A new approach towards security training and awareness amongst the Healthcare Community

Matthew WARREN[†] , Steven FURNELL[‡] and Peter SANDERS[‡]

[†] *Department of Computing & Mathematics, Deakin University, Geelong, Victoria, Australia*
[‡]*Network Research Group, School of Electronic, Communication and Electrical Engineering, University of Plymouth, United Kingdom*

Email: m.warren@deakin.edu.au

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 security awareness.

The paper describes a basic framework that HCEs could follow in setting up a training and awareness framework. The paper also describes how relevant security information may be disseminated to staff via the use of security guidelines, training seminars and world-wide web based services.

The paper is based upon work that is currently being undertaken as part of the European Union Health Telematics Project ISHTAR (Implementing Secure Healthcare Telematics Applications in euRope) project.

1. 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 operation, 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 issues [1].
Past research has shown the lack of training amongst HCE staff. A survey amongst a large European HCE [2] portrayed the problem that exists. The survey revealed, out of 75 overall respondents, 25% claimed to have received initial security related training and only 15% indicated that they has attended ongoing security awareness seminars. The survey also highlights some of the security problems that have arisen from the lack of security training, these include poor use of passwords, unauthorised data modification, attempted hacking, etc. This shows that there is a relationship between lack of security awareness and training and an apparent increase in security misuse incidents.

2. Key issues in Training

Training and awareness within HCEs is very important, but 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 [3,4] which resulted in many training and awareness recommendations relating to the following areas.

2.1. 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. All staff should be aware that disciplinary action will result from failure to observe security procedures and offenders should be seen to be disciplined in order to discourage others.

2.2. 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.

2.3. 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.

2.4. 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.

2.5. 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).

2.6. 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.

3. Current 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 through efforts in four key areas [5]:

3.1. 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 EU 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.

3.2. Enhancement of the SEISMED 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.

3.3. 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 Health care [6]. Its 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.

3.4. 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. 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://ted.see.plym.ac.uk/ishtar/ (see figure 1)

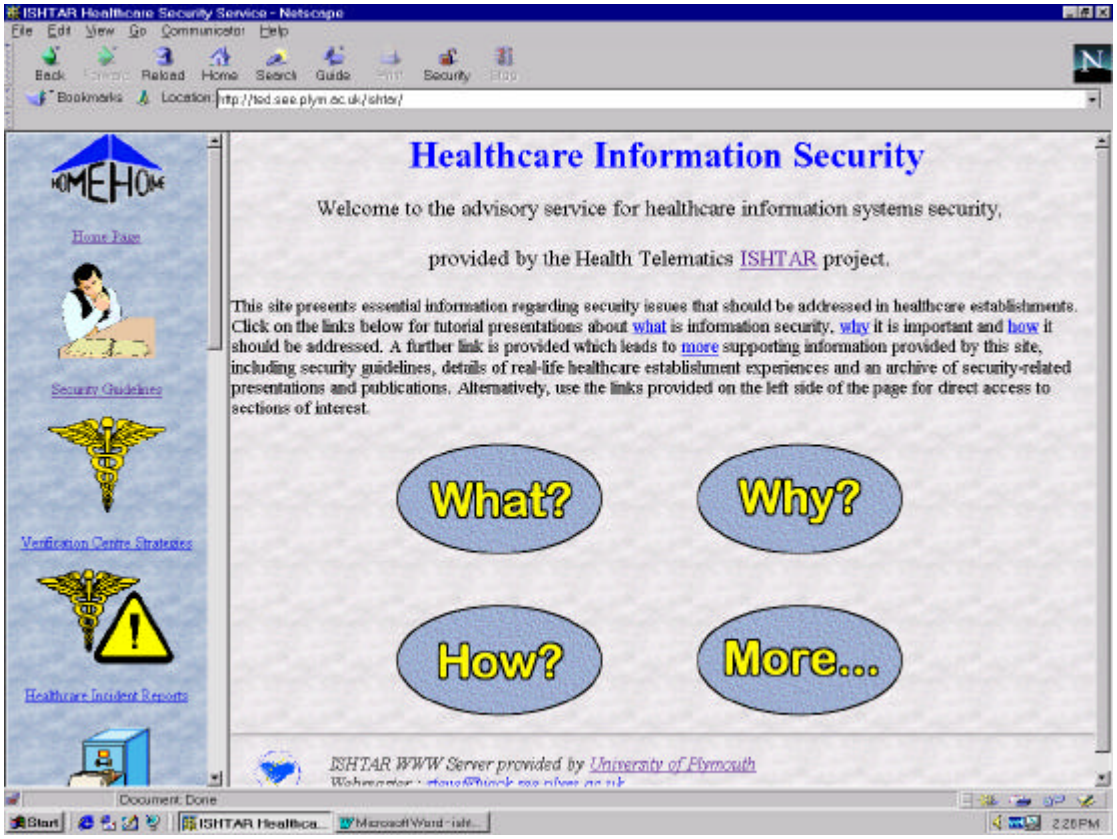


Figure 1 : The ISHTAR title page

and the main features of the website include:

3.4.1 Project overview

This page presents a general description of the project (taken from the Project Programme), with links to specific pages detailing workpackages and partners.

Partners
A general description of each of the partners, along with an associated list of work to be completed. Links are included to the partners home-pages of each lead partner.

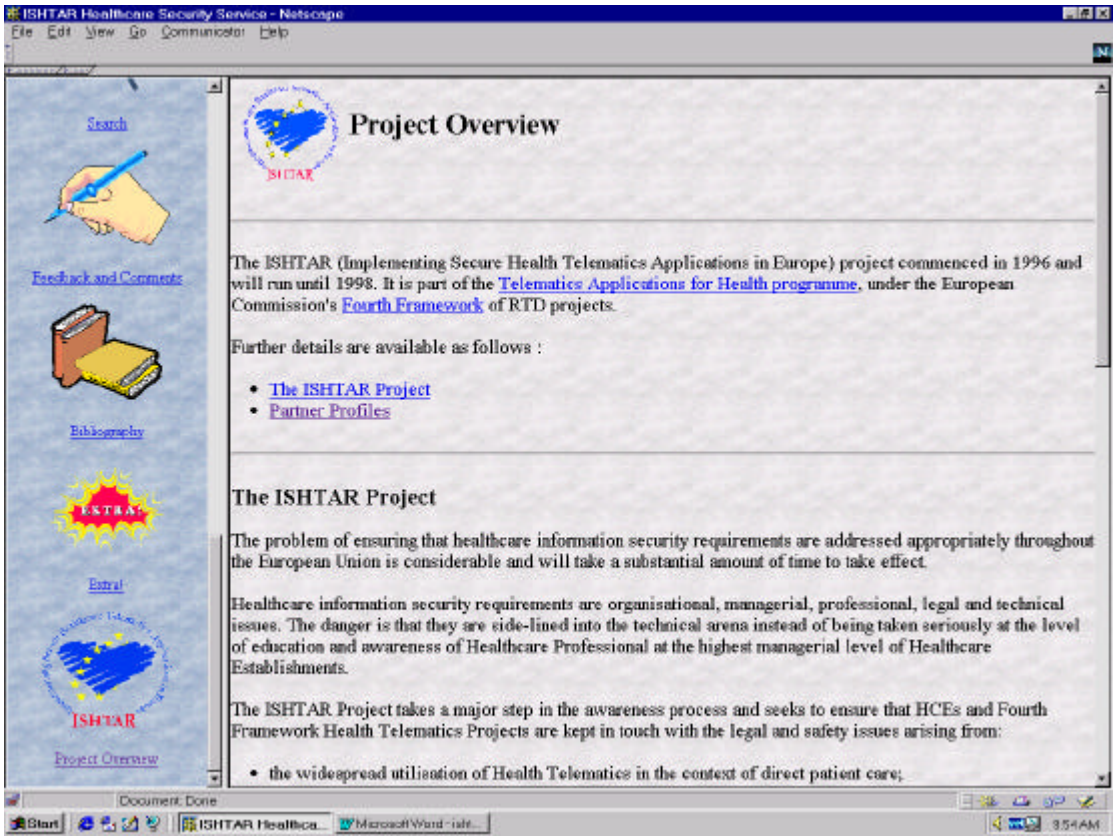


Figure 2 : The workpackages page

3.4.2 Security Guidelines

This section presents one of the main elements of the current site, namely highlights from the healthcare security guidelines produced by the AIM SEISMED project. The section contains the following information:

- an overview of the SEISMED project;
- three sub-sections for the user, management and technical guideline sets;
- details of the original guideline authors;
- a full-text paper describing the clinical need for security.

The page acknowledges that the guidelines described are the product of work conducted by SEISMED. This page also publicises the existence of the full guideline handbooks and includes appropriate contact details for IOS Press (in the form of a link to their WWW site).

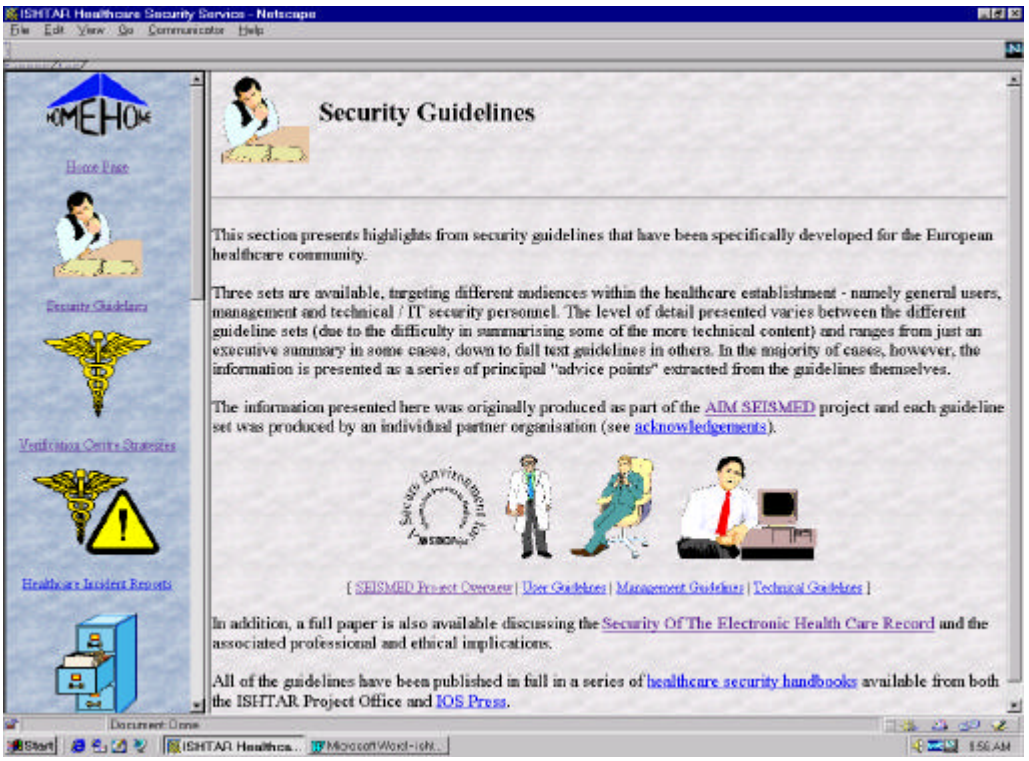
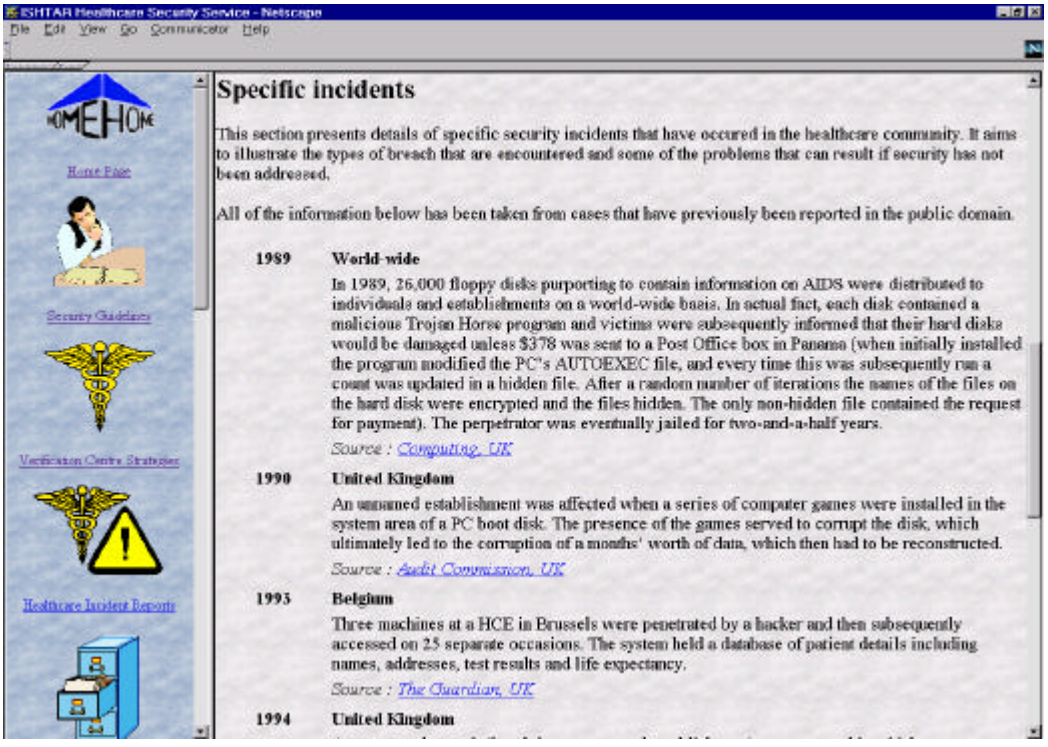


Figure 3 : The security guidelines index page

3.4.3 Healthcare Incident Reports

This page allows users to view anonymous examples of real security breaches. This will help to underline the importance of security and also aid understanding of the required solutions. The aim is to update this information on a regular basis in order to offer up-to-date



examples.

Figure 4 : The Incident Reports page

3.4.4 Archive

This section provides a repository of published papers and presentation material that interested parties can browse online. The materials offered include:

Published Papers
This section provides details of relevant published papers that have been produced by members of the consortium. It is also possible to provide full-text and/or downloadable versions of papers within this framework.

Presentations
Further information is made available in the form of online presentations relating to healthcare / security issues. These are based upon slideshows that have been used to support conference presentations and the like.

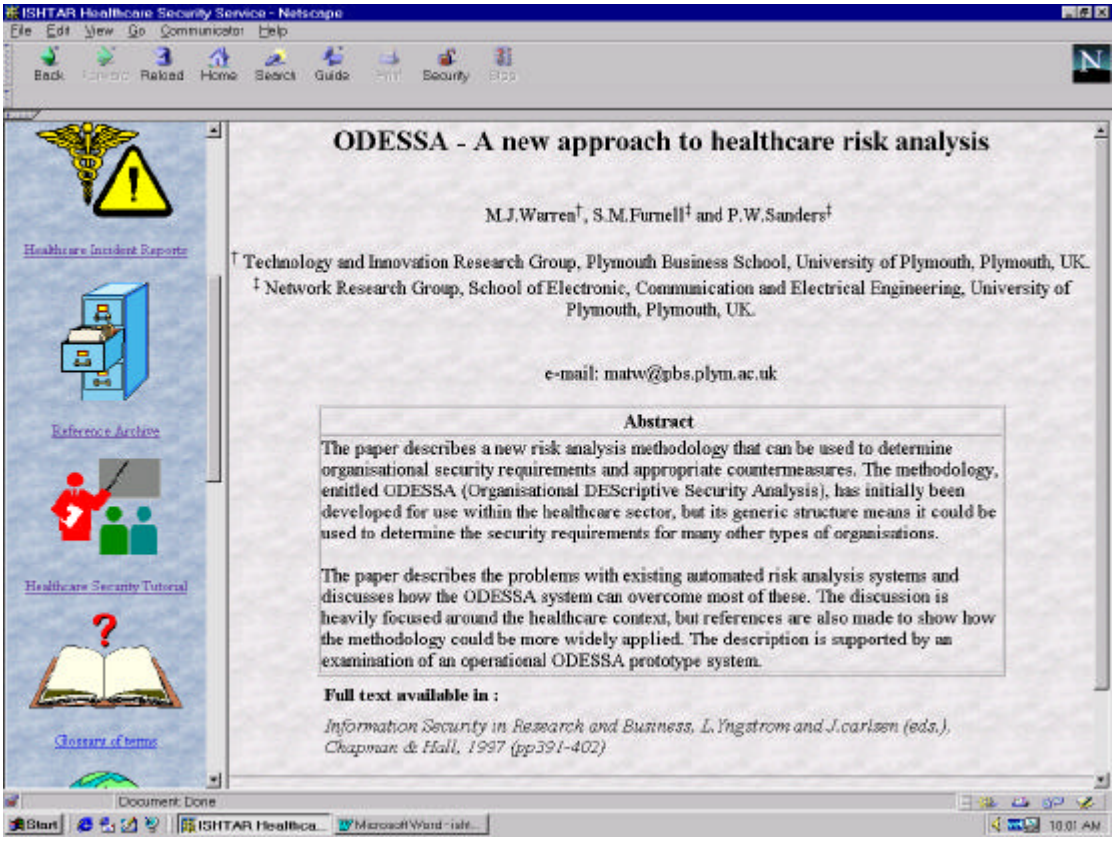


Figure 5 : An example published paper page

3.4.5 Glossary

The glossary service is necessary to help explain many of the terms that are used on the web pages (particularly in the guidelines sections). The principal basis for this is a reproduction of the SEISMED glossary, as it appears in the security handbooks (in actual fact, the vast majority of the definitions were originally extracted from other sources,). It will be progressively enhanced over time, with further terms and definitions being added in response to partner suggestions as appropriate.

3.4.6 Feedback and Comments

This facility provides a means for the end-users of the service to let the ISHTAR consortium to assess the system. Two approaches have currently been implemented :

1. the simple provision of the e-mail and postal addresses of the ISHTAR office (with the email address acting as an automatic "mailto" link);
2. the provision of a fill-out form to enable immediate submission of brief free-text comments.

3.4.7 External Links

Hypertext links are provided to a number of other Internet sites that may interest the service users. These are principally grouped according to the type of site that is accessible (e.g. WWW or FTP). Where a large number of links are presented, further subdivision then occurs under additional headings to denote the general nature of the content (e.g. security, health telematics, other EU projects etc.).

3.4.8 Bibliography

This page provides a number of references to the sources used in creating the technical / advice content of the service, particularly in relation to the security guidelines. The provision of this information will enable interested readers to obtain further relevant material to supplement that which they have encountered in the site.

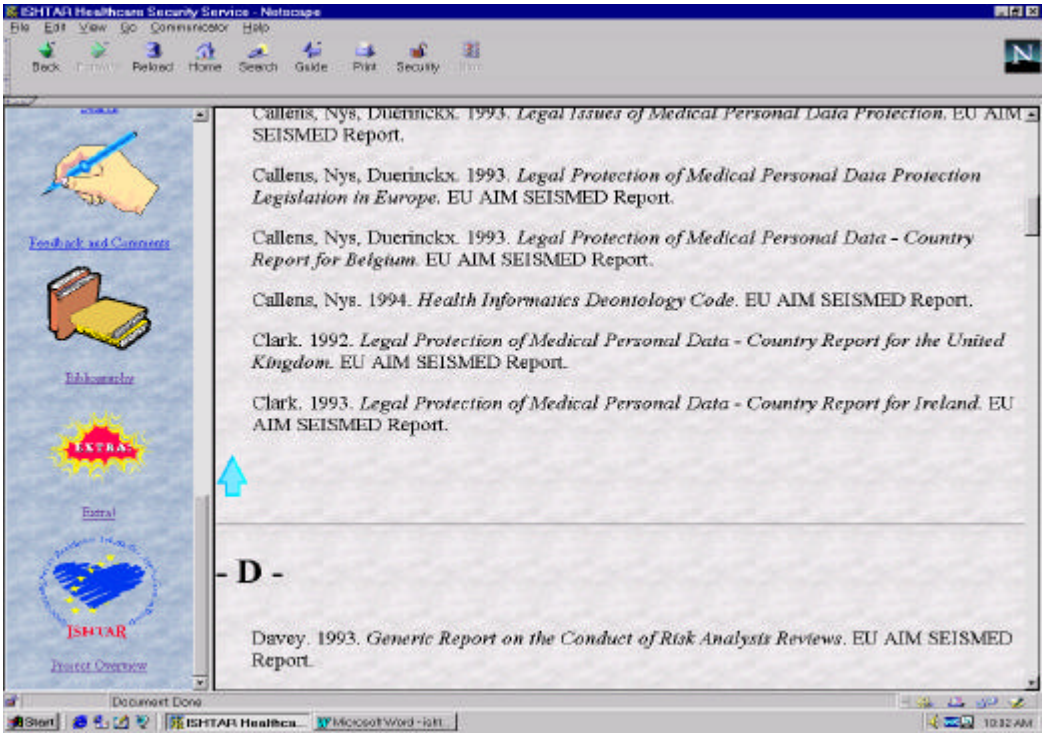


Figure 6 : The bibliography page

3.4.9 Extra!

This section represents the location for other miscellaneous information that does not fit comfortably under the headings already identified. Current examples here include :

- details of the ISHTAR training programmes;
- notification of relevant conferences;
- calls for papers;
- information gathering exercises (e.g. surveys of healthcare security attitudes).

4. Conclusion

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.

At the moment the ISHTAR project is currently addressing healthcare security in many areas and can considered to be making a significant contribution to the overall awareness issue. The success of the ISHTAR initiatives are dependent upon a receptive audience and adherence to the advice by the various HCE staff involved. It can, therefore, be concluded that in the same way as people represent the weakest link in the security strategy, they are also the potential weakness of the training programme. The paper also shows that many areas relating to training and awareness can be helped by the use of the Internet service offered by the ISHTAR project.

5. Acknowledgments

This paper has arisen from the authors' involvement in the ISHTAR Project (Implementing Secure Healthcare Telematics Applications in Europe). A Telematics Applications for Health Project (HC1028) of CEC DGXIII C.

References

1. 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.
2. 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*.
3. Sanders, P.W, Furnell, S.M. and Warren M.J. 1996. "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.
4. Sanders, P.W, Furnell, S.M. and Warren M.J. 1996. "Baseline Security Guidelines for Health Care IT and Security Personnel" in Data Security in Health Care - Volume 2, Technical Guidelines.
5. The SEISMED Consortium (Eds). Technology and Informatics 32, IOS Press: 189-234.

6. ISHTAR. 1995. Project Programme. Telematics Applications for Health Project HC1028, Implementing Secure Healthcare Telematics Applications in Europe (ISHTAR). 1 Nov. 1995.
7. ISHTAR 1997. ISHTAR Internal Paper - I04IM26B - ISHTAR White Paper.