2000

A Participational Managerial Method to Implement and Evaluate Information Security within a Healthcare Organizaton

Matthew Warren
Deakin University, mwarren@deakin.edu.au

Shona Warren
Deakin University, shona@deakin.edu.au

Peter Love
Deakin University, pedlove@deakin.edu.au

A Participational Managerial Method to Implement and Evaluate Information Security within an Healthcare Organisation

Dr Matthew Warren, School of Computing & Mathematics, Deakin University, Geelong, Victoria, Australia, mwarren@deakin.edu.au.
Shona Warren, School of Computing & Mathematics, Deakin University, Geelong, Victoria, Australia, shona@deakin.edu.au.
Peter Love, School of Architecture & Building, Deakin University, Geelong, Victoria, Australia, pedlove@deakin.edu.au.

Abstract

The use of participational approaches to system design has been debated for a number of years. In some situations it seems that participational approaches are not a suitable or practical method by which to design an Information System or to analyse a problem. Within this paper we describe a framework in which participation plays an active and effective role and describe a method that was used to effectively design information systems and implement computer security countermeasures.

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 the need for appropriate design and analysis of the "problem" before the production of such a system can take place. The development of a new information system can have an overwhelming result on the individuals contained within the organization as well as the organization itself (Zuboff, 1988).

An information system contains many different parts, including people and procedures, information, software and hardware (Flynn, 1998). Different approaches to the analysis tend to focus specifically on one or more of these parts. For example, JSD (Jackson Structured Development) which is orientated toward software rather than organisational need (Avison & Fitzgerald, 1995).

However, it is almost impossible to remove the participation and involvement of users and stake holders from the design of a system, at some point, users will have some degree of input into the system, whether it just be deciding upon the budget or determining the key functionality of a system. There are a number of methodologies used within Information Systems that specifically encourage users to have a large say in how the impending system is designed and key areas of functionality are implemented. The main example of this approach is ETHICS (Mumford, 1983). It is this participational (also referred to as a socio-technical Approach) 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, 1983a).

For those supporters of "user participation" in the design of systems, its forms an essential part of the design, analysis and eventual implementation of a system. Previous research (McKeen, 1994), which looked at the relationship between user participation and user satisfaction, found that the correlation between these two variables could be affected by other factors, such as the complexity of the task. Mckeen et al also noted that their study could not say that user participation was unproductive, unnecessary or dysfunctional when used in the design of a system.

But other studies have identified advantages in using a participational approach. Adams (1984) found that:

- staff have ideas which can be useful;
- effective upwards communications are essential to effective decision making at the top;
- staff may better accept decisions if they participate in them;
- staff may work harder if they share in decisions that affect them;
- workers participation develops a more co-operative attitude amongst workers and management;
- staff participation may act as a spur to managerial efficiency.

This paper introduces the SIM-ETHICS framework, which was used as part of a European Union IT security

research project within a healthcare environment. This is one example where the incorporation of user participation was particularly effective for the development of information system and implementation of security mechanisms.

The SIM-ETHICS Approach

To try and overcome the problems of implementing security a new management methodology was developed called SIM-ETHICS (SIM stands for **S**ecurity **I**mplementation **M**ethod and ETHICS stands for **E**ffective **T**echnical and **H**uman **I**mplementation of **C**omputer based **S**ystem) (Warren et al., 1995). The work on ETHICS was undertaken by Prof. Enid Mumford of the Manchester Business School, UK (Mumford, 1995).

The philosophy behind SIM-ETHICS is that computer security is not only a technical problem but also an organisational issue and hence a socio-technical approach. This organisational issue is concerned with the effect that the process of change could have upon the organisation as a whole. The new features of SIM-ETHICS as compared with ETHICS is the development of an evaluation criteria (explained later in the paper), a more detailed focus on technology and related impacts and a more effective manner of using user committees to develop user collective viewpoints.

Other considerations relate to availability and reliability of the systems once they have been introduced. The introduction of new technology into an organisation can also be thought of as a human issue, relating to (Mumford, 1995):

- User requirements

  New technology directly affects users. There is little evidence that managers have recognised the need of using IT (including security) to change the way they do business. User requirements should be incorporated fully into the system design from the start so that the system that is designed actually complies with user requirements.

- User job satisfaction

  The way in which security operates usually has a direct effect upon the user and the way they use the system. If the user is unsatisfied with the system they will become less motivated and users will take longer to carry out tasks, or might not even use the system at all.

The introduction of new technology including security is a method by which organisations can gain a competitive edge by increasing their efficiency. The main organisational issues are (Mumford, 1993):

- Technical Impact

  The introduction of new technology often has a technical impact within the organisation. Computer systems should be phased in gradually in order to smooth out compatibility problems that could arise.

- Training

  The introduction of new computer systems will require the training of users in order to use it effectively. Training considerations would relate to the level of training required, the number of staff requiring training and the amount of time lost by staff because of training. A particular consideration would be making users aware of the limitations and advantages of new security features.

- Costs

  An important organisational issue is the one of cost. Any new technology introduced will be more expensive then existing available technology. User costs also have to be considered, such as the cost of training.

- Culture

  The introduction of new types of technology could have a direct or indirect impact upon the culture of the organisation, i.e. new technology may be seen as a status symbol, as jobs are redesigned around the new technology.

All of these areas are related to the importance of establishing socio-technical systems within organisations. The issues described fall into the context of organisational and user issues. These are important because SIM-ETHICS was designed to implement technical computer security mechanisms into healthcare organisations which directly impact the organisation and staff of that organisation. The weakest link within the socio-techhnical systems described is the issue of cost evaluation. We will explore this problem later on within the paper.

The SIM-ETHICS steps

As stated before the aim of the SIM-ETHICS method is to develop a method that can be used to implement security countermeasures into an organisation and evaluate the impact it could cause. 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. e.g.:

- 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.

The SIM-ETHICS method uses the participational approach in order to allow user input into the process of change. There are various levels of participation (Mumford, 1983):

Consultative

This is when an existing body, e.g. security committee, is used to implement the change process. This committee would then consult users on the effect that change will have upon them.

Representative

This is when a cross selection of users affected by change, are brought together into a design group. This ensures that representatives effected by change have the same powers in the committee as those bringing about change.

Consensus

This is when all the staff affected by the change are involved in the design process. Representatives of the staff affected are elected to form the design committee.

The committee will decide initially what should be considered the major impacts, e.g.:

- the impacts of introducing security systems;
- training of users;
- cost of new equipment;
- compatibility with existing clinical and administrative computer systems.

Areas of consideration within the SIM-ETHICS method at this stage are as follows (Mumford, 1993):

Job Satisfaction

Job satisfaction is defined as the attainment of a good "fit" between what employees are seeking from their work (their job needs, expectations and aspirations) and what they are required to do in their work; their organisational job requirement.

Effectiveness

This is defined as ensuring that tasks already being carried could be carried out in a more effective manner.

Efficiency

Efficiency is a set of support services which help individuals to work in a organised way with all the necessary back-up facilities that they require. These will include information, materials, technical aids, specialist knowledge and supervisory help. Employees who do not receive support services, which they regard as essential to their job performance, are likely to become frustrated and dissatisfied.

This stage is important because that is defines the set-up of the committee that will carry out the SIM-ETHICS review.

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

How easy can new security features be added to a system and/or new security procedures added to an organisation?

Training Issues

What are the training requirements needed by the staff to use these new security features?

User Impact

What is the impact that security could have upon users, e.g. how does it affect user satisfaction, efficiency or effectiveness?

Organisational Impact

What will be the affect that security features could have upon the organisation, e.g. changing of the organisational culture?

Human Issues

What is the impact that security has upon a user from the human perspective, e.g. changes of peoples' jobs, creating new management roles?

A representative of the committee would meet the following people, for example:

- system managers of existing clinical systems;
- specialist IT managers, e.g. network managers;
- managers and staff involved in implementing the new security features.

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.

This stage is concerned with determining the impact that the different security technologies could have upon the organisation by obtaining the views of key individuals within the organisation.

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;
  e.g. how do you feel about having to use new security swipe cards.
- the type of user to be questioned;
  e.g. ward clerk.
- the number of users to ask;
  e.g. every ward clerk.

This stage of the process helps to determine what some of the initial problems may be in regards to implementing the security countermeasures. It also helps to define the areas that would have to be looked at in the user consultation stage.

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. This stage helps to define the user perceptive of implementing security countermeasures.

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. A key aspect of the discussion is the evaluation criteria that was used to asses the impact of each of the security countermeasures, this is expanded later within the paper.

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.

The use of SIM-ETHICS

SIM-ETHICS was used to determine the impact of two new security countermeasures, a new computer information system and also a multimedia information system (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 would be shared with other partners within the project consortium.

The areas looked at were:

Passwords

To determine users perception on the need and use of passwords as a form of access control for computer systems.

Physical Access Control Cards

The use of 'Swipe Cards' to control access of staff and visitors within the hospital. These cards were used to control access after working hours and in sensitive areas, i.e. maternity wards.

Information Message System

A universal information message display system, the information on the system related to:

- general administration notices;
- general guidelines, i.e. what to do in case of fire?
- clinical practices and protocols;
- clinical guidelines, i.e. nationally produced guidelines.

Some of the information contained on the Information Message System was considered as being sensitive in nature.

Feasibility of Medical Multimedia Information Systems
The proposed information systems related to the development of multimedia electronic health care records for all patients that are treated within the hospital described above for the treatment of certain cancers (Warren, et al, 1995).

The main lessons learned from the use of SIM-ETHICS were (Warren, 1994):

- the key to success was the sense of involvement by all staff affected by the security countermeasures;
- to explain to users which security countermeasures are being implemented;
- to follow up post interview queries from users.

Evaluation of the SIM-ETHICS method

The use of SIM-ETHICS in this environment appears to have been a success. One of the important features of the method was the evaluation criteria that was used to assess the different technologies and the impacts that they could have upon the organisation. The evaluation criteria focussed on the following areas:

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

An example of the evaluation criteria for the Access Swipe cards was (Warren, 1994):

Physical Access Card

Ease of Implementation	3
Training Issues	4
User Impact	2
Organisational Impact	2a, 3a
Human Issues	1

The above evaluation showed that the implementation of the countermeasure would have a major impact on the organisation. There would be extensive training across the whole of the organisation in order to use the access cards. The security countermeasures could cause some minor impact upon user satisfaction and would have a minor impact on the organisation when implemented. This was partly due to the security culture that already existed within the hospital. The use of the access cards would no individual impact upon staff.

The results of the final evaluation would allow management to make decisions relating to the change management aspect of implementing new information systems.

The biggest weakness of the SIM-ETHICS method is the cost. Due to the factors involved in this participational approach, the final cost cannot be easily determined at the onset of the project. Because the method is based around committees which contain a variety of individuals whom are affected by the system, a consensus approach to problem solving will only allow qualitative information to be discussed rather than a quantitative approach (Warren, 1999). But the use of SIM-ETHICS was a success, because of it use the hospital saved several thousand pounds. They changed their strategy to implementing the passwords and access control systems which resulted in a change in their training strategy – instead of all staff being trained, only certain key staff were trained who then trained the other staff in smaller numbers. There were also major changes made to the information systems to take into account the views of users.

Conclusions

The use of SIM-ETHICS has enabled management to collect the consensus view of users relating to new security systems and has given management the chance to implent solutions to future problems, before they occurred. This method also allows users to raise issues and concerns about implementing new security features. The use of SIM-ETHICS was a success because it allowed users to determine how information systems and security systems could be implemented within their organisations. It also allowed management to cater for problems before they occurred, e.g. developing training strategies for several hundred staff.

The method gives management information about problems that may occur, but it is the role of management to decide how to use this information when making decisions.
The method was originally piloted in the United Kingdom. The next step is to use the method in other countries to ascertain whether culture differences have any effect upon the methodology.

References

Adams, R. Participation Today, The Industrial Participation Association, UK, ISBN 0-9503090-36, 1984.

Avison, D.E. & Fitzgerald, G. Information Systems Development: Methodologies, Techniques and Tools. McGraw-Hill, UK, 1995.

Cavaye, A. User Participation in systems development revisited. *Information and Management*, Vol 28, pp311-323, UK, 1995.

Flynn, D. Information Systems Requirements: Determination and Analysis. McGraw-Hill, UK, 1998.

McKeen M. The Relationship Between User Participation and User Satisfaction: An Investigation of Four Contingency Factors. *MIS Quarterly*, December, USA, 1994.

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

Mumford, E Designing Human Systems, Manchester Business School, Manchester, UK, 1983a.

Mumford, E. Designing Human Systems For Health Care, The ETHICS Method, 4C Corporation, Netherlands, ISBN 90-74687-01-6, 1993.

Mumford, E. Effective Requirement Analysis and Systems Design: The Ethics Method, Macmillan, UK, 1995.

Warren, M.J. The use of SIM-ETHICS at (anonymous) Health Authority, SEISMED Report SP11-06, European Union, 1994

Warren, M.J. & Gaunt, P.N. The use of SIM-ETHICS, SEISMED Report SP11-04, European Union, 1994

Warren, M.J. Sanders, P.W & Gaunt, P.N. Participational Management and the Implementation of Multimedia Systems, MEDIACOMM 95 - International Conference on Multimedia Communications, Southampton, UK, 1995.

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

Zuboff, S. In the Age of the Smart Machine, Basic Books, New York, USA, 1998.