HUMAN RESOURCES SYSTEMATICALLY APPLIED TO ENSURE COMPUTER SECURITY

by

V.P. Lane and F.G. Wright
Southern Water Authority
Worthing, West Sussex,
UK

ABSTRACT

In order to maintain the integrity of a computing service, it is essential to assume that there is no limit to the ingenuity of men who wish to break the service's security measures and no limit to the carelessness of those parties given responsibility for maintaining its integrity.

From a statement of security requirements from the point of view of the user, the paper discusses the practicalities of satisfying these objectives. This is an extremely demanding task. However, if it is approached in a systematic manner it can often be achieved without any great increase in operating costs.

A great deal of attention has been given to security aspects of hardware and systems software, and consequently the personnel, a vulnerable area, has received little or no attention. The paper explores the contribution that end-user and computer personnel make to computer security through their routine duties. The paper identifies the need for, and the methods to achieve, a logically developed approach to security, to enable those responsible for computing, both end-users and data processing professionals, to identify, evaluate, and deal effectively with their own security requirements. The basic philosophy of physical, document and personnel security must be applied in concert, for if they are applied independently they are ineffective.

1. THE COMPUTING SERVICE AND ITS SECURITY

The data processing department is a production unit which receives raw material from the user in the form of data and converts this into information which is returned to the user or other users to form the basis of their decision making. The basic requirements of the user are that the service should provide results which are correct and to an agreed timetable not affected by outside influences, and such that the service cannot be used or influenced by unauthorised personnel.

The computing service as illustrated in figure 1 consists of four components, i.e. equipment, software, data and personnel. All four components require protection. Management generally appreciate that the computer system and the data comprise a major asset of an organisation and therefore that the equipment, the software and the data require protection without realising that personnel is the area of greatest vulnerability. Personnel create two problem areas:-

(i) data privacy

(ii) data integrity

Most organisations fall into one of two categories. The first category includes

organisations such as Water Authorities in which only a small part of the work has a need for high security because of its financial or confidential nature and the bulk of the work has relatively low security value. The second category is at the other extreme and includes organisations, like finance houses and Government bodies, for which the majority of the computing is high risk; however, it is common for this type of organisation to dedicate itself to a relatively small number of computer applications. In both categories, security is achieved in the same way. First standard protection is ensured for the equipment, the software and the data. Then in addition and most important of all, attention is directed to the personnel to create, through staff training and management supervision, simple but effective security procedures. All breaches of security being promptly investigated followed by swift disciplinary action which must be taken against defaulters. The result will be a secure service which meets the approval and the needs of the user without any significant increase in cost for security measures.

2. SECURITY - THE USER SPECIFICATION

The specification of the user's needs originates from his computing service requirements. As illustrated in figure 1, the computing service is made from four components, i.e., the equipment, the software, the data and the personnel. Each of these may be subject to threat and therefore requires protection.

The security specification from the user's point of view is that the computing service must be protected against a diverse range of unwelcome events which may be natural or man-made and planned or accidental. The service must be protected against:-

(i) Acts of God i.e., the service should be flood-proof, fire-proof, etc.

(ii) Accidental man-made disasters i.e., it should be safe:-

  (a) from machine failures such as from power cuts, mal-functioning of equipment, disc crash or disc dropped, tape torn, etc. and

  (b) from human error causing bugs in systems or application software

(iii) Planned man-made disasters from outside the organisation. This is generally directed at the premises although it might be aimed at the computer and its ancillary technology

(iv) Planned attack from inside the organisation e.g., program "time-bombs" to destroy data files

(v) Theft and espionage - crimes may range from selling time of the computer, or mailing lists, or application software; fraud or embezzlement (there is the incident of a credit card company having its list of members stolen together with a set of plastic cards which resulted in a loss of over £1 million)

(vi) Espionage - information may be wrongly disclosed within the organisation and although this is a breach of security it may not be so significant as cases where the privacy leak results in wrongful disclosure to an external party

In the final analysis, however, the user is only really interested in the integrity of his data, the confidentiality of information and in a service to an agreed timetable. The features of security which are not evident in this simple approach is of little interest to him as this is the responsibility of the Computer Manager.

3. A SECURITY STRATEGY

It is apparent that few companies could hope to justify in economic terms complete protection against the threats listed above. A government department with a high proportion of top secret data is one of the few installations attempting to achieve perfect security. Fortunately for the average data processing installation with a relatively small proportion of security problems, the task is less daunting, more likely to be satisfied, and correspondingly less expensive. A satisfactory service can only be achieved through an effective use of resources by concentrating on those areas of the business with a real security need [1] .

Responsibility, risk evaluation and defence priorities

The computer services manager is responsible for all aspects of the computing service security. However, as the service becomes less centralised, the users must bear more responsibility for the protection of their part of the system. In order to identify

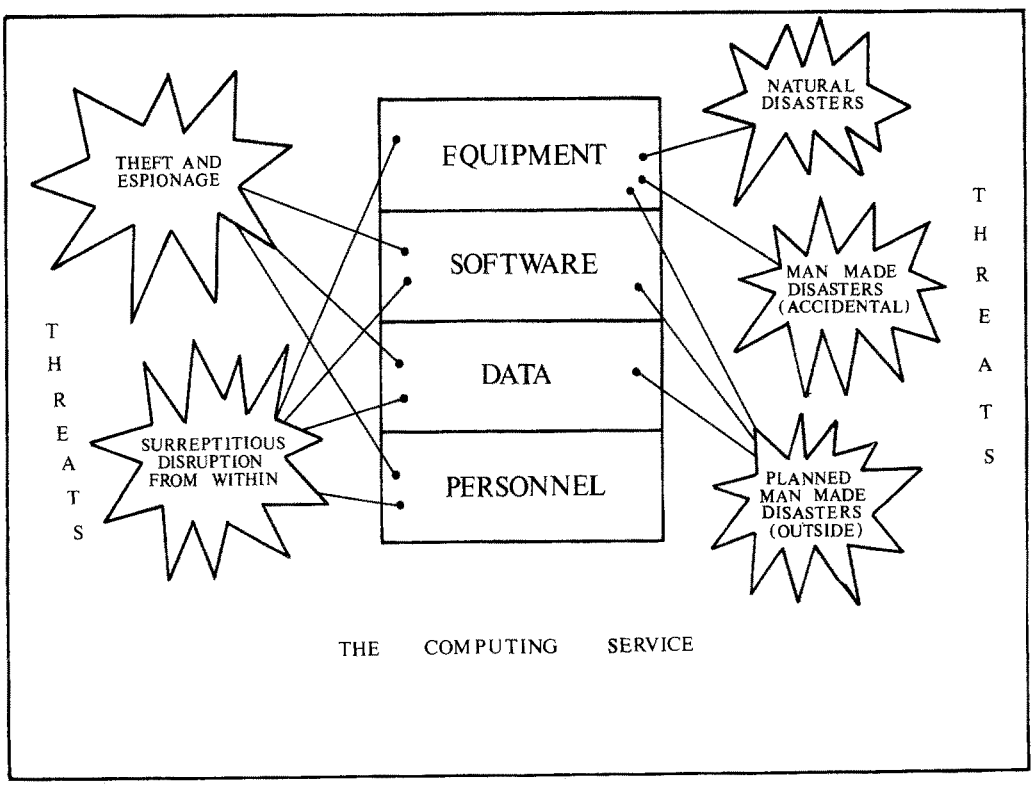

Figure 1 Threats to the computing service

those areas of the business which are worthy of special attention, it is necessary to evaluate the effect of each threat. First one calculates the loss if a breach of security occurred and this will indicate those parts of the business with a high priority in security terms. Then defences are considered, priced and selected. As implied above the computer services manager should complete the evaluation of those parts of the service with which the user does not have any direct contact.

Hardware and systems and application software

The majority of threats indicated in figure 1 are intimately associated with the hardware and software. Fortunately, this is under the direct control of the computer professionals. Organisations are generally sympathetic to funds being used for the computer equipment and its immediate environment. The user therefore expects basic security features without any effect on his budget. The user presumes that the equipment will be protected by fire detectors and extinguishers; that physical security is adequate through the use of locks, bolts and personnel entry control stations; and that the hardware is protected against mal-functioning.

The cost of developing the system software is such that few organisations can contemplate the writing of their own software. Therefore the computer manager and the user are dependent upon the manufacturer and this is generally perfectly satisfactory. In case of catastrophe, back-up on other computers [2] is taken for granted.

The computer professional will provide a service with all the above characteristics and the additional cost to the user, because of the security features, will be insignifcant since their cost is negligible in terms of the total data processing budget. It is common for an organisation to provide this type of service and the user computing service to be anything but secure.

The explanation is simple. Virtually all of the discussion and protection described above has been related to technological areas, whereas the major vulnerable parts are those in which there is significant human involvement. In many respects to talk of physical security of the computer or of back-up services are red-herrings in that they distract attention from the main area of security risk, namely the personnel in the computer department and in the user departments.

With respect to application software, the user expects it to be available not without bugs, but with controls [3] so that errors will be apparent to the user and will not damage the operation of the business.

In the last decade, the majority of reported security breaches have not resulted because of the mal-functioning of security with respect to physical protection of hardware or to systems software, but have resulted from the simple actions of personnel in situations where basic security was lax, and/or controls in the application software or computer installation were non-existent.

4. HUMAN FACTORS AND A SECURE SERVICE

Computers are employed by an organisation in order to assist the user in the operation

of the business. The computer and the data it holds are major assets of the company. Although the computer services manager must be responsible for the day-to-day operation of the computer services to a given minimum security standard, it is only the user who can specify what this security standard should be based on, from his practical knowledge of the cost of a breach of security.

The user, as with the design of computer-based systems, must be the major contributor in establishing security standards because of his unique knowledge of the business. Based on this contribution, the organisation will agree and establish security procedures. Although a user will initially state that a security system is required that is impregnable, it must be recognised that complete protection as an objective is impracticable except for high security government departments.

If the user is given the task of evaluating the cost of a security breach, he will quickly establish those parts of the business where security is essential and other areas where it is insignificant. Protection must reflect the sensitivity of the operation and not necessarily the equipment nor the applications. For example, a computer used for real-time control of a water distribution network which in the event of computer failure could be operated manually for hours or even days without any real damage does not justify the same defence as similar equipment used for air traffic control at a major airport - in this case both one hundred percent back-up facility, and contingency plans to ensure the service in the event of a major disruption are essential. Similarly, a payroll system, often considered to be an extremely sensitive area, can be regarded as low risk in an organisation in which the grades of staff are virutally common knowledge and personnel are employed on grades with corresponding salary scales - whereas in an organisation in which salary differentials are not common knowledge then payroll confidentiality is more important.

Following the user analysis of security objectives, it is necessary to recognise the threats. Referring to figure 1, the threats from natural disasters, accidental man-made disasters and from planned man-made disasters from outside the organisation have usually been considered in general defence plans for the computer hardware. It is the threats of theft, confidentiality of information, data integrity, espionage and internal disruption - all human threats - which are the biggest dangers because they have seldom been considered systematically. All computer applications must be examined by the users in terms of risk to attack from personnel. Although protection may be only economically justifiable for a few systems, the security procedures and working practices which ensue will bring benefits and protection to other systems which in themselves may be undeserving.

The user analysis will identify at least three major areas, namely:

(i) document security and information confidentiality,

(ii) data integrity - data processed in computer systems must be processed to give correct answers (i.e., accuracy of data) and all the data authorised, no more and no less, must be included (i.e., reliability of data) and

(iii) the need for at least similar levels of security within the computer department to those established in the user section.

Systematic examination for document security and data privacy

It is surprising that few computer organisations have requested a systematic study of the threats to company information in the manner outlined above and illustrated in figure 2. The computer professional is ideally equipped to encourage the user to embark on this type of study. One can only assume that the reason for this lack of systematic analysis of security needs is because the study will suggest a concentration on manual control procedures (rather than computer-based systems) within the user department and the computer departments and between the two units.

Manual procedures do not have the glamour and therefore the appeal of computer systems. It is regrettable that basic procedures of prime significance to the business do not attract the same degree of professional attention as sophisticated computer systems. The organisation must examine each involvement by a user with the computer, to establish for the systems identified, methods to give protection from user to machine and from machine to user - this will require procedures for registration of work, for transferring between machine and ultimate recipient, and for security classification.

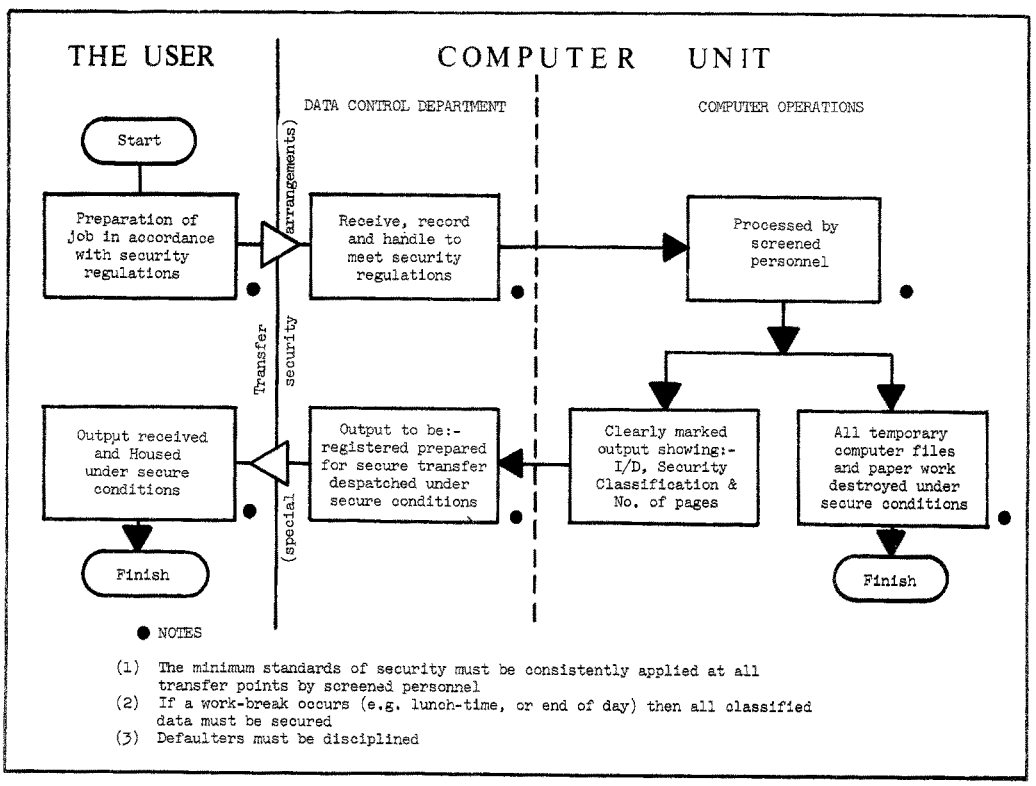

Figure 2 Data protection

It is apparent that security classifications established and operated by the user should be consistent throughout the organisation. The computer unit may give work a higher degree of security than the user requests but common minimum standards of protection are essential if one department is to entrust its work to another on the understanding that it will be adequately protected.

The examination will encompass the following:-

(i) identification of appropriate security measures for each user application - measures which reflect the sensitivity of the work
(ii) formulation of security and operating instructions
(iii) training plans for operatives and management
(iv) enforcement of procedures and
(v) provision for regular review of procedures.

User procedures for document security and data privacy

The threats to which the user department are prone include:-

damage to terminal equipment,
unauthorised viewing of information,
unauthorised copying of documents,
the introduction of irregular routing channels and
the introduction of unauthorised or irregular data.

Therefore the user must identify the degree of security which is appropriate to a particular job; agree this with the computer unit in order that they can establish similar or better security standards to that operated by the user; and then proceed in a methodical manner as illustrated in figure 2 with:-

(i) regular examination of operation logs in particular to locate unauthorised use of documents or for files being referred to at unusual times
(ii) management involvement to ensure that security procedures are followed
(iii) physical security of, and control of access to, the terminal, and
(iv) overall security of documents i.e., input forms containing data and unused forms, and computer output reports.

There are many methods which should be considered and operated by the user and these include:-

- all documents, especially those in transfer, should have clear and identifiable markings to show the security classification; colour coding is effective or plain language may be preferred
- the user must maintain a log showing where and what is held of a classified nature; this will enable classified data to be accounted for immediately at any time and assist with investigations if defences fail
- the storage of classified documents in "secure" containers; the standard of protection will reflect the sensitivity of the work and the storage environment.
- a routine procedure for the destruction under secure conditions of obselete doc-

uments will have a working life of days and others months but all documents at the end of their useful life must be totally destroyed and

- operational arrangements for special jobs i.e., non-routine work; in such cases it is imperative that other parties such as the computer manager are given notice of the user's irregular intentions in order that adequate safeguards can be brought into operation.

A secure service is based on the commitment of user management. Management must provide the impetus to set-up working procedures but most important of all they must give the leadership to make certain that the procedures are followed.

Data control for data integrity

The majority of errors in the use of computer applications is not generated by the computer system, but by the personnel involved in the system. Humans will always make mistakes and the purpose of data control is to identify human errors and thence remove their effect. In addition, data control will help to stop intentional entry of illegal data for theft.

It is not possible within this paper to describe the full nature of data control but it must be realised that controls within a computer system are fundamental to security. As such, data control must be considered in the first stages of the design of a system, and not added to a system as an afterthought; they must be considered in a comprehensive manner as described in [3] . The objective of data control is to create accurate and reliable data i.e., data integrity. Therefore controls must be introduced to ensure:-

(i) completeness of processing of input data
(ii) accuracy of processing of input data
(iii) authorisation of input data
(iv) authorisation of amendments to master files
(v) completeness and accuracy of processing of amendments to master files and
(vi) master file balancing

Some of the tasks which are essential to the above may include:-

raising of input documents
batching of input documents
authorisation of batches
recording of the above tasks
recording of receipt of computer output and
reconciliation checks before output is distributed and used.

It is possible to design good data control but still have insecure systems. As indicated earlier, hardware may be at risk because security procedures are not followed and similarly data control procedures will not be effective unless they are practised. For effective data control, the pre-requisite is a review and monitoring function by management.

If the above features together with good accounting practices are implemented, it is relatively easy to achieve data integrity.

The computer services department

The user's expectations may be summed up as a professional approach from the computer personnel to provide a service which includes computer department security procedures consistent with those enforced by the user; duplication and back-up facilities as necessary; the correct labelling of all output being directed to the user with the security classification, job identification, clear indication of beginning and end of output reports, and user identification; and contingency plans for continuation of services in the event of a major disruption. With respect to data held on behalf of the users on magnetic media or in other form. They must be controlled in a similar manner to that indicated in figure 2 to ensure consistent levels of security throughout the organisation.

These procedures are generally "observed" in any professional computer department, but it would be unwise if reference was not made to the weakness which is inherent in any computer system i.e., it is not the technology nor the procedures which are likely to cause danger but the personnel e.g., the major fraud case at Equity Funding Corporation of America [4] where the computer was utilised to cover a fraud involving $110 million. The integrity of the computing service will be maintained only if the computer controller exerts his management influence on his staff.

5. ILLUSTRATIVE EXAMPLES OF SECURITY FAILURES

The following case studies, well documented security failures, are described briefly and are then analysed to illustrate the significance of the security principles described in this paper.

A document security breach and personnel vetting

In this incident, two members of an ICI computer department stole 48 magnetic discs and over 500 tapes containing major company data and the back-up copies. Then they requested £275,000 from the company for the return of the files or threatened the files would be destroyed [5] .

This example illustrates the failure of the "document" security procedure. The procedure, shown in figure 2, should be followed between user department and Computer Unit - but the same procedure must be followed between other departments e.g. departments within the computer unit. The case study shows how simple it is for the elementary rules of security to be ignored. Operators had access to both main files and their back-up copies and the files could be obtained without any other authorisation. In effect the files were unprotected.

There is a further lesson to be learned from this case. The operator involved in the theft whilst awaiting trial was employed by a number of other computer organisations. A clear indication of the negligible extent of personnel vetting done at the inter-

view stage. When it was discovered who he was, the operator was removed immediately, not because of what he had done, but through fear of what he might do.

A data control failure

This second example is taken from a health authority paymaster's department [6] . Expenses incurred by personnel were normally paid at the end of each month with the monthly salary payment. However there was the facility to pay expenses separately via another system, quite independent of the main payroll system - presumably for special cases and for speedy payments. One of the pay-clerks took advantage of this. In general, doctor's expenses were paid via the main payroll to the doctor whilst the second system was used for a duplicate payment of the same expenses claim to the pay-clerk direct. After £13,000 had been stolen, the mal-practice was discovered because of the clerk being sick and absent. A doctor asked for payment of a claim he had submitted earlier in the month which (although he was not aware of it) would have been paid with his monthly salary. This enquiry brought to light the fact that the expenses had already been paid via the secondary system but the payment had gone astray.

This breach raises a number of questions. Was there no overall reconciliation i.e., control figures, between the two systems? Did the person who handled the money have the power to authorise payment? The case indicates (i) the failure to design and/or operate data control and (ii) the neglect of good accounting practices. In addition, it brings out the need for management to monitor procedures continually.

The role of senior management

In the security principles outlined in this paper it has been stated that the chief executive is the prime-mover in security matters. The example of the Equity Funding fraud involving $110 millions [3] involved its president and senior computer personnel. This security breach illustrates the corollary of the security principle i.e., if the chief executive with assistance of colleagues, conspires to breach security there is little hope of effective defense.

However in this example if effective security practices had existed, with respect to the operation of the computer together with comprehensive data control on the application software, prior to the commencement of the fraud, the president might not have fallen to the temptation. Both of these security features must have been lax or non-existent. If they had been operational it would have been difficult for the activities of the president to proceed without staff being at least suspicious if not aware of the irregularities. The result might have been that the crime never started or that the mal-practices were common knowledge earlier and the size of the fraud smaller.

6. MAINTAINING A SECURE SERVICE

It must not be assumed that once a secure method of operation as illustrated in figure 2 has been established that the position can be maintained without effort.

A secure service will only be maintained if it incorporates at its inception realistic methods by which it may evolve. The pre-requisites are:-

(i) simple staff training; supervision and defined disciplinary correctives for staff who fail to observe established procedures; disciplinary action must be enforced swiftly and strictly initially, for incidences such as general breaches of professional standards, circumventing despatch control procedures, or disclosure of passwords

(ii) report procedures for immediately informing management of all suspected breaches of security

(iii) a routine review (annually and also following each breach) of the procedures and a continuous programme of re-assessing security classifications; a good secure service depends upon the proportion of top security work being kept to a minimum and this pre-supposes that some high security work may at a later stage be downgraded, and

(iv) security exercise tests both as part of the regular audit of the organisation and its systems, and random unscheduled exercises being regularly carried out.

7. CONCLUSION - DEMANDING BUT NOT EXPENSIVE

Security is an essential feature of an efficient organisation. The introduction of security measures into a computing service which has grown negligent is difficult, can be costly in time and effort and be a traumatic experience for the personnel. All this inconvenience can be avoided by designing at the system inception total computer systems, from user back to user, with security as an essential and integral component.

Personnel are both the strength and the weakness of all security systems. Therefore every person from user through to computer operator must be made to realise the part they have to play in maintaining the security and the integrity of the computing service and must be trained to appreciate his individual responsibilities. If this is achieved the benefits of security to the efficiency of the company will accrue with the minimum of effort and corrective action.

The cost of devising security procedures is not expensive in terms of data-processing budgets. The significant cost is that required to ensure that the written security procedures become a reality. This is achieved through audit-checks and surprise visits to test the effectiveness of the defences. Although technological development may assist in security, the major threats are caused by human weaknesses and the best defence is good management.

ACKNOWLEDGEMENTS

The authors wish to acknowledge the help give to them by many previous colleagues and by Southern Water Authority. The opinions expressed in the paper are those of the authors and do not necessarily represent those of the Southern Water Authority.

REFERENCES

1. Kluwer Harrap Handbooks. 'Handbook of security'. Kluwer Harrap, Netherlands, 1977.
2. Hemphill, C.F., and J.M. 'Security procedures for computer systems'. Dow Jones-Irwin, Illionois, USA.
3. Sharrat, J.R. 'Data control guidelines'. National Computing Centre, Manchester, England, 1974.
4. Hamilton, P. 'Computer security' Cassell Associated Business Programmes, 1972.
5. Hampshire Regional Health Authority. 'Report of members enquiry into salary misappropriation at area headquarters'. Hampshire Regional Health Authority, UK, June 1977.
6. Computerview. 'The ICI ransom case: some lessons to be learnt'. Computer Weekly, IPC Business Press, 9 Feb., 1978, pp2.