilities program, providing the facility for experienced PC Support staff to examine and repair PC disks at a low level. NDD is the Norton Disk Doctor, a program that automatically identifies (and corrects, if required) many common faults that afflict hard and floppy disks. NU includes a special Maintenance Mode, under which the program will attempt to read a hard disk on a sector-by-sector basis even if it is not recognised as being in MS-DOS format.

The version of the Norton Utilities sold in the US has a DES file encryptor, but this is not provided in copies sold in the UK.

PC Tools

Probably the main competitor to the Norton Utilities, this utility package provides similar facilities. Like Norton, PC Tools includes a number of programs for data recovery, ie attempting to recover lost and deleted files, and formatted disks. PC Tools also includes a complete backup utility whereas the Norton Backup is a separate product. PC Tools also includes support for Novell NetWare. PC Tools is produced by Central Point Software and is available from dealers.

Fprint

An excellent set of utilities to aid security staff in the monitoring and auditing of PCs.

Fprint itself takes a snapshot (a fingerprint) of a PC. It records basic information about the machine (such as the DOS version, the screen type, whether a mouse is connected), plus details of every file on every hard disk. A number of additional programs are then supplied to manipulate this data and to produce reports. For example, Fprint/AU is a software auditing package which, with the aid of a database of recognised applications, provides an excellent software audit facility. It is the only software audit package available at present which provides all of the functionality listed in the section on software audits (see page 104).

Another package from the Fprint stable monitors changes to the contents of a PC, and will report changes to files or directories. There are versions for use on a Novell network, to monitor who is accessing which sets of files, who is logging in and out, who is changing the bindery and so on.

Such utilities can also detect files which change because of infection by a virus.

Details from Fprint UK on +44 71 937 0260.

PC Armour

A software package providing access control for PCs. The system provides protection in three areas: boot protection, program authorisation and access control. The boot protection facility gives you the option of allowing a machine to be booted only from its hard disk. If boot protection is turned on and the machine is booted from a floppy disk, the hard disk will appear not to exist and none of the programs or data stored on it can be accessed.

The program authorisation feature lets you specify which programs can

be run. There is no facility to allow specified users to access specified programs - a program is either authorised for use or it is not. A password is required to add or remove authorisation.

The access control facility adds a password to the computer, and this will be requested each time the machine is booted. The user has three opportunities to enter the correct password, otherwise the machine re-boots.

PC-Armour provides no encryption facilities. Because all software-based protection schemes can be broken, the security offered by PC-Armour is far from total. However it acts as a serious deterrent and hindrance to a casual hacker and is at least robust enough to be unbreakable by the common disk-fixing programs such as Norton. This is not true of all software-based protection systems.

PC-Armour is distributed and produced by S&S International, UK. Tel +44 442 877877.

Dr Solomon's Anti-Virus Toolkit

The best known and one of the most effective packages for detecting and, if required, automatically eliminating viruses. The toolkit includes both stand-alone and memory-resident virus detectors. There is also a program that lets you "authorise" floppy disks for use in your company, and the PC will refuse to read any disk that has not been so authorised. This can help to lessen the risk of catching a virus from a disk that a user has brought in from home or that has been supplied by a disreputable dealer.

The toolkit can be purchased from most UK software dealers. It is distributed and produced by S&S International, UK. Telephone +44 442 877877.

VIA

VIA is a programming language that lets you write resident programs that install themselves in the PC and monitor system activity. In response to certain predefined events, a VIA program can then initiate an action itself.

For example, a VIA program can watch the keyboard, and store a copy of all keystrokes to an audit trail file. Or, a VIA program could watch the mouse, and generate one of four keystrokes according to the direction in which the mouse was moved. This latter example can be used to add mouse control to any program even if you do not have access to the source code of the program.

VIA is a full-featured programming language with a BASIC-like syntax. No knowledge of assembly language is required, though you need to understand the principles involved in MS-DOS's low-level operation. The product is available in the UK from Loadplan Ltd in London on +44 81 200 7733. It's produced in the US by Portable Computing Systems of Dallas, who can be contacted on +1 214 380 5721.

Loadplan also sells a range of other security products, including authentication devices, virus detectors and access control systems.

Disk Audit

A software auditing package which scans a PC's hard disk(s) and attempts to identify the applications contained on the machine. The database of recognised software is configurable so you can teach it about new packages. There is a screen-full of information that lets you record the type of PC, plus details about its user, along with the details of the applications.

The data is saved in dBASE and/or plain ASCII text format, so that support staff can write the required report generators. There are no reporting facilities built into the package.

Disk Audit is produced by SW19 Software Ltd, and distributed by Total Control Ltd who can be contacted in Hungerford, Berkshire, UK on +44 488 685299.

While Disk Audit is slightly more powerful than SPAudit (as below under Federation Against Software Theft), neither is as powerful or flexible as Fprint/AU.

SMAP And MAPMEM

Two Public Domain utilities that perform the same task, namely that of scanning the PC's memory and listing the names of all memory-resident programs currently installed. You should normally expect to see one or two resident programs on all PCs, such as MOUSE, the mouse driver. However, the presence of programs such as KEYLOG or TRAPPER should arouse suspicion.

If you do not have SMAP or MAPMEM, the MEM command that's part of MS-DOS version 4.00 and above can be used instead. From the MS-DOS prompt, type MEM /DEBUG to see the list of installed programs. However, MAPMEM and SMAP go one better than MEM in that they display the interrupt vectors that the resident program has hooked into. This information allows a programmer to determine which area of

the PC's operation the resident program is interfering with. For example, keyboard, screen, monitor, disk and so on.

Kronos

A different type of backup software for the PC. Kronos works as a resident program. Each time information is changed on a hard disk, Kronos keeps a copy of the changes in a special file. In the event of a data loss, the contents of this file can be "played back", thus restoring the hard disk to any desired point before the data loss.

The special Kronos file can be on the PC's local hard disk, a floppy disk, or any one of a number of supported devices including Bernoulli drives and tape streamers.

The program is available from IQ Ltd in Devon, UK, on +44 822 614477.

Password Coach

A utility for Novell networks which ensures that users choose passwords which cannot easily be guessed by hackers. It's also available for the IBM AS/400 and the Vax.

If a user chooses a password that contains a sequential series of letters, or that consists of a common word, or that has been used before, the system refuses to allow it. If the user persists, the system will assign its own password.

The product is produced by Baseline Software in California, USA, which may be contacted on +1 415 332 7763.

TIMELOCK

A public domain program by Robert Schifreen that prohibits the use of commands during certain hours of the day. The program is available on UK bulletin boards, including Cix.

TIMELOCK splits a week into its 168 individual hours, and a program can be enabled or disabled for any one or more of these hours. For example, a game program could be disabled during all hours apart from weekday lunchtimes and weekends.

The program is far from totally secure, but provides a useful first-level of protection.

PC Crypto

Although there are restrictions on taking DES encryption programs out of the US, programs written in the UK can be safely used here without the risk of Customs and Excise breaking down your door.

One such supplier of a DES encryption program is S&S, UK, on +44 442 877877, with their PC Crypto utility. There are others, including Public Domain and Shareware offerings.

WPHD

A Public Domain utility that write-protects one or more hard disks. Any program attempting to save data to the hard disk will return an error message claiming that the disk cannot be written to. This is a purely software solution so it is crackable with effort. It is also a heavy-handed way of going about protection, but it's useful to temporarily disable a hard disk while trying out suspect programs for the first time. Ideally, suspect programs should not be tried for the first time on a machine whose hard disk is valuable enough to warrant any protection at all, but there are bound to be times when this is unavoidable.

Services

There are many security-related services. Some provide consultancy or programming services while others will attempt to recover data from damaged disks.

Office Of The Data Protection Registrar

The office which deals with registrations under the Data Protection Act. The office also handles enquiries about whether registration is required, and initiates prosecutions against non-registered users of personal data. The Office also publishes a regular newsletter giving advice on matters related to the Act.

Springfield House, Water Lane, Wilmslow, Cheshire, SK9 5AX, UK. Telephone +44 625 535777.

Microft Technology

Microft provides security consultancy, and also sells a range of PC security devices. Included in its range is MenuGen, a password-pro-

tected access control system for MS-DOS machines which allows the supervisor to control access to files and directories at a per-user level.

Among the company's other products is D-Lock, which prevents access to a hard disk, and S-Lock, which is a password-protected screen blanker.

Microft is based in Kew, UK, and can be contacted on +44 81 948 8255.

PC and LAN Disaster Recovery

Manchester-based Xenon is just one company providing disaster recovery services for PC and LAN users. In the event of a theft or fire at your premises, Xenon will install one or more PCs in your office or, if necessary, in a portable building outside.

The company can provide computers, network links, modems and software, and operate a UK-wide service. Details on +44 61 434 6133.

Temporary Fire Protection

RSM is a company which specialises in identifying fire-related risks to corporate information. The company is also involved in specifying and installing solutions. Among RSM's range of products is "interim information security", which provides short-term fire protection during vulnerable periods such as an office relocation or decoration, electrical installations, building works and so on. RSM is based in Maldon, Essex, UK, and may be contacted on +44 621 858410.

Dr Solomon's Data Recovery Service

The UK's best-known data recovery service is from S&S International. The company claims a 90% success rate in recovering data from hard disks, floppy disks and tape cartridges and no fee is payable if the data proves unrecoverable.

If you lose your only copy of a crucial disk, tape or file it is well worth speaking to S&S before attempting any action yourself, as a single slip-up could mean the difference between a professional being able to recover the information and the data being lost forever. S&S are on +44 442 877877.

The Federation Against Software Theft

This group, known as FAST, was set up to educate business users of software in the correct use of programs and operating systems. The

Federation provides consultancy, legal advice, plus posters and stickers for employees. It has also produced SPAudit, a software auditing program that analyses a PC's hard disk and attempts to produce a list of all the applications installed on that machine.

Although SPAudit is free of charge, the functionality is extremely limited. There are no reporting facilities - the data is simply placed in a text file for you to examine with a word processor - and the only way to combine a number of analyses to produce a company-wide audit is to draw it up by hand.

FAST can be contacted on +44 628 660377. The company's address is 2 Lake End Court, Taplow, Maidenhead, Berks SL6 OJQ, UK.

Cix

The Compulink Information Exchange, normally known as Cix, is a dial-up bulletin board run as a commercial enterprise. It currently boasts around 8,000 paid-up subscribers and costs approximately £20 to join and £3 per hour to use.

The benefit of Cix over all other bulletin boards in the UK is that it is inhabited by literally thousands of the UK's most knowledgeable PC users. These include journalists, programmers, support staff in multi-national companies and so on. All areas of expertise are covered.

The system is geared to the posting of publicly-accessible messages, though private mail and file transfers are supported. It's the sort of system where you can ask "does anyone know where I can get a product to do such-and-such" and receive at least half a dozen useful replies within three or four hours.

If your job involves supporting or purchasing PCs, a subscription to Cix is essential as you can tap into real users' experiences instead of having to rely on sales brochures.

The Cix office is on +44 81 390 8446. The author of this Guide appears on the system under the name "hex" and is to be found lurking mainly in the PC and MS.DOS (sic) conferences.

Books And Guides

During the preparation of this Guide I read through literally dozens of books that claimed to offer practical advice on data protection and security. Much of the information they contained was, at best, incorrect

and, at worst, dangerously misleading. One, for instance, stated that all add-in cards for performing DES data encryption have recently been taken off the market because they could easily be cracked with the Norton Utilities. Some of the better information sources are listed below and can be recommended as useful background reading. Omission from this list does not imply negative criticism of the book - I may simply not know of its existence.

The DTI Security Awareness Pack

A folder of information, produced for the UK's Department of Trade and Industry by the National Computing Centre. It contains a series of fact sheets which provide background information on such topics as legal requirements, backup, risk analysis, network security, fire protection and viruses. The Pack also includes a selection of case studies that illustrate how real problems were solved. The solutions consist mainly of resorting lost data from backups, though; there is little to be learned from reading them. The Pack is available free of charge from the NCC. Telephone +44 61 228 6333.

Datatheft

An excellent book by Peter Sommer, a.k.a. Hugo Cornwall, the author of the hugely successful Hacker's Handbook. The book contains around 400 pages that cover all aspects of computer security including risk analysis, how and where to build a computer room and more. The book is designed to be read from start to finish, and is heavy going if you are concerned primarily with PCs. For a general grounding in all aspects of computer security it is highly recommended.

ISBN: 0 7493 0217 8. Published in the UK by Mandarin Paperbacks.

Security Management Today

A monthly magazine dealing with all issues of security management, including fire safety, closed circuit TV surveillance and street lighting as well as computer security. Published by Blenheim IFSEC Ltd. Telephone +44 81 868 4466.

Virus Bulletin

An excellent, high-quality monthly newsletter covering all aspects of virus detection and advice on how to keep them out of your computers. Subscribers can also send suspected viruses to the newsletter's specialists who will provide confidential advice and analysis.

Virus Bulletin is published by Sophos Ltd, who are on +44 235 555139. Sophos also provide consultancy, training seminars, videos and software utilities to aid in preventing and detecting viruses. The company's technical director, Dr Jan Hruska, is a respected authority on viruses and how to prevent them affecting your computers.

The Legal Environment Of Computing

An excellent book by Peter Knight and James Fitzsimons that covers computing from a legal point of view. Much information in copyright is included, with lots of case histories to show how English law has been applied to real computer-related problems.

The latter half of the book includes sample contracts for software usage licences, software and hardware maintenance agreements, equipment loans, software development, assignment of copyright, confidentiality and non-disclosure, service level agreements and more. It's well worth the £17.45 cover price. The book is published by Addison Wesley (1990).

The ISBN is 0-201-41701-4.

Virus News International

A monthly newsletter comprising printed virus-related documentation and advice, an anti-virus program with monthly updates on disk, and a fax containing details of all new viruses as they are discovered. An annual subscription costs £195.

VNI is published by S&S International, on +44 442 877877.

Datawatch

This is the quarterly newsletter of the Electronic Data Processing Auditors' Association and is an excellent read for anyone involved in PC security and software auditing. Recent topics have included case studies on how consultants went about the process of planning and implementing a software audit, including details of how various problems along the way were solved as they arose.

The EDPAA (UK) can be contacted on +44 71 489 9000.

Privacy Laws and Business

A quarterly newsletter which "monitors data protection legislation, bills,

legal and administrative decisions worldwide and their impact on company operations".

An annual subscription costs £220. Details can be obtained from the publisher, Stewart Dresner, on +44 81 866 8641.

Data Protection News

A newsletter produced by the Information Protection consultants at Hoskyns plc and made available to clients. It is published quarterly and each issue runs to 20 pages. Topics are not limited to PC security, but cover everything under the umbrella of data protection. A recent article highlighted the widespread misuse of the Police National Computer to trace the movements of cars.

Hoskyns , UK, can be contacted on +44 71 917 4794.

Elsevier Advanced Technology Publications

Elsevier publishes several reports, guides and monthly newsletters concerning all aspects of computer security. Currently available titles include "Computers And Security", "Computer Fraud And Security Bulletin", "Computer Law And Security Report", "Computer Abuse Investigator", "Effective Information Security Management", "The Survivor's Guide To IT Centre Design".

Also available is "The PC Security Guide" which contains technical evaluations of many security products designed for PCs, and the company runs a number of courses for security staff.

256 Banbury Road, Oxford, OX2 7DH, UK. Telephone +44 865 512242.

Index