7

Code of Practice: A Standard for Information Security Management

Lam-for KWOK[1] and Dennis LONGLEY[2]
[1]City University of Hong Kong, Tat Chee Avenue, Kln., HONG KONG
Tel:+(852)27888625 Fax:+(852)27888614 cslfkwok@cityu.edu.hk
[2]Queensland University of Technology
GPO Box2434, Brisbane Q4001, AUSTRALIA
Tel:+(61)7-38645358 Fax:+(61)7-38641507 longley@fit.qut.edu.au

Abstract

The rapid development of networks has caused senior management to reconsider the vulnerabilities of their organisations to information security incidents. Such reconsideration often reveals that the fundamental vulnerabilities lie not with the emerging technology but rather with the lack of an information security infrastructure within the organisation. Appointing a security officer is a common reaction to this situation but the new appointees often find that there is a lack of immediately apparent support form senior management for additional budgets or organisational change and an agreed authoritative source of information security guidelines. The situation has to some extent been addressed by emerging Information Security Management standards such as the *BS 7799*. This paper discusses the manner in which a security officer may best employ such standards to enhance the level of information security in an organisation. The paper also discusses the fact that the application of the standards reveals the requirements for an organisational security model that may be employed to assist in standards conformance and auditing.

Keywords

Information security management, information security standards

1 INTRODUCTION

Surveys and statistical evidence suggest that many senior management have not traditionally given a high or even moderate level of priority to information management. The rapid

development of networks, particularly the Internet, has now caused senior management to reconsider the vulnerabilities of their organisations to information security incidents. Such reconsideration often reveals that the fundamental vulnerabilities lie not with the emerging technology but rather with the lack of an organisational information security infrastructure. A common reaction to this situation is to appoint a security officer, or to give an existing employee information security responsibilities.

Discussions with staff given information security responsibilities indicate that a common prime concern lies with a lack of an infrastructural framework for their roles and responsibilities. In recent years senior management have become aware of the potential deleterious impacts of inadequate information security, and have also succumbed to the pressures for the development of visible forms of quality assurance. However, information security management has, to date, lacked a universally recognised framework.

In the late 1960's risk analysis was postulated as the means to assist organisations to formulate their security requirements. The US Federal Government required its departments to undertake a Courtney style of risk analysis (FIPS 65,1979) and subsequently there were formal requirements to report on the implementation of security plans.

The public service managers did not react enthusiastically to these edicts and such practices were not thereafter widely adopted in the private sector. Nevertheless the traditional approach to information security management was based upon a risk analysis study, normally using some proprietary methodology, leading to a set of recommendations on countermeasures, security plan etc. For example, the UK government commissioned the development of the CRAMM methodology (Moses and Glover, 1988), for risk analysis, in an attempt to ensure a degree of uniformity in security management within government data processing units.

The pioneering work of the National Computer Security Centre (NCSC) in the development of TCSEC (Trusted Computer Security Evaluation Criteria) (DoD, 1985) represented an important initial step in the development of a framework for computer security. The significance of these criteria lies in the concept that organisations were required to demonstrate conformance to official guidelines of computer security. The Bell LaPadula security model provided a firm theoretical basis for the criteria. The criteria were extended in the Rainbow Series, to include risk analysis, trusted networks and databases, but the context of the criteria was always limited to the design of multilevel security systems and was therefore primarily directed to the military and government applications.

Subsequent developments of information security evaluation were undertaken by a number of European countries and then harmonised into ITSEC (Information Technology Security Evaluation Criteria)(CEC, 1991). This effort is now being incorporated into international standards, and the Orange Book has been replaced by a large volume of standards documents on CDROM.

The European criteria incorporated the Orange Book concepts of multilevel security but extended the granularity of evaluation assurance and range of system functionality. The

criteria thus extended into specific and general purpose security products, intended for a universal market. The criteria also incorporated the evaluation of systems; the essential difference between a product and a system being that the security environment of the system, and hence the security threats, could be more precisely enunciated.

The evolution of the Orange Book into the current set of draft of international standards, coupled with the experience of formal security evaluation over the past decade, have indicated the substantial complexity and costs of such exercises. Such costs may be justified for security products which will generate significant revenue. However, even large organisations are unlikely to include a formal security evaluation of their systems in the security budget.

The security manager therefore is not substantially assisted by the developments in formal security evaluation criteria developed over the past decade. Moreover none of the various risk analysis methodologies or packages appear to have gained universal acclaim or acceptance. Large consulting firms offer substantial risk analysis studies but the cost of such exercises is usually well outside the budget of the average security manager. Thus the security manager could often only glean recommended information security practices from various reference books, or best practice adopted by some organisation. However, if this approach were taken the subsequent proposals from the security manager lacked the credibility of a regulatory framework, and would often fail to gain complete acceptance from senior management.

The publication of a code of practice for information security management by the British Standards Institute (1995) therefore represented a major advance in organisational security management. This document has formed the basis of Australian and New Zealand standards, and is in the process of adoption as an international standard ISO (1995).

The standards are based upon recommendations of security professionals and thus represent a statement on best practices. The document contains recommendations on all facets of information security and hence provides a set of recommended controls and valuable checklists. The most significant aspect of the standards, however, is that they exist; a security manager can now warn recalcitrant senior management that the organisation does not conform to national or international standards of information security management. Such lack of conformance may have consequences for senior management in terms of fiduciary responsibilities, relationships with other departments or organisations etc.

The introduction of the information security management standards thus represents an important advance for the security manager, but the effective use of such standards requires some careful consideration, planning and tools.

2 SECURITY OFFICER AND THE STANDARDS

The emerging Information Security Management Standards (BSI, 1995)(SA/SNZ, 1995) provide an important framework for the role of the security officer, but the standards need to

be interpreted and introduced in a structured manner, in order to ensure that they have maximum benefit in terms of organisational information security.

The phases of the implementation may thus be structured:
- development of local set of standards;
- decision from senior management on the policy of conformance to standards;
- evaluation of current level of conformance;
- development of a security plan;
- development of a security model;
- auditing of conformance.

As will be shown in the next section, the standards require careful interpretation and customisation to ensure relevance to a particular environment. At first sight some sections appear to be designed for large computer centres. Upon more careful reading, however, it becomes clear that this experience can be exploited in the current distributed computing systems and the electronic office. The first stage will therefore require a considered review and interpretation of the standards to produce a version for the local organisation.

One of the major advantages of the standards is that they simplify the problem of gaining management commitment. The standards and the localised version can be submitted with a request for a decision after a commitment in principle to conformance to published standards. Senior management's acceptance of the policy of conformity to the proposed standards is an essential condition for the success of the subsequent stages.

Once the principle of conformance is established, i.e. assuming that the whole project is not to be abandoned, the next stage is to determine the current level of security vis-→-vis the standards. This is, to some degree a replacement, or at least a deferment, of the risk analysis activity that normally precedes the establishment of a security plan. At this stage the organisation is effectively evaluating itself at a baseline security level. At the conclusion of the whole exercise, the security manager needs to develop a security plan.

The effort of checking conformance is significantly reduced with use of a software tool such as CoP-iT™ (SMH, 1995). This package allows users to set the level of conformance with the *BS 7799* standard and then provides a series of screens seeking information on the current level of security, in accordance with the standards requirements. Users enter their estimates of the degree of compliance to each topic presented. Upon completion of the dialog the package produces a managerial report with graphs and details of the current level of compliance.

The major advantage of the package is that it provides a detailed and disciplined approach to the collection of security relevant data; effectively producing a series of checklists similar in manner to risk analysis packages such as CRAMM. The advantage of CoP-iT™ over many proprietary risk analysis methodologies is transparency; it is easy to correlate the screens with the printed version of the standards and hence place the questions etc. in a given context.

The second major advantage of tools such as CoP-iT™ is that they maintain the momentum of the process. Having obtained the approval in principle from management, the initial report can be produced and submitted within a couple of weeks. This assumes, of course, that the necessary data to answer the questions is readily available. In many cases the questions may require a search amongst organisational documentation, and/or interviews with operating staff, computer and network managers etc. The package can facilitate the conduct of such interviews by effectively providing a series of checklists.

The desired outcome of the dialog with senior management, following the submission of the initial conformance report, is an agreed security plan. If the report indicates an unacceptably low level of conformance then the first priority will focus upon the current detected deficiencies. The security plan will also address the security requirements beyond the baseline level as discussed in the next paragraph.

The standards emphasise that they primarily address the baseline security requirements. If the evaluation indicates a satisfactory level of conformance at a baseline level then the question of security requirements beyond the baseline level needs to be addressed. This phase will require some forms of risk analysis. It is suggested that the conduct of the risk analysis should be preceded by the formation of a risk model as described by Anderson, Kwok, Longley (1994). This approach overcomes some of the criticisms of current risk analysis methodologies which require extensive data collection in a form dictated by the methodology and the results may become quickly outdated.

Even if a risk analysis is not deemed necessary the formation of the proposed model is recommended for follow up security reviews but more importantly for predicted requirements on auditing of conformance. The initial evaluation using CoP-iT™, as described above, is adequate for its purpose but it assumes that the required information is readily available, and it does not require any evidence of the correctness of the responses. In future reviews the information collected for the initial review should be available in a convenient form. Moreover, if, as is to be hoped, the standards gain widespread acceptance then it is likely that internal or external security auditors will require evidence of the degree of conformance. The proposed model will greatly facilitate such conformance auditing.

3 INFORMATION SECURITY MANAGEMENT STANDARDS

3.1 Overview

The British Standards Institute published A Code of Practice of Information Security Management, the *BS 7799* (BSI, 1995). Standards Australia based the draft Australia and New Zealand Standard on Information Security Management (DR 95305) (1995) on this code of practice and formally adopted it in 1996. An International Standards Organisation document ISO/IEC DIS 14980 (1995) is similarly based upon *BS 7799*.

The standard is an important advance in information security management because it provides security managers with an authoritative statement on good information security practice plus a very helpful set of guidelines and checklists for their security plans. The document makes it clear that its contents require careful interpretation, in the light of the security environment of the organisation. The recommendations are aimed at baseline security and the proposed security measures will require enhancement in areas of high risk.

The standard provides a general section on information security management in which advice is given on the establishment of security requirements and the assessment of security risks, indicating its importance to organisations. The critical success factors are listed as:

- security objectives and activities being based on business objectives etc.;
- visible and commitment from top management;
- good understanding of security risks;
- effective marketing of security to all managers and employees;
- distribution of comprehensive guidance on information security policy and standards to all employees and contractors.

Many organisations develop their own guidelines based upon their individual circumstances but the standard recommends that any such guidelines should be cross-referenced to the standard for the use by future business partners or auditors.

The main body of the document comprises ten sections which will be discussed in the following sections. Each section commences with an objective and the key controls are highlighted within the appropriate sections.

3.2 Main Sections

3.2.1 Security Policy

This section emphasises the requirement for senior management to 'set a clear direction and demonstrate their support for and commitment to information security policy through the issue of an information security policy across the organisation'.

The section suggests the issues that should be addressed in the policy include definition of information security; statement of management intention supporting the goals and principles of information security; explanation of the specific security policies, principles, standards and compliance requirements; definition of general and specific responsibilities for all aspects of information security; explanation of the process for reporting suspected security incidents; and concludes with a recommendation for regular reviews.

Although such a policy must be blessed with the authority of senior management it would be optimistic to think that it will be originated by them. The development of the first policy, or updating of current policies, is an extremely important task for the security officer. It is also likely to be very demanding and time consuming task at the development stage. Although

feedback from senior management is essential during this process, it is important not to get bogged down in an excessive number of draft versions due to comments on phraseology etc.

Security officers may find it helpful to study existing security policies from other departments or organisations as a starting point, and to provide a checklist of potential items. Cresson Wood's book (1996) on information security policy can prove to be extremely useful in this regard, particularly since it has an accompanying floppy disk allowing sections to be transferred into organisational documents.

3.2.2 Security Organisation

The topics of the Standard in this section include information security forum; information security co-ordination; allocation of information security responsibilities; authorisation process for IT facilities; specialist information security advice; co-operation between organisations; independent review of information security; and security of third party access.

The useful role of the standard as a checklist is apparent here. For example, in the section co-operation between organisations, there is a mention of appropriate contacts with law enforcement agencies. Many organisations may never be subject to a serious hacking attack, or computer fraud, hence if such an event occurs there will be a dearth of experience of the actions to be taken: logs maintained, evidence collected etc. prior to calling in the police. Discussions with staff endowed with security responsibilities indicates that they readily appreciate the suggestion that a member of staff be given responsibility to liaise with law enforcement agencies and seek advice on the correct procedures.

Upon first reading the standard consistently gives the impression that it is designed for computer centres in large organisations. However, upon further study its relevance to small organisations, distributed environments and the electronic office become apparent. For example, the section on authorisation process for IT facilities is of increasing concern as users install powerful communication software on PCs and laptops, and third party access arrangements are as important today for dealings with electronically linked partners, and Information Services Providers (ISPs), as they were with mainframe maintenance companies.

3.2.3 Assets Classification and Control

This is a very short section containing only three items: inventory of assets; classification guidelines; and classification labelling. In this case the translation of the recommendations from traditional to current computing environments is fraught with difficulty. Physical computing assets have become smaller, more mobile and have proliferated throughout the organisation - and beyond to homes, hotel rooms and airport lounges.

The information assets are likewise widely scattered, and often under the direct control of organisational staff at many levels of responsibility. Classification guidelines are often non-existent and hence highly confidential material may be stored on unlabelled diskettes or transmitted over insecure networks. Most managers would be completely oblivious of the

route taken by their messages, or the multifarious nodes that would have handled their highly confidential company documents.

The standard does however make the important point that even when classification schemes are used, difficulties can arise in the absence of universal guidelines on information classification. Hence care must be exercised when exchanging information with other organisations since difficulties could arise from varying interpretation of document labelling.

3.2.4 Personnel Security

The objective of personnel security is given as 'to reduce the risks of human error, theft, fraud or misuse of resources'. These risks increased dramatically as computing was first moved from the computer centre to the office worker's desk, and even more so when organisations linked their computers with networks. There is now a much higher proportion of organisational staff with access to information processing facilities and assets. Moreover although traditionally information security is dominated by CIA (Confidentiality, Integrity and Availability), organisational connections to the Internet open up potential costs arising from misuse of access to the many consumer features of the superhighway.

The areas treated in this section include security in job descriptions; recruitment screening; confidentiality agreement; information security education and training; reporting of security incidents; reporting of security weaknesses; reporting of software malfunctions; and disciplinary process.

Each of these sections now apply to virtually all members of the organisation, and involve a much higher degree of complexity than hitherto. For example, confidentiality agreements need to be extended into codes of conduct covering usage of computing and communication facilities: guidance on email usage, avoidance of harassment on email, legitimate use of the Internet facilities etc.

3.2.5 Physical and Environmental Security

The contents of this section give an emphasis to the security of computer centres, but the introductory paragraph recognises the need for interpretation of the recommendations in other environments. The section deals with physical security perimeter; physical entry controls; security of data centres and computer rooms; isolated delivery and loading areas; clear desk policy; removal of property; equipment siting and protection; power supplies; cabling security; equipment maintenance; security of equipment off premises; and secure disposal of equipment.

The standard refers to the situation of the electronic office and, for example, the problems of security of laptop computers. It is recommended, for example, that personal computers processing sensitive data should be protected with key locks. However, the security officer faced with the managers imbued with the concept of **personal** computers, i.e. not subject to external control, will not find a great deal of assistance from this section.

3.2.6 Computer and Network Management

The objective of recommendations in this section is to 'ensure the correct and secure operation of computer and network facilities'. The introduction to the section emphasises that although there will be wide variations of environment 'in principle, the same security processes should be applied, with appropriate interpretation'. This is a very sensible statement but the reinterpretation of erstwhile computer centre procedures to the electronic office is no mean task.

The areas covered in this section include operational procedures and responsibilities; system planning and acceptance; protection from malicious software; housekeeping; network management; media handling and security; and data and software exchange.

The operational procedures and responsibilities recommendations emphasise the need for the allocation of responsibilities and the documentation of procedures for the secure operation of information processing systems. Although the wording is more apposite to the computer centre it provides a very useful checklist for current distributed environments: security reporting, segregation of duties, separation of operational and development environments, etc.

System planning and acceptance is becoming increasingly significant in the electronic office as packages make increasingly heavy demands on workstation storage and communication software soaks up network bandwidth. Change control is an important issue in large offices as customisation of workstations, development of templates for word processing, etc. by users, can impact upon the portability of electronic documents, and recovery situations where workstations have to be replaced.

Virus control appears to be one area in which management have been convinced to purchase appropriate defensive software. However, the emerging macroviruses and associated vulnerabilities introduced by integration of workstation software systems may require a much greater awareness of the need for an integrated approach to workstation security since such viruses are transmitted by electronic documents rather than software.

The importance of backup facilities is emphasised in the housekeeping section and the security of such backup media requires careful consideration, particularly when it involves user's confidential material that is normally protected by encryption or server password access. The network management section deals briefly with some aspects of the security of networks and it does highlight some common concerns in office environments, e.g. the security of servers located in remote offices.

Media handling and security was normally the responsibility of the tape librarian in the computer centre but this discipline does not seem to have been carried over to the ubiquitous office floppy disks. Clearly floppy disks holding highly sensitive data need to be administered in terms of labelling, receipts, minimisation of distribution, disposal etc., with as much care as the erstwhile magnetic tape. The final section deals, *inter alia*, with the electronic office and

some of the security factors of email etc., in fact this section does not give a good indication of its contents.

3.2.7 System Access Control

Access control will play a significant role in baseline security for most organisations. However, in many cases responsibilities for access control are spread around the organisation and the procedures are neither well co-ordinated nor documented. Such a situation can easily reduce the level of security attained; thus this section of the standards is extremely valuable in the formulation of a security plan and promulgation of procedures.

The headings of recommendations include business requirements for system access; user access management; user responsibilities; network access control; computer access control; application access control; and monitoring system access and use.

The standard emphasizes that access control must be defined on the basis of business requirements. Information flows are essential for the smooth operation of the organisation. However, most applications will require control of access to the associated information and it is important that consistent guidelines and policies are established based upon legislative requirements, need to know, organisational responsibilities etc. The use of standard access policies for defined organisational roles can facilitate this task.

The sections on user access management and user responsibilities provide invaluable checklists for the auditing of current procedures and an authoritative source for the introduction of new procedures. Network access control is a significant feature for most organisations, given the fact that many managers and the majority of users will be completely oblivious of the paths that their data will travel. This section deals with user and node authentication, inhibition of network roaming, design and segregation of networks to minimise security problems etc. Similarly the computer access control recommendations provide an excellent checklist of security measures relating to password management, secure log on procedures, terminal security etc.

Application access control is a significant feature now that users may be given access to extremely powerful software and communication facilities. When organisational workers were provided with a dumb terminal and a limited set of menu selections the potential for accidental or malicious damage to information assets was limited. The consumer computing market may now provide office workers with pentium processors, hosting massive software packages, connected to international networks. The need to control the facilities and software packages made available to users is now an important issue, particularly when it comes into conflict with the **personal** computer ethos.

Monitoring system access and use can impact upon areas other than technical, e.g. personnel issues are involved with questions of employee email privacy; monitoring of work performance and harassment; legal issues may be involved if the monitored data is to be used in evidence for disciplinary or criminal procedures etc.

3.2.8 Systems Development and Maintenance

There will be wide variations in the applicability of recommendations of this section. In the early days of commercial computing the possession of a computer automatically implied the existence of programming development team. Currently many organisations rely upon off the shelf software, or outsource their development effort. Nevertheless much of the material in this section requires a careful study by security officers to determine whether or not the recommendations need a re-interpretation in their environment. The detailed sections are security requirements of systems; security in application systems; security of application system files; and security in development and support environments.

The importance of the security officer's role in the planning of new systems is emphasised in 'security requirements of system' because retrofitting security is inevitably difficult and costly. A similar argument applies when new applications are to be commissioned for current systems, and in particular the questions of audit trails and monitoring need to be addressed at this stage.

3.2.9 Business Continuity Planning

Business continuity planning is an obvious component of a security plan and in this area it is essential that the security manager negotiates clear policy statements from senior management. Many of the activities associated with business continuity plans will impact upon operational staff and are likely to be given a low priority. For their own protection security managers need to ensure that they have gained, and documented, agreement and authority from senior management to undertake the recommendations in the standard. The recommendations cover business continuity planning process; business continuity planning framework; testing business continuity plans; and updating business continuity plans.

3.2.10 Compliance

Information security is not necessarily an option that can be accepted or rejected by senior management of an organisation. Increasingly there are legislative and regulatory requirements that require an information security infrastructure for compliance. This section highlights the need to ensure that all such legislative and regulatory requirements are met, and that conformance can be convincingly demonstrated. The section also deals with the need to ensure compliance with internal policies and regulations and concludes with a discussion on the mechanisms to audit such compliance and the protection of the auditing tools. The headings within this section include compliance with legal requirements; control of proprietary software copying; safeguarding of organisational records; data protection; prevention of misuse of IT facilities; compliance with security policy; technical compliance checking; system audit controls; and protection of system audit tools.

4 CONCLUSION

The published standards provide an invaluable tool to the security officer, in terms of comprehensive checklists, but more importantly they provide an authoritative source of information security procedures that should be accepted by senior management.

The standards represent the starting point for the development and implementation of a security plan. They cover baseline security requirements and must be complemented with some form of risk analysis to determine those areas, if any, of sufficiently high risk that warrant additional protection.

The starting point should be an interpretation of the detailed sections to the environment of the organisation, or organisational department, under consideration. This is followed by a survey to report upon the current level of conformance with the agreed interpretation of the standards. Following submission of the report and recommendations to senior management a security plan is then developed. Subsequently the actions may comprise:

- implementation of recommendations to achieve agreed level of baseline security;
- conduct of a risk analysis study to determine any level of risks that cannot be contained by baseline security;
- enhancement of security plan to include the results and agreed recommendations of the risk analysis;
- implementation of risk analysis recommendations; and
- review and auditing of security plans.

5 ACKNOWLEDGEMENTS

This study was conducted under the auspices of the ARC Collaborative Research Grant: An Information Security Model for Finance and Banking Sector, Reference No.: C195301033.

6 REFERENCES

FIPS 65 (1979) *Guidelines for Automatic Data Processing Risk Analysis*, Springfield:National Technical Information Service.

Moses, R.H. and Glover, I. (1988) "The CCTA Risk Analysis and Management Methodology (CRAMM) - Risk Management Model". *Proc. First Int. Computer Security Risk Management Model Builders Workshop*, Denver, Colorado, 24-26 May 1988.

Department of Defense (1985) *Trusted Computer Systems Evaluation Criteria.*

CEC (1991) Commission of the European Communities. *Information Technology Security Evaluation Criteria (ITSEC),* Provisional Harmonized Criteria, Version 1.2.

British Standards Institute (1995). *BS 7799: Code of Practice for Information Security Management.*

Standards Australia / Standards New Zealand (1995) *Draft Australian / New Zealand Standard: Information Security Management*, DR95305.

International Organization of Standardization (1995) ISO/IEC DIS 14980 *Information Technology - Code of Practice for Information Security Management.*

SMH Associate plc. (1995) CoP-iT™ *User Guide.*

Anderson, A., Kwok, L.F., and Longley, D. (1994) "Security Modelling for Organisations". *Proc. Second ACM Conf. on Computer and Communications Security*, CCS'94, Fairfax, Virginia, USA, 2-4 Nov 1994, ACM Press, 241-250.

Wood, C.C. (1996) *Information Security Policy,* Baseline Software.

7 BIOGRAPHY

Lam-for Kwok gained his degree in Computer Studies in 1983 and an M.Phil. in 1986. He is an Assistant Professor in the Department of Computer Science at City University of Hong Kong and is currently reading a PhD at Queensland University of Technology. His research interests is in information security modelling for organisations.

Professor Dennis Longley was Dean of Faculty of Information Technology and is now Director of Information Security Research Centre in the School of Data Communications at Queensland University of Technology. His main information security research interest is in the field of cryptographic key management for electronics funds transfer networks. He has performed consultancy studies in this field and is joint author of the books *Dictionary of Data and Computer Security* and *Information Security for Managers.*