Healthcare IT Security: Can the European Union experiences assist Australia

Shona Warren[1]
William Hutchinson[2]
Matthew Warren[1]

[1]Department of Computing & Mathematics, Deakin University,
Geelong, Victoria, Australia.
Email: shona@deakin.edu.au

[2]School of Management Information Systems, Edith Cowan University
Perth, Churchlands, Western Australia.

Abstract

This aim of this paper is to try identify key security issues within healthcare establishments (HCEs) and justify the need for training and awareness programmes. Security with HCE's is extremely important and as such the need to train users about security and raise general awareness. The paper is based upon work that has been undertaken as part of a European Union research project. The research is also looking at how these issues relate to Victorian hospitals and whether the European Union experiences can be applied within Australia.

Keywords

IS security, Information policy, Managing IS, Computer crime

INTRODUCTION

The increasing accessibility of information technology (IT) systems during recent years has had a significant effect upon the healthcare field. Many healthcare establishments (HCEs) now operate heterogeneous IT environments with equipment ranging from standalone PCs to minicomputer and mainframe installations.

The influence of information systems can now be seen in most areas of healthcare operations, with an ever increasing number and variety of medical applications. In addition, IT also facilitates the exchange of medical data between different HCEs at both national and international levels. A significant result of these advances is that healthcare professionals have become increasingly dependant upon the availability of systems and reliant upon the correctness of the data that they hold. As the adoption of information technology has increased so too has the requirement to protect the systems. A key area in protecting these system is training users about security and raising awareness of the associated issues (Fak and Hunstad, 1993).

Past research has shown the lack of training amongst HCE staff. A survey amongst a large European HCE (Furnell, et al, 1996) portrays the problem that exists. The survey

reveals that out of 75 overall respondents, 25% claim to have received initial security related training and only 15% indicate that they have attended ongoing security awareness seminars. The survey also highlights some security problems that have arisen from the lack of training. These include poor use of passwords, unauthorised data modification, and attempted hacking. This shows that there is a relationship between lack of security awareness and training, and an apparent increase in security misuse incidents.

Various surveys from the UK (Audit Commission Reports, 1990, 1994 and 1998) make interesting reading in terms of their implications for healthcare and the principal points are summarised below. In the most recent survey (1998), 153 abuse incidents were reported in the healthcare field - more than almost any of the other sectors surveyed (which included local government, education, finance, manufacturing, retail, IT and communication) - and represented 30% of the total abuse cases reported. This can be contrasted with only 127 incidents (equating to 24% of the total number) being reported in healthcare in the previous Audit Commission survey in 1994 and 18 incidents (10% of the total reported) in 1990. This leads to the strong conclusion that computer abuse in healthcare is increasing within the UK. The situation within Australia will be discussed later in the paper. The trend is illustrated in the graph below, both based upon results from the previous three Audit Commission surveys.

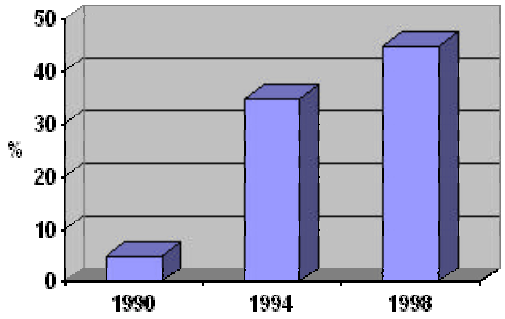

Figure 1: % of respondent healthcare establishments reporting security incidents

A total of 295 UK HCEs responded to the 1998 survey, with 45% reporting some kind of abuse incidents. These are broken down as follows:

- 12 reported incidents of hacking;
- 98 incidents of viruses (more than any other sector surveyed);
- 6 incidents of fraud;
- 10 incidents of invasion of privacy (again more than any other sector);
- 4 incidents of unsuitable material;
- 23 incidents of theft of data or software (more than any sector other than Local Government).

These statistics, and the magnitude of incidents in comparison to other sectors, seem to indicate that healthcare appears to be one of the more attractive areas to both internal and external abusers.

KEY ISSUES IN TRAINING

Training and awareness within HCEs is very important. By following some basic steps it is possible to address these issues. Previous research in this area includes the work undertaken by the AIM SEISMED (Secure Environment for Information Systems in MEDicine) project (Sanders, P.W et al, 1996a, 1996b) which resulted in many training and awareness recommendations relating to the following areas:

Job training

It is appropriate that staff should receive instruction in how to perform their day-to-day duties as well as any specific security issues relating to their role. It must be ensured that personnel have sufficient training to comply with any security requirements specified in their contract of employment.

Use of systems & applications

Staff should receive adequate training for any HCE systems and applications that they are likely to use, covering both general operation and use of any security features provided. Documentation should be available for general reference to supplement and re-enforce the training provided.

HCE training programmes

Internal HCE-wide training and awareness programmes should be operated as part of the induction of new staff and as refresher courses for existing personnel. These initiatives should be based upon the HCE existing security policy and concentrate upon providing basic security awareness for all personnel.

Specialist training courses

Some staff (e.g. IT managers, security staff) will require training beyond the basic level offered internally by HCEs. In cases where more detailed knowledge is required, the suitability of specialised courses should be examined. If the knowledge is then required by many personnel, the trained staff may be used as a local source of advice within the HCE / department.

Awareness of specific issues

The HCE must be able to cope with security issues that arise outside the scope of the normal awareness programmes. In many cases staff will need to be made aware of these immediately to ensure that they do not risk compromising security. IT / security staff should, therefore, ensure that other personnel are made aware of any specific events that may affect them (for example, discovery of a virus, discovery of errors in applications, updates of existing applications or system unavailability).

Training responsibilities

A Security Officer (or equivalent) should be central in organising any HCE-wide awareness programmes. At the departmental level, training should be handled by the appropriate senior / qualified personnel. The Security Officer and IT staff can also

provide guidance at this level. Senior staff should promote security issues in order to encourage compliance from those at lower levels.

By following these recommendations, an appropriate training framework may be established. However, a question remains as to where appropriate security advice could come from in the first instance. This issue is addressed in the next section.

CURRENT EUROPEAN UNION AWARENESS INITIATIVES

A number of security awareness initiatives are currently being promoted by the Health Telematics ISHTAR (Implementing Secure Healthcare Telematics Applications in Europe) project. This aims to provide awareness within European HCEs through efforts in four key areas (The SEISMED Consortium, 1996):

Formation of an expert advisory panel

The advisory group produces up-to-date reports on the current issues facing information security in healthcare and the implications of the European Union Directive on the protection of individuals with regard to the processing of personal data. These papers are distributed on a European basis and reviewed annually to maintain their relevance. Papers from the panel will promote general awareness of the key issues facing the healthcare community, facilitating a harmonized approach. It is also intended that information will be disseminated via the world-wide web.

Enhancement of the European Union security guidelines

The enhancement of the guidelines is being conducted on the basis of comments received from the ten European HCEs acting as Verification Centers within the project, along with updates to address recent developments in information security. The guidelines represent the most detailed treatment of the issue and seek to provide individual establishments with a key source of reference covering all major security considerations. The guidelines cover the following main areas:

- Health Informatics Deontology;
- IT Security Risk Analysis;
- High Level Security;
- Existing System Security;
- Security of Medical Database Systems;
- Network Security;
- Encryption.

Development of security training programmes

The training programmes are based upon information from the guidelines and other SEISMED project deliverables, standards work from CEN TC251 Working Group 6 and other relevant expertise. The sheer volume and depth of information contained within the ISHTAR security guidelines would ensure that few people would remember or understand the complete set. Many staff could encounter difficulties in identifying what is really relevant to them. The ISHTAR Security Training Course is the only one

known in Europe to be addressing the security issues in healthcare (ISHTAR, 1995). It is intended as a course for "training the trainers" in respect of the security issues so that they can design their own materials. This will help to ensure that local training is based upon a comprehensive set of material.

Usage of the world-wide web (WWW) for information dissemination

The WWW service sets out to promote and supplement the work of the project in a number of areas. These include the provision of on-line access to security advice, healthcare incident reports, security strategies from the verification centers and a repository for security-related presentations and publications. The world-wide web service seeks to provide a simplified source of information for day-to-day reference. Here staff may check their understanding of basic security concepts (based upon summarized guideline 'highlights') and find pointers to more detailed information if they are interested (ISHTAR, 1997). The web service also has the unique potential to deliver advice of a more dynamic nature to a wide audience (e.g. issuing virus warnings) - in a way that the guidelines and seminars cannot. The address of the Internet site is http://www.ishtar.org.uk/.

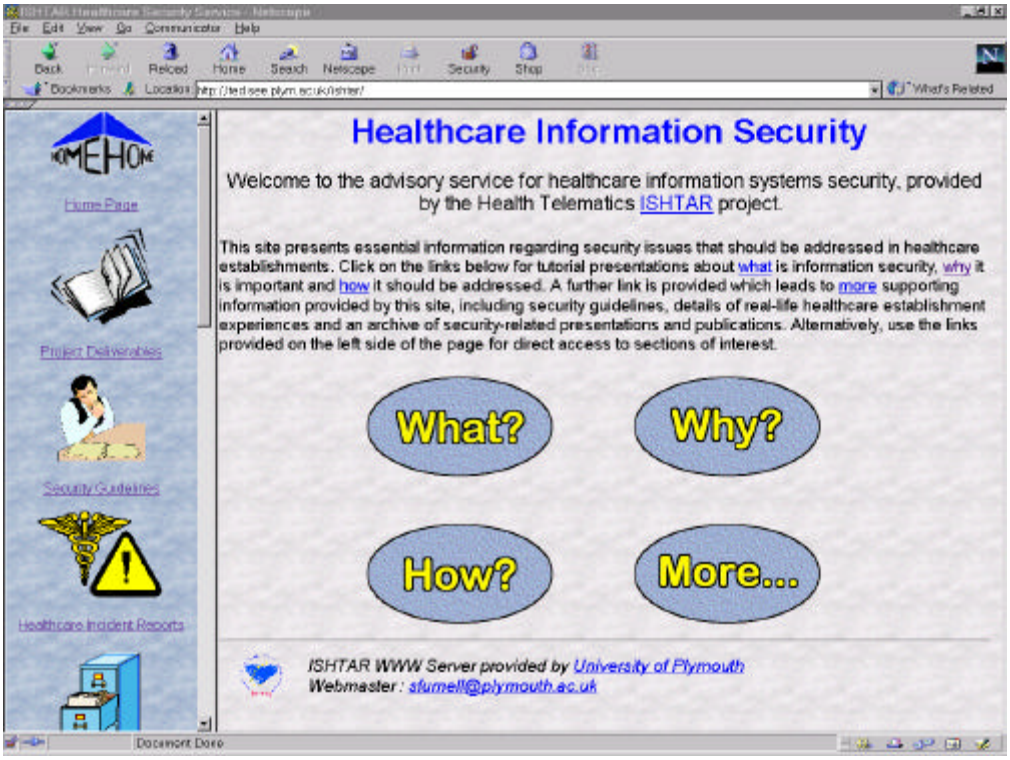

Figure 2: The ISHTAR title page

SITUATION WITH AUSTRALIA

The situation within Australia is very different. There has been no centralized development of security awareness courses across the whole of Australia. This is partly due to political development of healthcare within Australia that each state and terrority has developed their healthcare infrastructure and supporting information systems and policies.

The other problem is limited research into healthcare computer security. Within Australia only limited national surveys have been undertaken (Deloitte Touche Tohmatsu/Victoria Police, 1999) unfortunately this survey was only concerned with the 350 largest Australian companies. Therefore it was decided to conduct a survey of hospitals within Victoria to gain a snapshot of attitudes towards computer security within healthcare based upon the previous survey format.

Survey Methodology

The computer crime survey was sent out to 60 IT Security Officers, who were based within hospitals in the state of Victoria. Thirty surveys were sent to randomlyselected public healthcare establishments and thirty to private healthcare establishments The names of the hospitals surveyed were obtained from government directories, web sties as well as telephone directories. The responses were all anonymous. Each survey was supplied with a prepaid envelope. As some of the questionnaires were of a sensitive nature, no identifying information was asked for. This anonymity, it was hoped would add to the validity of the data.

The survey was sent out in April 2000. There were 22 valid responses, giving a response rate of 37%. Information on the number of respondents is provided in Table 1.

	Number of Responses	**Percentage**
Public Hospitals	12	40%
Private Hospitals	10	33.3%

Table 1: Number of valid responses

Table 2 shows the information of the size of the institution (by employee numbers).

Employee numbers	**Public Healthcare Establishments**	**Private Healthcare Establishments**
<500	75%	60%
<100	8.3%	40%
<5000	8.3%	0%
>5000	8.3%	0%

Table 2: Organisation size

Most of the questions (where relevant) had a space for the respondents to give specific comments, or include an answer of their own that was not offered within the question. The questions were intended to identify specific information about the establishment (size etc.) as well as determine their current security policies and uses. Also to establish current problems and possible future solutions.

Results and Discussion

Questions 1 through 4 of the questionnaire were designed to give the researchers an idea of the computer and organisational structure of each hospital. From both question 2 and 3, 100% of the private hospitals that responded were connected to the Internet and the same percentage informed us that their staff had access to the Internet, compared with only 18% of staff in public hospitals. However slightly more public hospitals (64%) had a formal policy regarding staff usage of the Internet than did private hospitals (44%). This posed a question of whether staff usage of the Internet was monitored, and the feasibility of emailing important medical information out of a HCE.

Questions 5 – 7, asked the healthcare establishments about their consideration of computer risk factors, misuse and awareness.

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 did 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 responses to Question 7 showed high "yes" responses. The majority of both private and public healthcare establishments have an active security awareness program for employees using computers. The responses indicated that the most popular issues that were covered under the security awareness program was "password management" and "virus protection" although more private healthcare establishments reported that they also considered "laws of misuse" and "ethics" as part of this awareness program.

Questions 8, 9 & 10 were designed to reveal attitudes to the increased use of the Internet in the workplace and the employers concerns that accompany it. Both the private and public healthcare establishments seemed to agree that a "user would act differently if their activity was being monitored and recorded". However when asked "whether they considered continuous monitoring to be acceptable" the public healthcare establishments attitude was 50% "yes" and 50% "no". This was not the case for the private sector, 70% indicated that they believed it was acceptable. Finally the healthcare establishments were asked whether "users should be aware they are being monitored?" All but 4 of the healthcare establishments surveyed believed that users should be made aware of the monitoring process.

Question 11 was made up of a number of parts. First of all it was to identify those healthcare establishments that had experienced any unauthorised use of their computer systems within the last year. Slightly more private (50%) had experienced such use as public (33%). Although there were was no significant difference. Of those that reported unauthorised use, 78% were between 1-5 attacks and the remaining 22%, 6-10 attacks. No companies reported over 10 attacks. The majority of unauthorised use was identified as being “unauthorised/nuisance”, “introduction of computer viruses” and “copying of data/programs”. However when asked “to indicate their impression of the source of the breaches, public hospitals identified “independent hackers”. Private hospitals also identified there was an impression that a number of the attacks were the result of the interference by a “corporate competitor”.

Questions 12 and 13, tried to gleam information as to the circumstances in which hospitals would be willing to report computer crime to a law enforcement agency, and their reasons for doing so. Private establishments expressed that they were more likely to report if there was” successful prosecution”, "it was mandatory by law” or “it could be immediately detected”. Although the public report also ranked these as high, they were more concerned with “recovering losses”.

Again the reasons for reporting the computer crime were similar in some respects, that is, both believed the prosecution of the offender would be a strong motivation. Interestingly, the public hospitals scored very highly on “the chance to recover costs/damages” and “ making an insurance claim”.

The final Question (number 14) was designed to discover where hospitals believed the threats of future computer crime would come from. The public healthcare establishments saw the threats as coming from “a greater use of encryption” and “hacking”, whereas more of the private healthcare establishments saw the threat of “theft” as having the most impact on their establishment (as well as “more encryption”).

The results suggest a few differences in the attitudes and experiences of public and private hospitals. In summary, more of the private hospitals have Internet access and therefore more of their staff consider security risks. Also they are more likely to have undertaken formal risk assessments and have policies in place to counteract any such risks. The decision process as to whether to report computer crime, brought out difference, in that the public hospitals seem to be more concerned about monetary issues. There is still concern over security issues in both private and public hospitals. Until all healthcare establishments put into place risk assessment procedures and policies for unauthorised use and other computer crime activities, there will continue to be a real risk with the security of healthcare data and information.

The survey showed the researchers that there is a need to develop a security training courses and awareness programme based upon the European models – with the attention of reducing the levels of unauthorized use of organization computing facilities,

CONCLUSION

It must be noted that the findings were based upon a small sample survey within Victoria. A more detailed survey across all of Australia will be undertaken in the future to reveal the true extent of the perceived problem.

The paper has suggested possible methods that could to help raise security awareness. But it should be considered that these methods may not resolve all the security issues that may exists within HCEs. It is essential that a training framework must be implemented and its content should be reviewed regularly in to maintain its relevance. The framework put forward is based upon research undertaken within the European Union, the next stage is to translate that research so that it can operate within the Australian framework.

REFERENCES

Audit Commission. (1990). *Survey of Computer Fraud & Abuse*. National Report, London, HMSO, UK.

Audit Commission. (1994). *Opportunity Makes a Thief: An Analysis of Computer Abuse*, National Report, London, HMSO, UK.

Audit Commission. (1998). *Ghost in the Machine – An Analysis of IT Fraud and Abuse*. Audit Commission Publications, UK.

Deloitte Touche Tohmatsu/Victoria Police. (1999) *Computer Crime & Security Survey – 1999*. Australia.

Fak, V. and Hunstad, A. (1993). Teaching security basics: The importance of when and how, in *Computer Security*, E.G.Dougall (Ed.), Elsevier Science Publishers B.V. (North-Holland): 23-30.

Furnell, S.M, Gaunt, P.N, Holben, R.F, Sanders, P.W, Stockel C.T. and Warren, M.J. (1996). Assessing staff attitudes towards information security in a European healthcare establishment, *Medical Informatics*, UK, Vol 21, No 2, 1996.

ISHTAR. (1995). Project Programme. Telematics Applications for Health Project HC1028, *Implementing Secure Healthcare Telematics Applications in Europe* (ISHTAR).

ISHTAR (1997). ISHTAR Internal Paper - I04IM26B - ISHTAR White Paper.

Sanders, P.W, Furnell, S.M. and Warren M.J. (1996a). Baseline Security Guidelines for Health Care Management, in: *Data Security in Health Care - Volume 1, Management Guidelines*. The SEISMED Consortium (Eds). Technology and Informatics 31, IOS Press: 82-107. The Netherlands.

Sanders, P.W, Furnell, S.M. and Warren M.J. (1996b). Baseline Security Guidelines for Health Care IT and Security Personnel, in: *Data Security in Health Care - Volume 2, Technical Guidelines*. IOS Press: 82-107. The Netherlands.

The SEISMED Consortium (Eds). (1996) *Technology and Informatics 32*, IOS Press: 189-234. The Netherlands.

Warren, M.J, Furnell, S.M and Sanders P.W. (1997) ODESSA - A new approach to healthcare risk analysis, *IFIP TC11 International on Information Security (SEC 97*), May, 1997, Copenhagen, Denmark.

COPYRIGHT