A SECURITY METHOD FOR HEALTHCARE ORGANIS ATIONS

MATTHEW WARREN AND WILLIAM HUTCHINSON[Ω]
School of Computing & Mathematics, Deakin University, Geelong, Victoria, Australia
'School of Management Information Systems, Edith Cowan University, Perth, Western Australia, Australia.

Keywords: Security Management, Implementation, and Users.

Abstract: The use of participationid approaches to system design has been debated for a number of years. Within this paper we describe a method that was used to effectively design information systems and implement computer security countermeasures within an healthcare environment and shown how it was used in a number of environments.

1. INTRODUCTION

There are now many different types of Information Systems in place in the world, from transaction processing systems to decision support systems. All of these have one thing in common is that they require security. An issue is how can you implement technology including security into an organisation. An example method that can be used is ETHICS (Effective Technical and Human Implementation of Computer based System). The work on ETHICS was undertaken by Enid Mumford of the Manchester Business School, UK (Mumford, 1983a). It is this participatory (also referred to as a socio-technical) approach that focuses upon people and procedures. This socio-technical approach is defined as "one which recognises the interaction of technology and people and produces work systems which are both technically efficient and have social characteristics which lead to high job satisfaction" (Mumford, 1983b). This paper

introduces the SIM-ETHICS fiamework, which was used as part of a European Union IT and within Australia.

2. THE SIM-ETHICS METHOD

The actual ETHICS methodology is a 15 level approach (Mumford, 1986) which details the steps needed to implement technology within an organisation. To try and overcome the problems of implementing security a new management methodology based on ETHICS was developed called SIM-ETHICS (SIM stands for Security Implementation Method). The philosophy behind SIM-ETHICS is that computer security is not only a technical problem but also involves organisational issues (Warren, 1999). The following are the steps used in the SIM-ETHICS method:

1) Initial Committee Consultation
The committee will be made up of a cross section of staff directly involved or affected by the implementation of the new security features. For example (Mumford, 1983a):

- representatives of staff from the different departments affected by the change;
- representatives of the IT department;
- representatives of the other users who will be using the new security systems.

2) Managerial consultation
The intended security countermeasures are evaluated against the SIM-ETHICS criteria to determine the level of impact its implementation will have. The criteria relates to (Warren, 1999):

- *Ease of Implementation;*
- *Training Issues;*
- *User Impact;*
- *Organisational Impact;*
- *Human Issues.*

At these meetings, issues relating to the introduction of the security systems would be discussed (as determined in Stage 1) as well as any other possible problems that managers could foresee.

3) Committee Stage
The views of the managers are discussed within the committee. It is now that initial problems are discussed, e.g. problems of introducing new security swipe cards.

The committee decides on how to approach the user consultation stage, such as:

- what questions to ask, for example, how do you feel about having to use new security swipe cards;
- the type of user to be questioned, for example, ward clerk;
- the number of users to ask, for example, every ward clerk.

4) Users consultation
A representative of the committee then meets the users to explain the proposed security countermeasures and then ask them a series of pre-set questions. The security countermeasures are then re-evaluated against the SIM-ETHICS criteria to take into account the newly raised user issues.

5) Committee Stage
The views of the users are discussed. If problems are found concerning the system, ways would be discussed on how to overcome the problem, e.g. increase the level of training.

6) Post implementation review
This meeting takes place after the implementation to determine if any unforeseen problems have occurred and if so discuss ways in which to rectify them.

3. RESEARCH OUTCOMES

SIM-ETHICS was used to determine the impact of two new security countermeasures (Warren, et al, 1995) within a major UK hospital. This major hospital was located in the South of England and was used as part of the European Union SEISMED (Secure Environment for Information Systems in Medicine) project. The hospital was used as a reference centre for the implementation of new security systems. The lessons learned from the implementation were shared with other partners within the project consortium. Based upon the SIM-ETHICS analysis the management of the hospital undertook the following actions:

Access Swipe Cards

Altered the staff training program by training key trainers from the separate departments. These key trainers would then train the rest of the staff in their department. A general promotion campaign was organised within the hospital to raise awareness of the new system and answer many of the commonly asked questions.

User Perception of Passwords

A general promotion campaign was organised within the hospital to raise security awareness especially when it was found that staff shared passwords and wrote them on the back of their ID badges.

SIM-ETHICS has also been used as part of a computer security risk analysis methodology called ODESSA (Organisational DEScriptive Security Analysis) and is used to determine the security requirements of healthcare organisations (Warren et a, 2000a). Any security countermeasures that are being implemented will effect the healthcare organisation as a whole. The SIM-ETHICS method is used to give management feedback on how security measures will impact an organisation (Warren, 2001). An example screenshot is shown at figure 1.

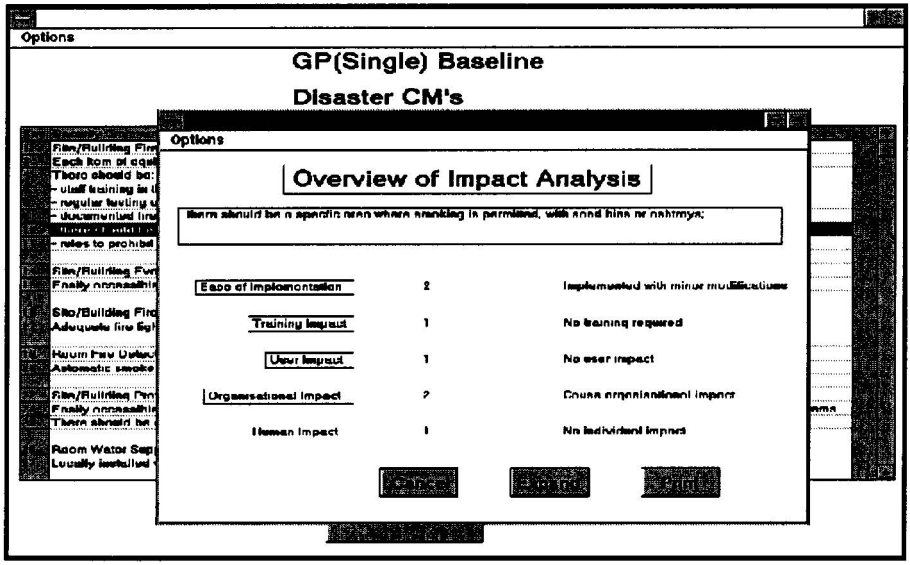

Figure 1. SIM-ETHICS analysis of Security Countermeasure

4. SIM-ETHICS 2000

The major problem relating to SIM-ETHICS was that the evaluation criteria needed to be fully developed and used with new technologies e.g. impact of the Internet upon Security Management. It was decided to use the SIM-ETHICS method within Australia. The first step was to determine if there was a need for security within Australian hospitals. A computer crime survey was sent out to 60 IT Security Officers, who were based within hospitals in the state of Victoria, Australia (Warren et al, 2000b). There were 22 valid responses, giving a response rate of 37%. We will look at some key questions of that survey. In relation to Question 5 – "Has your Healthcare establishment performed a formal assessment to determine potential areas of risk?" A significantly higher number of private hospitals had undertaken such a review (66% compared to 34%). The majority of the private healthcare establishments had reviews undertaken by professionals within the establishment. Most of the public healthcare establishment used security consultants. The use of risk analysis is considered one of the most basic steps in identifying security threats that an organisation faces and implementing security countermeasures to protect against those security risks (Warren, 1997). Many Victorian hospitals are not implementing this basic step. Question 6 was a follow on from question 5, asking establishments if they had a formal written policy concerning computer

security and the misuse of facilities. 64% of the public hospitals had a policy compared to 77% of private hospitals. The areas the policy covered were very similar for both private and public although more private hospitals responded that the policy covered "network intrusions" and "penalties for staff found committing computer crimes". Again the use of security policy is considered a basic step in developing a security culture, and surprisingly, one third of HCE did not have this in place. The survey provided that there was a potential need for a method such as SIM-ETHICS within Australia. One of the problems of the SIM-ETHICS method was there was a clear need to develop an appropriate evaluation mechanism. The following feedback criteria was developed to allow for the evaluation of security methods and allow for more focused feedback.

Within Australia there is a move towards the implementation of electronic healthcare records and allowing for on-line access to patient medical information. The Australian state of New South Wales is planning to implement such an on-line system by the year 2003. Each patient would have a single Unique Patient Identifier and use this with a password to gain access to their medical records (NSW Government, 2000). As the on-line medical system has not been developed yet, it was decided to evaluate the security requirements of a very similar style of on-line system. Web-CT is an on-line teaching system that is widely used by Universities to run courses. It allows students to remotely access the system and access their student records and post queries on discussion boards (as shown by Figure 2). The authors felt that this would be a suitable system to try and use the evaluation criteria.

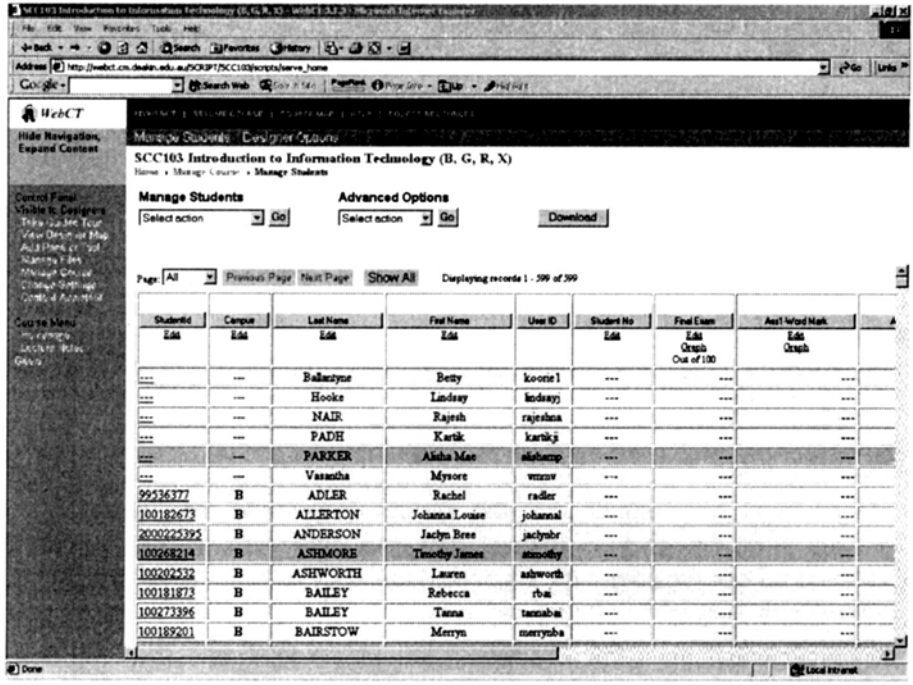

Figure 2. Example of Web-CT System

It was decided to evaluate a unit that contain 600 students and the review would look at how security could be implemented within the Web-CT system. The following is the outcome of the SIM-ETHICS review of that countermeasure using the evaluation criteria:

a) Impact of Security Mechanism
Implemented with minor modifications to existing systems or with the minimal amount of effort.

Points Raised:
The Web-CT system comes with built in passwords and each student is given a unique password (similar to a Unique Patient Identifier) to gain access to the system. There were some issues relating to giving passwords to new students.

b) Training Issues
No training requirements.

Points Raised:

Users were able to use the system very easily once they had their unique password.

c) User Impact
Countermeasure affects user satisfaction and caused a minor impact.

Points Raised:
Users were able to use the system very easily once they had their unique password.

d) Security Impact
Major Problem

Points Raised:
Once users had logged onto the system they could not log-out. This meant even though they thought they had finished a session, someone else could use the computer after them and access their Web-CT account. There is a danger that a user could masquerade as another user and post false messages to the discussion boards.

e) Human Issues
Results in restructuring a persons job or changing a persons individual power.

Points Raised:
Students could use a new technology in order gain access to their materials.

Outcomes
A message was posted on the Web-CT discussion board detailing the security fault and ways to deal with it such as clearing the Internet browser history file.

In this simple example we have assessed a similar systems to an on-line medical information system. We have proven in this case that the evaluation criteria work and posted warnings to the users about the security problem that was found.

A warning was posted on the Web-ct system describing the security weakness and ways to overcome the problem such as clearing the browser history or deleting the computers internet cache. The users then replied to the posting, raising a number of new issues that has not been considered such as:

- some users did not how to delete browser history or deleting the computers internet cache;

- the problem only affected certain types of browsers e.g. Internet Browser and not Netscape Communicator.

In conclusion the use of SIM-ETHICS 2000 has shown that a less structured method of SIM-ETHICS can be used to resolve problems quickly as well as ensuring full user participation and perhaps more importantly allowing feedback directly from the users after the review.

5. CONCLUSIONS

The use of SIM-ETHICS has successfully enabled management to collect the consensus view of users relating to new security systems and has given management the chance to implement solutions to future problems, before they occurred. We have shown that the method can work within a European or Australian environment. The new evaluation criteria that has been developed will be used to increase in validity. The method gives management and staff information about problems that may occur, but it is the role of management to decide how to use this information when making decisions.

References

Mumford, E (1983a) *Designing Participatively,* Manchester Business School, UK, ISBN 0-903808-29-3.

Mumford, E (1983b) *Designing Human Systems,* Manchester Business School, Manchester, UK.

Mumford, E (1 986) *Using computers for Business,* Manchester Business School, Manchester, UK.

NSW Government. (2000). *Report of the NSW Health Council – A Better Health System for NSW,* ISBN 0-7347-3 138-8, Australia.

Warren, M.J. (1997) A new hybrid approach for Risk Analysis, *In Proceedings of IFIP WG11.1 - Information Security Management Conference,* Copenhagen, Denmark, May.

Warren, M.J. (1999) *A Practical Soft System Management Approach to Implementing Security,* Deakin University Technical Report CC99/05, Deakin University, Australia.

Warren, M.J (2001) *A Risk Analysis Model to reduce computer security risks among healthcare organisations,* Risk Management: An International Journal, Vol 3: No 1, pp 27-37, Perpetuity Press, UK.

Warren, M.J, Gaunt, P.N (1994) SP11-06: The use of SIM-ETHICS at a UK Health Authority, *European Union SEISMED Research Report SP11-06.*

Warren S, Warren M.J (2000). The Role of Participation in Systems, *In Proceedings of International Conference on Systems Thinking in Management, (Incorporating the First Australasian Conference on System Dynamics and Sixth Australia and New Zealand Systems Conference),* Geelong, Australia, November.

Warren, M.J, Warren, S, Love, P.E.D (2000a) Using Participation Effectively to Implement and Evaluate Information Security within an Organisation, *In Proceedings of Americas Conference on Information Systems 2000 (AMCIS 2000).* Long Beach, California, USA, August.

Warren S, Hutchinson, W, Warren M.J (2000b), Healthcare IT Security: Can the European Union experiences assist Australia, *In Proceedings of ACIS (Australasian Conference on Information Systems) 00,* Brisbane, Australia, December.