Managing Information for Better Health Outcomes in Australia and the Asia Pacific Region

11 to 13 August 1997

Asia Pacific Association of Medical Informatics

HISA

CONFERENCE PROCEEDINGS

ISBN 0 646 30576X

National Library of Australia

Implementing Computer Security in a Small to Medium Sized Institution

Zelmer, A C Lynn

Department of Mathematics and Computing, Central Queensland University, Rockhampton 4702

The Computer Security Committee of Central Queensland University (CQU) has been responsible for CQU's adoption of an Information Technology Security Policy and Code of Conduct and for the implementation of that Policy within the multi-campus university. CQU is a regional institution with seven major campus sites in three states as well as overseas study centres, numerous networks and systems for connecting to the university computer systems. IT (Information Technology) security concerns over the past four years have included students and others hacking into and out of the institution's computer systems, computer-based harassment, equipment theft, the accidental loss of critical financial and other data, and the circulation of documents from the office of the Chief Executive Officer containing a computer virus.

Part of the ongoing implementation of CQU's Policy has included orientation sessions, workshops, the development of a student-oriented videotape, various information sheets available from the university's World Wide Web pages, and adapting the *Security and Privacy Guidelines for Health Information Systems* (1) from a health to a university setting (2).

This paper describes requirements for an IT Security Policy, the steps required to implement such a policy within a small to medium sized institution, and some resources available to assist these processes.

1 Introduction

1.1 Inherent insecurity

Information systems seem to be inherently insecure. Users seldom regard information *per se* as something which warrants even the same security considerations that they would provide for their own credit cards, wallet or purse. Patient records, for example, are routinely left in semi-public view on the counter at the clinic or nursing station or in a holder on the bottom of the patient's bed. Sensitive records have been disposed of at the tip rather than through shredding by a secure disposal service and medical practitioners have used live patient data when demonstrating clinical record systems or when training new staff.

Computer-based information systems increase the risk of loss and/or data corruption since the data stored on a computer can be copied or modified so easily. While many data system losses come from user error, including forgetting to make a backup of critical data or deleting a critical file, and data theft (typically copying data for use by a third party) is most likely perpetrated by a trusted user, computer systems do become significantly less secure once connected to a network.

Modem or Internet access means almost anyone with the appropriate knowledge can access the system from anywhere in the world, and some have been attacked:

> The 1996 Computer Security Institute/FBI Computer Crime and Security Survey found that 42 percent of the respondents experienced unauthorized use of their computer systems in the last 12 months. Almost 40 percent of these respondents

experienced frequent incidents through both remote dial-in and Internet connections.
(3) [Australian statistics are unlikely to be much different from the USA.]

Maintaining a secure information system requires a supportive management, a 'climate' of responsible use among all users of the system, and appropriate procedures to both minimise the risks of unauthorised access and to recover from disasters large and small.

In 1995 the author, a senior lecturer with the Department of Mathematics and Computing at Central Queensland University (CQU), Chair of CQU's Computer Security Committee, author/editor of materials for healthcare professionals on computer use (4, 5) and producer of healthcare training materials (6, 7), obtained permission from COACH (Canada's Health Informatics Association) to adapt their recently published *Security and Privacy Guidelines for Health Information Systems* (1) for use in a university setting. This paper provides the background to that decision and examines subsequent events as a case study of the implementation of a computer security policy within a small to medium sized public institution.

1.2 Central Queensland University

Central Queensland University is a regional university with one large and seven smaller campuses. It has a number of computers supporting administrative functions (payroll, student records, library, etc.) as well as a network serving both staff and students. While CQU has more users than a typical hospital or regional health authority because of its studentS, it is otherwise quite similar. The university's student record system, for example, requires much the same level of security and privacy considerations as a patient record system and has many of the same difficulties with users, including staff who cannot remember passwords and demand 'transparent' systems.

In 1994 after much debate within the Computer Security Committee, CQU adopted a policy (modelled after a similar policy at University of Sydney) on the security of information technology (8). Implementation of such a policy, however, is the responsibility of each operational unit and individual within the university and little has been done by most units to implement the policy.

The Computer Security Committee has posted (Figure 1) the Policy and Code of Conduct on the CQU WWW pages and in every university controlled student-use computer laboratory, and has begun a series of 'tip' sheets (currently E-mail: The Electronic Postcard, Making Backups a Regular Routine, and Password Use and Selection) (9) to assist users of the university's network and computer systems.

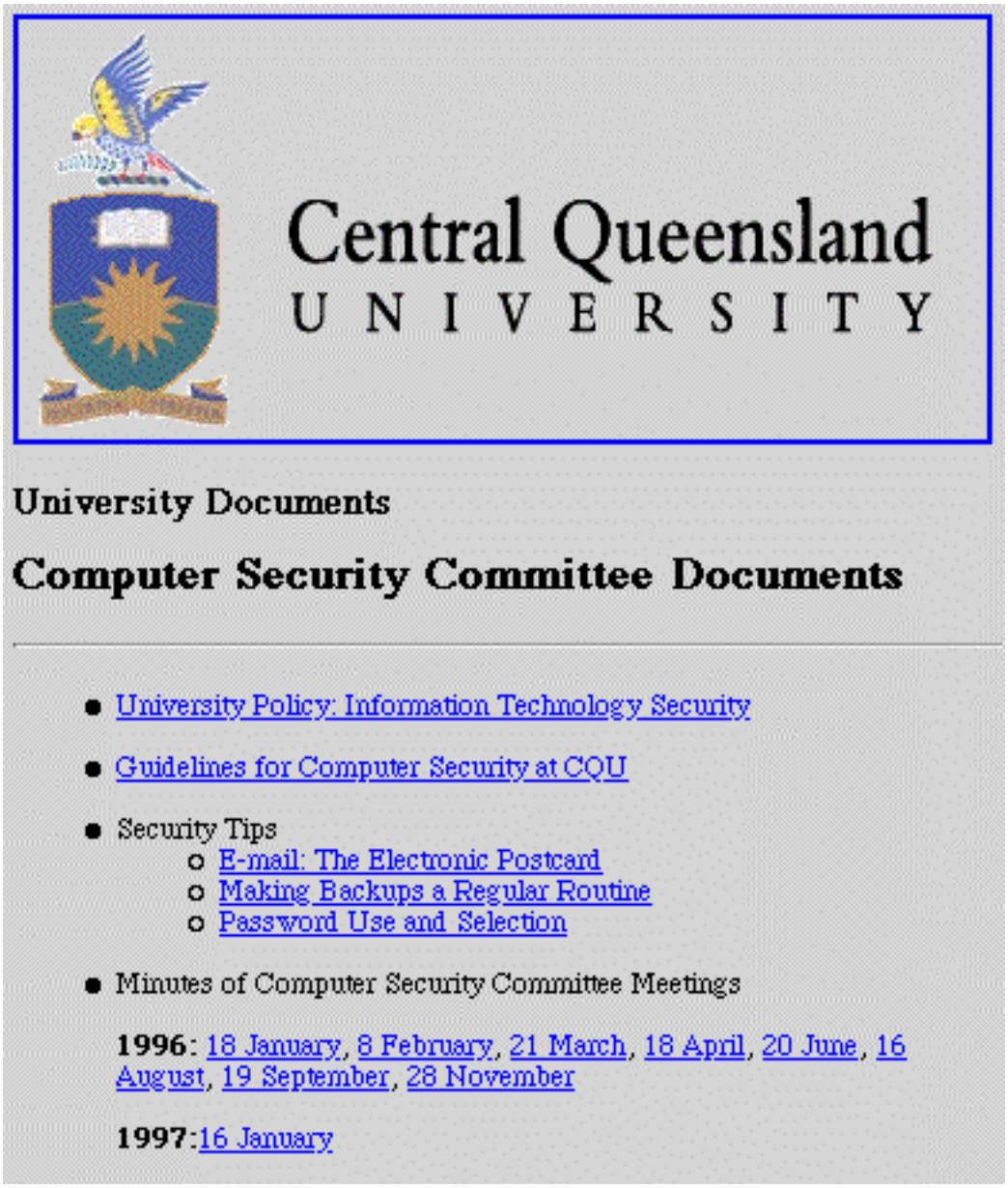


Figure 1 CQU Computer Security Committee home page: http://www.cqu.edu.au/documents/compsec/home.html

Slightly over a decade ago CQU had a single campus, a centralised computer system with a relatively small number of terminals and almost no external access. In 1989, for example, there were only two staff members using the external data link--the predecessor of the Internet--and one of them was the network manager. Data security seemed relatively easy to control through individual accounts and passwords. Unfortunately, this was a false sense of security as many individuals used easily guessed passwords or wrote their password on a note tacked to their office bulletin board.

The system became more complex with the increased demands for external communications, initially just electronic mail and file transfers, and the use of desktop computers, initially used in a stand-alone mode but increasingly networked. In 1997, the university has over 20 student laboratories on 8 campuses in three states plus approximately 1000 desktop and laptop computers for staff (research, productivity, and communications), administration and public access (as in the Libraries). It also has several larger computers for administrative and accounting purposes and an unknown number of file servers and other specialised network facilities. Maintenance and support services are provided both by the

central Information Technology Division (ITD) and Faculty/Division employed network managers, programmers, and computer service officers.

Student and staff traffic is normally on separate network zones to avoid some potential security conflicts but many students are much more knowledgable about the operation of the system than staff. Bachelor of Information Technology students, for example, learn how to break into a system as part of learning how to manage a system.

Some aspects of computer security are governed by external agencies such as the Federal Police, AUSCERT, Australia's emergency response team, and the university's auditors. This means, for example, that CQU reports any attempts at breaking into the system, whether from inside or outside the university, to the proper authorities. These agencies (Figure 2) also provide some on-going support activities for institutions building a secure system.

Figure 2 AUSCERT papers and other resources are available to assist in designing secure systems; Home Page URL: http://www.auscert.org.au/home.html.

The Computer Security Committee continues to deal with 'challenges' as diverse as students fraudulently gaining access to STD/ISD telephone facilities using improperly obtained PBX passwords, security staff stealing computers from student labs (caught by newly introduced closed circuit television recorders), sexual harassment via electronic mail, and students using CQU as a base to break into another university's computer system. However the expansion of computing and networking beyond the ITD, the general lack of knowledge about what is necessary and the costs involved means that university has not been able to conduct a proper information technology inventory, let alone a proper threat risk assessment or a disaster recovery plan.

Computer security *is* an individual responsibility but implementation of good security procedures depends upon a climate of administrative support. The University Chancellery has

been the source of one of the university's worst computer disasters when they circulated virus infected electronic mail 'attachments' late 1996 and early 1997. Obviously they didn't do this deliberately, however, through poor security management practices they managed to circulate such infected files (containing Word macro viruses) on at least three occasions, and did so to every member of the university staff.

The cost of these 'attacks' was in the tens of thousands of dollars in lost time, the nuisance of removing the infection, and for those individuals for whom the virus precipitated file loss, even hard drive failure. The problem was not alleviated when the initial Microsoft-supplied procedure for removing the viruses did not work or by the university's initial reluctance to supply continuous protection software to at least those staff, such as the Chancellery, who are regularly exposed to files originating outside the system.

Hopefully the experience will motivate Chancellery, staff and students to use virus protection software and has sensitised them to other potential computer security issues.

Unfortunately for the health sector, healthcare institutions may be even worse than the universities at implementing computer security procedures and related disaster recovery plans. The Computer Sciences Corporation annual survey which included 154 large corporate and government organisations from the Asia/Pacific region, Critical Issues of Information Systems Management, revealed that "Asia/Pacific companies lag well behind their European and North American counterparts in strategies for disaster recovery", and that "government and health organisations were responsible for the lack of disaster recovery strategies in this region" (10).

2. The Guidelines

The author was introduced to the COACH Guidelines shortly after they were published in 1995 and negotiated for permission to adapt them to a university setting. This was done in print form early in 1996, followed by an electronic version on the web (Figure 3) later in 1996. As the Guidelines (2) indicate, they are intended to be a resource, a goal, rather than a prescription:

> These guidelines are provided as a resource to assist the university to:
>
> - minimise the risk of unauthorised collection, use, disclosure, modification or destruction of university data;
> - maximise the integrity, availability and efficacy of administering authorised access to university information; and
> - protect the privacy of users and providers of university services.
>
> Implementation of these guidelines should be regarded as a goal to be attained to improve the security and privacy of university data held by the university. Since no system can be absolutely secure, application of the guidelines does not guarantee the confidentiality, integrity or availability of university data.

They go on to indicate that security and privacy decisions must be based on a process of risk assessment, and include information on how to conduct such a risk assessment:

> The university must make decisions concerning security and privacy based on an objective assessment of potential risks. Such risks must be balanced against the costs and other organisational priorities. Responsibility and accountability for the security and privacy of university data rests solely with the university.
> The university should make use of the Threat Risk Assessment Process to identify solutions that are cost effective while meeting security and privacy requirements.

While the guidelines are specifically targeted to the computerised information processing environment, many of the same principles will apply to traditional paper-based university information systems.

2.1 Structure of the Guidelines

The Central Queensland University *Security and Privacy Guidelines for University Information Systems* (Figure 2) closely parallel the COACH document and are structured as follows:

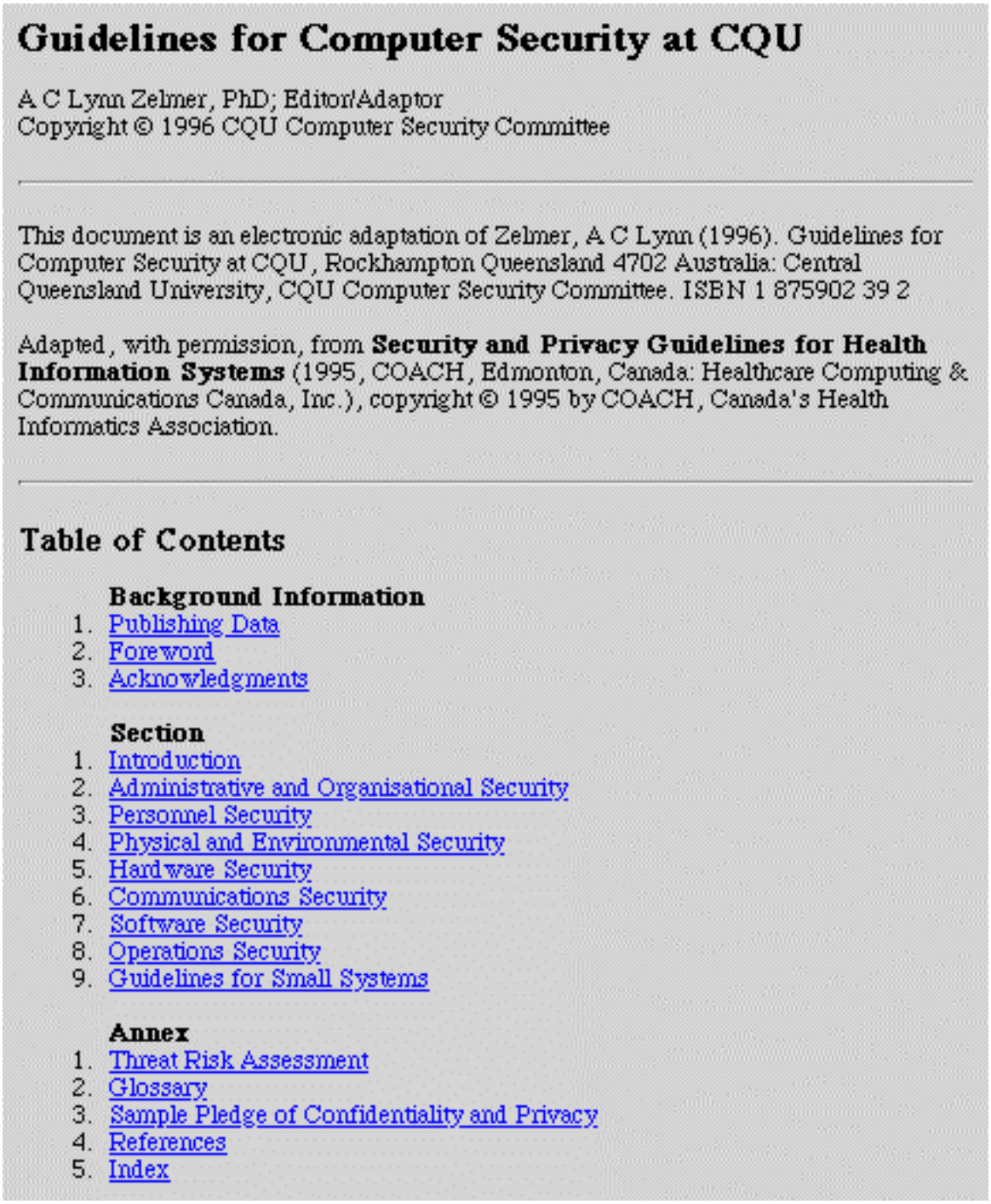
1. Introduction
2. Administrative and Organisational Security
3. Personnel Security
4. Physical and Environmental Security
5. Hardware Security
6. Communications Security
7. Software Security
8. Operations Security
9. Guidelines for Small Systems

Parts 2 through 8 are intended for the larger university systems, such as local and wide area networks, interconnected systems, central computer facilities and the Information Technology Division. These organisations typically have complex operational environments, large numbers of staff/users, and significant information technology assets.

Part 9 is intended for small systems, either stand-alone or independently operated. Typically operated by a single staff member, researcher, or student these might include a system in a faculty or department, clinic, lab, individual office (on campus or home-based) or small campus. These enterprises typically have limited technology assets, a smaller client base and fewer staff than the larger enterprise. Part 9 also applies to remote access from satellite locations (eg. remote access to the Library collection), labs, employee homes, or smaller campuses.

As the foreword notes, responsibility for implementation rests with the Faculties and Divisions:

> It has been suggested that the document would be more proactive if it had been written using *shall* be done, rather than *should* be done. That is probably true. In presenting this document as a set of guidelines, however, we are leaving the responsibility for implementation with the operational units. It is, therefore, the responsibility of each Faculty, Division, or other operating unit to implement (and enforce) those procedures which are appropriate to your individual situation.



Guidelines for Computer Security at CQU

A C Lynn Zelmer, PhD; Editor/Adaptor
Copyright © 1996 CQU Computer Security Committee

This document is an electronic adaptation of Zelmer, A C Lynn (1996). Guidelines for Computer Security at CQU, Rockhampton Queensland 4702 Australia: Central Queensland University, CQU Computer Security Committee. ISBN 1 875902 39 2

Adapted, with permission, from **Security and Privacy Guidelines for Health Information Systems** (1995, COACH, Edmonton, Canada: Healthcare Computing & Communications Canada, Inc.), copyright © 1995 by COACH, Canada's Health Informatics Association.

Table of Contents

Background Information

1. Publishing Data
2. Foreword
3. Acknowledgments

Section

1. Introduction
2. Administrative and Organisational Security
3. Personnel Security
4. Physical and Environmental Security
5. Hardware Security
6. Communications Security
7. Software Security
8. Operations Security
9. Guidelines for Small Systems

Annex

1. Threat Risk Assessment
2. Glossary
3. Sample Pledge of Confidentiality and Privacy
4. References
5. Index

Figure 3 Guidelines for Computer Security at CQU:
http://www.cqu.edu.au/documents/compsec/guidelines/ cqu_sec01.html

2.2 Threat Risk Assessment

Following a full asset inventory (data, personnel, software and hardware) it is necessary to conduct a threat assessment to identify the potential agents or events (theft, vandalism, viruses, etc.) that could place each asset at risk. Each agent or event must then be classified by the type of threat (disclosure, interruption, modification, removal or destruction), the likelihood of the event occurring (low, medium, or high), and the impact of the event (very serious, for example, may compromise "duty of care", serious--may disrupt normal operations, cause significant inconvenience to clients, or be costly to rectify--or less serious, that is may disrupt non-critical operations or cause limited inconvenience to employees). The threat assessment concludes by determining the consequences of the event happening. For example: What would be the

consequences of the Chancellery circulating electronic mail messages infected by a file damaging virus? How many hours of work would be required to replace lost or damaged data? How much data would be impossible to recover? Potential consequences include loss of privacy, loss of trust, loss of asset, and loss of service

Risk assessment assesses the adequacy of existing safeguards to protect against potential threats. Risk assessment starts by listing the existing safeguards to protect against the potential event, then looks at the institution's vulnerability before rating each potential risk as low (requires some attention and consideration as good business practice), moderate (requires attention and safeguard attention in the near future) and high (requires immediate attention and safeguard implementation).

Unfortunately, most institutions never get this far, let alone looking at what additional safeguards are required to lower risks to an acceptable level. There are two likely reasons for this; the first is a lack of policy and support from the senior levels of the organisation, the second is the perceived costs, since most organisations do not look at the costs of not having proper procedures and safeguards.

Assuming that the institution has got this far, however, the recommended safeguards and their alternatives can be ranked on the basis of the lowered risks of each event. Realistically, it is not always possible to implement every recommendation because of technical or physical limitations, time or financial constraints. Disaster recover planning also follows from the threat risk assessment. Unless an organisation knows its assets, and the threats/risks for those assets, it cannot develop plans for what to do in the event of a disaster, large or small.

3. Constraints and implementation activities

3.1 Constraints

An ACM (Association for Computing Machinery, the US equivalent of the Australian Computer Society) Special Interest Group article provides a framework for understanding computer security on an individual computer (11). The same framework applies to centralised systems and networks, and closely parallels the structure of the *Guidelines*.

> Security has two primary aspects: *overall system level and information level* which includes the software. Data security can be thought of as having three foci. These are *secrecy*, the protection of data and programs stored within the computer from unauthorized access; the second aspect is *integrity*, the protection of data and programs from unauthorized change; and finally *availability*, the protection of data and software from situations in which the data is not suable by those who have authorized access. System security is often characterized by a series of layers of protection. Those layers are policy, personnel, network, operating system, and application. [emphasis in original]

The framework similarly applies to many of the operational constraints: inadequate policy, lack of commitment from and training of personnel, a network which continues to expands without control, an operating system (or systems) which are inadequate to the task(s) for which they are used and were not designed for any form of security, and a variety of inconsistent, incompatible applications.

The *Guidelines* suggest that it is important to identify individuals who will have specific information security responsibilities at the university and faculty/division levels. The university-level Security and Privacy Officer should, it states, be a member of the CQU Computer Security Committee with the Faculty/Division Security and Privacy Officer reporting to the Dean/Head of Division to ensure that they have the necessary authority exists for enforcing the policies. Even more important, as such Officers would be unable to operate without management support and appropriate budgets:

> The Security and Privacy Policy should identify key management personnel who have responsibility for security and privacy, including the Chief Executive Officer, Chief Information Officer, and Faculty/Division Heads. These responsibilities should be included in position descriptions, mandates and goals of each position.
>
> As the ACM article cited above noted, however, policy is
> arguably the most important aspect of security. From two perspectives it is important in that an organization's management must recognize the importance of security and form some formal structure within which to deal with the issues that arise which impact security of computer systems. Even in a home computer this is essential. The owner must recognize that security of the computer is important and establish policy to assure that security is maintained... [This] is as critical as it is for those who deal with larger machines. Such things as establishing a regular pattern for backups and determining the environment for the machine fall into this category.

3.2 Implementation activities

Central Queensland University, in common with most Australian universities and healthcare agencies, has not yet implemented the *Guidelines*. Given that the university is currently 'restructuring' its academic operations it is unlikely that a major change of priorities will occur in the near future.

However, the CQU Computer Security Committee has undertaken a number of activities to inform staff and students about computer security and to begin creating a favourable 'climate' for more effective computer security. As previously mentioned, the Committee has developed and disseminated the University's Information Technology Policy and Code of Conduct as well as developing a [small] number of 'tips' for specific security functions. Committee minutes are posted on its World Wide Web site, except for confidential matters, and it has ensured that relevant authorities will be advised in the event of an attack on the computer system, regardless of whether the breach occurs from inside or outside the university. As well, the Committee has participated in International Computer Security Day activities, sponsored an orientation video for students (1996), run two workshops for network administrators (1995 and 1997) and other staff involved directly in managing the computing infrastructure, and scheduled (1997) general briefing sessions for Chancellery, staff and students.

4. References

1. COACH, Canada's Health Informatics Association (1995) *Security and Privacy Guidelines for Health Information Systems*, Edmonton, Canada: Healthcare Computing & Communications Canada, Inc. Coach URL: www.agt.net/public/coachorg/.
2. Zelmer, A C Lynn (Ed/Adaptor) (1996). *Guidelines for Computer Security at CQU*, Rockhampton: CQU Computer Security Committee, 54 pp, ISBN 1 875902 39 2; and in electronic form [http://www.cqu.edu.au/documents/compsec/ guidelines/cqu_sec01.html].
3. Markham, Tom (1997) Internet Security Protocol, Dr Dobb's Journal, June, 70-75.
4. Zelmer, A C Lynn (1993) *Computer Basics for Health Practitioners 1993*, Milton Centre: Australian Health Informatics Association (QLD) Inc, 84 pp, ISBN 0 646 14657 2.
5. Zelmer, A C Lynn (Ed) (1996) *Computer Basics for Health Practitioners 1996*, Rockhampton: CQU Department of Mathematics and Computing for the Australian Health Informatics Association (Queensland) Inc, 118 pp, ISBN 1 875902 34 1.
6. Zelmer, A C Lynn (Principal Investigator) et al (1996). *Diabetes Education* [an interactive multimedia package], Rockhampton: CQU, Draft on CD-ROM distributed for evaluation purposes, May 1996. A 1995 CAUT-funded project.

7. Klotz, Jenny (1997) *Remote Area Nurses: Stories to be told*, Rockhampton: Central Queensland University Centre for the History of Remote Area Nursing, CD-ROM, ISBN 1 875902 49X.
8. University Policy: Information Technology Security and Code of Conduct: Information Technology Security, URL: http://www.cqu.edu.au/documents/compsec/itsec.html.
9. Accessible from URL: http://www.cqu.edu.au/documents/compsec/home.html.
10. Bryan, Louisa (1997) Asia/Pacific lagging in disaster recovery, *ComputerWorld*, 2 May, 4. (www.idg.com.au/ computerworld)
11. Unger, Elizabeth A (1994) Security for Individual Computer Environments: Introduction by the Guest Editor, *ACM SIGICE Bulletin*, 20:1 July, 3-6.