DATA SECURITY PART 2: PRACTICAL STEPS TO PROTECTION

In Data Security Part 1: Problems and Legal Remedies (PL&B February '89 p.23), Norman Jackson, Digital Equipment's UK Computer Security Manager, discussed the various threats to electronically stored data and the work currently being undertaken on new legislation which would make unauthorised access to a computer or network a criminal offence. But legislation takes time and meanwhile organizations around the world must respond to essentially similar problems of data security. They must devise practical steps to data protection.

Why is good security essential?

Obviously, sensitive data cannot be left in an insecure state until adequate legislation is passed in each country where your company operates. (For a summary of Australia's new anti-hacking bill, see p.19). In any case, successful prosecution under any such new law may well depend on the "victim" of a hacking offence demonstrating that his systems are at least adequately protected against accidental intrusion. In other words, to gain a conviction, it will probably be necessary to prove that a hacker has deliberately circumvented a system or network's security mechanisms. An analogy is the case of a householder who, leaving his front door wide open, cannot sue for trespass (under English law), whereas someone whose door is forced open has a legal remedy.

Clearly, the introduction of adequate security measures is essential for all system owners. The following action points will help you design your corporate data security system.

Classify information

Before one can decide what protection methods to use, it is first necessary to classify the data which needs protection in terms of strategic importance or confidentiality. In fact, classification is an essential component of any effective security policy.

My own company, Digital Equipment Company (DEC), in recognising this need, has adopted a Proprietary Information Protection Policy, at the heart of which are four categories of information classification. Three of the categories relate, in descending order of strategic importance, to DEC's proprietary information, ranging from the most critical (disclosure, loss or alteration of which could cause "very serious damage") to in-house information of a non-critical nature (for example, DEC's internal telephone directory). The remaining category relates to personal data, and covers data typically protected under national data protection laws.

To support the policy, DEC has established rules (or "standards") aimed at achieving appropriate levels of protection for the information within each of the four categories. These standards cover such activities as:

- processing

- labelling

- distribution (including transmission)

- storage

- disclosure

- destruction and disposal

Identify individuals with information responsibilities

Each person who is involved in the creation or handling of information needs to be identified. Furthermore, each of these persons or groups needs to be provided with security procedures to control their information. The following have been identified as persons normally involved in the creation or processing of information, but this list is not necessarily exhaustive:

- the originator

- the owner (the responsible person within the organisation who determines information's appropriate classification)

- authorized users

- the custodian (e.g. responsible for processing the information)

- the administrator

Each of these persons and the areas in which they work represent potential threats to the confidentiality and integrity of information.

Assess potential data security threats and prepare counter-measures

The computer environment, computer applications, communications, personnel, external services and the physical environment all contain potential threats. Each will be examined with the purpose of suggesting measures and techniques that can be employed to protect information from such threats.

1. COMPUTER ENVIRONMENT AND COMPUTER APPLICATIONS

(This area comprises the system software and hardware upon which applications are run, together with the computer applications themselves).

There are a number of controls that can be employed to restrict access to a computer system, and to limit the extent to which a user can gain access to information within a computer system or database.

1.1. Identification and authentication controls

1.1.1. Passwords

Passwords are the simplest, yet (because of their ease of use) the most abused form of user authentication. It has been quoted by a self-confessed hacker that 12% of all passwords are less than two characters in length. However, intelligent use of passwords can form a very effective defence for information. The following are some techniques which can be employed to make passwords effective:

* multiple passwords for sensitive activities

* enforced minimum length

* passwords selected to be not easily identifiable

* restricted duration (i.e. forced change, or automatic expiry)

Additionally passwords should be:

* stored within the system in encrypted format only

* not displayed (or "echoed") on the terminal screen

1.1.2. Biometric devices

Although biometric devices still have a long way to go, in terms of user acceptance, reliability and cost-effectiveness, they probably represent the greatest potential growth area of any type of security product. Whilst eye retina pattern and finger-print recognition devices may continue to have a limited appeal, electronic signatures are already achieving some considerable success in commercial applications, and a great deal of work is being undertaken towards perfecting voice recognition systems - possibly the biggest growth market of all.

1.1.3. Tokens

There are a number of products on the market, similar in shape and size to hand-held calculators, which give an additional level of security to system administrators. These devices usually provide an automatic one-time password which the user keys into his terminal in response to a challenge from the host (or target) system.

1.1.4. Restricted access to data and software

One very effective, yet extremely simple, method of restricting access to information which needs to be protected is the use of menus. They provide the user with a list of options which he is entitled to examine and use. Outside of these menus, access is prohibited.

1.1.5. Encryption

Another method of limiting access is the use of encryption, whereby specific files can be encoded so that the contents are unintelligible without the means of de-encryption (usually a key). Encryption can be in the form of software (for file protection) or hardware devices (usually for end-to-end encryption).

1.2. Physical access controls

Since the successful implementation and use of logical access controls depends upon the limitation of access to only those persons who have a need to know, strict control must be applied to the issuing of privileges enabling such access. It is very important, therefore, that the responsibility for allocating privileges and for managing the specific security controls is vested in a separate trusted individual. Special care must be taken in the selection of such an individual.

The person who allocates privileges (usually the system manager) must be aware of the special needs of, and also the potential risks associated with, the following groups of individuals who will most probably require privileges in order to perform their duties:

* computer operators
* engineers
* development staff
* technical support staff.

2. COMMUNICATIONS

Since the need for computers to communicate with each other remotely is becoming increasingly important in today's business environment, there is also a corresponding need to place controls on access to confidential and strategically-sensitive information which is transmitted over networks. The following is a selection of network controls and techniques which can be employed to make transmitted data more secure:

* terminal identification and authorisation
* restricted availability of dial-in lines
* confidentiality of dial-in telephone numbers
* intelligent modems (which demand passwords)
* automatic call back modems
* restricted information on network protocols to gain access to the system
* encryption
* dedicated port connections to specific systems

- packet switching system (PSS) access authentication to ensure that only authorised users may gain access to the organisation's nodes. (A node is an accessible intelligent computer on the system)

- automatic log-out of systems in the event of line disconnection (software monitors terminals ensuring no users whose terminals have been disconnected remain logged into their applications systems - otherwise it provides easy access for an unauthorized user).

3. PERSONNEL

The most sophisticated security controls and techniques can be totally jeopardised by ineffective and careless application by the persons to whom they are entrusted. The setting up of procedures, and the monitoring and use of these procedures by all persons who come into contact with confidential information is, therefore, very important. The careful selection and screening of potential employees who will be working in a computer environment is also essential.

4. EXTERNAL SERVICES

To accommodate flexible work-loads and working arrangements, more and more external services are used nowadays. Such use includes, for example, the employment of on-site contract personnel (e.g. computer operators and programmers) the transfer of excess work at peak operating times to external service bureaux, and the use of such services as microfiche bureaux and confidential waste agencies. In all cases where such organisations or personnel are employed, strict controls must be implemememented to ensure that such persons are not allowed access to any information other than that which is essential for them to carry out their duties.

5. PHYSICAL ENVIRONMENT

Although a complete book could be written on the subject of physical environment controls for computers, shortage of space permits only a passing reference to this subject. It is vital that adequate access controls should be placed on computer rooms, telecommunication equipment rooms and areas used to house confidential magnetic media. There is little point in employing sophisticated logical access controls if free physical access is granted to these areas.

Develop a contingency plan

This report has been devoted to considering security measures that can be employed to protect confidential and strategically-important information. However, what happens if these measures fail and an organisation finds itself without access to its vital computer systems? If it has been forward-thinking, the correct answer to this question is that the organisation will resort to its contingency plan.

For companies which rely heavily on computers to run their key business activities (nowadays the vast majority), the implementation of a contingency plan is essential to ensure quick recovery in the event of a "disaster."

The key steps which need to be taken in the development of a contingency plan are:

- Prepare a risk assessment of key assets for which the organisation needs backup, for example, computers, telecommunications equipment, people and supplies;
- Identify the location of these backup resources;
- Define and allocate responsibilities;
- Adopt recovery procedures;
- Prepare documentation;
- Test the plan;
- Monitor and update, as necessary.

Manage security effectively

An organisation cannot be confident of prospering without having good security in place. The management of any company, therefore, must be aware of the need for security and must be prepared to allocate adequate resources to achieve effective security. Similarly, to succeed, security itself must be properly managed.

The following is a suggested sequence of steps which should be followed to achieve effective security:

1. Define your security policy;
2. Assess threats, risks and vulnerabilities;
3. Establish a security plan;
4. Set up a security administration;
5. Implement countermeasures;
6. Establish contingency plans;
7. Constantly review;
8. Update where necessary.

Norman Jackson is UK Computer Security Manager, Digital Equipment Company Limited. Contact PL&B if your organization would like further information or advice on data security.