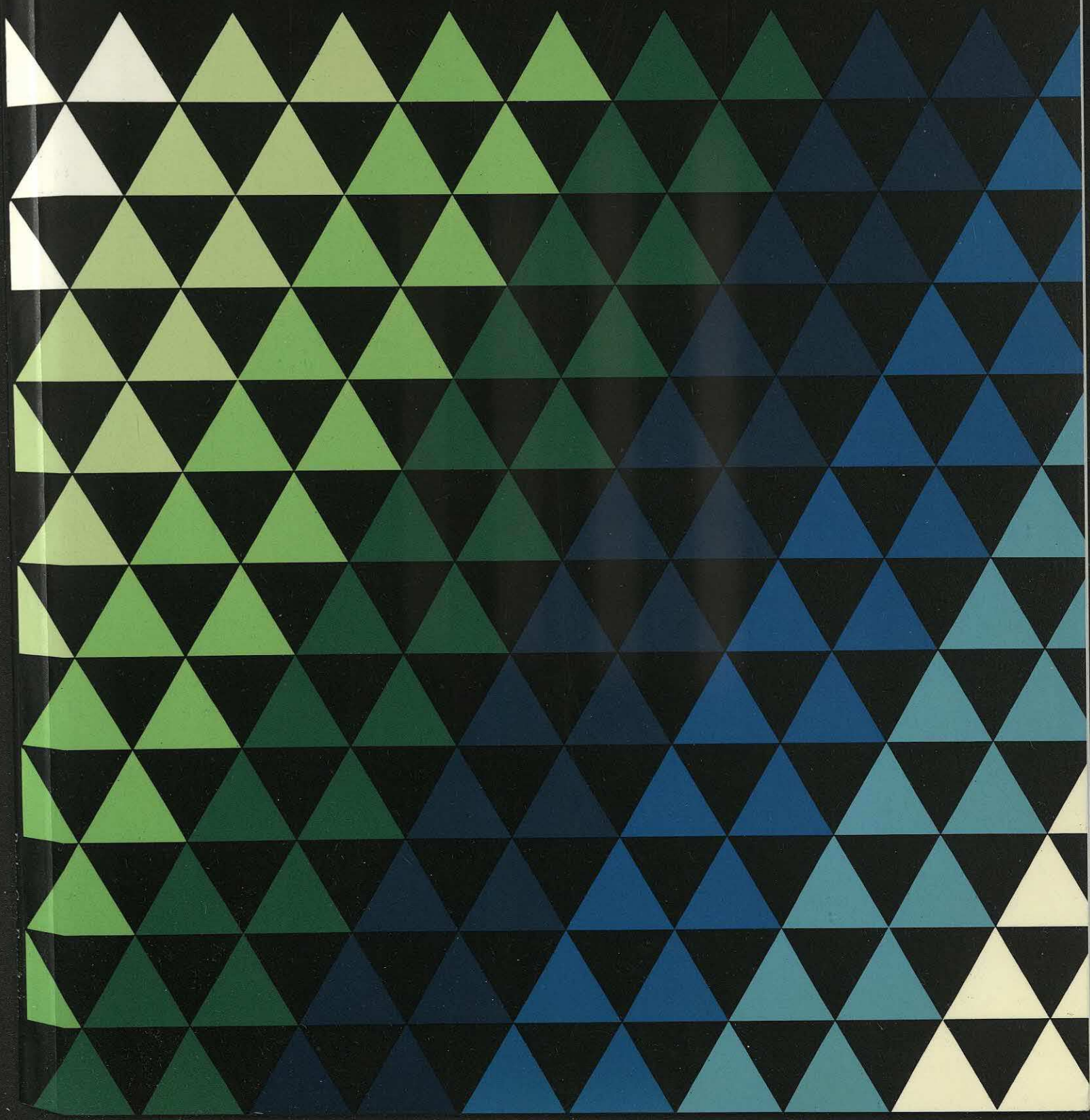
Threats to Computer Systems

BUTLER COX FOUNDATION

Research Report 51, May 1986



Threats to Computer Systems

BUTLER COX FOUNDATION

Research Report 51, May 1986

Published by Butler Cox & Partners Limited
Butler Cox House
12 Bloomsbury Square
London WC1A 2LL
England

Availability of reports and report summaries
Foundation reports are available only to members of the Butler Cox Foundation. Members receive three copies of each report upon publication; additional copies and copies of earlier reports may be purchased from Butler Cox. Reprints of the summary of research findings for each report are available free of charge.

Butler Cox & Partners Limited

LONDON
AMSTERDAM NEW YORK PARIS

Threats to Computer Systems

BUTLER COX FOUNDATION

Research Report 51, May 1986

Contents

	Summary of research findings	v
1	**Unauthorised access to data**	1
	Hacking	1
	Listening to deliberate electromagnetic broadcasts	4
	Listening to inadvertent electromagnetic broadcasts	4
	Wiretapping	6
	Summary	6
2	**Computer fraud**	7
	Losses from computer fraud	7
	Perpetrators of computer fraud	8
	Methods used to defraud computer systems	9
	Defences against computer fraud	12
3	**Threats from sabotage**	14
	Violence	15
	Theft	15
	Data corruption	16
	Jamming	16
	Logic bombs	17
4	**Misuse of computer resources**	18
	Legal and contractual restrictions	18
	Use of resources for private work	19
5	**Reducing the threats to computer systems**	21
	Inform senior management of the risks being run	21
	Increase staff awareness of security	21
	Install appropriate defence measures	21
	Appendices	
1	**Methods used by hackers**	25
2	**Common faults in systems security**	28
3	**Encryption methods**	30
	Annotated bibliography	32

BUTLER COX FOUNDATION

Threats to Computer Systems

BUTLER COX FOUNDATION

Research Report 51, May 1986

Summary of research findings

The use of computers is now growing as never before, and this growth is likely to continue for the foreseeable future. As a result, individuals and organisations are becoming much more dependent on the accurate operation of their computer systems. In the developed countries, the majority of high-value financial transactions are already carried on electronic funds transfer systems, and new systems are being developed for the much larger number of smaller transactions in the retail and wholesale trades.

Organisations have always made provision in systems design and operation for accidents and errors, and have provided a means for limiting the damage that they can do. Users have also been aware that a single major accident could destroy a whole computer centre and have made some plans for recovering from such disasters. Even so, few organisations have comprehensive disaster plans.

Recently, organisations have realised that deliberate human acts may pose threats to their computer systems. Unscrupulous people may extract confidential data, malicious people may damage systems, and criminal people may steal money and other assets with the assistance of computers.

These risks have been increased by the spread of timesharing, end-user computing, microcomputers, and electronic interbusiness communications. Timesharing has spread, providing many more people with the use of computers. End-user computing has put more people in direct contact with computer systems, bypassing the controls of the systems department. Microcomputers have consolidated both trends, and provide highly portable data storage. Electronic interbusiness communications give people who are not even employees, and thus not subject to management discipline, access to the organisation's systems.

Most standard textbooks instruct the information systems manager faced with these threats to perform a formal risk analysis and to allocate resources to security measures according to its results. This is a difficult task for a manager who lacks experience in assessing the various threats to his systems. It is particularly difficult in the case of deliberate attacks because:

- Reliable statistics about the incidence of the various threats to computer systems are rarely available.
- The defence measures adopted may work only for a limited time. The person causing a threat will adapt his or her behaviour to bypass the known defences, exploiting any loopholes that remain.

This report therefore focuses on the threats to computer systems posed by deliberate actions, and the defences that may be used to combat the threats. The report does not discuss risk analysis methodologies because these have been the subject of many books and articles. Instead we aim to provide the information systems manager with a perspective on the threats that are posed, the losses that they can cause, and the possible defences.

We have divided the risks into four categories — unauthorised access to data, fraud, sabotage, and misuse of computer systems — each of which is the subject of one chapter of this report. The final chapter provides guidelines for reducing the threats to computer systems.

In summary, the guidelines show that organisations can make their computer systems much more secure, both physically and logically, by adopting certain basic good security practices. Most of the reported cases of penetration by hackers and of computer fraud would have been prevented by very simple management practices. The appropriate defences are detailed in the body of the report.

Summary of research findings

RESEARCH METHOD

The research for this report was carried out during the second half of 1985 and early 1986 and was led by David Flint, research manager for the Butler Cox Foundation. He was assisted by Roberto Sasso, a consultant with Butler Cox in London, Didier Goy, from Butler Cox's Paris office, John Derks from Butler Cox in the Netherlands, and Statskonsult, Butler Cox's agents in Scandinavia.

The members' responses to the scope document showed considerable differences in the level of concern and the degree of sophistication in security matters. With the exception of Sweden, the responses showed a surprisingly low level of experience of risk analysis, even though this technique has been the subject of a great deal of academic attention and is widely recommended by security experts. In Sweden there is extensive experience of Security by Analysis, a methodology sponsored by the Swedish Vulnerability Board.

Because risk analysis is a complex technical subject with only limited application experience, we decided to concentrate instead on the risks that form the subject of any risk analysis. Guided by members' responses, we focused on the 'new' risks associated with personal computers, networks, and business computing.

Our research included a comprehensive literature search, and an annotated bibliography is included at the end of the report. We also met with organisations that had suffered attacks on their computer systems and with computer suppliers and experts in computer security.

Chapter 1

Unauthorised access to data

All organisations use their computer systems to store data that are vital to the efficient functioning of the business, and unauthorised access to this data (by people within the organisation or by outsiders) can have grave consequences. The severity of these consequences may range from embarrassment to loss of trade secrets or market advantage, and even to threats to health and life in the case of medical research data. The organisation may also be prosecuted if it fails to prevent unauthorised access to particular types of data. (Chapter 4 describes the legal requirements for ensuring that data are secure.)

Some organisations regard all of their data as confidential. However, in most organisations unauthorised access to most of the data would cause little more than minor embarrassment. In most cases, there is only a limited amount of genuinely sensitive data, which usually falls into one of seven categories:

- Personal data is sensitive because it may include information that the individual would not wish to be generally known. Furthermore, most developed countries now have laws governing the collection, storage, and use of such data.
- Research data is sensitive, as it may lead to improvements in products or to new products or may reveal previously unknown side effects of current products or processes.
- In a competitive situation, bid data (price and terms, qualifications, method to be used, etc.) may be highly sensitive.
- Trading data (quantities and prices of goods that are traded) may be sensitive either because the facts would cause unfavourable comment or because knowledge of the price would affect the behaviour of competitors.
- Fault data can also be sensitive because competitors can sometimes gain an advantage by knowing which products or services are most troublesome.
- Accounting data is sensitive, particularly prior to the announcement of results.
- Executive correspondence and board minutes may be sensitive, especially where they deal with plans for developing the business.

Regardless of whether data are stored in conventional media (paper, microfilm, index cards, etc.) or in computer systems, the major threat of unauthorised access comes from the organisation's own employees. In this report, however, we are concerned mainly with external threats to data stored in computer systems. Nevertheless, the threats from your own staff should be kept in mind when considering security measures. There is little point in spending large sums of money to encrypt data that could be obtained by buying a few drinks for a clerk.

Unauthorised access to computer systems by people from outside the organisation may be gained in four main ways:

- By hacking: hackers use their skill to 'fool' the system into believing they are genuine, authorised users.
- By listening to deliberate electromagnetic broadcasts.
- By listening to inadvertent electromagnetic broadcasts.
- By wiretapping.

We now discuss each of these threats in turn.

HACKING

In recent years, considerable media attention has been given to the practice of hacking. Films such as *WarGames* and *Les Spécialistes* and the prosecution of some hackers have drawn attention to the problem. The publication of books such as *The Hacker's Handbook* and *Out of the Inner Circle* and notorious penetrations such as that of British Telecom's Telecom Gold messaging system and of the Rijksinstitut voor Volksgezandheid en Milieuhygiene's systems (Dutch Government's Institute for Health and Environment) have revealed both the scale and sophistication of hacking. And the

penetration of Prince Philip's Prestel mailbox received considerable publicity. The list of organisations whose systems have now been penetrated by hackers ranges from department stores to research institutions to the United States Department of Defense. Access has been gained via all types of networks (public telephone, Telenet, videotex, public electronic mail, and so forth).

Hacking is not a new problem, however. In 1974, a pupil at Westminster School, London, broke the security of a major timesharing service by reading passwords from the line buffers used by the operating system. In this way he obtained the password of a highly privileged user, which he could have used to destroy files, change other peoples' passwords, and alter bills for computer services.

PROFILE OF A HACKER

The typical hacker is a bright teenage boy with a home computer and a modem. Today, the equipment need cost only a few hundred dollars, and costs will continue to fall. The telephone bills can be high, however. Speaking on a radio programme in autumn 1985, an anonymous hacker said that most dedicated hackers in the United Kingdom have telephone bills of £500 per quarter, whilst even the occasional hacker may spend £200. In Europe, hacking is clearly inhibited by this expense.

As a consequence, most hackers are found in the United States, where free local calls, ubiquitous data networks, and the custom of billing the cost of incoming calls to the host make hacking easy and inexpensive. Nevertheless, hackers can be found in all the advanced countries, and we expect their numbers to increase. Alhough it is difficult to estimate accurately, we believe there are, for instance, a few hundred active hackers in the United Kingdom, of whom only a dozen or so employ the most sophisticated methods.

The typical hacker is neither criminal nor malicious. He is motivated by a consuming interest in computers and is, as a person, rather similar to some systems programmers. His energy and dedication are considerable, and some hackers are prepared to spend many months attempting to penetrate a single system.

Hackers communicate with each other via primitive electronic mail systems called bulletin boards, using them to share information and to coordinate attacks on specific systems. In many cases, hackers mounting a coordinated attack on a system have not met personally and are known to one another only by pseudonyms.

Bulletin boards are usually based on microcomputers with hard discs and most often are not principally concerned with hacking. Sometimes, a bulletin board is concealed in a commercial multi-access system. This type of bulletin board is known as a 'cuckoo's nest'. By the end of 1985, there were at least 30 bulletin boards in the Netherlands, 150 in the United Kingdom, and thousands in the United States.

Some hackers are extremely resourceful. Appendix 1 describes some of the methods actually used by hackers. They range from the very simple (try all possible one-character passwords) to the very sophisticated (use of a 'Trojan Horse' program to obtain secure passwords). Some hackers are also very well informed. They even obtain (and read) suppliers' manuals on the internal workings of operating systems.

For most organisations, the greatest hacking threat comes from their own timesharing users and data processing staff. These people already have access to the computers and to lists of account names, and they have programming skills, so they are ideally placed to launch an attack on the confidential parts of systems. In one case reported to us, a programmer was able to tell managers the results of their annual salary reviews before they had learned them officially.

THE DAMAGE CAUSED BY HACKERS

Most hackers interfere little with the systems they penetrate. They obtain their satisfaction from the intellectual challenge of circumventing a system's password or security procedures. A minority of hackers — known as crashers — get their satisfaction from crashing systems. In 1985, such a hacker brought down a large minicomputer system operated by the United States Geological Survey in Reston, Virginia, by changing a job queue. Though no data were lost, the recovery procedures were expensive. In another case, crashers were estimated to have caused damage worth $100,000 to a computer company in California.

A few hackers are also thieves, however. Again in 1985, teenagers, coordinating their attack via bulletin boards, hacked into TRW's computer systems and ordered thousands of dollars' worth of equipment. It took the police 130 hours of online work to identify them. In yet another case, this time in the Netherlands, a hacker damaged part of a database and threatened further damage unless he was paid five million guilders.

There is little direct evidence to suggest that hacking is being used for industrial espionage purposes

– but it could be. The potential is illustrated by a case where an industrial spy was able to read oil companies' geological data stored at a computer bureau. He did this by asking for a scratch tape, and then read the previous users' data from it.

Hackers may sometimes alter data in the systems they penetrate. After a hospital computer was penetrated by hackers it was only the vigilance of a nurse that prevented the wrong treatment being given to a cancer patient.

In practice, most hackers are a nuisance rather than a real threat. The nuisance may, however, be considerable, and may lead to substantial expense. The United States Department of Agriculture has admitted to spending over $50,000 to track down one hacker, for example, and this is probably a considerable underestimate.

A further risk of having hackers on your system is that they may reveal passwords and access procedures to people who are malicious or criminal. We know of several cases where crashers (hackers who enjoy crashing systems) found out about access numbers and passwords via bulletin boards. We know of no cases where criminals or spies have done this, but that, of course, does not prove that it has not happened. In our view, penetration by hackers is a real threat to any system containing either confidential data or applications that could be interfered with.

THE DEFENCES AGAINST HACKING

Most hackers are able to gain entry because of poor password management. The following guidelines should keep out most hackers:

- All passwords should be at least six characters long, with alphanumeric characters and some punctuation marks being allowed.
- Proper names, account numbers, telephone numbers, car registration numbers, and 'obvious' passwords such as 'PASSWORD' and 'SECRET', should not to be used.
- Passwords should be changed at least twice a year.
- Passwords should be kept secret.
- Passwords should not be shared by different users.
- After three incorrect attempts to input a password, immediate warnings should be issued to the organisation's systems security staff. Ideally, the system should continue to accept further log-on attempts, but should be programmed to reject even the valid password so that there is a better chance of tracing the hacker.
- To reduce the possibility of an unattended terminal being used for hacking purposes, users should be logged-off (after a warning message) if the keyboard has not been used for a predetermined time. This time can vary, depending on the location of a particular terminal.

These guidelines will not prevent the most dedicated hackers, using the more sophisticated methods described in Appendix 1, from entering your system. Additional defence can be obtained by getting your network security staff to seek out hacker bulletin boards and check for references to your own systems. It may even be worthwhile establishing your own hacker bulletin boards, either on your own systems or separately. One large network operator has a security officer who has gained the confidence of hackers and who can thus locate their private files and messages. In this way, the network operator has been able to thwart the attempts of hackers to break into its system. Another user is building a 'maze' to divert the attention of hackers who penetrate his videotex system.

In 1983 Charles Symons and James A Schweitzer of Xerox published a specification for software to support the minimum security regime Xerox thought was necessary for a multi-access commercial system. Xerox called this the Automated Logical Access Control Standard (ALACS), and have sought, without success so far, to interest the official standards bodies. ALACS supports a rather higher degree of security than that described above, and it should exclude in most cases both coordinated attacks by hackers and ordinary attacks by criminals.

In our view, however, future security systems will rely on a portable 'gadget' (possibly a smartcard) and a remembered secret password. The password will be used to activate the gadget. When the connection has been made to a host computer, the host will issue, as a challenge, a randomly selected number or word. The gadget will transform this challenge into a correct response, which the host will recognise, and which will be different for every authorised user. The gadget will also remember the time of the last session with the computer and will compare this with the computer's own record to ensure that no intruder has impersonated this user since he or she was last logged on. (Delegates on the Butler Cox Foundation 1983 Study Tour of California saw demonstrations of such a gadget at Sytek. The United States Government, for national security reasons, has banned the export of this equipment.)

We are also aware of research aimed at confirming a user's identity from the way in which he or she types. Eventually, this form of user-authentication

technique might make gadgetry unnecessary for some purposes.

The hacker's challenge is to gain logical access to a computer system. But logical access control is worth little unless the computer is physically secure. Most personal computers and office systems are not kept securely, and discs and diskettes can easily be removed. Protection against theft of information on removable media requires either securing the media when not in use or encrypting stored data. In principle, the latter is safer and more convenient, but it is not always possible. Encryption may also be used on larger computers if the data is particularly confidential or the security is otherwise weak.

LISTENING TO DELIBERATE ELECTROMAGNETIC BROADCASTS

Under some circumstances, confidential data may be broadcast as electromagnetic signals, and it may be possible to recover the data by listening to these signals. Most speech, television, and data broadcasting systems in current use transmit signals using standard ways of representing the data, usually at easily determined fixed frequencies. This is true for many military as well as civilian systems. Private radio links, cellular radio, and satellite teleconferences are therefore completely insecure. Terrestrial microwave systems are largely secure, however, because they require point-to-point communication.

Private radio links and public cellular radio systems often operate at frequencies that can be received on household radios. Other systems require the use of commercially available all-band equipment to recover the signal. The equipment is easy enough to operate, but considerable patience may be required before anything interesting is found.

Until recently, there has been little of interest to be gleaned from the airwaves except, perhaps, police messages. In September 1985, however, the magazine *New Scientist* drew attention to the ease with which the cellular radio transmissions now being widely used for mobile telephony could be received. The freedom with which callers spoke made it clear that they thought the system provided privacy. It does not. Furthermore, scanning receivers specially designed to find cellular radio transmissions have now become available in Europe.

In exceptional circumstances, extremely sensitive information may be captured from the airwaves. During the *Achille Lauro* hostage crisis in 1985 President Reagan used an unprotected radio link to discuss interception of an Egypt Air airliner. (The scrambler on his plane was broken.) The conversation was overheard by a radio ham. If the ham had telephoned the Egyptian Embassy, the consequences might have been quite dramatic.

Satellite broadcasts are also quite easy to receive, and some television hams in the United States regularly listen to company teleconferences. To receive data-and-voice calls requires the demultiplexing of a complex high-speed bit stream, but standard units are available to achieve this. It seems likely that governments tap some of this traffic routinely, and it is quite possible that industrial spies do so as well.

The interception of public microwave transmissions is probably beyond the capability of anyone except a major government agency. There have been reports that the Soviet Embassy in the United States has been routinely capturing calls to certain telephone numbers in Washington DC, by analysing leakage from a local microwave system. The security of private microwave transmissions depends largely on the exact location of the equipment at each end of the link.

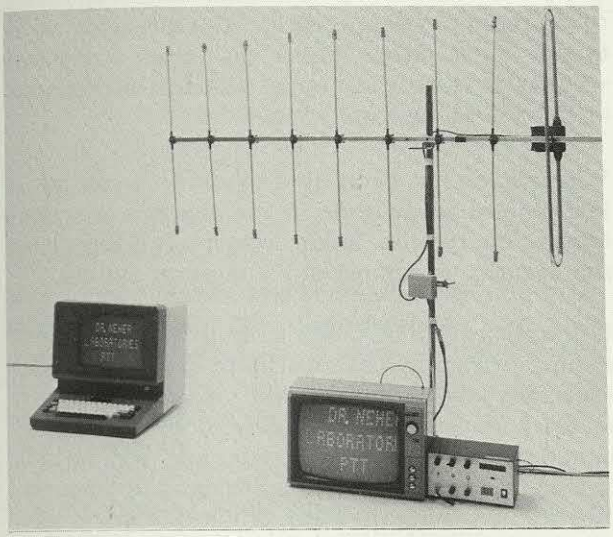
Radio broadcasts may be protected against unauthorised access by the use of scramblers or encryptors. However, analogue scramblers have only limited effectiveness — as much as 90 per cent of the speech may still be intelligible to a trained listener. To safeguard all calls on public radio telephone systems would require scrambling or encrypting equipment to be built into mobile phones. Apart from the cost, managing the encryption keys would present formidable problems.

The same techniques may also be used to protect satellite transmissions. Some American satellite television services now scramble their signals, not for secrecy, but to ensure that receiving CATV and local TV stations pay their bills.

LISTENING TO INADVERTENT ELECTROMAGNETIC BROADCASTS

All electronic equipment emits electromagnetic radiation as a by-product of its use, although the amplitude and complexity of the signals vary greatly. During 1985 this phenomenon attracted considerable public attention in the United Kingdom when a television programme showed that private correspondence on a word processor could be read from mobile equipment parked in an adjacent street. This programme was based on the work of Wim van Eck at the Dutch PTT's Dr Neher Laboratories. The equipment used is shown in Figure 1.1.

Figure 1.1 Equipment used to listen to the radiation produced by a CRT screen



(Photograph reproduced by kind permission of the Dutch PTT's Dr Neher Laboratories)

According to Dr van Eck, screen displays can in most cases be reconstructed at distances of up to 1 kilometre, and up to 8 kilometres for some particularly 'noisy' terminals.

We have seen a simple do-it-yourself piece of electronic equipment that is able to reproduce the picture on a CRT screen at distances up to 50 metres in an electrically noisy environment. The equipment costs about $200 and requires only technician-level skills to build. It is compact and portable (the largest component is the aerial), and it is quite straightforward to operate. A schematic representation of the equipment is shown in Figure 1.2.

Keyboards also produce signals that can be detected by the same methods. The signals are, at least in some cases, characteristic of the key pressed, allowing the sequence of key depressions to be identified by careful study of a recording. We have no doubt that fairly simple electronic circuits could now be built to automate this identification.

The implication is that personal computers, terminals, and other electronic machines (possibly including banking terminals) are vulnerable to radiation eavesdropping by people with very modest means. Technically, it is possible to build much more sophisticated eavesdropping equipment that would make it even easier to listen to, and interpret, the inadvertent radiation emitted by these types of electronic machines. Some possible technical enhancements are:

— Additional tuning circuits.

— A more directional aerial.

— Automatic screen synchronisation.

— The addition of a video recorder.

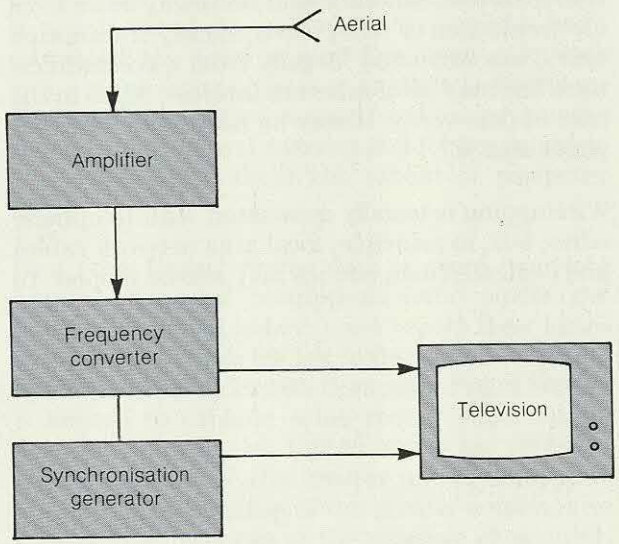
— Enhancement of the signal by processing it on a personal computer.

— The use of OCR techniques to reconstruct the characters on the screen.

We believe that judicious application of these means, and considerable experimentation, could increase the range of the equipment to at least 500 metres, even in a noisy environment. If this proves to be possible, this form of unauthorised access could be used against equipment in large factory and office sites.

Although reliable information is hard to come by, we understand that at least one such receiving system has already been discovered under suspicious circumstances. It would be surprising if others were not in use.

Figure 1.2 Schematic representation of do-it-yourself CRT eavesdropping equipment



It is not easy to suggest defences against radiation eavesdropping. Electrical screening does work, but only if installed by experts, and it is expensive and often inconvenient for users of computer equipment. The use of non-CRT displays, possibly based on plasma displays or LEDs, is fairly effective, however, and equipment with very low radiation levels ('Tempest-protected') is commercially available in some countries. These nonconventional types of equipment are expensive, however, and less expensive technical solutions are being studied by several suppliers.

Perhaps the easiest and quickest defence against radiation eavesdropping would be to install a few inexpensive games machines in sensitive areas. The intensity of their signals will tend to 'dazzle' a receiver.

The signals that are radiated from a terminal are also transmitted over mains wiring. Anyone with access to the same mains circuit and reasonably adjacent to a particular terminal may well be able to recover screen images from the mains. This method of eavesdropping might, in some cases, be attractive to industrial spies.

Again, it is not easy to suggest specific defences. Filtering might work, but jamming is probably an easier option.

WIRETAPPING

Although we do not doubt that wiretapping is sometimes used for criminal purposes, we believe that criminal wiretaps are usually aimed at telephone conversations rather than data communications. Only a very small minority of professional criminals would be able to extract useful information from encoded data, and not many more from electronic mail or other electronically transmitted text. Data extracted illegally from a communications line may be of inherent interest, or, as in the case of passwords, it may be needed as part of a wider attack.

Wiretapping is usually associated with telephone wires, but, in principle, local area network cables and dedicated data circuits may also be tapped. To tap landlines and local area network cables requires physical access to the lines. This presents difficulties even where no special steps have been taken to maintain physical security. The intending wiretapper must either break his target's physical security or identify the target's lines in an exchange or in an underground tunnel.

Wiretapping has been used to obtain secret information and passwords. In the absence of scrambling or encryption, it can completely compromise the security of almost any computer system.

Wiretapping can be made more difficult by maintaining strict physical security over premises, and especially over conduits and switchrooms. Such security measures are unlikely to defeat a determined opponent, however, who may well be able to gain access by posing as a journalist or labourer, or even by joining the staff. If wiretapping is seen as a serious threat, then care must be taken to ensure that security does not depend on passwords that are transmitted in plain text, for example, before encryption takes place.

SUMMARY

In this chapter we have described the most common methods for gaining unauthorised access to a computer system. Many hackers will be satisfied just with gaining entry and leaving their 'electronic visiting card' in the system. Others, however, will see the means of gaining unauthorised access as a first step towards perpetrating some form of computer-based crime.

Chapter 2

Computer fraud

Many organisations, and particularly the financial management of the organisations, are now dependent on computer systems. Organisations may therefore be robbed or defrauded through their systems. Such theft and fraud is the subject of this chapter.

Computer-based theft and fraud can result in spectacular crimes. In the Equity Funding case, for example, an IBM System 3 computer was used to create fictitious life insurance policies that were then reinsured with other companies. In the end, two-thirds of all the company's policies were fictitious. An IBM mainframe was also used to mislead auditors. When Equity Funding collapsed in 1973, reinsurers and shareholders lost some $1.5 billion. Saxon Industries went from the Fortune 500 to bankruptcy in 1982 through a similar process.

Auditors and criminal justice systems have failed to keep up with the changes in the opportunities for, and consequences of, computer-based crime. Auditors failed to detect the Equity Funding fraud, and prosecutors have seen some perpetrators of computer fraud escape with ridiculously short sentences.

LOSSES FROM COMPUTER FRAUD

Information about the incidence and extent of computer fraud is extremely confusing and contradictory. Some surveys suggest that it is uncommon and leads to only modest losses. Other evidence, and many experts, suggest that it is very common and leads to substantial losses.

Of 1,262 organisations who responded to surveys by the United Kingdom's Audit Commission in 1981 and 1984, 11 per cent reported a 'computer fraud' within the previous five years. Of these 144 reports, about one-quarter were not actually frauds and did not result in any direct loss. (We classify these cases as 'sabotage' or 'misuse of resources' and discuss them in Chapters 3 and 4, respectively.) The survey identified losses totalling only £1.1 million in 1984 (and £900,000 in 1981) and found an average loss of about £14,000, though the largest loss was over £200,000. Because the survey is voluntary and because it is known that several large frauds were not included, these figures represent a bare minimum.

In France, a sophisticated research exercise carried out by the French organisation ASPAIRO estimated the losses from fraud, disclosure, and sabotage in 1984 to be 1,230 million francs (about $150 million).

But this figure is considerably lower than those quoted by some experts, and is much lower than those quoted for the United States. According to David Dryer of the consultants BIS, for example, the average computer crime in the United States is worth about $1 million; other experts have estimated the total annual loss from computer crime in the United States at as much as $3 billion. There are at least two reasons for the discrepancies between Europe and America and for the considerable uncertainty about the extent of computer fraud.

First, the United States data is more complete because financial institutions (who suffer the largest individual losses) must report their losses in the United States but not in the United Kingdom. Furthermore, the British Computer Fraud Survey is known to exclude some recent major losses. Second, losses in the United States are probably higher because of the greater use of computers and, perhaps, because of the greater emphasis on competitive response at the expense of security.

Nevertheless, there is evidence to suggest that, in Europe, the extent of computer fraud is increasing considerably. Between January and May 1985, insurance premiums in the Netherlands for losses caused by computer fraud rose by 300 per cent.

Reported and estimated computer fraud losses in the United States, the United Kingdom, and France are given in Figure 2.1 overleaf.

There is no doubt that there have been some very large computer frauds and that some very large losses have been sustained. Figure 2.2 describes some of the more notable computer frauds.

Figure 2.1 Reported and estimated annual losses from computer fraud

Country	*Source*	*Losses (millions)*
Reported losses		
United States	Donn Parker (SRI)	$100
United Kingdom	Computer Fraud Survey	£0.9 (1981) £1.1 (1984)
Estimated losses		
France	ASPAIRD	FF1,230*
United Kingdom	*Daily Telegraph*	£500 to £2,500
United States	Donn Parker (SRI)	$3,000
	American Bar Association	$145 to $730

*Includes losses from disclosure and sabotage.

The total loss due to computer fraud is highly uncertain. All that can be said with confidence is that annual losses in Western Europe probably exceed $100 million, and may even be much larger.

Apart from the direct losses, fraud may cause losses of goodwill and market share. A company, especially a financial institution, that sustains a large loss can easily lose the confidence of its customers and shareholders, who may even begin to doubt its viability.

PERPETRATORS OF COMPUTER FRAUD

Most computer frauds are committed by employees, and staff at all levels have been guilty of computer fraud. For example, the perpetrators of 54 frauds reported in the 1984 British Computer Fraud Survey were:

Clerks	26
Clerical supervisors	15
Managers, accountants	7
Professionals	3
Suppliers or claimants	9
Customers or taxpayers	7

(The total is more than 54 because 13 cases involved collusion between people in more than one category.)

Many frauds are committed by quite junior staff and involve the manipulation of computer input — to make excessive payments to claimants, pensioners, or suppliers, for example. Not surprisingly, senior staff make off with larger sums of money.

Unlike bank fraud in general, collusion is common in computer frauds. Usually, a person with access to the computer works with someone who can 'liberate' the money. There may be more than two conspirators — there were 64 in one case. Another difference is that ordinary frauds are committed by people who handle negotiable instruments and cash. In computer fraud cases, the perpetrators are those with access to the computer and a good knowledge of the applications systems, especially of the controls built into the systems.

The increasing use of microcomputers and timesharing systems means that more and more

Figure 2.2 Some notable computer frauds

Cenco
According to the US Securities and Exchange Commission, the data processing manager and 18 staff stole some $40 million from Cenco Inc., a Chicago-based manufacturer of technical products, in 1973 and 1974. Inventory records were altered to show scrapping that had not occurred.

Wells Fargo Bank, Los Angeles
The operations manager stole $21.3 million by the old trick of 'kiting'. Computer use was incidental. The fraud grew over two years and by January 1981 the manager was manipulating at least 26 separate accounts, each requiring a transfer every five days, to conceal the loss. There were several other conspirators. It should be noted that all bank frauds in the United States in 1980 totalled less than $42 million.

Chase Manhattan Bank
In 1980, Chase Manhattan Bank had to write off $20 million in loans that had been fraudulently issued by two staff members, one a vice-president.

Bank of Colombia and Bogota
In August 1984 a team of criminals stole $13 million from this bank, transferring the money through 14 countries "in as many minutes". During the investigation some of those involved fled to West Germany, the chief investigator was murdered, and the Chief of Police was attacked with a bomb.

Security Pacific Bank
In 1978 Stanley Mark Rifkin, employed as a consultant to design Security Pacific Bank's Bankwire system, fraudulently transferred $10.2 million to a Swiss bank account by Fedwire. Rifkin exploited a previously unknown fault in the control system that had not existed in the previous manual system.

Pacific Telephone and Telegraph
By an astute combination of intelligence work, bribery, hacking and theft, Jerry Schneider stole goods worth $1 million from Pacific Telephone and Telegraph in 1971. He was caught when an accomplice betrayed him to police. After serving 40 days in jail, he went into business as a computer security consultant.

Calculator Factory – Vilnius, Lithuania
Between 1975 and 1979, three employees stole 78,584 roubles (over £55,000) from this calculator factory. Sentences ranging from 8 to 15 years were given.

West Somerset District Council
In 1985, a computer manager with West Somerset District Council was jailed for 18 months after stealing £30,000 by computer.

Melbourne ATM network
in 1985, a youth obtained 12 ATM cards in false names and stole money during periods when the network was offline for central batch processing. He faces 400 charges of stealing a total of $A40,000.

people have access to computers and have the skills and confidence to exploit that access. Where microcomputers are used for processing financial transactions or transactions that relate to valuable items (stock control records, for example), new opportunities for fraud arise. The controls associated with microcomputer systems are often inadequate, and it is usually possible for someone with only moderate technical skills to tamper with the system for fraudulent purposes.

Mainframe timesharing systems are, in general, less vulnerable because the technical controls are better. They do, however, provide a challenge to the expert hacker, and several major transaction processing systems have been broken into by hackers.

A small proportion of computer frauds (probably 5 per cent or less) are committed by outsiders without collaborators inside the organisation. The clearest examples are the frauds on automatic teller machines (ATMs) that have recently become prevalent (one such fraud in Melbourne, Australia, was described in Figure 2.2).

The risks of computer fraud by outsiders will increase as more companies provide their customers and business associates with access to their systems. Electronic funds transfer systems have long been tempting targets for criminals because the amounts of money involved are so large (£250 billion per day in the United Kingdom, for example), and their speed of operation facilitates a quick getaway. Electronic funds transfer systems played key roles in the frauds against the Security Pacific Bank and Bank of Colombia and Bogota described in Figure 2.2. In the future, interbusiness networks may encourage such attacks on businesses other than banks.

METHODS USED TO DEFRAUD COMPUTER SYSTEMS

Computer frauds are often opportunistic. They are usually possible only because of defects in the controls or because one person is given too many responsibilities — for example, where the same person is allowed to register a supplier and to authorise payment of an invoice.

Of 60 frauds analysed in the 1984 British Computer Fraud Survey, there were clear deficiencies in the control arrangements in all but seven cases. Indeed, in 16 cases there were two control deficiencies, and in five cases there were three deficiencies. (The 79 deficiencies identified are described in more detail in Figure 2.3.) On the basis of this evidence, it is clear that greater attention to the controls and checks built into computer systems could significantly reduce the incidence of computer frauds.

Figure 2.3 Deficiencies leading to fraud

Deficiency	*Number of incidents*	*Comments*
Weak accounting controls	19	
Inadequate division of responsibility	14	
Poorly controlled logical access	11	Person should not have been able to initiate certain transactions. This category includes, but is not limited to, password problems.
Weak supervisory checks	10	Probably understated.
Inadequate controls on main file update	7	Controls on non-money data.
Poorly controlled physical access	7	Access to computer, input documents, stationery, or terminals.
Defective system interfaces	6	Manual-computer, computer-computer, cash register-computer. Some overlap with accounting controls.
Weak management	2	Probably understated.
Offline ATM operation	2	
Errors by bank	1	
TOTAL	79	

(Source: 1984 Computer Fraud Survey, HMSO)

In the remaining seven cases there was either a breach of trust by an employee, or the fraud could not have been detected by any practical control procedures. In one case, for example, a clerk in a benefits payment office input false information to the claimant payments system. The false input was not detected for 15 months, and nearly $4,000 in unauthorised payments were made.

A variety of methods have been devised for carrying out computer-based fraud. We have classified them into three main types:

— Manipulation of transaction input by employees.

— Interference with files or programs by employees.

— Penetration by outsiders.

MANIPULATION OF TRANSACTION INPUT BY EMPLOYEES

The manipulation of transaction records by employees is the commonest kind of computer fraud. In many cases, however, the use of a com-

puter is incidental. The same methods were used to defraud organisations long before computers were installed.

Of the 60 frauds identified by the 1984 British survey, 58 were carried out by manipulating transaction input. This type of fraud usually fits into one of five patterns:

— Frauds on payment systems.

— Frauds on billing systems.

— Bad stock frauds.

— 'Kiting' frauds.

— Forgery of money transfer orders.

Frauds on payment systems

This type of fraud can be further subdivided into payroll frauds, frauds in which the rights to payment are misrepresented, and frauds that involve payments to nonexistent beneficiaries.

One Foundation member has reported to us a case in which a supervisor stole £64,000 from the organisation during the eight years that he was in charge of a payroll section. The supervisor used several methods, including stealing cash and cheques, subsequently concealed by adjustments to nontaxable gross pay items. The frauds were possible only because the perpetrator had both cash-handling and authorisation responsibilities. The fraud was discovered when the supervisor retired after 32 years' service, and there were balancing problems in connection with a loan/savings club.

In a rather more serious case, a small group of young criminals in the United States robbed the Youth Corps of $2.75 million. The group began their conspiracy in September 1967. One of them was able to become payroll director of the Youth Corps, and the gang then invented large numbers of Corps members. Wage cheques for these nonexistent members were collected by the gang and paid into their own bank accounts. The fraud was discovered only when police found uncashed cheques in an illegally parked car.

A benefit system operated by a local government organisation was used by a clerk to invent a fraud that required rights to payment to be misrepresented. The fraud was operated 11 times over six months, and produced more than $6,500 for him and his friends. The clerk made out spurious claim forms in favour of his friends, forged the signature of the authorising officer, and passed the forms to the payments section. The money paid was then divided between himself and his friends. After leaving the organisation, he continued the fraud by entering the office outside normal hours. He was caught after submitting further fraudulent claims on out-of-date forms.

In 1971, the audit department of a German corporation noticed that an exceptionally high proportion of pensioners appeared to die in January and February. To continue receiving their pensions, the pensioners had to make personal appearances every March. Realising this, a member of the data processing staff was withholding notifications of death from the computer, and changing the receiving bank account number to his own. The death notifications were put through in January and February, leading to the anomalous death rates.

Frauds on billing systems

Frauds on billing systems can take the form of improper authorisation of credits and misappropriation of cash or cheques. Examples of both types are given below.

A clear case of improper authorisation of credits concerned a supervisor, well regarded by his employer, who exploited his position of trust to reduce bills to himself and to his family, and to transfer suspense amounts to the credit of these accounts. After the fraud was detected, it was realised that he had operated the scheme throughout the ten years he had worked for the organisation and that $7,000 had been stolen. The perpetrator was dismissed and prosecuted.

In one interesting case involving misappropriation of cheques, an assistant credit control manager stole $50,000 over 18 months (the whole period of his employment). He only misappropriated cheques from customers with smaller account balances because management focused its attention on the larger accounts. He then concealed the discrepancy by incorrectly ageing the cash received and suppressing the customer's statements. Ultimately, he removed the debt from the accounts by allocating suspense items to the relevant accounts. Interestingly, the fraud was not detected by the banks, who repeatedly credited cheques to accounts other than that specified, sometimes despite an 'account payee only' stamp applied by the drawer.

Bad stock frauds

One of the most spectacular bad stock frauds occurred in South Korea in the 1960s and was committed against the United States Army. According to evidence given to the Senate Committee on Government Operations, a criminal conspiracy (consisting of American Army personnel, South Korean civilians, and members of the South Korean government) stole goods worth more than $10 million per year over a period of years.

The conspirators used the Army's Computer Center at Taegu in South Korea, which was operated by Korean civilians. Each unit of the Army kept its own stock records on the computer, and goods were stolen when they were moved between units. The stock records of the stolen goods were then destroyed, leaving no trace of the goods. The conspirators used the computer systems to manage their activities. These thefts were possible only because the operating personnel understood the systems better than the Army did.

In a more modest case, a financial controller adjusted his company's accounts by $350,000, not for personal gain, but to ensure that the 'actual' results were in line with previous forecasts. In other cases, asset accounts have been adjusted to conceal a fraud in a payment or billing system.

Kiting

The term 'kiting' refers to a long-established method in which money is removed from one account and the loss concealed by continually transferring it between accounts. To avoid detection, the perpetrator must maintain a continuous series of such transfers.

In one well-known case, the chief teller of a New York savings bank stole $1.5 million to finance his compulsive gambling. The thefts continued over three years, ending in 1973. The teller exploited his position of trust and the weaknesses in the bank's computer systems and operating procedures. He began by stealing from his own cash box and then made good the shortages by transferring funds from large, but inactive, accounts. When a customer complained about the resulting deficit, the perpetrator would 'explain' it as a misposting or a computer error, and he would make good the deficit with funds from yet another account. In the end he was manipulating more than fifty accounts. When he was eventually caught, he admitted that the strain of manipulating so many accounts had taken its toll on him. "I started making stupid mistakes. I did not cover my tracks very well." Even so, the frauds came to light only when the police raided his bookmaker and found that he was losing up to $30,000 a day.

An even larger sum was stolen by the operations manager of a Los Angeles bank, who ran a kiting conspiracy with non-employees. The manager started by making a fictitious deposit, then covered this a few days later with a transfer from another account, before the bank's computer reported a shortfall. Building up a chain of such transactions over two years, he had stolen $21.3 million before a clerical error led to an investigation that revealed the fraud.

Usually, it is the sheer pressure of maintaining an ever more complicated chain of fraudulent accounts that leads to the collapse of kiting. Sometimes the perpetrators confess just to put an end to this pressure.

Forgery of money transfer orders

The classic computer fraud involving the forgery of money transfer orders occurred in 1978 when Stanley Mark Rifkin used his knowledge of a bank's electronic funds transfer security system to impersonate a bank officer. As a result, the Security Pacific Bank, Los Angeles, transferred $10.2 million to Rifkin's account in New York. The money was then transferred to Zurich, where Rifkin used it to buy diamonds. He was caught only because he returned to the United States to convert the diamonds into cash. Rifkin was sentenced to eight years in prison. With remission, he was released early, and he now works as a computer security consultant.

INTERFERENCE WITH FILES OR PROGRAMS

Staff in user departments access computers through applications systems, and their use of computers is subject to the controls built into the applications and is likely to be recorded in logs and reports.

Data processing staff, by contrast, often have direct access to computer systems, and they sometimes use their specialised knowledge to interfere with the files and programs. In one case reported to us, data processing staff used Easytrieve to produce reports from a bank's main ledgers. Periodically, they were also asked to adjust these ledgers, again using Easytrieve. The bank did not ask for evidence that the required changes, and only those changes, had been done correctly, nor were there relevant security systems or logs, nor did the internal auditors ever ask to see the relevant authorisations and records.

In 1970, inadequate control procedures of this kind were exploited to steal $137,000 from a small American bank. The operations supervisor used a utility program to manipulate the files during the conversion to a new banking system. Pressure on the data processing department during the conversion meant that proper maintenance procedures were neglected, and the supervisor was repeatedly asked to alter files using this utility. Just before the old system was closed down, he transferred funds from inactive savings accounts to his own accounts and those of four conspirators. These funds were then withdrawn. The fraud was discovered when a customer complained of a shortage in his account.

In another case, a programmer working on a money order system used a more subtle method to steal $100,000. He defined an extra type of money order that would be honoured for payment but would not be listed on the printout. He then presented money orders of this new type and collected the cash.

In general, however, data processing staff are rarely involved in computer fraud. Even when they are, the frauds are likely to be conventional (false expense claims, for example), rather than frauds relying on their specialised knowledge. In view of the potentially high revenues from computer fraud, and the vulnerability of many systems, it is perhaps surprising that so few data processing staff are involved in fraud. It is possible, of course, that the criminally inclined data processing professional is too clever to be caught, although we have no evidence to suggest that this is the case.

PENETRATION BY OUTSIDERS

It is difficult for people from outside the organisation to operate a computer-based fraud because of the need to extract assets from the organisation. Because of this, computer fraud by outsiders does not happen very often.

In the best-known case, a teenage hacker, Jerry Schneider, stole goods worth $1 million from Pacific Telephone and Telegraph in 1972. From discarded operating manuals, and by posing as a journalist, he learnt that PT&T's central supply organisation would continue to deliver goods to local depots as long as the total values remained within the budgets held in the computer system. He then used his hacking skills to discover the budgets and to order goods from the central supply organisation.

Schneider purchased a key to a local depot from an ex-employee, which he used to remove the goods delivered against his requisition, signing the paperwork on behalf of the depot staff. He then sold the goods through his own supply business. His crimes were revealed by a disgruntled business partner, and he was sentenced to two months in prison and a $500 fine. He subsequently became a computer security consultant.

In a more recent case, a 24-year-old programmer in Texas was charged with obtaining $100,000 by false pretences. According to the Assistant District Attorney for Houston, the accused person accessed the database of the Greater Houston Credit Bureau to obtain personal details of wealthy people living in the area. He then obtained credit cards in their names and used the cards to extract cash from automated banking machines.

DEFENCES AGAINST COMPUTER FRAUD

The way in which most computer frauds are discovered illustrates that deficiencies in operational control procedures are usually a contributory factor in the frauds. Analysis of known cases shows that relatively few frauds, especially the larger ones, are discovered by routine checks or audits. Of course, such checks do catch some frauds and may deter others, but it is clearly unwise to rely on them. Of the 60 frauds analysed in the 1984 British survey:

- Seventeen were discovered by routine checks (13 by accounting controls and four by spot checks).
- Twenty were discovered largely by chance (11 through information or queries from non-employees, usually customers; eight through the vigilance of other employees; and one because the perpetrator confessed).
- In the remaining 23 cases, there was insufficient information to identify the cause of discovery.

Thus in 55 per cent of the cases where the cause of discovery can be identified, there was a significant element of chance in the discovery.

The main defences against computer fraud are therefore basically the same as the defences against fraud in manual systems:

- Careful selection of the staff who will be employed in positions of trust.
- Responsible supervision of junior staff.
- Dividing responsibilities so that staff are not provided with opportunities that might tempt them to engage in fraudulent activities. Thus, the same person should not be able to create a record for a new supplier and to authorise the payment of that supplier's invoices.
- Maintaining adequate controls for physical access to computers and logical access to data. Staff should be given access to only those facilities that they need to do their jobs.
- Ensuring that normal accounting controls, including balances and spot checks, are carried out. Many people begin to defraud their employers when they realise that some mistakes are not noticed. Effective procedures for detecting errors are therefore a vital part of the defences against fraud.

Computer systems make it possible to carry out a whole range of new kinds of checks, including:

- Checking the plausibility of data as it is input to a system.

– Checking the integrity of a database.

– Searching for patterns of unusual events, posting errors, for example.

These additional checks can be extremely valuable in guarding against errors as well as against fraud. One Foundation member, an insurance company, told us about the considerable problems experienced in the late 1970s during implementation of systems changes brought about by changes in tax relief for life insurance premiums. This organisation told us that its database audit programs saved the company from disaster.

Additional defences are required to guard against the possibility of fraud by data processing professionals, however. Criminally inclined data processing staff understand the existing measures against fraud, and they work round them. Their ability to do this may be restricted by keeping secret the exact nature of some defences, such as checks on database integrity and plausibility checks. Potential fraudsters may also be deterred by tight physical and logical access controls and by keeping records of computer accesses.

Nevertheless, there are some people who are able to circumvent all these controls for any computer system currently available. Most competent systems programmers would have the required skills to do just this, if they so desired. A completely secure operating system might be able to prevent these people from breaking into a system, but such systems are unlikely to be in widespread commercial use for at least five years, more likely ten.

Every organisation is therefore obliged to trust in the honesty of, at least, its system programmers. Fortunately, data processing staff generally seem to be fairly honest, but organisations should recognise that systems programmers are in positions of trust and should consider this when recruiting and managing these staff members.

Chapter 3

Threats from sabotage

Sabotage of computer systems may take the form of logical sabotage of software or physical sabotage of the computing facilities. Although this type of threat to computer systems does not receive very much attention, it is, in fact, relatively common. Logical sabotage may take the form of an employee with a misplaced sense of humour interfering with a system, or, more seriously, a disgruntled former employee introducing a 'logic bomb' into a system for the purpose of revenge or blackmail. Sometimes, a hacker may also deliberately set out to damage the system he penetrates.

Physical sabotage of computer installations by politically motivated groups is also a risk. Such groups are increasingly aware that many organisations use their computer systems to store sensitive information, and that damage to the computer installation can severely embarrass the organisation. The types of organisation that may be particularly susceptible to politically inspired sabotage include:

- Government departments.
- Embassies.
- Organisations engaged in activities to which significant minorities are opposed (the nuclear industry, for example).
- Companies or universities with defence contracts.
- Organisations using animals for research purposes.

Most sabotage, however, is relatively minor and is committed by disaffected staff, often in quite junior positions. Sometimes, though, the effect of sabotage can be quite dramatic, as the following examples illustrate:

- In 1983, a dismissed programmer installed a logic bomb in an order-entry system that made the system unusable on a date after his departure. He provided the code required to make the system operational again, but when the system failed again on the next day, he demanded £4,000 to provide the necessary code.
- After being dismissed for gross inefficiency by a company in Lanchester, England, a programmer entered the computer room and granted every client with an outstanding bill the maximum permissible discount. The company said that this would take months of work and cost thousands of pounds to sort out.
- In 1970, a politically motivated group bombed the Mathematics Research Center at the University of Wisconsin. The bombs killed one person, destroyed several computers, and caused the loss of research data estimated to have cost $16 million to collect.

The impact of sabotage of computer systems ranges from annoyance and embarrassment to substantial financial loss, and even to loss of life. The risk of sabotage varies with the nature of the organisation, but most organisations have experienced the trivial or petty sabotage inflicted by practical jokers or dissatisfied staff.

Most of the cases of sabotage known to us involve dissatisfied staff. The disaffection that leads to sabotage attacks may be due to an identifiable, perhaps even a reasonable, cause, most commonly lack of promotion, failure to obtain a salary increase, or dismissal. Disaffected staff rarely use the more extreme forms of violence, however.

The number of cases of sabotage reported is much lower than the number of frauds, but this may be because minor incidents hardly seem worth reporting, and many others can be settled by disciplinary measures, often dismissal. Once an employee has been dismissed, there may seem little point in pursuing him through the courts.

Sabotage, or the threat of sabotage, has also been used as part of extortion plans, but without much success. The preferred means seem to be logical rather than physical, so that the damage can be rapidly reversed.

Whatever their motivation, saboteurs have a variety of means available to them. We have classified these into five types — violence, theft,

corrupting data, jamming communications, and logic bombs — which we now discuss in turn, suggesting possible defences and ways of limiting the damage that could be caused.

VIOLENCE

Violent action against computer installations is largely restricted to politically motivated groups, and its incidence varies considerably from country to country and time to time. It can take many forms, the most common being:

- Planting incendiary and explosive devices.
- Using firearms.
- Feeding petrol vapour or acidic gas in through the air-conditioning system.

Acts of violence are sometimes also committed by employees. For example, in 1979 a period of exceptionally bad industrial relations in a British company led to three fires being started at the computer centre. These fires caused substantial damage (but the computer survived).

Employee-caused damage is generally of a more limited nature, however, as in the case of a data processing employee who threw five disc packs from a fifth-floor window. Because there were no backup copies, the disruption caused to the work of the department was considerable. (Bars were subsequently fitted to the windows in question.)

Major acts of violence against computer installations can cause considerable damage and loss. The bombing of the Mathematics Research Center at the University of Wisconsin cited earlier resulted in direct property damage of some $2.4 million.

The primary defence against such attacks involves restricting physical access to the computer facilities. The basic methods are well known and will often be required as defences against other threats, such as theft of movable property. The methods include fences, patrols, surveillance of the site perimeter, security guards, card entry systems, and video surveillance of the computer room. For greater security, the computer centre may be placed underground and separated from public and private roads and car parks.

Secondary defence measures are aimed at limiting the impact of any sabotage attempt. There should be smoke detectors and firefighting equipment, and staff should be trained in the use of emergency equipment. There should be emergency exits (which should be kept clear) and a dependable means of calling the emergency services.

After a violent attack, it will be necessary to restore the computer facilities to full operation as quickly as possible. Backup copies should exist for most data, and additional copies of the most important data should be held off-site. Documentation must also be secured. Most organisations should also consider the need for a backup computer centre, at least for their key systems.

Finally, it would be prudent to insure against the losses that might result from all these types of sabotage.

Many of these measures are also required to protect against accidents, and will have been considered by most systems managers.

THEFT

An organisation can be damaged by the theft of key files, or even of systems documentation. We were told of several cases where programmers removed documentation on their departure. This type of sabotage is generally committed by data processing staff, because only they can identify the media that represent the key resources and ensure that backup copies are also stolen or corrupted.

In a few cases, computer data has been stolen as part of an extortion attempt. In 1977, a computer operations manager and a systems analyst employed by ICI at Rosenberg in the Netherlands conspired with a financier in an attempt to extort money from ICI. The employees took 48 disc packs and 540 tapes, including backup tapes from the backup centre at Wynhaven (to which the operations manager also had access).

They stored the disc packs and tapes in an air-conditioned apartment, and then demanded £275,000 from a senior ICI executive for their safe return. After being chased through the streets on a motor scooter, the thieves were arrested and subsequently sentenced to 11 years in prison between them (although the financier seems not to have been caught).

The first line of defence against theft is to employ loyal and honest staff. Beyond this, the defence measures are similar to those required for protection against violence, specifically:

- Physical access to computing facilities must be controlled. The media library should be subject to separate access controls, and media should be removed from the library only after proper authorisation has been granted.
- Backup copies are essential.

— Recovery procedures should exist and must be tested periodically.

Physical and logical access controls can usually protect mainframe systems and shared systems fairly readily from the risk of theft. If data files are stolen or damaged, they may generally be re-created from backup copies produced in conventional ways.

Systems and data based on personal computers are much more difficult to protect against theft. It is all too easy to slip a diskette into a pocket or briefcase, and it is very easy for those with legitimate access to them to make additional copies. Potential thieves will be deterred if diskettes are locked away when they are not in use or if the data stored on them is encrypted.

DATA CORRUPTION

Data volumes can be corrupted by the use of magnets or by creating programs (or versions of programs) that deliberately overwrite the data. The use of magnets is a relatively slow process and requires physical access to the media, which will be difficult in a well-run computer centre.

Corruption by program potentially has much greater impact, especially if the program used to corrupt the data is a version of a standard file-copy program. In most installations it would not be difficult for a malicious member of the data processing staff to corrupt some data volumes, but it would be difficult for him or her to corrupt all the backup copies as well. In general, the necessary skills and knowledge required to corrupt data in this way are restricted to data processing staff, so the risks are limited.

Microcomputers and office systems are much more vulnerable to malicious data corruption, however. A great number of people have the necessary knowledge and skills, and the backup arrangements are generally poorer. The risk is thus much greater. In our view, the only practical way to protect microcomputer files from deliberate corruption is to keep them locked up when they are not in use, and to make backup copies, some of which should be stored separately.

JAMMING

In most organisations, the computer systems depend on the communications system, and the communications system itself thus becomes a possible target for sabotage. Communications managers routinely plan backup measures for transmission lines and electronic components, but these measures are designed to cope with accidental failures that, in general, occur randomly and infrequently. These backup measures would not necessarily be able to cope with a deliberate attack on the communications system.

Moreover, backup communications facilities are often of lower quality than the primary ones, and because of this they can result in longer response times and higher error rates. Though tolerable if it occurs infrequently, the performance provided by the backup facilities may be unacceptable if the primary facilities are severely damaged.

Communications systems can be sabotaged by jamming techniques. Jamming can be used only against communications systems that share some resources with the intending saboteur. Thus, radio systems are directly vulnerable, and so are all dial-up facilities (to anyone with access to several telephones), and local area networks (to anyone who can attach to the network).

Jamming was used by striking Honeywell staff in 1971. Every day, a central Honeywell computer retrieved data from terminals at branches of the Metropolitan Life Insurance Company. After processing the data, the central computer polled each branch, confirmed the identity of the branch, and then deposited output data. The strikers used a recording of the polling signal to interfere with the operation of branch terminals. As a result, the central computer could not confirm the identities of the branch terminals and thus could not deliver the output data. In this way, the flow of data to 25 branches was blocked for a month before the strikers were caught and charged with 'aggravated harassment'.

The jamming of a dial-up computer service usually requires the cooperation of several accomplices. The most likely source of such a conspiracy is organised labour.

Another possibility for jamming computer systems is presented by security systems that suspend all further use of an account after a few unsuccessful log-in attempts have been made for that account. A saboteur could cause considerable disruption merely by making a few attempts on a large number of accounts.

It might also be possible to use powerful microwave transmitters to interfere with the operation of a computer. We doubt that these would work, however, and they would be easily detected.

The threat of sabotage by jamming is quite small; we have been able to find only two examples, compared with hundreds of frauds.

Defence against the threat of jamming is difficult. It may be possible to keep secret the telephone numbers of some dial-in lines, but it will be hard to maintain this secrecy within an organisation. It is probably wise to keep a few numbers secret, but it may not be worth the effort and cost of doing so.

Some interbusiness electronic funds transfer systems are known to be vulnerable to interference that could, by delaying the flow of transactions, cause the sending or receiving institutions to lose interest on the funds or to switch to some less secure money transfer system. This type of sabotage might therefore create the conditions for a major fraud. Conventional line-quality monitoring methods should detect any attempts at jamming and allow the use of backup lines.

And as we finalised this report, a British newspaper reported that a church in the United States is suing a systems analyst for jamming one of the toll-free lines used by people to pledge donations. The church is that of rightwing fundamentalist Jerry Fallwell, and the line was jammed for over nine months because the saboteur's home computer called the toll-free line twice a minute.

LOGIC BOMBS

A logic bomb is a piece of coding added to a program to make it do something unusual, and usually destructive, at a future date. Some suppliers of package software use logic bombs to prevent the use of their packages either on machines for which no licence fee has been paid or after the licence has expired.

The effect of a logic bomb may be anything from trivial to disastrous. Trivial effects include congratulating the shift leader on his birthday, displaying obscene messages and pretending that there is an 'electronic ghost' in the system. The worst effects include deleting or randomly corrupting operational files, or making an application system unusable. One Foundation member has reported to us a case in which a disgruntled member of the data processing staff corrupted the complete operating system. It took 48 hours to restore all the files from backup tapes.

Only people with competent programming skills can create logic bombs, but with the increasing use of computers, such people need not be employed as programmers. Installing a logic bomb requires access to program libraries, however, which means that most logic bombs are installed by professional programmers.

The use of logic bombs for sabotage is not common, although a spectacular case occurred in France in 1971. A programmer employed on a large file-update program was discovered to be processing accounts for his girlfriend's husband. He was dismissed, but was allowed to stay on until he had finished the program in hand. The logic bomb that he planted during this period of grace erased all the company's files — on New Year's Day two years later.

The first line of defence against sabotage by logic bombs lies in recruiting the right staff and managing them properly. The second line of defence concerns the way that systems are developed and implemented. Programs should be introduced into the operational environment only after they have been approved and validated by someone other than the developer, ideally a representative of the user department.

This procedure should, in any event, be adopted to protect the organisation against errors and accidents. These requirements may seem to run counter to the trend, which we endorsed in Foundation Report No. 47 (The Effective Use of System Building Tools), towards integrated development teams. In fact, it does not do so. Inspection is a valid technique in such an environment, and the user's representative may play an independent role when authorising programs.

How the user's representative assures himself of the program's quality and integrity will vary with the environment, the application, and the effectiveness of the damage-limitation procedures. For a program written for personal use in a well-protected timesharing environment, no check need be carried out. For a multi-user transaction-processing system, the minimum level of checking should be either acceptance tests by the user department or close inspection of the program code by another programmer. Sometimes, a great deal more checking may be required. For example, separate approvals may be required from the user department, operations management, and technical audit staff, together with code inspections and thorough testing by programmers, analysts, and customers.

The damage that may be done by a logic bomb can be limited by providing programmers and users only with the data access, and especially deletion and modification rights, that they actually need. On some computers, the operating system can provide adequate controls, but on others the required controls may have to be provided by special security software.

Chapter 4

Misuse of computer resources

The final type of threat to computer systems arises from the misuses to which such systems may be put. Some of the misuses are now the subject of legal or contractual restrictions. Others are determined by individual organisations as they decide what constitutes improper use of a valuable company asset (the computer systems). Some companies are prepared to tolerate a limited amount of use of their computer systems for private purposes; others will explicitly ban all private use.

LEGAL AND CONTRACTUAL RESTRICTIONS

Computers and data communications are increasingly subject to legal restriction. In many countries, laws to protect personal privacy restrict the kinds of personal data that may be held in computer systems. These laws may also give people the right to inspect the data that relates to them, as well as imposing obligations on the owners and custodians of such data to safeguard it. Penetration by hackers may make an organisation liable under the data protection laws. The United Kingdom Data Protection Act of 1984, for example, allows people to sue for actual damage caused by the unauthorised loss of, access to, or disclosure of data about them. To avoid liability, system operators must take 'reasonable care' or appropriate security measures for data protection. This requirement does not apply just to mainframe systems — it affects all data holdings covered by the Act.

Laws on transborder data flow restrict what may be sent between countries, and PTT rules may control the way in which it can be sent. We know of one company that was unable to extend its staff locator system to certain European countries because of these laws.

There is also increasing pressure for the censorship of electronic media, including mail systems, bulletin boards, and videotex systems. We are not aware of any electronic-censorship laws at present, but British Telecom has already voluntarily withdrawn one videotex service that was being used to arrange sexual contacts, and the United States Congress has discussed a bill to outlaw 'computer pornography'.

We believe that the next few years will see more and more laws and regulations governing computer communications and the uses to which computer-based data may and may not be put. As computers and communications equipment proliferate, the likelihood increases that these rules will be broken, whether deliberately or inadvertently. Each organisation must keep abreast of any changes in the legal environment that affect computer systems and must ensure that all relevant staff members are aware of the way the laws affect them.

The consequences of the changing legal environment are difficult to assess and will vary from country to country. However, the new laws do create criminal offences, raising the possibility that organisations might be fined or served with restraining orders, and the possibility of legal action against individuals cannot be excluded. A French law enacted in January 1978, for instance, prescribes a maximum fine of the equivalent of $3,000 for failing to take reasonable care of information.

An area of particular concern at the moment is the illicit copying of computer software. Computer programs and, sometimes, text and data in machine-readable form are works that deserve the same legal protection as other published material. At present, the legal position about copyright of software is not entirely clear, and many countries are considering amending their copyright laws specifically to include computer software. In the meantime, however, software suppliers are imposing their own legally binding terms and conditions to prevent the illicit copying of their products.

Before the introduction of personal computers, useful programs were so complex that they usually required the supplier's assistance to install and support them. Copying of software was difficult without the supplier's help. The introduction of personal computers changed this situation profoundly. Suddenly there was a flood of packages that required minimal support and that

could be copied easily. As a consequence, many copies of microcomputer software have been made. Some of the copies have been made for legitimate reasons; others have been made to avoid paying additional licence fees. Whether making a copy is illegal or not depends both on national law and on the exact terms of the supplier's licence agreement. (Some agreements, for example, permit the making of one security copy.)

The software industry has repeatedly stressed the considerable loss of revenue that widespread copying has caused them. The scale of the problem was revealed in a study by Future Computing Inc., which showed that, on average, there is one pirated copy of PC business software for each legitimate one. It also showed that copy-protected software is pirated at the same rate as unprotected software. And in France, a survey of 300 organisations carried out by the Agence pour la Protection des Progiciels (Software Protection Agency) estimated the losses from illicit copying in 1984 to be 750 million francs ($95 million).

Since 1984, software suppliers have given their arguments added force by instituting legal proceedings against several large and reputable organisations. In January 1984 Lotus Development Corporation sued the Rixon Corporation for $10 million, claiming that Rixon had violated copyright and the Lotus agreement for the 1-2-3 product by making at least 13 unauthorised copies and distributing them to branch offices. This suit was settled out of court for an undisclosed (but reportedly substantial) sum, and an injunction against further illicit copying was issued. Later in 1984, Lotus sued a health care organisation in Tennessee. This case was also settled out of court.

In January 1985, Adapso sued American Brands Inc. and a subsidiary (Wilson Jones Co.) for illicitly copying Mailmerge, Spellstar, Wordstar, and other packages. Adapso claimed that copyright and licence agreements had been violated and that the companies were engaging in unfair competition.

Besides litigation, software suppliers are continually trying to devise new techniques to prevent copying. These 'copy-protect' techniques are usually based either on unusual disc formats or on special hardware that has to be installed in each computer before the software can be loaded. The former are fairly easily circumvented, whilst the latter is inconvenient and nonstandard. Furthermore, special 'security-copy' programs are readily available to circumvent most anticopying techniques.

Where a package is used widely in an organisation, it will sometimes be possible to negotiate a site licence, or other multi-user licence, that either permits copying or makes it unnecessary. Micropro has recently announced a discount structure that allows Wordstar 2000 to be made available to several users via a local area network. Other suppliers, notably Lotus, are refusing to issue such licences. Some large organisations have chosen not to use Lotus 1-2-3 precisely because of this restriction, and this option may appeal to other organisations.

It is also fairly common for copies of mailing lists and other saleable data to be stolen. Such a theft is often difficult to detect because the original is not affected. The use of 'sleeper' entries (names and addresses of staff or friends of the company) is one way of protecting mailing lists.

Illicit copying cannot be physically prevented. The only way of preventing such copying, and thus of eliminating the possibility of legal action and consequent financial penalty, is for the organisation to make all its staff aware of the risks both to themselves and to the organisation. Contractual and legal obligations must be made plain, and there must be clear and enforceable rules to prevent illicit copying.

An organisation has a legal and moral responsibility to safeguard data and software entrusted to it, whether by the public, by customers, or by suppliers. The potential costs of failing to meet this responsibility are high. There is no technical fix for this moral and legal problem: the organisation must know what the law is, must determine to abide by it, and must ensure that its employees share that determination.

USE OF RESOURCES FOR PRIVATE WORK

Whenever people are trusted with an organisation's assets, there will be some who use them improperly. Company telephones may be used for personal calls, company petrol for private trips, and company photocopiers to produce party invitations. The difficulty is that different organisations set different limits for what is considered to be proper use — each of the examples listed above is legitimate use in some organisations but is cause for disciplinary action in others. All organisations, however, set some limits.

Similar considerations apply to the use of computer resources. An obvious example of the misuse of computers concerns the use of business computing resources for playing computer games. Such games have existed since the earliest days of computing, but in recent years the increasing use of time-sharing services and personal computers have made a wide variety of computer games available

in offices. Both the opportunities for, and attractiveness of, misuse have therefore increased.

Computer resources may therefore now be misused by an increasingly wide range of staff. Within five years such misuse will be possible for almost everyone in an organisation. The impact of misusing computer resources may be trivial, or it may be quite serious. Typical of the trivial cases are the following:

- In 1985, a temporary terminal operator in the BBC Sports Department wrote a letter to her friends on her word processor. This was discovered because she accidentally sent a copy to every terminal and printer.
- In another case, a programmer used the office computer to write a system to handle bookings for his holiday cottage.
- In yet another case, a laboratory technician used the laboratory's computing resources to do private work for an outside company.

The more serious cases include a data processing manager who was recently prosecuted for "theft of computer printout". He was the manager of a small data processing department and, reporting to the finance director, was responsible for all aspects of systems work. He used his firm's computer system to develop and run a system for a firm of accountants, and some of the department's programmers were paid in cash for developing the system in their own time. The system ran for 18 months, with the firm of accountants making payments to the manager's home address.

This misuse of computer resources became known when the manager left and his successor discovered the previous billing arrangements. The former manager was subsequently convicted, fined £1,200, and ordered to compensate his former employer for the computer resources used, estimated to be worth some £2,000.

The objection to the behaviour in these cases is that staff are using company resources — power, paper, computer resources, and so forth — for their own personal benefit. The costs are unlikely to be high, and the problem can usually be contained within the organisation.

Chapter 5

Reducing the threats to computer systems

This report has shown that there are many kinds of threats to computer systems and that both employees and outsiders may be the source of these threats. Often, organisations regard the threats as imaginary, rather than real. Indeed, it is difficult to determine how widespread the threats are, and, in any case, each kind of threat is relevant to different organisations to very different degrees. For instance, banks are particularly vulnerable to major fraud, whereas pharmaceutical companies, which have major investments in trade secrets and research results, are more concerned about industrial espionage.

It is therefore not possible to identify any one set of security measures that are equally applicable to every organisation. It is almost as difficult to find common policies for a single business sector. Nevertheless, we believe that almost every systems department needs to take three initiatives in order to reduce the threats to its computer systems:

- Inform senior management of the risks being run.
- Increase staff awareness of security.
- Install appropriate defence measures.

INFORM SENIOR MANAGEMENT OF THE RISKS BEING RUN

Some of the risks identified in this report are unavoidable, given practical constraints such as the need to preserve existing investments in systems and data and the limited resources that can be made available for implementing security measures. It may be justifiable to run such risks, but, because they may lead to business losses, the decision to accept a particular level of risk should be a business decision, not a technical one. The decision should therefore be taken by those charged with the welfare of the business.

The responsibility of the systems department is to evaluate the threats to the organisation's data and systems, and the security measures currently in force. Any shortcomings in the security arrangements should be reported to senior management, who should be informed clearly of the likelihood of a breach and its possible consequences. Management should also be advised what, if anything, can be done to reduce the risk, and at what cost.

This initiative may lead senior management to take no action, or it might lead to commissioning of a formal risk analysis or to immediate further investment in security measures. Whatever the outcome, systems management will have done its job.

INCREASE STAFF AWARENESS OF SECURITY

The threats to an organisation's computer systems can be reduced considerably by increasing staff awareness of the need for security. This report has shown that many security breaches result from inadequate attention to systems security either by system developers or by users. This neglect is rarely malicious; rather, it is due to a failure to understand the importance of security measures. In turn, this is due to management's failure to explain the risks and the costs associated with them.

The systems department should therefore educate users about the importance of security, emphasising the key role played by passwords and the need to manage them properly. In addition, the systems department must itself become more aware of the opportunities for fraud and the means available to prevent or detect it.

INSTALL APPROPRIATE DEFENCE MEASURES

In the earlier chapters of this report, we dealt with the various ways in which an organisation's computer systems can be threatened, and we suggested defence measures appropriate to each kind of threat. We now classify the defence measures into six categories that provide a framework for an environment that will both minimise the risks of an attack and limit the damage caused by any attack that does occur. Appendix 2 lists some common faults in security that make it easy for an attack to occur;

implementing the measures outlined below will eliminate such faults.

There are also measures that computer suppliers can take. These include the introduction of better password systems and more flexible access control regimes and the plugging of the many obvious gaps in operating system security.

The six kinds of defence measures available to computer users are:

— Management measures.

— Physical access control.

— Logical access control.

— Disguise of systems and data.

— Monitoring.

— Insurance.

MANAGEMENT MEASURES

Organisations should seek to recruit only honest and responsible people — at least where they must deal with money or control funds. References should always be taken up. For people in positions of trust (including systems programmers, database administrators, and systems security staff), some more positive investigation may be needed.

For all staff, the importance of security (especially password control) should be continually stressed. It is not adequate to emphasise the need for security only during the initial stages of employment.

When systems staff are dismissed, they should be given no opportunity to cause damage and should be escorted off the site. Any passwords and keys allocated to them should be changed immediately.

Supervisors and managers should be vigilant and look for signs both of unusual use of computers and of personal problems — drinking, drugs, marital difficulties — that might make an employee unstable or vulnerable to external pressure.

Some kiting frauds require the perpetrator to manipulate different accounts continually. Management should therefore insist that staff in positions of trust take their annual leave and other holidays. Management may also wish to enforce rotation between jobs.

PHYSICAL ACCESS CONTROL

Controlling the physical access to computer systems is the most basic security measure and is an essential complement to the more elaborate electronic logical control measures discussed below. Physical access is usually subject to several layers of control. The site, computer centre, and computer room will have their own control systems. Access to media stores, whether within the computer centre or off-site, should be separately, and strictly, controlled.

Confidential data need not necessarily be stored in conventional mainframe computer installations, however. Increasingly, confidential data may be held on microcomputers or office systems, and access to this type of system should also be controlled. Shared office systems may be kept in a locked room, as may file servers on local area networks, but it is generally impossible to protect personal computers in this way. Instead, discs containing confidential data should be locked up when not in use, or the data should be disguised by encryption.

LOGICAL ACCESS CONTROL

Logical access control has two parts: authentication and the control procedures. Authentication establishes that the user is who he or she claims to be, and the control procedures restrict the user to those computer facilities to which he or she is entitled.

Authentication

The main means of authenticating a user is still the password. Passwords can make a system reasonably secure, provided that user discipline is good and repeated access attempts by hackers are detected and denied.

Several other authentication systems are available commercially, among them systems based on ciphers and special sensors that measure the pressure pattern during a signature. The latter have been available for some years but have not yet been widely used.

In the future, authentication systems based on the user's physical characteristics may become available. Research is under way on the use of fingerprints, retinal patterns, and other more obscure physical characteristics. All these systems require special terminals and therefore require the system to authenticate the terminal before trusting its report of the user's characteristics. These methods will add significantly to the cost of the terminal.

Another approach to authentication is to use secondary security measures to confirm the user's identity. These measures may include:

— Automatic callback, in which the connection is broken and the system dials the user at his expected location.

— Personal questions, usually drawn randomly from an extensive list.

– Encryption (see Appendix 3).

Control procedures

Once the user's identity has been established, he or she should be given access only to those resources that are needed. For users of transaction processing systems, who are often clerks, this restricted environment may be managed by a teleprocessing monitor. A good monitor will restrict the user to the specified transactions and will prevent direct access to the operating system. A similar approach may be taken with videotex and specialised information retrieval systems. In every case, it is essential that a failure of the supervisory program should not leave the user in contact with the operating system.

Timesharing users cannot be restricted in this way, since they must be given access to the operating system. A good operating system will limit each user to authorised files and operations. In other cases, however, the operating system must be supplemented by a security package such as RACF or ACF2.

Most operating systems and security packages can only control access to complete files and programs. In many cases, however, there is a need to restrict the fields that a user can retrieve, and even to make such restrictions value-dependent. These conditions can usually be enforced only by a database management system, which must therefore be regarded as part of the control regime.

An ideal logical access-control regime would provide:

- Completely flexible definition of users' rights to access programs, data, and other resources.
- The ability to restrict access to data by files, records, and fields.
- Separate controls for reading, modifying, deleting, executing, and adding to the contents of files.
- Reports of attempted violations and unusual patterns of activity.
- Complete enforcement of the security rules in both batch and online operation and during failure conditions.
- Convenience in use.
- Low overheads.

In practice, these characteristics are difficult to reconcile, and most control regimes fall somewhat short of these ideals in their efficiency, convenience, and completeness.

Complete security in the area of logical access control requires the implementation of a 'reference monitor' to prevent the operation of Trojan Horses (see Appendix 1). The monitor must be implemented in both hardware and software, and its correct operation needs to be established formally. To date, only one commercially available system, Honeywell's DPS6-based SCOMP, comes near to meeting the highest standards in this regard.

DISGUISING SYSTEMS AND DATA

Many organisations make it easy for an outsider who may accidentally come across printed computer output to identify the meaning of the data. Computer printout that has been lost or stolen can usually be identified because the organisation's name is printed as part of the heading of the report or is preprinted on every sheet of stationery. These practices are often of no practical value to the organisation. Omitting the organisation's name from printouts would make it that much more difficult to identify the meaning of the data.

If the data held are particularly sensitive or valuable, or if the system is especially vulnerable to penetration, it may be worthwhile disguising the nature of the information itself. The best means of disguising data is to encrypt it under a proper key management scheme (Appendix 3 describes the most commonly used encryption methods).

If encryption is impractical or too expensive, a simple alternative way of disguising data is to omit descriptive headings and text. In our view this method should only be regarded as a temporary expedient because:

- It makes systems harder to use and maintain.
- It does not provide much protection. Organisations consistently overestimate the protection provided by secrecy. Often a well-briefed journalist or commercial rival knows enough to interpret quite cryptic data.

MONITORING SECURITY SYSTEMS

To ensure that the security systems work, their operation should be monitored. Valid actions and invalid attempts should be recorded, and some of them should be investigated at regular intervals. There is little point in keeping records unless they are analysed, at least sometimes. The following activities should be monitored: password changes, key changes, log-in attempts, overall activity levels, and other specified events.

INSURANCE

The final action that can be taken to limit the damage that may be caused to computer systems is to take out appropriate insurance cover, but

some risks may be uninsurable, at least for a reasonable premium. These vary from country to country, but may include strikes, war, riot, radioactivity, and dishonesty by certain staff.

We believe that organisations can minimise the risks to their computer systems by adopting these six kinds of defence measures. Examining the current situation with regard to these defence measures will assist any organisation in evaluating the security of its computer systems and in identifying areas of vulnerability.

Appendix 1

Methods used by hackers

The aim of most hackers is to gain access via public data networks to interesting files and applications. To do this, the hacker has to solve three main problems:

- To locate a host computer.
- To persuade the host that he is an authorised user.
- To upgrade his access rights in order to see more of the system.

Once a hacker has penetrated a system, the increasing use of user-friendly applications and 'help' facilities (which are themselves excellent developments) make it easy for him to find his way around the system, its files, and applications.

LOCATING A HOST COMPUTER

Locating a host computer is probably the easiest problem for a hacker to solve. The telephone numbers and data network addresses of some hosts are published, whilst others are divulged by staff and swapped between hackers. If these sources fail, the hacker may program his microcomputer to search a range of numbers, listening for a modem tone in each case. A flowchart for such a program is given by Hugo Cornwall in *The Hacker's Handbook.*

PERSUADING A HOST THAT THE HACKER IS AN AUTHORISED USER

In order to persuade a host that he is an authorised user, the hacker must first identify some authentic authorised users. This is usually easy to do. Some computer centres have pigeonholes marked with account names; some timesharing systems will list the users online, even for an unidentified user; some account names are published in either internal or public directories; some computer centres do not destroy out-of-date lists of account names but throw them away with their waste paper. It is virtually impossible for account names to be kept secret from a determined hacker.

The next task is generally the most difficult facing the hacker. He must subvert the system's authentication facilities — usually some sort of password protection. The commonest method is password guessing, but hackers may also use spoofing and offline methods. In addition, the hacker may have to subvert a secondary security system, such as data encryption or automatic callback.

PASSWORD GUESSING

The simplest kind of password guessing is an exhaustive search. Every possible password is tried in turn until the correct one is found. On many modern systems, this method cannot be used from online terminals because the connection is broken after a small number of unsuccessful attempts. This greatly increases the time required for an exhaustive search and usually triggers some alarm signals. In the absence of such precautions, this method will always work, but it is generally slow. If, for instance, a hacker knew that a password was four alphanumeric characters and could try one every second, it would take him over 230 hours to find a password. Because of the time taken (and the associated connection costs), exhaustive search is rarely used. Instead, the hacker exploits the fact that users choose their passwords in predictable, rather than random, ways.

The database hack is a popular method of password guessing. The hacker constructs a list of commonly used passwords (a partial list is given in Figure A.1) that he then tries on every account he can identify. This works in a surprisingly high proportion of cases: more than half, according to some hackers.

Another selective method of password guessing is the reverse hack. A few of the commonest passwords are tried in succession on each of several accounts. This method sometimes avoids the security system's limit on the number of log-in attempts allowed, and it also makes the attack rather harder to find on a system log.

The hacker may exploit specific knowledge of the people involved, especially if he works in the same organisation. For instance:

Figure A.1 Some commonly used English passwords

A single alphabetic character	Kill
Account	Love
Aid	Mickey Mouse
Alpha	No
Batman	OK
Beta	Okay
Computer	Password
Dead	Please
Demo	Robin
Dollar	Secret
Donald Duck	Sex
Games	Superuser
God	System
Hello	Test
Help	Work
Intro	Yes

Names of pop groups
Versions of the company name
The account name

- He may try their car registration numbers, telephone numbers, and names of their families, pets, and favourite fictional characters.
- He may see that they have written their passwords in their diaries and look in their diaries whilst they are away from their desks.

Finally, there are some specific password-guessing rules that the hacker may use:

- If an account has been created for the chief executive, it will often have a particularly easy password.
- The accounts used by customer engineers have standard names, and, often, the passwords used during the initial testing of a system are not subsequently changed.

SPOOFING

A spoof program mimics the log-in dialogue for the target system. The hacker arranges for an unsuspecting user to reach his spoof program, rather than the system log-in routines, when he attempts to access the system. The spoof program then collects the user's account name and password, files them, and aborts the session with a plausible message, such as "LOGIN REJECTED DUE TO NAME POOL OVERFLOW. TRY LATER". On his next attempt, the user is connected to the genuine log-in dialogue, and is unaware that his account name and password are now available for collection by the hacker.

The key difficulty in spoofing is to arrange for the user to reach the spoof program, not the normal log-in routine. Several methods are available to achieve this:

- If the terminal is a PC, then the spoof program may be loaded on the PC.
- If the hacker can meddle with the PABX or electronic public exchange, he may have calls to the host redirected to a PC running the spoof program.
- The user may be informed that the host is available more conveniently or cheaply via a 'new access route', which is, of course, the hacker's own computer. In this case, the spoof program collects the password and then announces that the access route is not yet available.

Spoofing is an immensely powerful method, not least because it does not alert system management in the way that exhaustive search does.

OFFLINE METHODS

Sometimes it is easier to fool people than machines. An astute hacker may be able to persuade the system operator, by telephone, that he has lost his password and urgently needs computer access. Ex-hacker Bill Landreth reports a more elaborate method in which a student hacker collected personal data from employees of a company, in the guise of a college class project. Some employees were using their first names as passwords, which allowed the hacker to gain access to that company's computer.

SUBVERTING SECONDARY SECURITY FEATURES

Some systems use automatic callback, automatic encryption, or questions about personal matters as a secondary layer of systems security. These procedures add to the hacker's work, but they can sometimes be subverted.

Where automatic callback is used and the callback unit uses the same line for incoming and outgoing calls, the hacker may be able to keep the line open when he should have closed it, and impersonate the telephone system by using a suitable gadget. Even if the unit uses separate lines for outgoing calls, the hacker can play the same trick if he can identify those lines. Call-forwarding PABXs and public exchanges can also be used to divert the return call to the hacker's own telephone.

There is little experience of using encryption as an authentication measure, though it is now being used (see Appendix 3). A standard algorithm is, of course, only as secure as the secrecy of the key. At the least, this acts as a second password. If the key is built into the encryptor, and encryptors are only made in matched pairs (as in some proprietary systems), then theft seems to be the only means of breaking the system. Most hackers will not go that far.

Finally, the hacker can answer questions about personal matters if he knows the target user well enough.

UPGRADING ACCESS RIGHTS

There are two main ways in which a hacker may increase his access rights once he has penetrated a system. Either he may obtain access to another account that already has greater rights, or he may be able to upgrade the rights for the account he does have access to. Alternatively, if he can get access to a sufficiently privileged account (that of the system operator or the security officer, for example), he may be able to create a new account with many privileges.

OBTAINING ACCESS TO A HIGHLY PRIVILEGED ACCOUNT

To gain access to highly privileged accounts, the hacker must first identify such accounts. Systems usually list the names, either of all accounts or of currently active accounts, and privileged accounts often have distinctive names. In addition, as a system user, the hacker will be able to find the names of the people likely to have privileged accounts. If these methods do not work, the hacker will proceed by trial and error until he finds such an account.

In order to obtain access to a highly privileged account, the hacker can use the same means he used to acquire an account, but he can often do so more efficiently. For example, if the system allows someone else's privileges to be used during a session, password guessing may be conducted at machine, rather than terminal, speeds. It may therefore be possible to try hundreds, even thousands, of passwords per second, greatly reducing the time needed even for an exhaustive search. According to a recent supplement to the *Computer Fraud and Security Bulletin*, a hacker was able to obtain the password for someone else's file in 178 seconds on a Prime 370, even though the passwords could be up to seven characters long. The author of the supplement suggests a way in which even this time could be greatly reduced.

Spoofing, too, is easier once the hacker has access to an account:

- The hacker may load the spoof program on a public terminal and wait till someone else uses it.
- If a network break does not close a timesharing session, a hacker may load his spoof program and then break his network connection. The next user to access the port he had been using will access the spoof program.
- On some systems, the interactive message facility can be used to persuade the user that a 'system fault' has occurred, and the hacker can then present a spoof version of the log-in screen.

On systems that allow a user to read the main memory used by the operating system, the hacker can read the input and output buffers associated with other users. Account names and passwords will appear there from time to time.

Some programming aids may be used to bypass security controls by accessing files at physical level. This may give direct access to passwords or even to the tables that define the privileges of the hacker's own account.

On some systems (some IBM System 38s, for example) passwords are recorded in a system journal.

On systems in which the passwords are stored in clear text, the hacker may simply read the file of passwords. Even when the file is secure against online users, it may be readily accessible from a batch job that the hacker submits from his online session.

On systems in which the user's password is held in his own area, the hacker may write a Trojan Horse. This may take the form of a computer game or an attractive utility program that collects the passwords of every person who uses it and returns them to the hacker.

UPRATING THE ACCOUNT PRIVILEGE

In most systems, users are not able simply to grant themselves additional privileges; this right is reserved for particular users. Hackers use two methods to subvert these controls, rapid fire and Trojan Horse.

With the rapid fire method, the hacker writes a program that issues a valid command to the operating system but then changes it to a 'grant privilege' command between approval and execution by the operating system.

When a Trojan Horse is used, its behaviour is innocuous until it is called by a highly privileged user. It then performs the 'grant privilege' command that the hacker requires, before continuing in its normal manner.

A more powerful variant of the Trojan Horse is known as a virus. Virus programs insert copies of the Trojan Horse into the user's own programs. Experiments have shown that a virus may be written in just a few days and that it will usually take less than an hour to obtain all the privileged facilities for its creator.

Appendix 2

Common faults in systems security

A failure in systems security is usually due to one of four reasons:

- Neglect of basic security procedures by staff.
- Neglect of ordinary good professional practice.
- Betrayal by one or more staff members in a position of trust.
- Risk-taking by management.

NEGLECT OF BASIC SECURITY

Any security safeguards are only as good as the diligence of the least diligent operator, because a breach at one point can often be exploited to create others. This is clearly true for physical security. A single intruder will usually be able to admit others through emergency exits, or even windows. It is also true for logical security. A hacker will be able to tell others the passwords he has learnt, and he may be able to create accounts for other hackers.

The most common faults in physical security include:

- Doors propped open.
- Admitting visitors without checking that they are expected.

The most common faults in logical access security are:

- Failure to change the standard passwords and system engineer's accounts created when a system is first installed.
- Sharing accounts and passwords.
- Use of one-character passwords.
- Failure to change passwords regularly.
- Use of forename, spouse's forename, and other easily guessed passwords (some of the most frequently used English passwords were listed in Figure A.1.).
- Writing down passwords and account numbers and sticking them onto a terminal.

NEGLECT OF GOOD PROFESSIONAL PRACTICE

In most commercial and professional fields there are good practices that are well understood, but that are not always followed. In data processing, such practices include making a program operational only after it has been tested and authorised by a responsible person and including checkpoints in long-running batch programs. In finance, these practices include minimising the number of people who have to be trusted by avoiding the concentration of authority and by authenticating requests for funds transfer. In banking, the practices include insisting on people taking all their annual leave and mandatory job rotation.

Most computer frauds described in this report would have been impossible if the target organisations had followed established professional practices.

BETRAYAL BY ONE OR MORE STAFF MEMBERS IN POSITIONS OF TRUST

A betrayal of trust is probably the most difficult fault to deal with because it is a fault in the employee rather than in the organisation.

Every organisation has people in positions of trust, people whose honesty must be assumed. This is probably very well understood in most organisations, and great care will be taken in recruiting and managing people such as buyers and credit controllers.

It is less well understood that the job of systems programmer is now also a position of trust. A competent systems programmer is likely to have the skills that would allow him to sabotage a significant part of the company's operations, subvert major financial systems, and conceal both the method and his own responsibility from management and auditors.

Applications programmers, on the other hand, pose less of a threat to the organisation's computer

systems. They can be kept out of the operating system (by defences maintained by the systems programmers), and inspecting and testing their work will usually prevent them from committing a fraud.

RISK-TAKING BY MANAGEMENT

No organisation can make itself completely secure against fraud, spying, and sabotage. As in other areas, complete systems security is unobtainable, and every organisation has gaps in its security coverage, of which it is more or less aware.

One of the best examples of calculated risk-taking is provided by those ATM networks that will dispense money after fewer checks than normal when the central computer is down. The managers of these networks have clearly chosen to maintain public service despite the increased exposure to fraud.

A second example of calculated risk-taking concerns the use of ordinary operating systems, all of which are insecure. This insecurity takes many forms, including the following:

- Lists of passwords are held in clear text.
- The security files for the online system are freely available to batch programs. (The TSO-SPF backup management file may generally be read in this way.)
- A delay occurs between the validation of a command to the operating system and its execution. During this delay, the program issuing the command may change it from a permitted command to one that would not be permitted.
- Passwords are held in main memory, open to inspection from other programs.
- On one popular minicomputer, programs given very high privileges on one installation retain those privileges when transferred to another.

It is probably impossible to make an operating system completely secure, and it is certainly impossible to prove that this has been done. Given that attempts to improve operating system security are expensive, particularly in systems programming effort, management will generally have little choice but to accept some degree of risk.

Appendix 3
Encryption methods

Encryption is the systematic transformation of the information that is to be protected, called the plaintext, into an apparently random data stream, called the ciphertext. Decryption is the reverse process. In communications systems, encryption may be used either to conceal data from an eavesdropper or to authenticate the sender.

All encryption (or cipher) systems require an algorithm and a key. The algorithm is usually built into hardware and may be published. Cipher systems are of two kinds: private key and public key.

PRIVATE KEY CIPHER SYSTEMS

Most cipher systems are 'private key'. The same key is used for encryption and decryption and should therefore be kept completely secret. To reduce the chance of keys being divulged, they must be changed fairly frequently. There are several ways of helping people keep keys secret, including:

- Containing the key within a tamperproof encryption unit.
- Distributing the key in a physical key carrier.
- Distributing the key using an even more secure cipher.

The best-known private key cipher is the Data Encryption Standard (DES). DES was developed by IBM and adopted as the United States standard in 1977. The International Standards Organisation is currently considering adopting DES as an international standard under the name Data Encryption Algorithm No. 1.

In a paper published in 1977, two computer scientists (Whitfield Diffie and Martin Hellman) at Stanford University showed that the 64-bit DES keys could be broken by exhaustive search on a specially built parallel computer. The machine would have one million custom-designed chips, each comparing a known plaintext with the corresponding ciphertext for a series of keys. Diffie and Hellman estimated that it would cost some $20 million to build such a machine. IBM subsequently estimated an end-user price of $200 million for a hypothetical machine to be delivered in 1981.

The proposed machine would be able to break a DES key in an average of 12 hours, at a cost of about $5,000. Diffie and Hellman also showed that, for ASCII text, a variant of the proposed machine would be able to break DES in the absence of known plaintext.

The proposed machine would benefit fully from the falling cost of electronics. Diffie and Hellman estimated that, by 1987, the machine could be built for about $200,000 and that each DES key would then cost about $50 to break. They point out that, in some cases, it might be worthwhile keeping ciphered text until it became possible to break the key economically.

The DES standard could be made immune to attack by these methods by using a longer key. For a key of 128 bits, the expected search cost would be $\$2\times10^{25}$. The actual key length (64 bits) was chosen after pressure on IBM from the National Security Agency of the United States. The reasons for the pressure are still secret, but it is widely assumed that the NSA wished to ensure that it could break messages sent using the DES key cipher.

We are not aware of any evidence that anyone has actually built a 'Diffie-Hellman machine', but we believe that anyone who has strong reasons to conceal data from any national intelligence agency should not rely on a single stage of DES encryption. This is clearly the view of the United States government. American law makes it a criminal offence to transmit classified data protected only by DES. Two stages of DES encryption, with different keys, should provide sufficient security (and the United States has forbidden the export of certain double-encrypting devices).

Non-DES encryption units are being sold by several companies, including British Telecom, CASE, Randata, and Zeta. These companies have not published their algorithms, but they claim that their

ciphers are at least as secure as DES. They maintain that their secrecy is an added advantage. Their refusal to publish makes it impossible to evaluate their claims, which may well be true. By contrast, we know the level of security provided by DES.

PUBLIC KEY CIPHER SYSTEMS

In a public key cipher system, the transmission and receiving keys are different. Though these keys are mathematically related, the relationship is so complex that it is not possible to deduce one from the other (in either direction) in a reasonable time. When used to conceal data, the sending (encryption) key is published; this allows anyone to send data that only the intended recipient can read. The recipient's security requires only that he keep the receiving key secure, and this is relatively easy to do. He is not dependent on other people to maintain the secrecy because only he has the receiving key.

For authentication purposes, the sender publishes his receiving key. He is the only person who can generate messages that can be decoded using that key.

The best-known public key cipher is that of Rivest, Shamir, and Adleman, which is currently said to be much more secure than DES. However, like all public key systems, it requires long keys and a lot of processing. Public key systems are currently impractical for the protection of data transmitted at even moderate speeds, but they can be used for authentication and in special circumstances, such as the distribution of DES keys.

Public key systems are appropriate for providing authentication in the public and semipublic networks that are now emerging for the exchange of mail and commercial information between organisations. Experience has shown that electronic mail systems are not entirely secure, and we look forward with some impatience to the introduction of public key authentication in public mail systems.

Annotated bibliography

CASE HISTORIES WITH ANALYSIS

UK Audit Commission (1985); Computer Fraud Survey. HMSO.

Nielsen, N R; Brandin, D H; Ruder, B; and Wallace G F (1976); Computer System Integrity Safeguards System Integrity Maintenance. SRI, 1976. (Analysis of a file of 291 breaches was followed by cost-effectiveness analysis of defence measures. The authors conclude that there are few or no defence methods of broad applicability, so every computer centre must use several to combat each kind of threat.)

Norman, Adrian R D (1983); Computer Insecurity. Chapman and Hall.

Parker, Donn (1976); Crime by Computer. Charles Scribner's Sons.

HACKERS

Landreth, Bill (1985); Out of the Inner Circle. Microsoft Press. (Excellent discussion of hacking with advice on keeping hackers out of your systems.)

Cornwall, Hugo (1985); The Hacker's Handbook. Century Communications.

Cecula, Adolf; Agencies' hacker troubles blamed on bulletin boards. Computerworld, 8 July 1985.

TECHNICAL ASPECTS

National Bureau of Standards (1977); Data Encryption Standard. NTIS NBS-FIPS PB 46.

Akl, S G (1983); Digital Signatures – A Tutorial Survey. Computer, 16(2), pp 15-24.

Azuma, Kenneth I (1976); Operating System Security – How the Flaws Are Found. Lawrence Livermore Laboratory, University of California. (There are no secure operating systems and the faults have been categorised.)

Boebert, E; Kain, R; and Young, B (1985); Trojan Horse Rolls up to DP Gate. Computerworld, 2 December 1985, pp 65-69.

Carlstedt, J (1978); Protection Errors in Operating Systems: A Selected Annotated Bibliography and Index to Terminology. University of California. NTIS AD A053 016.

Diffie, W; and Hellman, M E (1977); Exhaustive Cryptanalysis of the NBS Data Encryption Standard. Computer, 10(6), pp 74-84.

Diffie, W; and Hellman, M E (1979); Privacy and Authentication: An Introduction to Cryptography. Proc. IEEE, 67(3), pp 397-427. (Excellent background paper.)

Hsiao, David K; Kerr, Douglas S and Madnick, Stuart E (1979); Computer Security. Academic Press.

Rivest, R; Shamir, A; and Adleman, L (1977); A Method of Obtaining Digital Signatures and Public Key Cryptosystems. MIT/LCS/82. 4/77.

Xephon; Access Control Packages. Xephon Buyers Guide.

MANAGEMENT

Candeland, A N (ed) (1972); Computer Guide 7: Insuring a Computer System. National Computer Centre.

Fine, Leonard H (1983); Computer Society. Irish Management Institute.

Goldblum, Edward (1982); Computer Disasters and Contingency Planning. Published by Butler Cox on behalf of Amdahl.

Squiers, T (1980); Computer Security: The Personnel Aspects. National Computer Centre.

Murray, W H (1984); Security Considerations for Personal Computers. IBM Systems J., 23(3), pp 297-304.

Parker, Donn B (1978); Computer Security Differences for Accidental and Intentionally Caused Losses. AFIPS Conf Proc – 1978 NCC, 47 pp 1145-1149. (Accidents can be treated statistically, but frauds and sabotage cannot. Therefore, identify all deliberate threats and choose defences against the most likely kinds. Continue, subject to cost, until the residual probability is low enough; then tackle accidents statistically.)

BUTLER COX FOUNDATION

Butler Cox
Butler Cox is an independent management consultancy and research organisation, specialising in the application of information technology within commerce, government and industry. The company offers a wide range of services both to suppliers and users of this technology. The Butler Cox Foundation is a service operated by Butler Cox on behalf of subscribing members.

Objectives of the Foundation
The Butler Cox Foundation sets out to study on behalf of subscribing members the opportunities and possible threats arising from developments in the field of information systems.

The Foundation not only provides access to an extensive and coherent programme of continuous research, it also provides an opportunity for widespread exchange of experience and views between its members.

Membership of the Foundation
The majority of organisations participating in the Butler Cox Foundation are large organisations seeking to exploit to the full the most recent developments in information systems technology. An important minority of the membership is formed by suppliers of the technology. The membership is international, with participants from Australia, Belgium, France, Italy, the Netherlands, Sweden, Switzerland, the United Kingdom and elsewhere.

The Foundation research programme
The research programme is planned jointly by Butler Cox and by the member organisations. Half of the research topics are selected by Butler Cox and half by preferences expressed by the membership. Each year a shortlist of topics is circulated for consideration by the members. Member organisations rank the topics according to their own requirements and as a result of this process, members' preferences are determined.

Before each research project starts there is a further opportunity for members to influence the direction of the research. A detailed description of the project defining its scope and the issues to be addressed is sent to all members for comment.

The report series
The Foundation publishes six reports each year. The reports are intended to be read primarily by senior and middle managers who are concerned with the planning of information systems. They are, however, written in a style that makes them suitable to be read both by line managers and functional managers. The reports concentrate on defining key management issues and on offering advice and guidance on how and when to address those issues.

Selected reports
5 The Convergence of Technologies
8 Project Management
11 Improving Systems' Productivity
13 The Trends in Data Processing Costs
15 Management Services and the Microprocessor
17 Electronic Mail
18 Distributed Processing: Management Issues
19 Office Systems Strategy
20 The Interface Between People and Equipment
21 Corporate Communications Networks
22 Applications Packages
23 Communicating Terminals
24 Investment in Systems
25 System Development Methods
26 Trends in Voice Communication Systems
27 Developments in Videotex
28 User Experience with Data Networks
29 Implementing Office Systems
30 End-User Computing
31 A Director's Guide to Information Technology
32 Data Management
33 Managing Operational Computer Services
34 Strategic Systems Planning
35 Multifunction Equipment
36 Cost-effective Systems Development and Maintenance
37 Expert Systems
38 Selecting Local Network Facilities
39 Trends in Information Technology
40 Presenting Information to Managers
41 Managing the Human Aspects of Change
42 Value Added Network Services
43 Managing the Microcomputer in Business
44 Office Systems: Applications and Organisational Impact
45 Building Quality Systems
46 Network Architectures for Interconnecting Systems
47 The Effective Use of System Building Tools
48 Measuring the Performance of the Information Systems Function
49 Developing and Implementing a Systems Strategy
50 Unlocking the Corporate Data Resource

Forthcoming reports
Organising the Information Systems Function
Using IT to Improve Decision Making
Integrated Telecommunications Networks
Planning for the Future Corporate Data Centre
The Effect of IT on Corporate Organisational Structure

Availability of reports
Foundation reports are available only to members of the Butler Cox Foundation. Members receive three copies of each report. Additional copies may be purchased from Butler Cox. Reprints of the summary of research findings for each report are available free of charge.

Butler Cox & Partners Limited
Butler Cox House, 12 Bloomsbury Square,
London WC1A 2LL, England
☎ +44 1 831 0101, Telex 8813717 BUTCOX G

France
Butler Cox SARL
Tour Akzo, 164 Rue Ambroise Croizat,
93204 St Denis-Cedex 1, France
☎ (1) 4820.61.64, Telecopieur (1) 48.20.72.58

The Netherlands
Butler Cox BV
Burg Hogguerstraat 791
1064 EB Amsterdam
☎ (20) 139955, Telex 12289

United States of America
Butler Cox Inc.
115 East 57th Street, New York, NY 10022, USA
☎ (212) 486 1760

Australia
Mr John Cooper
Business House Systems Australia
Level 28, 20 Bond Street, Sydney, NSW 2000
☎ (02) 237 3232, Telex 22246

Italy
SISDO BDA
20123 Milano – Via Caradosso 7 – Italy
☎ 498 4651, Telex SISBDA 350309

The Nordic Region
Statskonsult AB
Stortorget 9, S-21122 Malmo, Sweden
☎ 46-401 03 040, Telex 127 54 SINTAB