Managing Information Security in Healthcare - an Action Research Experience

HELEN ARMSTRONG
School of Computer & Information Science
Edith Cowan University
Bradford Street, Mt Lawley
Western Australia
h.armstrong@ecu.edu.au

Key words: Information Security, Information Security Management, Action Research, Soft Systems Methodology

Abstract: This paper describes a project involving the planning and management of information security at a large private hospital. A high level model derived using the Soft Systems Methodology [5] named the Orion Strategy, was implemented and further developed during its application using Action Research. This method features a high level of user participation, including education seminars and workshops with senior and middle managers of the hospital. The project resulted in a noticeable improvement in information security measures at the hospital, a raised awareness of security issues and an acceptance of ownership by staff of the resultant security plan

1. INTRODUCTION

The literature shows the management of information security is inadequate and levels of awareness regarding security issues is low. The findings of the SEISMED (Secure Environment for Information Systems in MEDicine) survey in security awareness highlighted the low awareness of security issues as well as means for improving security in medical situations[10]. In health organisations in the UK it was noted that even the lowest levels of security measure were not always in place [3]. The nature of risks in a changing health-care environment is unique [8]. Information

The original version of this chapter was revised: The copyright line was incorrect. This has been corrected. The Erratum to this chapter is available at DOI: 10.1007/978-0-387-35515-3_53

S. Qing et al. (eds.), *Information Security for Global Information Infrastructures*

security in the health care industry is not purely a technical issue, with social and organisational factors also playing a major part [1]. The concept of user responsibility for information security is still in its infancy. Following development of a high level model (the Orion Strategy) to encourage users to accept responsibility and ownership of information security within their work environment, the researcher implemented the model at a large private hospital in Western Australia. This paper discusses the Orion Strategy and its implementation over a three year period, together with the findings from the research.

2. THE ORION STRATEGY

The Orion Strategy uses the original Soft Systems Methodolgy (SSM) by Checkland [5] as a foundation. One of the most important aspects of SSM is the handing over of the problem analysis and desired action to those persons who have a stakeholding in the problem situation. A high level interpretation of the Orion Strategy appears in Figure 1. This diagram shows the major activities involved in the method. As with SSM, the Orion Strategy also has two planes of reality or conceptualisation. The first plane is the physical or real world where actions and processes can be seen, heard and measured. The second plane is the abstract or ideal level where situations and processes are visualised, and scenarios built at an abstract level. Activities are illustrated by oval shapes and the arrows indicate inputs and outputs to and from these activities. A boundary encompasses the main activities, separating the area under study from external influences such as external bodies imposing statutory requirements; directives from boards of managers and the like. These influences can flow through the boundary to affect any of the activities within. The high level model contains seven main activities. The first activity is the acknowledgement of possible security vulnerability, followed by an analysis of the current security situation (activity 2). The systems and information are then classified based upon sensitivity (activity 3), and an ideal security situation defined (activity 4). A comparison between the current and ideal situations is undertaken (a gap analysis), resulting in identification of areas needing consideration (activity 5). Security measures to address the gaps are identified and evaluated (activity 6) and a plan of action to implement appropriate security measures is established and implemented (activity 7). This provides feedback to activity 1 and the cycle can continue. These activities are numbered for guidance only. Although the sequence is logical there is no rule for activities to be followed in the sequence of their numbering. In many cases it is necessary to go back and revisit past activities as the environment changes and new influences take effect. This is illustrated by the circle in the centre of the dividing line between the real world and the ideal world. During implementation, it was found that this revisiting of activities occurred regularly in the area contained within the broken line surrounding activities 2, 3, 4 and 5.

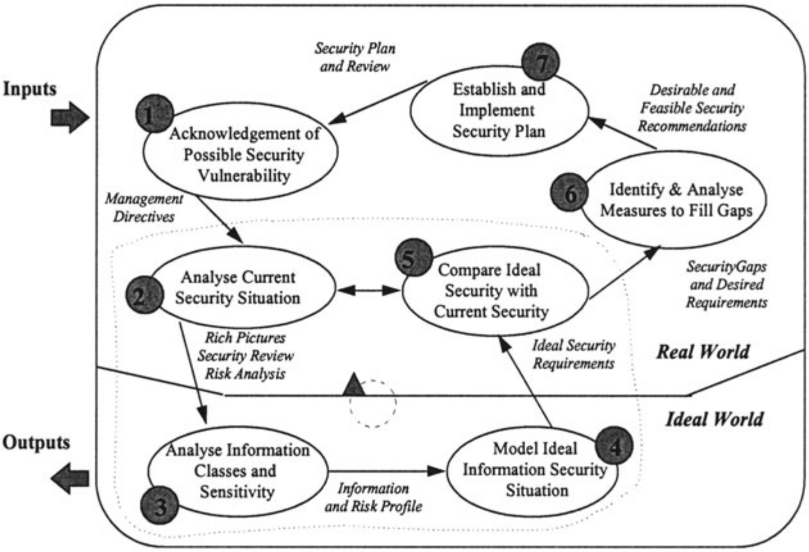
Inputs
Outputs
Security Plan and Review
7
Establish and Implement Security Plan
Desirable and Feasible Security Recommendations
1
Acknowledgement of Possible Security Vulnerability
Management Directives
6
Identify & Analyse Measures to Fill Gaps
2
Analyse Current Security Situation
5
Compare Ideal Security with Current Security
SecurityGaps and Desired Requirements
Rich Pictures Security Review Risk Analysis
Ideal Security Requirements
Real World
Ideal World
3
Analyse Information Classes and Sensitivity
Information and Risk Profile
4
Model Ideal Information Security Situation

Figure 1. The Orion Strategy (high level diagram)

3. RESEARCH METHOD AND RESEARCH THEMES

The Orion Strategy had been developed at a high level with actual application required to build the model more fully. Due to the complexity and human interaction within healthcare environments it was difficult to build a detailed model without immersion into the situation under study. Specific hypotheses to be tested and proven using statistical methods were difficult to define. It was decided to employ Action Research as the methodology because in this approach the researcher is not dealing with hypotheses, but in research themes within which lessons can be sought [6]. For more than a decade leading researchers and academics have published support for interpretive research methods in information systems and information security (see [4,7,9]. The social setting is important in action research, as different social settings may produce different results with the same stimuli [4]. The soft systems approach is based upon systems theory, and incorporates socio-technical aspects into the analysis of human activity systems. User participation and critical thinking are basic elements, and action research provides an ideal mode to achieve its goals. The people directly involved in the situation under study are stakeholders, and should be involved in the process of change regarding that situation. Where change is a desired outcome participation can generate greater commitment and action from those involved. This is because change is more easily achieved if people are committed.

At the beginning of a study it is difficult to know precisely what research question to pursue, and in action research the initial question is likely to be fuzzy due to the nature of social systems. In this case it was recognised that the overall research objective was a desire to improve information security planning and management in the organisation under study. The literature suggests that poor information security management occurs hand in hand with a lack of awareness of security issues. It was felt that by raising the awareness of staff at middle and senior levels and involving them substantially in the process they would 'own' and accept responsibility for security measures subsequently implemented.

The three main objectives of this research were to firstly, improve information security management in the organisation under study; secondly, increase awareness of security issues in middle and senior management; and finally, engender staff ownership of the security plan developed.

4. APPLICATION OF THE MODEL

The Orion Strategy was implemented and further developed at a large private hospital over a three year period. The application included a security review of the hospital, information security education sessions, numerous workshops and interviews. Sixty middle and senior managers at the hospital were involved with the application. Data was gathered from these activities in addition to numerous questionnaires at different stages of the project. As the presence of the action researcher can affect the situation under study an independent facilitator was used for the workshops. This allowed independent observation to take place, plus the researcher was less able to directly influence the direction or decisions made within the workshops. Triangulation of methods was also used to increase the validity and reliability of the findings. The application of the Orion Strategy encompassed a high level of user involvement and resulted in a security plan devised and implemented by the staff of the hospital. This application activity was not intended to test the model as such, because the detailed model was developed as the research progressed. This part of the research was focussed on building the lower levels as the study progressed (this is characteristic of action research projects).

The first phase of the application involved an introductory seminar on security awareness for all participants. A security review was carried out at the beginning of Phase 2, by physical inspection of the computing and networking facilities, observation of the working environment, the flow of information and paper throughout the hospital, and study of written procedures, manuals and other working documents. The first workshop analysed the current security situation, identifying problem and potential problem areas within the hospital situation and associated potential security risks. These risks were considered under the headings of 'lack of confidentiality', 'lack of integrity' and 'lack of availability'. Phase 3 in the theoretical model involved the identification and analysis of systems of information and security and a definition of missions for each system. The deliverables of this stage - the mission statements, were to be developed by the use of CATWOE (Customer, Actors, Transformation, World View, Owner, Environment) analysis and the defining of root definitions in SSM terms. CATWOE analysis was found to be inappropriate for analysing the security component of the hospital's information. The 'systems of information' were, in fact, not systems, but types of information that supported other systems within the hospital. Each type of information had different security characteristics relating to sensitivity and risks and as such were difficult to include and illustrate via CATWOE's and root definitions.

During Phase 3 a second set of workshops was held to analyse the information used in the hospital and draw up a security profile of this information. This involved identifying and classifying information used by type, identifying the source or author of the information, determining the sensitivity of each information type and possible risks to that information. Using the information and risk profiles from the previous phase, Phase 4 involved an analysis to determine the risks of each information type over its life-cycle. The life-cycle phases considered were information creation, transportation, storage, use and destruction. The principles of integrity, confidentiality and availability were applied and an ideal scenario developed. It was originally intended to use conceptual modelling as per SSM, however, this type of modelling was not able to fully illustrate the ideal security situation. This was possibly due to the security situation under study being contextual rather than systemic, its influence extending across the boundaries of the organisation's activity systems. The ideal situation was brainstormed on the whiteboard in the workshops with ideas, modifications and enhancements added as discussion progressed.

Phase 5 compared the present security situation with the ideal security defined in Phase 4. The security review highlighted current areas of concern where control measures were insufficient, and the risk analysis and rich picture added areas of vulnerability. Although the ideal security requirements from the previous phase were not in the same format as the documents portraying the current situation, gaps and differences were easily identifiable. Phase 6 of the implementation commenced with an investigation of possible security measures to meet the desired solutions. As the managers had little knowledge of security products and procedures, information and material on possible solutions was gathered from numerous sources. Alternative solutions were discussed and action options presented. Compromises were necessary in the determination of the most feasible and appropriate solutions. Some of these limitations were posed by financial considerations, computer capacity restrictions and staff availability to carry out tasks. The final activity to take place in this phase was a prioritisation of the chosen solutions in preparation for the development of an action plan. This was achieved by a questionnaire given to the participants at the completion of the workshops.

Following integration of the security review and findings from the study, the executive director of the hospital took on the responsibility for information security and established a small task force to activate and manage the design and implementation of the chosen security measures. At this time the architectural plans for a new hospital building complex were near completion, and the task force moved quickly to alter the designs to incorporate the physical security recommendations. Another high priority was the classification of information and the implementation of a secure records management system. A security education program was developed and implemented as a priority area. A two year plan was developed to integrate security measures into normal hospital and administrative operations, and the implementation of high priority issues commenced immediately. Security reviews were carried out during the implementation of this two-year plan.

5. FINDINGS

In order to ascertain whether security had actually improved at the hospital as per the first research objective, ratings of the implementation of security measures were conducted at three stages during the research process. The security measures reviewed were drawn from recommendations in the literature (see [2]). The first stage was prior to the commencement of the research, the second mid-way, and finally several months after the completion of the research. The ratings over the three time periods are summarised in Figure 2. A rating of 1 indicates the measure does not exist and 5 indicates it is fully implemented and active. As can be seen in Figure 2, the implementation of security measures improved over this period, with the hospital moving to a rating of 5 in many areas by the third year. Areas receiving early attention can be seen in the improvement between the first and second reviews.

Security Measure	**Prior to Study**	**Mid-Way**	**End of Study**
Corporate Security Policy	1	2	5
Security Planning	1	3	5
Risk Analysis	1	3	5
Contingency Planning	1	3	4
Security Manager	2	4	5
Supervision of Security	1	4	5
Security Education	1	2	4
Quality Assurance	1	5	5
User Responsibility	1	3	5
Physical Access Controls	2	3	4
Logical Access Controls	2	4	5
System Logs & Error Handling	2	3	4
Change Control	1	4	5
Communications Controls	1	2	4
Independent Audits	2	4	5
Backup Procedures	2	4	5
Project Management	2	5	5
User in Development Team	1	5	5
Development Methodology	1	5	5
Requirements Specifications	2	5	5
Systems Documentation	2	5	5
Design Controls	2	5	5
Walk-throughs	2	5	5
Testing Procedures	2	5	5
Separate Environments	1	5	5

Figure 2. Ratings of Security Measures at the Hospital over the three-year period (Ratings: 1=Measure does not exist, 5=Measure is fully implemented and active)

The original security task force assigned at the end of the workshops completed the implementation of new and reviewed security measures over the ensuing two years. The ongoing responsibility for the management of security has since been accepted by a six-member security committee, comprising senior staff from the Nursing, Medical Records, Marketing, Library, Information Services and Quality sections, reporting directly to the Executive Director of Corporate Services.

By using a high level of user involvement in this project it was hoped that participants would become more aware of security issues thus addressing the second research objective. In particular the initial education seminar was designed to increase knowledge about potential risks and the importance of effective security management. In addition, the workshops were designed to walk the participants through risk identification within their own working environment and devise appropriate solutions to support the hospital's mission and goals.

In order to measure how effective the education seminar and workshops had been participants were asked to rate their awareness of security issues at three stages throughout the planning project: before it began, after the security education seminar, and finally at the end of the workshops. These three ratings were all completed at the end of the workshops. The responses are shown in Figure 3. A notable shift in awareness is indicated as a result of the initial education seminar, with all respondents claiming a rise in the level of awareness after attending the seminar. A similar rise in levels of awareness is apparent after the workshops were completed, with all participants claiming a high or very high level of awareness.

Question	**1 Very Low %**	**2 Low %**	**3 Med %**	**4 High %**	**5 Very High %**
Security Awareness Before Project Began	0	18	41	41	0
Security Awareness After Education Seminar	0	0	29	41	30
Security Awareness After Risk and Solution Workshops	0	0	0	41	59
Desired Staff Involvement in Security Planning	0	0	6	76	18
Ownership of Responsibility for Security Measures	0	0	6	59	35

Figure 3. Summary of Findings Relating to Awareness and User Involvement

The high level of user involvement in the project was designed to encourage ownership of the hospital's information and the resultant security plan, addressing the third research objective. Contribution levels by managers attending the workshops were high and there was good interaction between participants. A much broader view was developed due to the varied areas of responsibility represented in each workshop group. The impact of security problems across the organisation was more evident. In addition, managers were able to dove-tail solutions to enable other areas to be supported rather than hindered. The staff participating in the study were asked to rate how much involvement they believed staff should have in the security planning process. A summary of the responses is contained in Figure 3. The results illustrate a high desire to involve staff in the ongoing planning and management of security, i.e. 94% of participants stating there should be either a high or very high staff involvement.

At the completion of the workshops the participants were asked to rate their level of acceptance of responsibility and ownership of the solutions implemented. Figure 3 also summarises their responses. Taking on the responsibility for security and owning the security measures was rated highly, with 94% rating their ownership at a high or very high level. These findings were also consistent with information collected via interviews with the participants.

6. USE OF SOFT SYSTEMS METHODOLOGY

One of the basic underlying problems was the assumption that the research would be systems based. It was, however, predominantly contextual. It follows, therefore, that the tools used in SSM for the analysis of systems, i.e. root definitions and conceptual models, need to be adapted for 'non-systems' analysis in a project of this nature. As SSM requires adapting to the given situation, the flexibility of the methodology allows these modifications to be encompassed in the application of the theoretical model.

7. CONCLUSION

It is clear from the above discussion that the implementation and active supervision of security measures has increased in the hospital over the three year period of this study. This positively supports the research theme that information security management has improved following the use of the Orion Strategy. The participants felt positive about staff involvement in the planning and management process, and showed evidence of acceptance of ownership and responsibility for the security measures planned for implementation. In addition, staff believed their awareness of security issues had risen over the period of the project. The high level of involvement by users in the design and implementation of protective measures suggests that users can be highly aware of needs and required action to fill those needs. This indicates that information security may not be too technical for users to handle where specialised security knowledge or guidance is provided. Although this method has only been applied in one organisation, the results of this research encourage security specialists and managers to continue in the quest to empower users to own and take on the responsibility for information security planning and management.

8. REFERENCES

[1] Anderson, J.G., 1997, "Clearing the Way for Physicians' use of Clinical Information Systems", *Communications of the ACM,* Vol 40 no 8, pp 83-90

[2] Armstrong H, 1999, 'A Soft Approach to the Management of Information Security', PhD Thesis, Curtin University, Perth, West Australia

[3] Barber B., Davey, J., 1996, 'Risk Analysis in Health Care Establishments', in Barber, Treacher, Louwerse, (Eds), "*Towards Security in Medical Telematics*", IOS Press, Amsterdam, pp 120-124

[4] Baskerville, R., Wood-Harper, A.T., 1998, 'Diversity in Information Systems Action Research Methods', *European Journal of Information Systems*, Vol 7, no 2, June, pp 90-107

[5] Checkland P, 1981, '*Systems Thinking, Systems Practice'*, John Wiley & Sons, Chichester, UK

[6] Checkland P, 1991, 'From Framework through Experience to Learning', in Nissen, Klein & Hirschheim (Eds), '*Information Systems Research: Contemporary Approaches and Emergent Traditions*', Elsevier, Amsterdam

[7] Klein H, Myers M, 1999, 'A Set of Principles for Conducting and Evaluating Interpretive Field Studies in Information Systems, *MIS Quarterly*, Vol 23, No. 1, pp 67-93

[8] Smith, E. & Eloff, J., 1998, 'Modelling Risks in a Health-Care Institution', *Proceedings of the XV IFIP World Computer Congress*, Vienna/Budapest, September

[9] Straub D, Welke R, 1999, 'Coping with Systems Risk: Planning Models for Management Decision Making', *MIS Quarterly*, Vol 22 No 4, pp 441-469

[10] Treacher, A. Bleumer, G., 1996, 'An Overview of SEISMED', in Barber, Treacher & Louwerse, (Eds), "*Towards Security in Medical Telematics*", IOS Press, Amsterdam, pp 4-9