APAMI - HIC 97

Handbook and Proceedings

Fifth National Health Informatics
and the Second Asia Pacific Association of
Medical Informatics Conference
Sydney Australia 11 - 13 August 1997

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

Editors
Sarah McGhee
Terry Hannan
Ian Symonds

ISBN 0 646 30576X

Implementing Computer Security in a Small to Medium Sized Institution

Zelmer, A C Lynn

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

Abstract

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.

As an ACM (Association for Computing Machinery, the US equivalent of the Australian Computer Society) Special Interest Group article (1) notes, 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.

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 (2) from a health to a university setting (3).

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.

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.

References

1 Unger, Elizabeth A (1994) Security for Individual Computer Environments: Introduction by the Guest Editor, ACM SIGICE Bulletin, 20:1 July, 3-6.

2 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/.

3 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].