DATA SECURITY PART 1: PROBLEMS AND LEGAL REMEDIES

National data protection laws demand adequate security for protecting personal data from improper access and transfer to other parties. Firstly, in this issue, Norman Jackson, UK Computer Security Manager at Digital Equipment examines the scope of the problem and how data protection laws do not give legal remedies against hackers, those who break into data files.

In our next issue he will provide guidance on how to implement the data protection laws' requirements that data users and controllers should protect the data they collect. Only a few countries, such as Norway, offer help on this issue (see page 25).

The Problem

A 25-year old hacker, Kevin Mitnick, is currently in custody in Los Angeles, awaiting trial on various charges of gaining unauthorised entry into a number of computers, including one owned by Leeds University in the UK.

Mitnick was only 17 when he committed his first offence - breaking into Pacific Bell's computer system, secretly channelling his own system via a pay phone, to alter telephone bills, penetrating other computers and (inadvertently) destroying $200,000 worth of data belonging to a San Francisco corporation. A juvenile court judge at the time sentenced Mitnick to six months in youth custody.

Shortly after his release, Mitnick's probation officer found that her phone had been disconnected, although the phone company had no record of this; a judge's credit record at TRW Incorporated was inexplicably altered; police computer files on the case were accessed from outside. Later, he was convicted in Santa Cruz of stealing software under development by Microport Systems. There is, however, no record of the conviction in Santa Cruz's computer files!

In the current case, the US magistrate took the unusual step of ordering Mitnick to be held without bail, ruling that when armed with a keyboard, he posed a "danger to the community."

* * * * * * * * *

Last October, Edward Austin Singh was arrested in the UK on a burglary charge involving Surrey University, whose terminals he used without authority as a means of carrying out widespread hacking, via the UK Universities' Joint Academic Network.

During the investigation into Singh's activities, it was alleged that he broke into more than 200 UK and overseas computers, including those belonging to the US banks Chase Manhattan, Citicorp, and Security Pacific; military networks such as Ptarmigan (UK) and Milnet (US); the US Defense Nuclear Agency and the UK Admiralty Surface Weapons Research Establishment. Singh is quoted as saying, "When I was arrested, I had documentation out of at least 250 systems worldwide. Geographical constraints are irrelevant in the context of hacking." Following a caution, Singh was released without charge.

* * * * * * * * *

In Germany, a hacker enthusiasts' organisation, the Chaos Computer Club, enjoys a membership of hundreds and are so organised as to hold an annual conference. Another German group, the VAXbusters, specialises in attempting to break into systems manufactured by Digital Equipment, as the the name of the organisation implies.

* * * * * * * * *

During recent months, outbreaks of new computer viruses have reached almost epidemic proportions. Many of these (carrying such names as "Italian," "nVIR," "Vienna," "Marijuana" and "Friday the Thirteenth") have been reported in the popular press. Whilst some of these are innocuous, several can cause the complete contents of a PC's hard disk to be over-written.

Up to now the problem of viruses has largely been confined to personal computers, which have become infected through the inadvertent loading of infected floppy disks. The rapid growth in networking, however, coupled with the hacker's endless desire for new fields to conquer, means that no system owner can realistically feel safe from attack.

* * * * * * * * *

In May 1986, Dean Talboys, a former programmer employed by Dixons, the photographic and electronics retail chain, was charged with accidentally crashing the company's head office computer system by trying to flash a goodbye message on terminal screens. The defendant, who pleaded guilty, was discharged for one year and ordered to pay Dixons £1,000 compensation.

* * * * * * * * *

The incidents above, which are illustrative of many similar cases reported over the last few years, are quoted in order to show that:-

a) There is is a rapid increase in computer misuse.

b) The problem is a global one.

c) The skills levels of computer "criminals" are increasing at a far greater rate than those of system owners, managers and users.

d) Symptoms of hacking, viruses and other forms of computer abuse are becoming increasingly difficult to detect.

e) Legislation to deal with the problem is inconsistent from country to country.

f) In the UK, there is no legal remedy against hacking, viruses or any other form of computer misuse, unless the victim suffers damage as a direct result of the activity.

The Legal Position Worldwide

Many countries now provide comprehensive computer crime legislation. These include, for example: Austria (see PL&B Nov '88 p.2), Canada (see PL&B August '88 p.19), Denmark, France, Norway, Switzerland, USA (In addition to a federal law, some individual States have computer crime legislation) and West Germany. Other countries are in the process of drafting computer crime bills.

The Legal Position in the UK

As stated earlier, there is currently no law against hacking, or any other form of computer misuse, in the UK.

The Scottish Law Commission (SLC) undertook an extensive review of the problem about two years ago (see PL&B February '88 p.19), inviting views from many representative bodies as well as individuals. In its Report on Computer Crime, presented to Parliament in July 1987, the SLC strongly advocated a new law against hacking (or unauthorised access to computers).

However, it considered that other types of computer misuse (e.g. criminal damage and fraud) could adequately be dealt with under existing laws. But the outcome of recent trials, including the famous "Prestel" case (R. v. Gold and Schifreen) has disproved this theory, mainly because information as such is not recognised as having a legal value, or title.

To date, no Parliamentary action has been taken on the Scottish Law Commission Report, but growing demands for action have led the Law Commission (England and Wales) to also seek views. In its Green Paper ("Computer Misuse"), completed in August 1988, the Law Commission considers at some length all of the various "offences" against computers. Like the Scottish Law Commission, it argues that existing laws can adequately cope with most types of computer misuse. It singles out hacking as the sole form of misuse for which a new law (making hacking a criminal offence) might be considered. After a lengthy argument on the advantages and disavantages of such a law, the English Law Commission is inconclusive in its recommendations. However, "Computer Misuse" is only a consultative document and it is possible that, given a weighty response in favour, the Law Commission will recommend a new crime of hacking in its final report to Parliament.

The main law in the UK which addresses computer usage is the Data Protection Act. Ironically however, whereas the Data Protection Act imposes penalties on legally-recognised data users who misuse personal data, it has no powers to deal with hackers - who may gain unauthorised access to, unlawfully disclose, alter, and even destroy, personal data.

In conclusion, therefore, computer managers and users in the UK cannot depend on a current legal remedy if they become victims of hacking or other forms of computer misuse. Furthermore, there is no prospect of new legislation being passed in the near future.

Given this situation, and with the incidence of computer misuse growing by the day, the effective protection of information by data users themselves is essential. In the next issue of Privacy Laws & Business I shall be discussing the formation of security policies and suggesting various countermeasures and techniques available to computer managers and users.