COMPUTER CRIME: NEW PROBLEM FOR THE INFORMATION SOCIETY*

Tom Forester and Perry Morrison

The new information and communication technologies bring many benefits to society, but they also create new social and ethical problems — such as software theft, invasions of privacy, hacking and the creation of viruses. Computer-assisted crime is one of the most serious and its apparent growth in recent years demonstrates clearly how new technologies create new opportunities for criminal activity. The available evidence on the nature and extent of computer crime is reviewed, together with the available data on participation. Techniques for improving computer security are then discussed and the appropriate lessons drawn.

Keywords: Information society, information technology, computer crime, computer security.

On Christmas eve, 1987, a 26-year-old clerk at Lloyds Bank in Amsterdam, Frans Noe, ordered that sums of US $8.4 million and $6.7 million be transferred via the SWIFT international funds transfer system from the Lloyds branch in New York to an account he had opened with the Swiss Bank Corporation in Zurich. The young Dutchman then flew to Switzerland to collect the money. But owing to an unforeseen computer malfunction, the transfer of the $6.7 million failed to go through. Returning after Christmas, fellow employees saw the failed transaction on their screens and reported it. Noe was subsequently arrested and returned to Amsterdam, where he then threatened to leak news of his security breach to the press unless the bank dropped all charges against him. In May, 1988, the 'flying' Dutchman was jailed for 18 months for breaking into a computer system and his two accomplices got 12 months.[1]

THE RISE OF THE HIGH-TECH HEIST

Computers have created opportunities for crime that never existed before. Changes in technology generate both new types of crime and new techniques of detection.[2] Consequently both criminals and crime-busters compete to stay one jump ahead of each other. The convergence of computing and telecommunications technology — and more recently

* Parts of this paper have been adapted from Tom Forester and Perry Morrison, *Computer Ethics: Cautionary Tales and Ethical Dilemmas in Computing*, which will be published in Australia this month by Basil Blackwell (distributed by Allen & Unwin).

the rapid spread of personal computers and distributed processing — has provided ample opportunity for new kinds of crime. The huge increase in the number of people with some degree of computing skills also means that there are many more potential computer criminals. It has thus been claimed that new technology is democratizing white-collar crime, because it enables even the humblest programmer, operator or clerk (like Frans Noe) to participate in sophisticated frauds that were once the preserve of top management. In his book, *Technocrimes: the Computerization of Crime and Terrorism* (1987), August Bequai even alleges that organised crime and the Mafia are using computers for record-keeping, not to mention extortion, blackmail and sabotage — and that the very future of Western society is now threatened by computerized crime and high-tech terrorism.[3]

The arrival of automated teller machines (ATMs) provides a good example of how new information technologies create new opportunities for criminal activity. The number of ATMs in the US, for example, grew from 4,000 to over 50,000 between 1975 and 1985.[4] The value of transactions is believed to have grown about ten-fold and with it ATM fraud has allegedly mushroomed into a major growth industry. Plastic card abuse of all kinds has also increased: in 1985, for instance, cheque card fraud alone reportedly cost UK banks about A$55 million. Foreign currency and other financial frauds have also grown in parallel with the rapid growth of electronic funds transfer (EFT) systems, while the widespread use of information systems in manufacturing and distribution has made possible the illegal diversion of goods on a scale not possible before.

Still more opportunities for deviant behaviour have been provided by an even newer communications technology — cellular mobile telephones. In March, 1987, eighteen New Yorkers were arrested on charges of illegally reprogramming memory chips in their mobile phones in order to make calls without being charged for them. The fraud had cost the local mobile phone company about US $40,000 per month. It was the first time anyone in the world had been arrested for this type of offence. Commenting on the case, Laurence A. Urgenson, the chief assistant US attorney for the Eastern District of New York, said: "Every new technology carries with it an opportunity to invent a new crime."[5] In the same year, US Sprint, one of AT&T's new competitors in the long-distance phone market, unmasked another new type of fraud in which a group of hackers had used computers to identify and steal US Sprint authorization codes. The codes had then been sold to a large number of individuals and companies who, between them, had allegedly helped themselves to over US $20 million worth of long-distance calls.[6]

Computer crime has been broadly defined as a criminal act that has been committed using a computer as the principal tool. Some have also talked in terms of a distinction between computer-related fraud (in which the computer is purely coincidental) and computer-assisted fraud (in which the computer is used to commit the fraud), while others have

argued that a genuine computer fraud is one which could not take place without the use of a computer. If we accept this tight definition, then the real computer fraud needs computer expertise and greater skills to perpetrate than do the computer-assisted and computer-related frauds. But when most people talk about computer crime, they are usually referring to the fact that a computer has either been the object, subject or instrument of a crime.[7]

Thieving by computer can take the form of the theft of money (for example, the transfer of payments to the wrong accounts), the theft of information (for example, by tapping into data transmission lines or databases at no cost), or the theft of goods (by their diversion to the wrong destination). Two techniques of theft by computer are *The Salami,* which involves spreading the haul over a large number of transactions like slices of salami (for example, a bank clerk might shave a trivial sum off many customer accounts to make up a large sum in his or her own account) and the *The Trojan Horse,* which involves the insertion of false information into a program in order to profit from the outcome (for example, a false instruction to make payments to a bogus company). Theft is undoubtedly the most common form of computer crime: of 191 cases reported to the Australian Computer Abuse Research Bureau (ACARB), for example, 111 involved theft of some kind.[8]

Computer abuse can also take the form of unauthorised use or access to information systems or the modification of programs to benefit the fraudster. Techniques include *piggybacking,* which involves tapping into communication lines and riding into a system behind a legitimate user with a password and *data diddling,* which entails swapping one piece of data for another. Computer crime can also take the form of hacking, sabotage and blackmail. Hacking or computer burgling involves breaking-in to other people's systems for fun or with intent to blackmail or commit sabotage. Techniques include *scavenging* for stray data or 'garbage' for clues that might unlock the secrets of a system; *zapping,* which means penetrating a computer by unlocking the master key to its program and then destroying it by activating its own emergency program; *worms* or worm programs entail the deletion of portions of a computer's memory, thus creating a hole of missing information; and *time bombs and logic bombs,* which involve the insertion of routines which can be triggered later by the computer's clock or a combination of events. When the bomb goes off, the entire system — perhaps worth millions — will crash; *viruses* are self-replicating programs which can have a similar effect.

Computer crime should not present an ethical dilemma for computer professionals or computer users. Theft is theft and fraud is fraud and both are generally accepted by our society to be morally wrong. Criminal activity is not a new problem. But what is new is that the widespread use of information systems has created many grey areas in which right and wrong have not been clearly defined by society or the legal system. Computerization has also placed great temptation in the hands of

ordinary programmers and systems developers, who are often, among other things, the only persons who know how a particular system works. For a minority of computer professionals, it is a temptation and an opportunity which is hard to resist — especially if they see a systematic way to cover-up their crime which makes detection of their crime difficult or impossible. Computers have also had the effect of further depersonalizing crime: in explaining their illegal activities, some guilty computer professionals have talked about so-called victimless crimes (for example, against large corporations or banks) as being somehow more acceptable than crimes with human victims. But this is hardly a justification.

IS REPORTED CRIME THE TIP OF AN ICEBERG?

The true extent of computer crime is not known, can't be known and never will be known. The American Bar Association (ABA), in a major report published in 1984, concluded that losses arising from computer crime sustained by US business and government institutions were "by any measure, huge." Their survey of 300 top US corporations suggested that annual losses in each company could range from US $2 million to as high as $10 million. "If the annual losses attributed to computer crime sustained by this relatively small survey group are conservatively estimated in the range of half a billion dollars, then it takes little imagination to realize the magnitude of the annual losses sustained on a nationwide basis," said the report.[9] More recently, the Cleveland accounting firm Ernst & Whinney estimated that the losses sustained by US companies in total amount to between $3 billion and $5 billion a year. Of the 240 companies surveyed, more than half admitted that they had been a victim of computer fraud.[10]

In the UK, an Audit Commission survey of 1,200 organisations, published in 1988, found that reported computer crimes had risen in value from around 1 million pounds in 1981 to around 3 million pounds in 1987. Nine out of ten respondents believed that they had not suffered from computer fraud. Yet a large number of the 118 frauds detected were only discovered by accident. And only 38 of the 118 cases resulted in prosecutions. Meanwhile a 1986 survey of 50 British companies by insurance brokers Hogg Robinson led them to estimate that frauds involving computers were costing UK firms 40 million pounds a year and others have suggested that total UK losses are a lot higher. In France, an association of French insurance companies estimated that problems with computer systems were costing French firms about US $1.1 billion a year, and 44 per cent of this was accounted for by fraudsters, hackers and disgruntled employees (the rest were caused by accidents, such as fire, malfunctions and human error).[11]

Are these estimates correct or do they merely represent the tip of an iceberg? Or is there no iceberg of undetected computer crime lurking below the surface of society? There are two main reasons why many

experts believe that the amount of computer crime is much greater than we think. First, it is clear that many crimes go completely undetected because so many are discovered quite by accident and because so many are, by their very nature, simply very hard to detect. A 1986 official guide produced for US Federal Agencies stated that detected computer crimes are less than 1 per cent of the total. Second, very few computer frauds are made public because companies — especially banks and other financial institutions — are loath to admit that their security systems are fallible. Publicity of this nature is disastrous public relations and it could lead to the loss of customer confidence, so they prefer to cover things up.

Of those crimes that are detected only a small percentage arrive in court: for example, a 1986 survey by the Los Angeles-based National Centre for Computer Crime Data found that fewer than 100 cases of computer fraud in the USA had actually been prosecuted in the preceding two years. IBM security analyst Robert Courtney told the US Office of Technology Assessment (OTA) in 1985 that of the 1,406 computer crime cases known to him, 89 per cent were never taken to judicial process and convictions were obtained in only 18 per cent of the remainder.[12] Cornwall lists some reasons why non-reporting of computer crime is so widespread: " . . . there is very little benefit to the victim. The law is unlikely to be able to undo the damage caused, the criminal is unlikely to be convicted, much staff time is likely to be tied up assembling evidence (if it can be collected at all), and wider knowledge of the crime is likely to harm the future prospects of the victim organization."[13]

What is therefore clear is that nobody is very clear about the true extent of computer crime — but most analysts who have looked at the problem seem to think it is large and growing. Even if the percentage of installations affected may be small, the sum involved in the average computer crime is probably much larger than in conventional robberies — according to the FBI, for instance, the average computer crime is worth about US $600,000. As to the future, the American Bar Association report concluded: "It would seem beyond dispute that computer crime is today a large and significant problem with enormous potential for becoming even larger and more significant." While Hugo Cornwall has written: "Datacrime deserves to be as much a social issue as more traditional areas of 'law and order' such as crimes against the person, crimes against property and the maintenance of public peace."[14]

TARGETS OF THE COMPUTER CRIMINALS

Banks and financial companies are major targets for high-tech criminals. Banks are vulnerable to frauds committed by insider employees and to frauds committed by outsiders playing 'vault invaders'. Of the computer crimes detected in a British survey by BIS Applied Systems, 37 per cent

were in the financial sector, while over 50 per cent of the crimes by value reported to the ACARB were in banking and finance.[15]

The increased reliance of the financial sector on electronic funds transfer (EFT) systems — it is said that that over US $200 billion changes hands daily in the New York banks' automated payments system — has greatly increased the opportunities for crime. If the electronic authorization codes used in EFT fall into the wrong hands, huge sums of money can be moved about — including out of the country — in a matter of seconds. For example, in a famous case back in 1979, Stanley Mark Rifkin, a computer consultant to the Security Pacific National Bank, visited the bank's wire transfer room where he learned the EFT codes. Later, posing as a branch manager, he phoned the Los Angeles bank and used the codes to transfer money, in amounts of less than US $1 million, to a New York bank. Then he instructed the New York bank to send the money — by now totalling US $10.2 million — across to a Swiss bank account. Having flown to Switzerland, he converted the money into diamonds and then returned to the USA. It was only when he boasted openly of his feat that he was caught and convicted.

What is probably the largest-ever computer crime in history involved a foreign exchange contract fraud. In 1987, it became apparent that the Volkswagen company (VW) in West Germany had lost around US $260 million in a fraud which took place in 1984. Very little is known about the fraud, except that it entailed tampering with programs and the erasure of tapes. It is also known that VW sacked the head of its foreign exchange department and suspended four others, along with the heads of the financial transfer department and the cash and currency clearing sections.

Some of the biggest frauds ever attempted have involved EFT and banks. In early 1988, a huge sum (variously reported to be between US $33 and $54 million) was illegally transferred from the Union Bank of Switzerland branch in London to a private bank account in the small Swiss town of Nyon, near Lausanne. The stunt would have succeeded except for a computer glitch at the Swiss end which forced the bank that day to make manual checks of payment instructions that normally would have been processed automatically. Suspicions were aroused and the Swiss police were waiting to pounce on the man who arrived to collect the cash. Further arrests followed.[16] A similar attempt in 1986 to transfer by EFT the sum of US $8.5 million from the London branch of the US investment bank, Prudential-Bache Securities, to another Swiss bank account was foiled after the bank hastily obtained a court injunction in Switzerland to stop the money being paid out. In September, 1987, two men admitted conspiracy to defraud in a London court and were sentenced to three years and 18 months. While in May, 1988, seven men were arrested in New York after an attempt to embezzle $70 million by creating phony transactions transferring money out of First National Bank of Chicago accounts of Merrill Lynch, United Airlines and Brown-Forman. The amounts exceeded the threshold of

permissable transactions, but the perpetrators had been able to control the telephone response that requested authorization. The transaction was detected when the Merrill Lynch account became overdrawn.[17]

Speaking at a British Computer Society Security Committee seminar, Detective-Inspector John Austen of the Computer Crime Unit at New Scotland Yard, London, highlighted the threat to EFT systems from both criminals and terrorists: "EFT now represents 83 per cent of the value of all things paid for — money transferred — in Britain. Money, as an invisible export, is a major part of our GNP. Foreign exchange markets in London transfer US $200 billion daily using EFT via satellite. The transactions take a very short time, and once complete there is no calling them back. A lot of people are aware of this. And many, both here and abroad, are prepared to steal from EFT systems. The rewards are tremendous. Companies, and even the economies of smaller countries, could be crippled by a sustained hit of EFT systems. Terrorists, such as the Middle East factions, the IRA and the Red Army Faction are particularly aware of this — and they need money. The Red Army Faction has already, unsuccessfully, made moves to intercept EFT in Germany. They and others will try again."[18]

ATM fraud has also become increasingly common in recent years. In 1987, for example, a 35-year-old former ATM repairman, Robert Post, was apprehended after illegally obtaining US $86,000 out of New York City ATMs. Post would spy over customers' shoulders to get their Personal Identification Numbers (PINs) and whenever someone left their receipt, he would take it and discover their account number. Then he would go home, forge a card using a US $1,800 machine he had bought, and return to the ATM and make withdrawals. He was caught because his encoding of the account number and the PIN, while good enough to work in the machine, was flawed. Manufacturers Hanover managed to program its network to detect the flawed cards and capture them. After capturing two and verifying that they were fake, they reprogrammed the machine to notify security when one was being used, and dispatched guards to catch Post. Interestingly, when questioned about his crime, Post said he was not like someone who mugs a customer and steals a card: "I'm a white-collar criminal," he proclaimed, adding that he was surprised that the bank had not offered him a consulting job![19]

In the UK, City of London police in 1987 arrested four suspected ATM fraudsters after finding no less than 1,864 cash cards in their possession. Their arrest followed a denial by the major high street banks that their ATMs posed a security risk after TV viewers had seen a cash card fraud demonstrated on national television. In the US in 1988, someone successfully used a Security Pacific National Bank master card to steal US $237,000 and a plot to bilk Bank of America and other banks on the Plus System of ATMs out of US $14 million over one weekend was only foiled at the last minute by an insider tip-off. Meanwhile from New Zealand came the astonishing tale of a schoolboy called Simon

who outsmarted a United Building Society ATM by using cardboard from a lollipop packet to transfer NZ $1 million into his account. All the 14-year-old did was to slip the cardboard into a deposit envelope and insert it into the machine, while punching up $1 million. When Simon checked his account a few days later he was amazed to find that the $1 million had been credited. So he withdrew $10. When no alarms went off or police appeared, he withdrew another $500, but suddenly got cold feet and put it back again. A few days later, Simon withdrew $1,500 but his nerve failed again and he told one of his teachers, who took him along to the United Building Society for a chat with the manager. His headmaster commented that Simon had not been considered one of the brightest pupils . . . "at least until now."[20]

But it is not just banks that are the target of computer criminals. Computer thieves have also been attracted to insurance companies, where there is scope for manipulating computers to pay out on fictitious claims and to grant bogus premium refunds. One of the largest computer crimes ever discovered involved an insurance company — only this time it was the employers rather than employees who were responsible. From 1965 to 1971, Equity Funding Inc used its computers to generate thousands of phony insurance policies that were later sold to re-insurance companies for a total of over US $27 million.[21] In a more recent case of systematic fraud by a company, Hertz Corp allegedly overcharged customers who damaged rental cars and were liable for repair charges. Hertz's computers were apparently programmed to generate two estimates — one for the actual cost of repairs at discount rates and one with the higher price which was sent to customers and insurers. According to the story, Hertz had already issued refunds of about US $3 million and it is estimated that they may have collected $13 million through these questionable practices.[22]

Brokerage houses and government departments are not immune to computer-based financial fraud. In 1986 a New York brokerage house decided to speed up the operation of its IBM system at peak hours by switching off the applications-level software that recorded information for the audit trail of each transaction. Knowing this, a crafty clerk selflessly volunteered for overtime, during which he sold the stock holdings of many customers and credited the money to 22 phony bank accounts he had set up. The money subsequently made its way to Switzerland and the clerk disappeared without trace. To this day, the company has no clear idea of who has lost what and has appealed to customers to come forward and provide details of their losses, but one report puts the total cost of the scam at US $28.8 million.[23] In a recent case in California, four employees of the Defense Contract Administration Services Region (DCASR) office in El Segundo were accused of having rigged the DCASR computer to issue a cheque for US $9.5 million to one of them individually as payment for a legitimate invoice from a legitimate contractor. A bank officer became suspicious

when the person trying to deposit the cheque wanted $600,000 in cash on the spot, and called the police.[24]

Computers are being used to steal goods by altering inventories and re-directing items, which can then be sold for cash. Computer records can be doctored to make it seem that goods have been damaged and disposed of, shipped to a customer but returned, or have simply gone missing. For example, an 18-year-old college student, Jerry Schneider, posed as a magazine reporter doing a story on Pacific Telephone's parts distribution system. In this way, Schneider learned that requests for parts came in via touch-tone phones and were delivered to any location. With a foolproof method for convincing the company's computer that his instructions were legitimate internal orders for parts, Schneider collected enormous quantities of parts at specific pick-up points, which he then sold through his new company, Creative Telephone. By the time Schneider was turned in by a Creative employee, over $1 million worth of phone equipment had gone missing from Pacific Telephone.[25]

Stealing information from computers is another growth industry. In a famous case some years ago, three computer operators attempted to sell *Encyclopaedia Britannica's* list of 2 million customers to a direct mail company, while in 1984 the Waterford Glass Company in Ireland had 25 computer discs stolen which held unique instructions for their glass-cutting machines. These probably made their way to counterfeiting factories in Asia.[26] Many a computer professional has been induced to part with commercial information which has value to a competitor company. Computerized mailing lists or lists of potential or actual customers can change hands for considerable sums of money. Some are acquired legitimately, some are not. In fact, database marketing is a rapidly expanding area — and it explains why consumers who have purchased a product or service from company A are then deluged with mailshots not only from company A, but also from companies X, Y and Z. This explains why the volume of junk mail has grown enormously, particularly to upscale customers or residents of upscale areas, and why postal services are once again becoming profitable — despite the predictions about paperless electronic mail replacing conventional surface mail.

Changing the information stored is an equally serious form of computer abuse. Recent cases have included the New York college students who paid other students doing vacation work for the college to change the grades on their college records and the alleged alteration of driving licence records at Britain's national Driver and Vehicle Licensing Centre (DVLC) in Swansea, South Wales, so as to erase traffic violations and other offences. This licence 'cleaning' service was allegedly on sale in London pubs and clubs.

There have also been cases of the deliberate destruction of information stored on computer as a form of commercial or even political sabotage. For example, in 1986 someone entered the Capitol Hill computer systems of two Republican congressmen, Ed Zschau of California and John

McCain of Arizona, and destroyed records of letters sent to constituents and mailing lists. One break-in took place over the lunch hour, the other late at night. The police were called in and they recommended better controls in future. But Rep. Ed Zschau said: "The entering of my computer was tantamount to someone breaking in to my office, taking my files and burning them . . . the police would be more concerned if this were a physical break-in. Because people don't see the files overturned or a pile of ashes outside the door, it doesn't seem as bad . . . But it is equally devastating."[27]

WHO ARE THE NEW COMPUTER CRIMINALS?

The theft of computer time, usually in the form of the unauthorized use of an employer's computer, is another grey area in which there are no easy answers. Unauthorized use may be technically theft of processing and storage power, yet most employers turn a blind eye to employees using the company's computers in moderation for such purposes as preparing individual tax returns or biorhythm charts or doing the mailing list for the local church. Unauthorized use rarely leads to prosecutions, but at some point such activity could be deemed excessive and therefore improper. Using company computers for financial gain such as private consulting work is clearly unethical, unless the employee's employment contract (for example, with a university) specifically allows for it. Sackings for this kind of computer abuse are not unheard of, although managers have to tread warily for fear of destroying staff morale.

The thorny problem of unauthorized use demonstrates how new possibilities opened up by new technologies can lead otherwise honest and loyal employees down the slippery slope to more serious misconduct and perhaps outright criminal behaviour. Indeed, from the studies that have been done by US computer crime specialists such as Donn Parker and Jay BloomBecker, a picture has emerged of the typical computer criminal as being a loyal, trusted employee, not necessarily possessing great computer expertise, who has been tempted, for instance, by the discovery of flaws in a computer system or loopholes in the controls monitoring his or her activity. Like most fraud, it is the opportunity more than anything else that seems to generate this kind of aberrant behaviour.

In a review of the major British studies of computer crime, Keith Hearnden found that the vast majority (80 per cent) of crimes involving computers were carried out by employees rather than outsiders. While 25 per cent of all crimes were carried out by managers or supervisors and 24 per cent by computer staff, a surprising 31 per cent were committed by lowly clerks and cashiers who had little in the way of technical skills. Moreover, nearly all computer criminals were first-time offenders who were motivated, says Hearnden, by greed, pressing financial worries and other personal problems such as alcohol or drug dependency. Love and sex can also provide a powerful stimulus: in one

case, a 23-year-old male bank clerk became infatuated with a 32-year-old woman. In trying to impress her with expensive gifts, travel and good living, he spent his way through £stg 23,000 stolen from four bank accounts, covering the theft by transferring cash through a computer from seventeen other accounts. He lost £stg 10,000 in casinos, trying to repay the money. By the time he was finally caught, the woman had deserted him![28]

There is a commonly held view that the typical computer criminal is something of a whiz kid, with highly developed computing skills and a compulsive desire to beat the system.[29] But Hearnden shows that the substance for this image is absent: "Not many crimes . . . demonstrate high technical ingenuity on the part of the perpetrator. Most exhibit an opportunistic exploitation of an inherent weakness in the computer system being used."[30] Ball states that most computer criminals " . . . tend to be relatively honest and in a position of trust; few would do anything to harm another human, and most do not consider their crime to be truly dishonest."[31] While Cornwall says we must understand the process by which "nice suburban people with jobs that give them access to sensitive information, systems and data are able to justify to themselves and their friends the committing of certain types of criminal act."[32]

Jay BloomBecker has listed eight motivations that can lie behind computer crimes. Some computer criminals, he says, think of crime as a game and see the computer environment as a kind of playpen for their own enjoyment. Others see computer systems as a land of opportunity where crime is easy, or a cookie jar which will readily solve pressing financial or personal problems. Some see computer and/or communication systems as a kind of soapbox for political expression, while others see them as a fairyland of unreality; a toolbox for tackling new crimes or modernizing traditional crimes; or a magic wand that can be made to do anything. Finally, crimes involving sabotage are often based on a view that the computer environment is a battle zone between management and alienated employees.[33] This latter perspective has found backing in a recent US survey which found, for instance, that 63 per cent of accountants and 75 per cent of computer professionals believed that employees steal because they feel frustrated or dissatisfied about some aspect of their job."[34] This could be an accurate reflection of the lack of autonomy, minimal job variety and poor management communications often endemic in computer work.

Others have surmized that the intellectual challenge of fooling a system plays an important role in motivating individuals to commit computer crimes, while still others have emphasized that computer crimes involve very little physical risk (unlike, for example, a bank hold-up); that computer crimes can be committed alone, without talkative associates, thus further reducing the risk of detection; and that (as in BloomBecker's fairyland) computer crimes can often appear not to be a criminal act — shuffling numbers around in a remote and abstract

way is not quite the same as handling gold bars or huge piles of paper money.[35]

IMPROVING COMPUTER SECURITY

The growth of computer crime calls for new kinds of security measures, measures which can be costly and can involve the use of computers. But improved security often lags behind the discovery of new crimes — computer security experts are forever trying to shut the stable door after the horse has bolted. Many companies are still extremely lax about computer security, often believing that computer frauds could never happen to them. Market researchers Computer Intelligence estimate that a mere 10 per cent of IBM mainframes had data security software in 1982 and this figure had only grown to 35 per cent by late 1988.[36] Yet vulnerability to computer break-ins has increased because the operations of so many companies — especially in the service sector — are now entirely dependent on computers. A good illustration of poor security is provided by the recent case of Herbert Zinn, a 17-year-old Chicago high school student who broke into AT&T's computer systems using a personal computer in his bedroom. Some reports say he copied software worth US $1 million, including material on AT&T computers at military bases. AT&T spokespersons blamed the lapse on employees who had not followed proper security procedures, rather than their security systems.[37]

"The problem with computer security is that everyone talks about it but not enough people do anything about it," says one New York analyst. Bank security and industrial security are well understood — it is comparatively easy to stop cash or materials going out of the door — but the need for computer security is less well appreciated and the task of protecting information is much more difficult. A 1988 study by the accountants Coopers and Lybrand, for example, found that only one out of a sample of 20 top European companies was "adequately secure." Most computer security experts lay the blame for poor security squarely at the door of top management. Often they do not understand their computer systems, they cannot be bothered, they do not wish to restrict ease of use, or they do not appreciate what their information is worth. But there are signs that the whole issue is now being taken more seriously: in 1987, for instance, the leading British banks and building societies launched a major review of their security measures.

Computer security can be greatly improved by the adoption of relatively simple, common-sense measures. Passwords allowing access to systems, for instance, can be made less obvious and memorable by avoiding such passwords as girlfriends names. Passwords should be issued only to the absolute minimum of people requiring access. A 1968 survey by British insurance broker Hogg Robinson found that the words chosen for passwords were mostly useless and very easy for colleagues to guess. Top of the list in Britain was 'Fred', followed by 'God', 'Pass'

and 'Genius' while many chose the names of their spouses or family pets. (In America, apparently, the favourite password is 'Love', closely followed by 'Sex' — indicative of an obsession which is absent in the British ratings.)[38]

A growing market is now developing for access-control software that closes password loopholes. This software restricts users — individually identified by passwords and codes — to only authorized functions, such as adding or deleting information, and they can no longer browse through parts of the system which they are not entitled to enter. One obvious and major limitation with access-control software, however, is that it does not protect a company against frauds committed by employees while going about their legitimate tasks — and as we have seen, a high proportion of computer crimes occur in this way.

Many companies are installing dial-back or black-box systems to protect their assets. When a user calls into a computer, a black box intercepts the call and asks for a password. The unit then disconnects the call, looks up the password in the directory and calls the user back at his or her listed telephone number: fraudsters calling from another number will be screened out. A large mainframe may have hundreds of 'ports' of entry from remote stations and each one has to be protected by these dial-back systems which can cost many hundreds of dollars.

Scrambling devices and encryption software are additional, expensive items which scramble messages for transmission so that only the legitimate recipient can understand them. Anyone tapping into say, a bank's communication line or eavesdropping on the electromagnetic waves emitted from a computer or piece of electronic equipment will pick up only a jumbled list of zeros and ones. Encryption devices in the form of digital signal processors (DSPs) are being used increasingly to scramble voice and data messages over telephone networks. Voice encryption is obviously vital in the military and in security agencies. However, even the best encryption codes can be broken — and so the codes have to be changed frequently — like every hour, for example. This is what the Pentagon sometimes does with very sensitive information. It is also spending US $200 million under its *Tempest* program to eliminate or muffle electromagnetic signals from machines used by the military, security agencies and defense contractors.

Audit control software packages are also available which can monitor transactions or the use of a computer. These enable auditors to trace and identify any operator who gains access to the system and when this occurred, such as after-hours. Audits can also highlight an abnormal number of correction entries, which often indicates the trial-and-error approach of fraudulent activity. But a major problem is that the demand for auditors with computer skills is high, and there are not enough who are capable of outsmarting crooked computer personnel.

Computers are also being used increasingly in the fight against crime, both conventional crime and computer-based crime. A British company has developed software which enables a computer to browse through

vast amounts of financial data looking for possible connections which might indicate insider trading or foreign exchange fraud. A similar system is at work on the New York Stock Exchange. A British firm of management consultants used computers to search for illegal multiple share applications made during the UK government's privatization program. An Australian insurance company has developed a system which searches through its claims files attempting to associate random items of information about the company's customers. It is credited with unmasking scores of fraudulent injury claims.[39] The vast amounts of so-called transactional information — records of phone calls, air travel, credit card purchases etc — stored on computers are providing a fertile field for crime-busters. One spectacular recent example was the discovery that all the messages passed between Colonel Oliver North and his collaborators in the illegal sale of arms to Iran and the illegal transmission of aid to the Contras in Nicaragua were faithfully recorded on a local area network they used, IBM's Professional Office Systems Network (PROFS). So much for covert action.

Another weapon in the fight against crime is Biometrics, or the digitizing of biological characteristics. These include not only fingerprints, but also voices, the veins on the back of the hand and the pattern of blood vessels in the retina. Police forces all over the world are now using computerized fingerprint identification systems which have a remarkable record of cracking hitherto unsolved cases, while fingerprint scanning devices are now being used to control access to computer rooms, to bank vaults and to military bases. An Oregon company is marketing a retinal scanner rather like the one used in the James Bond film *Never Say Never Again*.

In conclusion, we would argue that improving computer security is a management problem rather than a technical problem. Careful vetting of employees in the first place can, of course, be a great help. Then sensible security procedures, starting with rules for password usage and including sophisticated access-control systems, should be formulated and rigidly enforced. Obviously the latest technology should be used where possible, but it is no guarantee of total security. Ultimately the best security might be to manage employees effectively, because in the final analysis even the best security systems cannot stop the determined fraudster. Employers must be able to rely on the goodwill of their employees and that goodwill needs to be earned by sensitive and intelligent managers.

NOTES AND REFERENCES

1. From reports in *Software Engineer Notes,* 13, 2, April 1988, p. 5 and *The Australian,* 24 May 1988.
2. Jay S. Albanese, 'Tomorrow's thieves', *The Futurist,* September-October, 1988, p. 25 and Hugo Cornwall, *Datatheft: Computer Fraud, Industrial Espionage and Information Crime,* Heinemann, London, 1987, p. xi.

3. August Bequai, *Technocrimes: the Computerization of Crime and Terrorism,* Lexington Books, Lexington, MA, 1987.
4. Albanese, *op. cit.,* and Tom Forester, *High-Tech Society,* Basil Blackwell, Oxford, UK and MIT Press, Cambridge, MA, 1987, pp. 219-22; 261.
5. *The New York Times News Service,* 27 March 1987, cited in *Software Engineering Notes,* 12, No. 2, April 1987, pp. 8-9.
6. *Communications Week* (USA), 31 August 1987.
7. R. Doswell and G.L. Simmons, *Fraud and Abuse of IT Systems,* National Computing Centre, Manchester, UK, 1986, pp. 32-5.
8. *The Australian,* 1 September 1987.
9. *The Financial Times,* London, 22 October 1984.
10. *PC Week,* 4, 21, 26 May 1987 and *Business Week,* 1 August 1988, p. 51.
11. *The Australian,* 5 January 1988 and 26 April 1988; *The Independent,* London, 30 October 1986.
12. Cornwall, *op. cit.,* p. 46.
13. *ibid.,* p. 342.
14. *ibid.,* p. xiii. See also Jeffrey A. Hoffer and Detmar W. Straub, 'The 9 to 5 Underground: are you policing computer crimes?', *Sloan Management Review,* Summer 1989, pp. 35-43.
15. *The Financial Times,* London, 3 January 1986 and *The Australian,* 1 September 1987.
16. *The Australian,* 11 July 1988 and *Information Week,* 11 July 1988, cited in *Software Engineering Notes,* 13, 3, July 1988, p. 10.
17. *The Financial Times,* London, 2 September 1986 and *The Australian,* 15 September 1987; *Software Engineering Notes,* 13, 3, July 1988, p. 10.
18. *Computer News* (UK), 15 January 1987.
19. *The Wall Street Journal,* 18 May 1987, cited in *Software Engineering Notes,* 12, 3, July 1987, p. 11; and *Computing Australia,* 10 August 1987.
20. *The Chicago Tribune,* 15 August 1986, cited in *Software Engineering Notes,* 11, 5, October 1986, pp 15-6; and 'Are ATMs easy targets for crooks?', *Business Week,* 6 March 1989.
21. Leslie D. Ball, 'Computer Crime', in Tom Forester (ed.), *The Information Technology Revolution,* Basil Blackwell, Oxford, UK, and MIT Press, Cambridge, MA, 1985, p. 534, reprinted from *Technology Review,* April 1982.
22. *Software Engineering Notes,* 13, 2, April 1988.
23. *Digital Review,* 6 April 1987, p. 75.
24. *Evening Outlook,* Santa Monica, CA, 4 February 1988.
25. Ball, *op. cit.,* pp. 534-5.
26. Cornwall, *op. cit.,* p. 102.
27. *The New York Times News Service,* 21 March 1986, cited in *Software Engineering Notes,* 11, 2, April 1986, p. 15.
28. Keith Hearnden, 'Computer Criminals are Human, too', in Tom Forester (ed.), *Computers in the Human Context,* Basil Blackwell, Oxford, UK and MIT Press, Cambridge, MA, 1989, pp. 415-26.
29. 'Technological Ability Not Needed to Commit Crime', Australian Associated Press report in *The Australian,* 14 March 1989.
30. *ibid.,* p. 420.
31. *ibid.,* p. 536.
32. Cornwall, *op. cit.,* p. 135.
33. Jay BloomBecker, 'Introduction to Computer Crime', in J.H. Finch and E.G. Dougall (eds), *Computer Security: A Global Challenge,* Elsevier, North-Holland, 1984.
34. Hearnden, op. cit., pp. 420-1.
35. Other useful taxonomies of computer crime have been provided by Donn B. Parker, *Fighting Computer Crime,* Scribner's, New York, 1983 and Detmar W. Straub and Cathy Spatz Widom, 'Deviancy By Bits and Bytes: Computer Abusers and Control Measures' in J.H. Finch and E.G.Dougall (eds), *op. cit.*
36. Katherine Hafner *et al.,* 'Is Your Computer Secure?', *Business Week,* 1 August 1988.
37. *The Washington Post,* 18 September 1988 and *The Chicago Tribune,* 17 September

1987, cited in *Software Engineering Notes,* 12, 4, October 1987, p.14.

38. Michael Cross, 'How Fred Lets the Fraudsters In', *The Independent,* London, 30 October 1986.
39. *The Australian,* 14-15 March, 1987; *The Financial Times,* London, 24 July 1986; *Computing Australia,* 15 June 1987; and *New Scientist,* 20 November 1986.