A human approach to security management in HealthCare

H. James [a], *K. Andronis* [b] *and W. Paul* [c]

[a] *Lecturer, School of Information Systems, Curtin University of Technology*
GPO Box U1987, Perth WA 6001, Australia. Phone: +619-351 7055
Fax: +619-3513076   Email: james@ba1.curtin.edu.au

[b] *Manager, Information Services, Hollywood Private Hospital.*
Monash Avenue, Nedlands WA 6009, Australia. Phone: +619-346 6578 Fax: +619-389 8470

[c] *Managing Director, Personal Consulting.*
9/18 Fogerthorpe Crescent, Maylands WA 6051, Australia. Phone: +619-272 6326 Fax: +619-272 6326 Email: williampaul@acslink.net.au

Abstract

Past research and practical experience in information security suggest that management of information security in general is inadequate, with executives and employees lacking in security awareness. At core, security problems are people related: people use and manage information systems on a day to day basis, and people are both perpetrators and victims. This paper presents an approach to computer security management which is people oriented, developed based upon the Soft Systems Methodology (SSM). The planned application of this security management approach in practice to a private hospital in Western Australia is also discussed.

Keywords

Information security, security management, information security management, soft systems methodology, SSM, information security planning

S. K. Katsikas et al. (eds.), *Information Systems Security*

1 INTRODUCTION

Lack of security awareness at all levels of the organisation is a problem reported with repeated monotony. Although management is reluctantly becoming more aware of the risks of computer crime, there still appears to be the attitude that it won't happen to us. Unfortunately, the law of averages must strike home eventually, when the reported hit-rate of organisations continues to rise. A recent study by the National Computing Centre (NCC, 1994) in the UK found 80% of respondents had suffered at least one security breach over the two year period studied.

2 SECURITY AND PEOPLE ISSUES

Security measures may be technically perfect, but be let down by the unavoidable reliance on the human component. For example, a password system correctly implemented provides, in theory, an excellent barrier against unauthorised access to systems and data, but failure to keep passwords private renders the controls useless. As security experts and auditors have been preaching for years, the weakest link in computer security is the human one (Becker, 1977; Gasser, 1988; Hitchings, 1994; Lane, 1985; Watney & Turney, 1990; Wood, 1982).

In the USA a team of military officials sat by and watched a hacker they had hired, use technical knowledge and social engineering (impersonation skills) to break into their system. In less than 20 minutes this hacker had produced classified information on the screen. The female hacker (yes, they're not all males!) stated "*the more people with access the better. In the military, hundreds of people have access. At corporations, thousands do. I don't care how many millions of dollars you spend on hardware, if you don't have the people trained properly I'm going to get in if I want to get in.*" (Hafner & Markoff, 1993: 77)

The biggest problem facing any organisation when establishing an effective security system is the people issue. No matter the sophistication of the hardware and software, if staff do not have understanding, ownership and proper training a security system / plan will not work.

Security in a hospital environment encompasses all aspects of the organisation from patient and staff safety to deeply personal information about staff and patients that is distributed throughout the organisation.

While the entire breadth of security issues apply in a hospital, the problem of confidentiality - having information fall into the wrong hands - is perhaps most prominent. In an age when a person's social, financial and professional standing can be destroyed by the revelation of a diagnosis, the sensitivity of such information is extreme. For example, pathology results may be delivered to and left on a counter, where a passer-by can view them; staff may look at "a friend's" results and pass on information to their friends and family. These are breaches of confidentiality that do occur in all health institutions.

There is a rapid assimilation of confidential information - pathology results and medical records - into the electronic information systems. This greatly reduces the hospitals' capacity to control access through the "informal" security systems which operate everywhere: in which the information item, existing uniquely on a single piece of paper, is treated with reasonable care by whichever individual has responsibility for it at any time. Once held electronically, the information "exists" in an infinity of places and can potentially be seen on hundreds of screens, on numerous reports - and on any hacker's Personal Computer.

In addition to the serious consequences of confidentiality breaches, a hospital is one of the few places in which a relatively minor loss of access to information may be life-threatening. For example, failure to alert a prescribing doctor to a patient's allergic response to an otherwise beneficial drug may cause severe illness or death. In today's paper-based systems, clinical staff take immense personal responsibility for ensuring that such data is properly recorded and made available. In future electronically-managed systems, will information systems staff feel the same sense of responsibility for ensuring that the item of data has both integrity and is seen by clinicians at the crucial moment?

These issues demand a more systematic response to making safe and controlling access to significant information. The only way to avoid risking harm to patients is to train staff on the implications of such types of action, to develop systematic security controls and to train staff thoroughly in correct procedures.

The methodology employed in developing and implementing security plans in such an environment must above all engage the commitment of the *people* on whom security depends. People make opportunities, through lack of awareness, through carelessness and laziness. People are the perpetrators of deliberate security breaches, people are the victims, people are the systems users with capacity to support or ignore security provisions, people are the managers who set the rules (practical or onerous), involve the staff (enthusiastically or casually), monitor compliance (with commitment or just by-the-book).

Security planning and management involves an integration of people in an organisation who are stake-holders (in the broadest sense) in the integrity, privacy and continued availability of systems and data.

3 A SOFT SYSTEMS APPROACH

SSM was developed in response to the inadequacy of systems engineering approaches to situations where objectives are complex and poorly defined, and where differences of opinion are numerous. Most management problems are characterised by obscurity and complexity, while systems analysis is useful where the *objective* is a given, and the *task* is to devise a system which will meet the objective with efficiency and reliability. SSM has an emphasis on human activity systems, comparing ideal or conceptual thinking in the systems world with what is currently occurring in the real world. The gaps are then analysed and solutions which are considered feasible and desirable are implemented.

Von Burlow (1989) explains SSM as "a methodology that aims to bring about improvement in areas of social concern by activating in the people involved in the situation a learning cycle which is ideally never-ending. The learning takes place through the iterative process of using systems concepts to reflect upon and debate perceptions of the real world, taking action in the real world, and again reflecting on the happenings using systems concepts. The reflection and debate is structured by a number of systemic models. These are conceived as holistic ideal types of certain aspects of the problem situation rather than as accounts of it. It is taken as given that no objective and complete account of a problem situation can be provided".

The following diagram indicates the main structure of a soft systems approach.

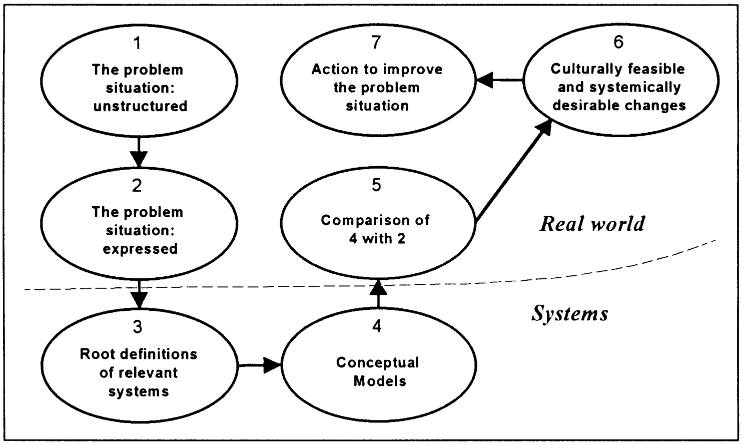
1
The problem situation: unstructured
7
Action to improve the problem situation
6
Culturally feasible and systemically desirable changes
2
The problem situation: expressed
5
Comparison of 4 with 2
Real world
Systems
3
Root definitions of relevant systems
4
Conceptual Models

Figure 1 Soft Systems Methodology in outline. Source: Adapted from Checkland (1981).

Activities 1 and 2 seek to build the richest possible picture of the problem situation, in all its complexity and according to the various perceptions of the stakeholders. Techniques include the Rich Picture (see Figure 3 below), a pictorial representation illustrating perceived problems. Activities 3 and 4 build models of the activities relevant to the problem situation, taking into account the organisation's future, and aiming at an ideal solution to the risks and inadequacies of the present day. Techniques include Root Definitions (high-level system definitions), CATWOEs (identification of stakeholders, reason for existence, environmental constraints and other factors) and Conceptual Models (Figures 4 and 5).

The models are then compared with the problem situation (activity 5). Participants debate the differences and identify the means by which improvements may be made. Strong reality-checking takes place in activity 6, to ensure that proposed actions emerging from the process are both practically feasible and culturally desirable in their implied effect.

The human interaction in this approach is extremely important. As suggested by Davies and Ledington, "*this methodology is a means of guiding the tackling of real world situations which are perceived as problematical for some of the time by at least one member of that situation. This is the nature of the problem situation. It is necessary to do some analysis of that situation before embarking upon the generation of relevant systems in order that the world of systems thinking can be entered.*

"*It is considered of more use if the analysis can be carried out by those within the situation. This means handing over the methodology to those in the perceived problem situation. This is not always easy but is an ideal type prospect for the use of the methodology.*" Davies and Ledington (1991):11,12)

The use of the SSM in information security has been recommended previously by Hitchings (1994), and this paper expands upon this view. In addition, the model proposed herein has been designed for practical application in security planning by management in a private hospital

4 SECURITY MANAGEMENT MODEL

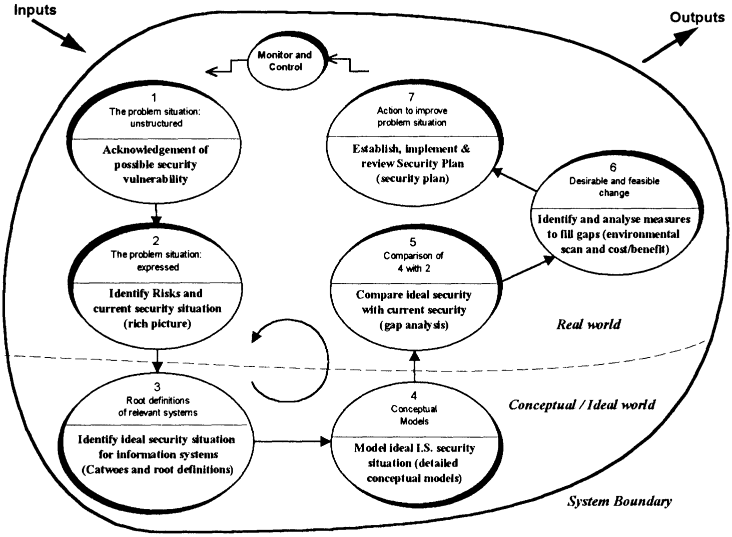
Inputs
Outputs
Monitor and Control
1
The problem situation: unstructured
Acknowledgement of possible security vulnerability
7
Action to improve problem situation
Establish, implement & review Security Plan (security plan)
6
Desirable and feasible change
Identify and analyse measures to fill gaps (environmental scan and cost/benefit)
2
The problem situation: expressed
Identify Risks and current security situation (rich picture)
5
Comparison of 4 with 2
Compare ideal security with current security (gap analysis)
Real world
3
Root definitions of relevant systems
Identify ideal security situation for information systems (Catwoes and root definitions)
4
Conceptual Models
Model ideal I.S. security situation (detailed conceptual models)
Conceptual / Ideal world
System Boundary

Figure 2 Information Security Management using SSM.

The above security management model, which takes into account the human dimensions of security as well as different views of security needs, has been derived using a Soft Systems approach. Several adaptations have been made to the Checkland SSM model illustrated in Figure 1, one of the major additions being the recognition of system boundaries and the influences of entities external to the system. Wilson (1990) emphasises the importance of system boundaries in the conceptual modelling stage, the inclusion of information flows for analysis of information systems, and the use of activities to monitor and control performance. These are all essential items required to build the big picture, offering a holistic view rather than segmented analysis and synthesis. Figure 2 illustrates the proposed information security management approach. **Activity 1** is acknowledgment of possible security vulnerabilities. The second stage identifies the risks and analyses the organisation's current security situation. Identification involves workshops representing all stakeholders, which develop rich pictures of the problem situation. An analysis of present information security measures and vulnerabilities within and around the systems should also be carried out to provide an accurate and detailed picture of the current situation.

The first two activities are undertaken in the real world, engaging people in the problem situation. The next two stages are conceptual (or according to Checkland, 1981, *systems thinking*) activities where high level analysis is carried out. Their aim is "to get a carefully phrased explicit statement of the nature of some systems which will subsequently be seen to be relevant in improving the problem situation" (Checkland, 1981:164). This in effect involves the development of ideal or conceptual security approaches for the organisation's information assets. **Activity 3** offers ideal security situations for information systems, in the form of root definitions. A root definition defines a system at a high level, recognising the stakeholders involved, the reason the system is active, the world view and the environment in which the system exists and operates. Root definitions are formulated by considering the following CATWOE elements (Checkland & Scholes, 1990:35):

C	customers	the victims or beneficiaries of T
A	actors	those who would do T
T	transformation	the conversion of input to output process
W	'Weltanschauung'	the worldview which makes this T meaningful in
context		
O	owner(s)	those who could stop T
E	environmental constraints	elements outside the system which it takes as given.

Activity 4 expands the root definitions into more detailed conceptual models of ideal security approaches (or *systems* in its widest sense). This represents the necessary security activities the system must perform to become the system defined in the root definition. The models will be compared to the real world in **Activity 5** to ensure relevance and identify any gaps. To fill these gaps, **Activity 6** scans available security products and techniques, and analyses which changes will be most desirable and feasible for the organisation in question.

Activity 7 works to improve the problem situation by the establishing a security plan, incorporating features and measures deemed appropriate in the previous stage. The security plan is implemented and regularly reviewed to ensure compliance and continued meeting of needs. This review process links directly into the process which monitors and controls the system. The zigzag arrows to and from this activity in the diagram indicate that this function receives input from all other activities and disseminates output to all activities.

The boundary around the system illustrates the system's actions and responsibilities. Any entity or factor appearing outside the boundary line is external, over which the system has little control. Activities appearing within the boundary are the minimum set of activities required to fulfil the root definition previously devised.

5 APPLICATION AT HOLLYWOOD HOSPITAL

As emphasised by Gritzalis and his co-authors, health information systems are now critical to the health care industry, and managers must ensure the confidentiality and integrity of data held and continued availability of these critical systems (Gritzalis et al, 1994).

Hollywood Private Hospital, with 300 beds, is the largest private hospital of the Ramsay Group, an Australian-based organisation that has 16 hospitals Australia, 14 in the United States and 2 hospitals in Europe, as well as managing a hospital in Asia. Hollywood Hospital is unique in Australia in its patient mix and its relationships to federal and state government. Until early 1994, it was a federally-run Veterans' Hospital with a vigorous role in teaching and research. On its sale to the private sector, it was determined that all its public-sector functions should be continued. Consequently, it now cares for Veterans, general public and (in the very near future) private patients. It remains a Teaching and Research institution, with strong links to the state's major public hospitals and the University of WA. Its funding - and therefore its information-exchange responsibilities - encompass the federal Department of

Veterans' Affairs, the state and federal Departments of Health, and the private health insurers. In addition, it is in a competitive marketplace, and plans to invest substantially in the complete reconstruction of its facilities, intending to become the prestige private health facility in the state.

In this complex position, and having the intense duty of care which applies to all hospitals, a wide range of areas of concern apply to Hollywood Private Hospital when Information Security is under consideration:

- *Integrity* of patient and staff information.
- *Confidentiality and safety* of patient and staff information.
- *Risk to persons* which may arise from lack of correct access to information, such as patient allergies, patients who may attack staff.
- *Loss or damage* to property, through theft, fire or other cause, where poor information or security breaches complicate the risk.
- *Risk to competitiveness* where Hollywood's market position may be at risk through:
  - losing confidence of patients and therefore reputation;
  - failing to maintain confidentiality of commercially-sensitive information;
  - losing the confidence of any of the many institutions - state and federal agencies, hospitals, universities, laboratories - on which commercial success rely.

The "unstructured problem situation" may begin to take form in the following Rich Picture, which represents a part of the raw material from which the security planning study will develop an achievable solution.

The study will employ SSM as applied to security management in Section 5 above. Its progress as a project will take the form described below. To ensure ownership of both security concerns and proposed remedies, wide stakeholder representation will be essential. Consultation will take place with representatives from the all departments within the hospital.

Inter-departmental workshops will be held to determine the nature of the concerns regarding security problems as faced in a large hospital. Using SSM's problem-definition techniques, these areas of real-world concern will be grouped and expressed in a systematic fashion.

Root Definitions and CATWOEs

The workshop groups will define the ideal objectives and nature of security management at Hollywood in the future, at the broadest level and for each of the main areas of concern (such as confidentiality of patient information). For each area, a Root Definition will be developed that expresses the goal, perspective and means around which the plan will be built. Using the CATWOE technique, a comprehensive definition will be reached of the stakeholders, environment and activities concerned with each area of security management.

The following theoretical examples demonstrate the nature of these definitions.

Root Definition of a system to control confidentiality of pathology results:

> *a system engaging the efforts of clinical, pathology and records staff, which ensures that pathology results are safe from unauthorised observation yet available for patient care, so that patients' rights and well being are safeguarded, in the complex, pressured and sometimes crises-driven hospital environment.*

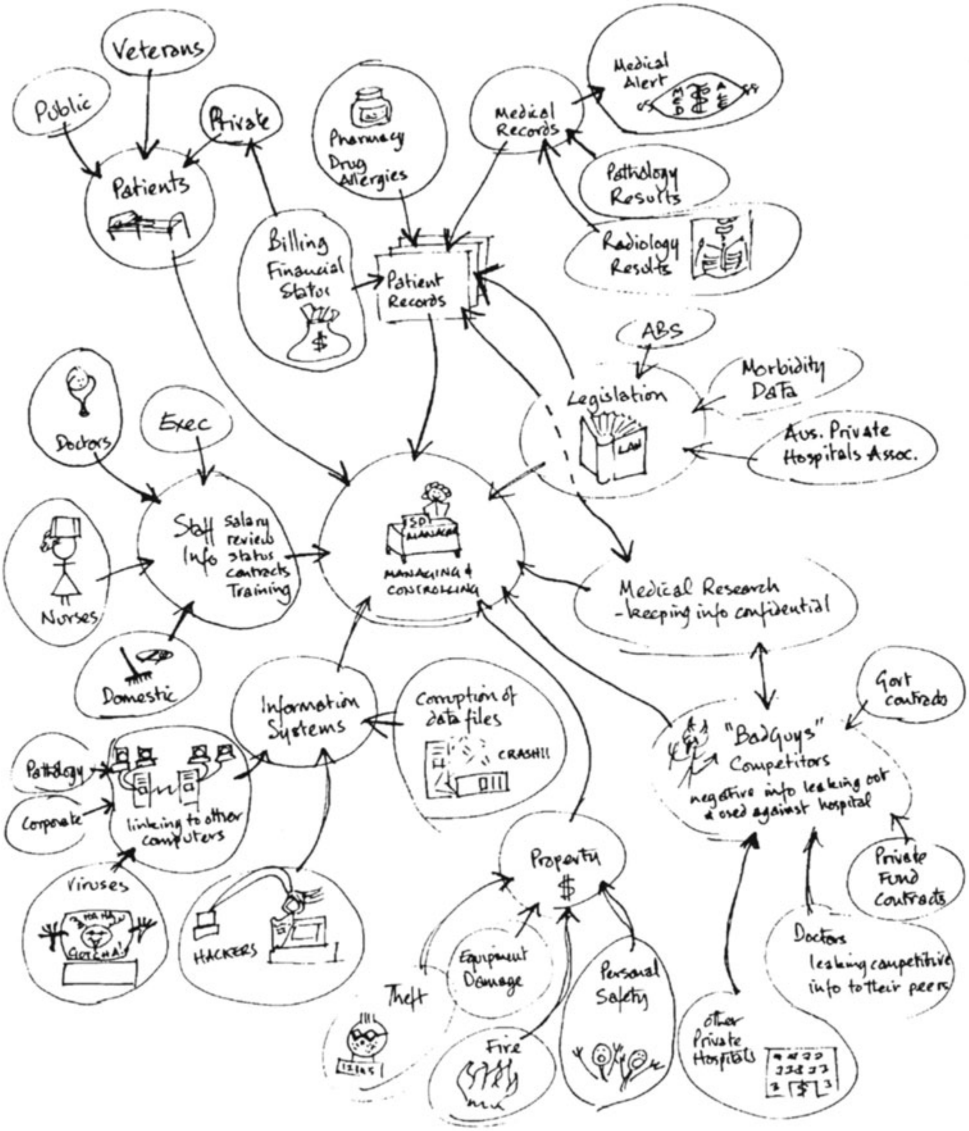

Figure 3 *Rich Picture* of Security Issues at Hollywood Private Hospital

CATWOE of the process controlling confidentiality of pathology results:

Clients	patients associated with Hollywood Private Hospital
Actors	staff of the hospital; staff of pathology laboratories
Transformation	· pathology information is reliably available to clinicians when required · such information is never accessible by others
Weltanschauung	to ensure that information which should be available only for the purpose of providing patient care is not available or used for any other purpose
Owners	Hospital management
Environment	· legislation · reporting requirements of government agencies and health insurers · social attitudes changing information management technologies

Figure 4: Root Definition and CATWOE.

Conceptual Modelling

Working from these definitions, the workshop teams will develop a graphical model of the activities which would comprise the ideal security management system for the hospital, including models of its subsystems. These models will describe the key activities, the flow of information and control from one activity to another, the inputs and outputs to the activity systems, and the influences of the outside world. A theoretical example follows.

Gap analysis

The conceptual models will describe an ideal system - that is, the system would apply an ideal level of control over security risks. In the next phase, the workshop teams will look in detail at the differences between the present and the ideal, determining what steps would lead to the ideal system, how they could be undertaken, how much they would cost and what impact they might have on working practices and the social environment of the institution. During this gap analysis the teams can agree priorities for attention, based on the potential improvements in security practices and the likely reduction of risk attached to each activity.

Finally, the potential changes will be considered by the teams to determine which are *feasible*, that is: affordable; achievable; manageable - and which are also *systemically desirable*, that is: socially acceptable; having a positive balance between additional effort and beneficial effect; compatible with the business and management objectives of the organisation.

The change actions which fit these criteria comprise substance of the Security Plan. The plan itself will need to address the actions in terms of procedures meaningful to staff in the operational areas affected, and set performance indicators which enable managers to monitor the degree of implementation success.

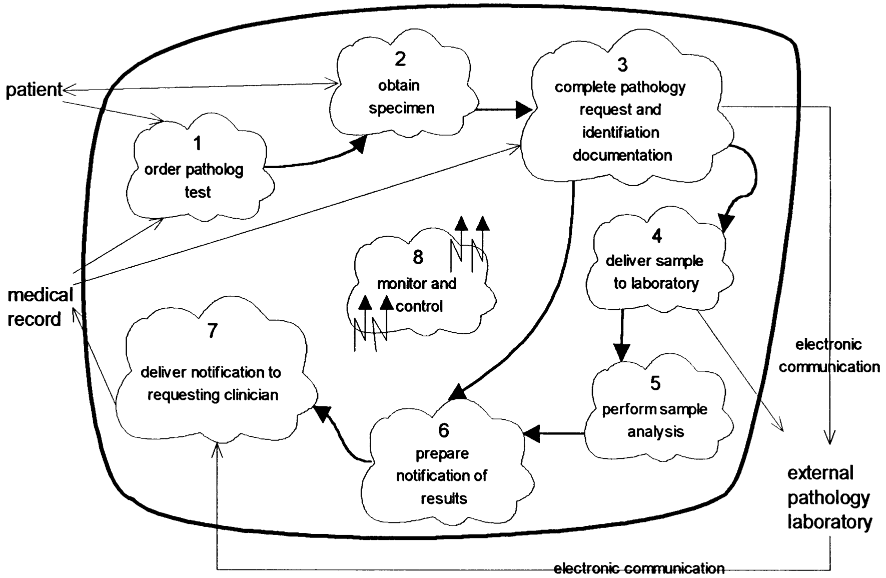

Figure 5: Example of a Conceptual Model.

Implementing the Security Plan

The details of practical implementation of security management are, of course, unique to the circumstances of the organisation. The final component of the planning phase will be to develop an implementation process in which all stakeholders will take ownership. At a minimum, the process must include -

- implementation schedule: timeframes, responsibilities and costs
- training plans and competency targets
- a formal review cycle and process to accommodate changes in the security environment
- security performance measurement targets and processes, to make it possible to evaluate the success of security management in practice.

6 CONCLUSION

The application of a soft systems approach to information security planning is seen as an important step in raising the security awareness of all employees. By acknowledging different views of security problems within an organisation, the stakeholders are able to understand the need for security measures and take part in the systems designed to minimise the associated risks.

The opportunity to apply this approach to Hollywood Hospital during the next year will provide a testing ground for the methodology proposed in section 5 above. No doubt modifications will be made to the model as we progress through the experiment, however, we feel sure that all parties involved will benefit from this 'people' approach to security planning.

7 REFERENCES

Becker R.S. (1977) *The Data Processing Security Game*, Pergamon Press

Checkland P. (1981) *Systems Thinking, Systems Practice*, John Wiley & Sons, Chichester

Checkland P. & Scholes J (1990) *Soft Systems Methodology in Action*, John Wiley & Sons, Chichester

Coopers and Lybrand (1988) *The Security of Network Systems*, USA

Davies L & Ledington P. (1991) *Information in Action: Soft Systems Methodology*, MacMillan Education, Hampshire, UK

Gasser M (1988) *Building a Secure Computer System*, Van Nostrand Reinhold

Gritzalis D, Katsikas S & Darzentas J (1994) *A High Level Security Policy for Health Care Establishments*, Proceedings of IFIP SEC 94, Curacao

Hafner K & Markoff J (1993) *Cyberpunk*, Corgi Books, London

Hitchings J & Williams B. (1992) Information Technology, Management Control and Security, *Management Accounting*, October, pp 34-35

Hitchings J (1994) *The Need for a New Approach to Information Security*, Proceedings of IFIP SEC 94, Curacao

Lane V.P. (1985) *Security of Computer Based Information Systems*, MacMillan

NCC (1994) *IT Security Breaches Survey Summary*, National Computing Centre Limited, UK

Office of the Auditor General (1992) *Management of Information Systems in the Public Sector*, Report of the Auditor General to the Western Australian Parliament

Power, K. (1994) Crooks Among Colleagues, *Informatics*, November, pp 22-26

Seah V, Kamay V, Adams T, and Sung H (1991) *A Study of Computer Security and Computer Abuse in Singapore - 1990*, SIM Monograph No. 3, Singapore Institute of Management

Stemman R (1987) The Hidden Face of Fraud, *Business Computing & Communications*, Sept, pp 34-36

von Burlow I. (1989) *The bounding of a problem situation and the concept of a system's boundary in soft systems methodology*, Journal of Applied Systems Analysis, No 16, pp 35-41

Watney D & Turney P (1990) *Auditing EDP Systems*, Prentice-Hall

Wilson B. (1990) *Systems: Concepts, Methodologies and Applications*, John Wiley & Sons, Chichester

Wood M (1982) *Introducing Computer Security*, NCC

8 BIOGRAPHIES

Helen James

Helen James is a lecturer with the School of Information Systems at Curtin University of Technology. Her major research interests include computer crime, managing computer security and ethics. Helen has twenty years' experience in computing, audit and security, and currently consults in security and information technology to government departments, private organisations and educational institutions. Helen has been a judge for the annual IT awards of the Australian Computer Society in Western Australia for the past five years and is also secretary of the Australian Computer Abuse Research Bureau in Western Australia. Her personal interests include scuba diving, raising Australian native trees and sampling Australian wines.

Katerina Andronis

Katerina Andronis is Manager of Information Systems at Hollywood Private Hospital, a 320-bed institution which is almost unique as a teaching hospital combining private, public and Veterans' Affairs patients. She has supervised the transition of the hospital from a centralised mainframe environment to network-supported distributed-processing, in parallel with its move from government to private ownership. Katerina's experience in control of HealthCare information covers almost 20 years, from software development to IT management over one of Australia's largest private hospital groups. Her personal interests include performance and visual arts, and she is Past President of the WA Friends of the Australian Archeological Institute at Athens.

William Paul

William Paul consults to the Western Australian government and industry in business process and information management. He is presently coordinating construction and implementation of the state-wide network of systems which will manage the state's public health and health funding information, and playing a similar role in the creation of systems to manage the state's land and building assets. He has developed security plans for the WA Law Courts and Telecom Network Services. His 25 years in management have included Health, publishing, international charities and IT, in London, Paris, New York as well as Australia. His interests include literature and opera.