The Parliamentary and Scientific Committee

INFORMATION FOR MEMBERS

From the

Parliamentary Office of Science and Technology

Briefing Note

9

February 1990

Computer Misuse

Misuse of computers ranging from the mischievous to the criminal, has excited Parliamentary interest in the last year, culminating in Michael Colvin's Computer Misuse Bill, due for second reading in the House of Commons on 9 February.

This briefing note describes how computers can be 'misused', the damage that may or may not result, and the issues raised.

WHY ARE COMPUTERS VULNERABLE?

Society today is more and more dependent on computers; we use them to store and process accounts, personal and medical records, credit cards, criminal records, business plans, inventories. Their role in defence is crucial. They organise fund transfers between banks, companies and countries, insurance schedules, airline reservations and almost everything one can think of. Some uses are critical to public safety, e.g. blind landing systems for aircraft, railway signalling systems, safety shut-down systems, weather forecasting. The list is endless. The information required for all these tasks is stored on databases to which, if computers are to be of any use, access must be readily available.

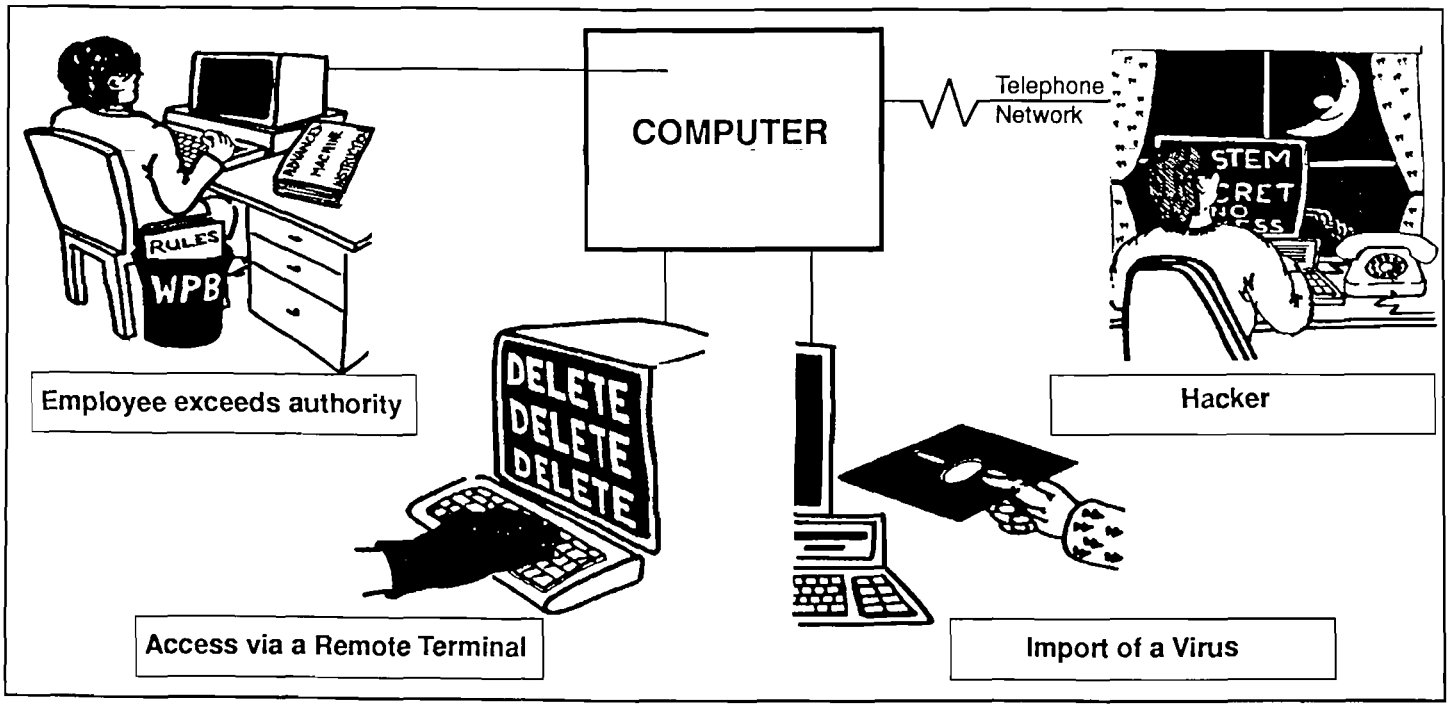
Many computer systems thus operate via networks of terminals and datalinks, which use telephone connections employing either dedicated links or public telephone systems. Such systems need to provide ready access to authorised users, whether they are working on a terminal directly linked to the computer or connected via the telephone from a remote location. Security measures such as passwords and keys are widely used to restrict access to authorised users only, but there are many points of access which can be probed by someone attempting to access the system for purposes ranging from inquisitiveness, through mischievous vandalism to criminal fraud, blackmail or damage. Smaller computers, including the personal computer, can also be vulnerable whenever connected to another system via the telephone, or when data or programs are exchanged with other users. The figure below illustrates some of these points of vulnerability.

WHAT IS COMPUTER MISUSE?

This term covers a number of different activities by both 'insiders' (people who have legitimate access to a computer system) and 'outsiders' (those who don't).

Unauthorised Access

Hacking refers to 'outsiders' gaining unauthorised access to a computer system, regardless of purpose. Hackers generally operate from a simple personal computer and a 'modem' connecting it to the target computer via



the public telephone system. Once connected, the hacker is faced with getting past one or more protective measures built into the computer system. If access is gained, the hacker can read, modify, or delete data in the system, and may also seek to modify the computer programs which control the computer's operations.

'Insiders' can also gain unauthorised access to a system or parts of it. For instance, someone authorised only to use accounts files could attempt to access personnel or confidential business information on different parts of the same computer system.

Viruses etc.

While some hackers only observe information, others modify data or programs, by inserting their own sets of instructions. Such modifications can also be made by 'insiders' deliberately, or unknowingly, by using data or programs from other sources which already contain the relevant instructions. These can take several forms and have attracted their own popular names of 'viruses', 'trojan horses', 'logic bombs', 'worms' etc.

Once loaded into a computer (e.g. via a floppy disc or a telephone transmission), some programs (viruses) proliferate by copying themselves, using up the computer's memory and progressively overwriting the data stored in it. They can copy themselves to other programs, thus transmitting the virus whenever the infected machine shares data or programs with another machine. The originator has no control over how far or how fast the virus will spread - some viruses have infected thousands of machines across national boundaries due to the extensive interlinking of international computer systems.

A variant of the virus is the 'logic or time bomb', whose actions are triggered by some pre-planned event. Some have been initiated on reaching a date such as Friday 13, or when a certain action or logic is activated in the program that has been infected. 'Worms', like viruses, reproduce themselves, but overwrite programs and progressively make nonsense of them.

'Trojan Horses', as their name implies, may be inserted to collect passwords used in the system, or other functions designed to facilitate unauthorised access at a later date. Alternatively they may be an apparently useful program which contains a hidden and generally malicious set of instructions.

Viruses etc. have two components. The first is the instruction that causes the infection or transmission and triggers the activation of the program. The second provides the set of instructions that determines what it will do once triggered. Most common activities are:

- To delete or alter data
- To destroy hardware or machinery (e.g. by adjusting the speed of some video or disc drive functions, causing overheating);
- To use up available memory;
- Displaying messages;
- Disabling the keyboard or monitor, preventing the user from communicating or using the computer;
- Engaging in fruitless tasks, preventing the computer from carrying out its legitimate instructions.

Some types of misuse require only minimal expertise, while others can present a challenge to even the highly skilled. Some examples of computer viruses and other forms of misuse in action are listed in the box.

HOW TO PROTECT AGAINST MISUSE

Prevention

Protection against unauthorised access is normally achieved by passwords, but these can be trivial and easily broken. Systems with many authorised users also find it difficult to keep passwords secret and they may become widely known and even disseminated by hackers via their own network of electronic 'bulletin boards'. More security-conscious installations may automatically alert operators to repeated attempts at a password. Other systems may insist on calling back the caller to ensure verification. All, however, add costs and barriers to access by legitimate users, and experience has shown that even more secure systems can still be entered by expert, determined or just plain lucky hackers[1], or those with some inside knowledge.

Since they can also be transmitted unknowingly through normal, legitimate computer operations, viruses present a different problem to simple hacking. There is currently no known technical way of eliminating the possibility of infection by computer viruses, but there are many 'good practices' which can reduce significantly the danger of such infection - for instance by keeping uninfected backups of data or programs, and by validating the source of all data and software (illegally copied or 'pirated' software could be one source).

Detection

Once infected, viruses can be easy or difficult to detect, depending on their sophistication. Once the instructions contained in the virus are triggered, it may be obvious that a virus has been activated (for instance, if files are deleted). On the other hand, some viruses may contain instructions to corrupt data files with misleading or irrelevant information rather than delete them entirely, when detection may be less straight-forward.

1. **Because of this, action is being taken in the UK to ensure that safety-critical systems are never accessible from public networks.**

SOME EXAMPLES OF COMPUTER MISUSE

Hacking

- UK hacker accessed sensitive car design records via a university network connected to the company system.
- UK National Police Computer accessed and criminal records interchanged.
- A life support system in a French hospital intensive care unit turned off.
- German hackers allegedly recruited by the KGB to enter US Research establishment networks.
- A major company detected that a safety-critical system had been accessed by a hacker and had to undertake expensive checking and replacement of programs and data.
- Various acts of disruption, e.g. misdirecting mail-shots, false orders for holidays in a travel agency network, a university system entered with loss of 2 years research results.
- Telephone company admits that a sizeable number of hackers have been obtaining free telephone calls at the expense of other users.

Viruses etc.

- A West German student attached a Christmas message to a virus which swamped an international IBM network.
- The West German 'CHAOS' computer club planted logic bombs in a US NASA Network.
- 'Trojan Horse' disseminated via 15,000 free AIDS Information discs. Program disables computer and demands payment to Panama box number for restoration.
- Widespread infection of PC's by viruses such as the 'Brain', 'PLO', 'Lehigh', 'Fu Man Chu', the 'Italian'. Some distracting (e.g. ball bouncing on screen), others disabling (causes all screen characters to fall into a heap). One originated in Pakistan yet infected US computers.
- Royal National Institute for the Blind system infected by a 'Friday 13' virus and records lost.
- An employee inserted a 'logic bomb' that would erase all the company's computer records if they sacked him.
- A student circulated a virus which put 6,000 US Government and University work stations out of action by attacking their UNIX operating systems. He has been convicted under the US Computer Abuse Law.

Ideally, detection should allow identification of a virus before it is activated, so that it can be eliminated before damage occurs. Unfortunately, while some specific viruses can be detected, each one is different and general detection methods are cumbersome and difficult.

Treatment

Most systems record attempts to gain access, and require an identification for successful callers in order to record the use made of the computer's facilities. Careless hackers can be identified by their repeated attempts at passwords which may allow their call to be identified and traced. More experienced hackers however, by using complex diversionary routes to attack, make detection and tracing very difficult.

Once an unauthorised modification has been discovered in the system, various treatment strategies can be used, although they are specific to each problem. Certain viruses can be dealt with by anti-viral commercial software packages, with names, appropriately, like 'Flu-shot'. An antidote to the AIDS information virus (see Box) was developed. On the other hand, some can only be treated by rather drastic 'disinfection' which involves the destruction of floppy discs or regeneration of the computer's main hard storage discs with the loss of all data. This can be very expensive and may involve the permanent loss of information.

Where hackers have left traces of attempts to gain access to the system, the computer owner may be unsure of whether anything has been changed as a result. In view of the critical importance of many systems, days or weeks of very costly work may be then required to check that nothing is amiss - either by elaborate checking or by replacing all data and programs with versions stored before the hacking took place.

ISSUES

How Serious is Computer Misuse?

Some descriptions have characterised hacking as a pastime for intelligent teenagers, pitting their wits against 'authority'. Others, however, emphasise that even 'innocent' hacking can cause much damage inadvertently, and that increasing use has been made of hacking for criminal or malicious purposes.

The specific events in the box illustrate the damage that can be caused to certain organisations - the loss of personnel or member records, major systems failure, etc. Because computer misuse may not always be detected or reported, it is difficult to estimate its prevalence and the amount of damage resulting. The IBM PC User group is currently receiving notice of 4-6 new cases of misuse per day. The Information Technology Minister has reported 270 verified cases of computer

misuse from 1985-9 comprising the categories of unauthorised access (42%), fraud (37%) and damage (20%).

The French insurance industry estimated that deliberate acts (fraud, sabotage, theft, disclosure of data and programs etc.) caused French industry losses of around £300m in 1986. Based on this, damage to UK businesses from all forms of computer misuse has been estimated at £400 to £1bn annually. Studies have shown that most of these losses resulted from insiders' activities rather than unauthorised access by 'outsiders'.

Should there be Legal Sanctions?

The main issue is over whether the law covering computer misuse should be extended. A number of different points have been made in the debate:

Adequacy of Current Law. Some argue that the current law already covers the use of computers for several criminal ends (e.g. fraud, theft, damage) covering the main areas of financial loss, and do not favour extending the law to cover attempts at unauthorised access to a computer *per se*. They see analogies in the law of trespass where entering a room and examining the contents of an unlocked filing cabinet is not a criminal offence.

Others however, point out that hacking (even when lacking any destructive or criminal intent) results in a lack of confidence in the computer system, denies the system to its authorised users, and involves costs in checking whether the system has been affected. Passwords and other computer security are seen as the electronic equivalent of locks on doors, filing cabinets etc., and attempts to thwart computer security as more analogous to breaking and entering the target organisation. Moreover it has been pointed out that hackers have not always foreseen the effects of their actions and have caused damage far in excess of their expectations.

Computer Security. Some regard improved computer security as the preferred response to the threat of misuse and point out that many examples of misuse were only possible due to lax security. They question whether reliance on the law may encourage such laxness. Others point out that security can never be perfect and that installing extra measures not justified for other reasons, adds considerably to costs. It also reduces the effectiveness of systems which depend on the ease and extent of access provided to authorised users.

Protection of Information. Another element in the debate accepts the need to strengthen the law to deter computer misuse, but differs over the means of so doing. Some have pointed out that better legal protection of information as such may allow computer misuse to be controlled, since most cases involve unauthorised access to, or interference with, information held on computers. In response, it has been pointed out that there is no consensus on the value of information or the ownership rights; changes to the law on information would also have very broad ramifications. It is thus argued that specific laws targetted at computer misuse are justified.

The legal position on computer misuse has been reviewed in many countries since the problems first surfaced some years ago, and laws have been enacted in six EC States as well as the USA and Canada.

In the UK, the arguments have been considered at length by the Law Commission[2] who recommended changes in the law which are the basis for the Computer Misuse Bill. This covers both unauthorised access and unauthorised modification of computer material. The Bill is supported by the Department of Trade and Industry who have assisted in its preparation.

An International Dimension

Due to the international nature of many computer networks, cases of computer misuse may originate in one country but be transmitted to other countries via the network. One hacker is believed to have penetrated, from his base in the UK, research establishment computer systems in the UK, Germany, Italy, USA, and the Netherlands.

This raises the issue of whether legal sanctions should be applied at the point at which the misuse originated, the point at which the effects occurred, or at either location. The Bill contains provisions that follow the Law Commission's recommendation that Courts should have jurisdiction over computer misuse either originating from, or directed against computers in this country.

FURTHER READING

Additional details and background information are available from POST, 2 Little Smith St., London SW1P 3DL, tel: 01-222-3912 or 01-222-7085.

2. Criminal Law: Computer Misuse (1989). Law Commission No 186. Cm 819.