ABC of Computing

J PAYTON
A J ASBURY

COMPUTER SECURITY

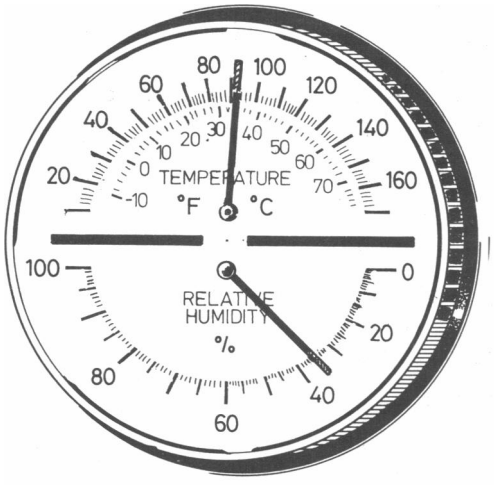
Environmental hazards

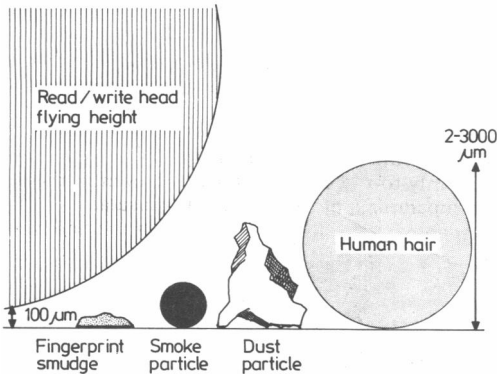
Accidental damage and malfunctions

Unauthorised access to data

Computer security is concerned with protecting both the computer program and data from corruption and unauthorised access. As such it covers all aspects of computing and all sizes of computer from the multimillion pound mainframe to the desk top microcomputer. A computer system is exposed to the three main types of risks shown in the box.

Environmental hazards



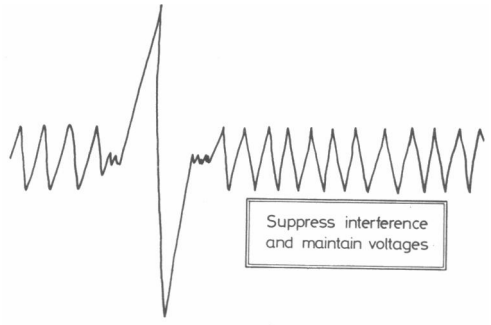


Computers are a combination of sophisticated electronics and precision engineering and they need a controlled environment. Mainframe computers are housed in special rooms and powered from a specially stabilised electricity supply. The air in the room is highly filtered, and temperature and humidity are controlled. A considerable amount of air cooling plant is required to extract the heat generated inside the computer itself. As computers have decreased in size and become more available, these problems have been tackled by the manufacturers, and the modern microcomputer can now work in an office environment. The amount of heat produced by a computer is being reduced with each generation of components and the electronics will continue to work up to a room temperature that the human operator will find acceptable. Nevertheless, an increase in temperature will still result in more frequent faults and the aim should be to keep the room temperature below 70°F when the computer is operating.

The problem of airborne dust, which is the main threat to magnetic disks, has been tackled in two ways for microcomputers. The high capacity fixed disks are now built in a completely sealed container which cannot be contaminated by dust. Such disk drives are known as Winchester disks. Floppy disks which are used on microcomputers are not as sensitive to dust as the removable disks used on bigger computers because the speed of rotation is much lower. Some larger microcomputer systems have disc drives with one sealed and one removable hard disc. Although the removable discs have a protective case they are vulnerable to dust and to mechanical stresses.

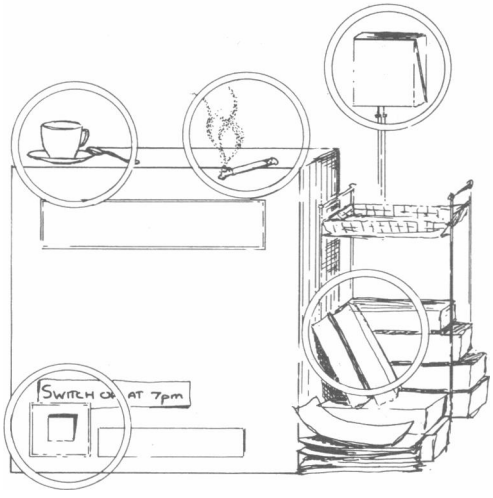
The electricity supply in Great Britain is a nominal 240 volts alternating current, and apart from occasional power cuts any long term variation from this figure can be accepted by most small computers. Nevertheless, there are two types of interference that can come through the electricity supply which may cause severe trouble to the computer. How serious these are depends very much where the machine is sited and what activities the neighbours engage in.

The first problem is the occurrence of very short (10 microsecond) high voltage spikes superimposed on the mains supply. These can be fed into the logic circuits and persuade the computer, for example, that it has just read a



"1" from memory rather than an "0." The two main causes of this type of interference are the switching off of an induction load such as a lift motor or the use of the older type of light dimmer or variable speed controller for motors. Fortunately the use of a simple mains filter will remove all but the most stubborn case of this type.

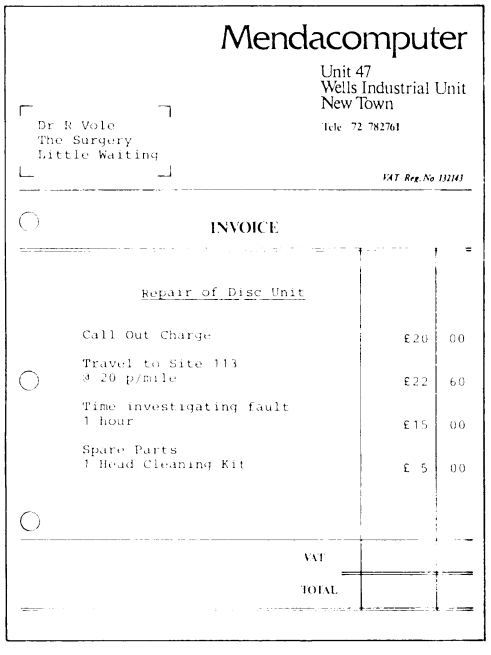
The second type of interference is caused when the voltage drops to a low level, even if this is only for 20 milliseconds. This is more common either in remote rural areas or where the supply system is near overload at any point in its passage from the generating station to the point of use. This effect can be noted when, say, the switching on of a kettle or heater results in a noticeable dimming of the lights. The cure for this problem can be more expensive and consists of a constant voltage transformer. On all but the smallest computer these become quite expensive and, if you have this problem — for example, in a general practice — computer specialist advice is most probably needed.



All these problems may seem distant to a home computer user who does not normally require reliable storage of vast volumes of data, but to the general practitioner with a newly installed microcomputer this is important. Though microcomputers work well in offices, there is not the same discipline in managing the computer environment as there is with a mainframe. A secretary using a computer in a general practitioner's surgery may simply put her coffee on the shelf above the computer, something she has always done. One day, sooner or later, coffee will be spilt into the computer, which will inevitably cause a system failure. Unfortunately the effects can be even greater because a failing microcomputer can easily send out random signals, which if received by an active disk unit may corrupt thousands of patient records.

Electrical interference problems are a much greater problem for the GP in his surgery as many microcomputers are inadequately protected. The carpenter working next door with an electric drill, or the cleaner with her vacuum cleaner may both produce spectacular corruption of computer files.

Accidental damage and malfunctions



Mendacomputer

Unit 47
Wells Industrial Unit
New Town

Tele 72 782761

Dr R Vole
The Surgery
Little Wailing

VAT Reg No 132143

INVOICE

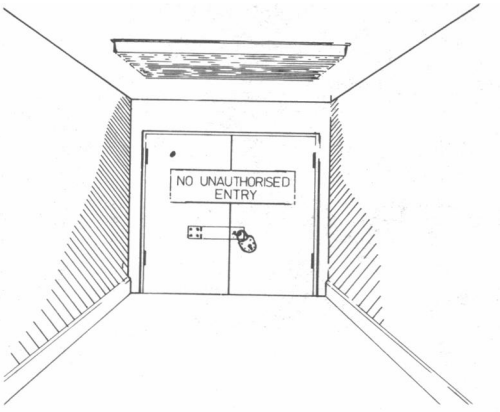
Repair of Disc Unit		
Call Out Charge	£20	00
Travel to Site 113 @ 20 p/mile	£22	60
Time investigating fault 1 hour	£15	00
Spare Parts 1 Head Cleaning Kit	£ 5	00
VAT		
TOTAL		

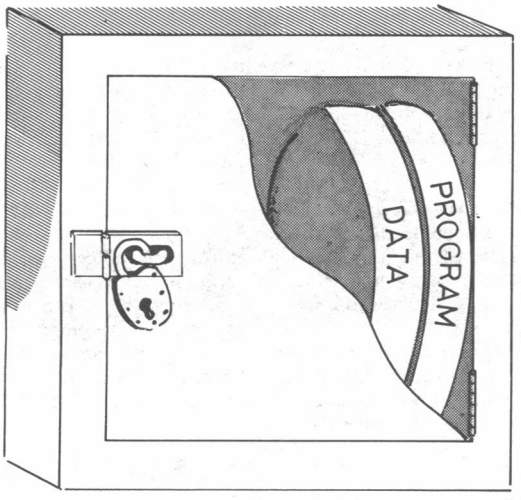
Computers are relatively immune to accidental damage arising from normal use and are not particularly hazardous themselves. The many smoke detectors present in a large computer installation are more a reflection of the value of the equipment and its importance to an organisation than an indication of a high inbuilt risk. In the case of microcomputers the precautions are simple and obvious—for example, always switch off after use and control the accumulation of paper near the machine. Unless you are an expert never remove the cover, particularly that of a visual display unit, which contains lethal voltages. Ensure that all ventilation holes are kept free of obstruction.

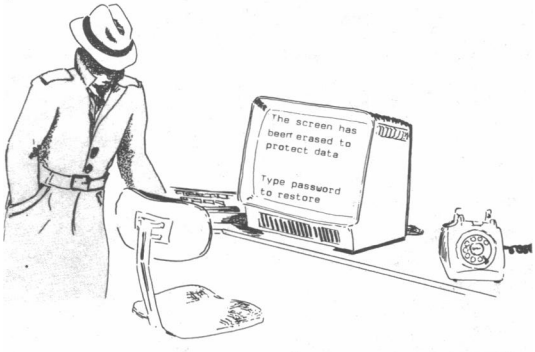
Computers may fail for two reasons, either because the electronics develop a fault or because the peripheral devices and the storage media fail. The modern computer is electronically extremely reliable and electronic faults in microcomputers are rare. Nevertheless, because the repair of such a fault is beyond the capability of the user he should always have either a maintenance contract, insurance cover, or a budget for the occasional call of an engineer on a time and materials basis. This can be an expensive addition to the general practitioner's running expenses, especially if the service engineer's charges for time are from the moment he leaves the depot some 50 miles away.

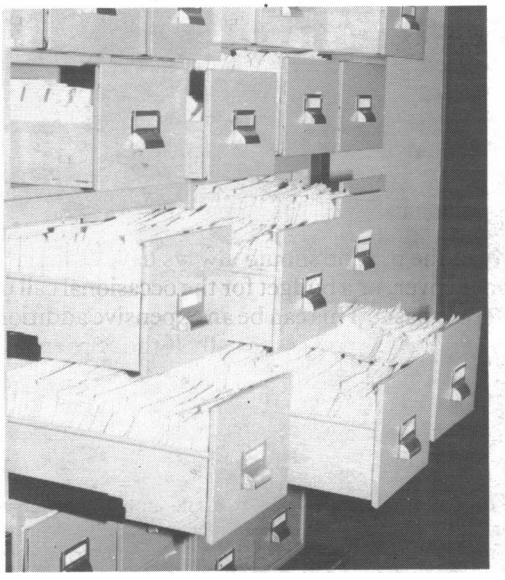
Faults on peripheral devices are more common, and most of them are beyond the user's ability to rectify. On floppy disks the most common cause of error is not a fault on the disk drive but damage to the actual disk itself. This is caused by dust particles or the break up of the oxide covering on the disk.

Intentional or accidental unauthorised access to data









Confidentiality is often considered as though it were a separate subject from security. It is only one aspect of security and without an overall security policy it is impossible to impose confidentiality.

The first principle is to control access to both the computer and the magnetic media that hold the data. This control must be applied both during the normal working day and also when the owner of the data is absent. The sensitivity of the data will determine the extent to which these precautions are taken, but the rule should be to apply at least the level of protection that you would apply to the same data if it were written. Although it is not so easy to read a magnetic disk as it is to read a case file, the fact that a disk may contain many thousands of records which can be searched quickly makes the problem more severe. The easiest place for someone to read a disk of your records is on your computer using your programs. Every program that processes sensitive data should ask the operator for a password to ensure he has the authority to run that program. On more sensitive data more than one level of password may be justified.

To guard against breaches of confidentiality when you are called to the telephone after you have logged on to the computer, the machine should put itself in a state where it needs the password again and cleans any possibly sensitive information from the screen if it is not used for a certain length of time. If somebody obtains a copy of your data and a copy of your program, even though these are protected by a password, he has all the time he needs on his own computer to break your password; this will be very easy if you have used a friendly language such as Basic, particularly if you have documented the program well. One answer is the separation of programs and data. Given only the data the intruder may have access to your data, but he will not know what it means as he cannot arrange it in a meaningful way. As an additional safety measure the data may be encoded.

Where computers are connected to terminals the opportunity for interception of data is increased as both the remote terminal and the communication link can be used to gain access to data. Data encryption devices are being developed by the industry which can be used to code data in transmission so that even if it is intercepted it cannot be understood.

The proliferation of computers has led to considerable and reasonable worry about protecting data. Interconnection of computers, already extensive, could in future allow the assembly of data files on individuals and with it concern about the correctness of information and rights of access. Legislation is currently being considered which will control data bases, but it is very hard to legislate in this area.

The legislation is likely to enable people on whom data is held to have the right of access to personal data held in registered systems and to have errors corrected. There will be special exemptions for medical data, where access may be through a clinician to protect the existing status of patients and their medical records. Also likely to be exempted are those areas judged relevant to national security. For those systems which have to register and provide client access there will obviously be an increase in operational costs.

One of the key problems in computer security as a whole is the human user. It is the user who leaves sensitive printed information on his desk overnight before he resumes data input in the morning. Once information is stored on a computer it is safe and virtually incomprehensible until a careless user allows access to the data. It is fashionable to blame inanimate computers for all sorts of problems, but the computer only magnifies faults that are human.

Security and confidentiality both depend on risk analysis, the estimation of the possibility of damage to the integrity of an installation, the cost of such damage and the cost of preventing or minimising such damage. As the intelligence services have found, no computer system is absolutely secure, but most computers are more secure than a filing cabinet in an unprotected office.

Mr J Payton, BSC, is regional computer services officer for Trent RHA and chairman of the NHS Microclub, and Dr A J Asbury, PHD, FFARCS, is a lecturer in anaesthetics, University of Sheffield. A book of this series will be published later this autumn.