Addressing information security training and awareness within the European healthcare community

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

[†] *Network Research Group, School of Electronic, Communication and Electrical Engineering, University of Plymouth, United Kingdom*
[‡] *Business Security Group, Plymouth Business School, University of Plymouth, United Kingdom*

E-mail : stevef@orac.pbs.plym.ac.uk

Abstract. This paper discusses the need to promote information security issues within modern healthcare establishments and the consequent need for appropriate training and awareness initiatives. Security is an area of extreme significance in healthcare information systems but, whilst the need is generally recognised, many personnel are not familiar with even basic concepts and procedures. As such, adequate promotion of security through training and awareness initiatives is viewed as a vital first step.

The paper highlights a series of basic factors that healthcare establishments (HCEs) should consider in setting up a training and awareness framework. The discussion then examines a number of ways in which relevant information may be disseminated to staff, including security guidelines, training seminars and world-wide web based services.

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

1. Introduction

Modern healthcare establishments (HCEs) are now heavily oriented towards the use of Information Technology (IT) systems in most aspects of their work. Furthermore, the sensitivity of the data utilised dictates a significant need for information security to maintain its confidentiality, integrity and availability. However, it has been stated in [1] that security can only be maintained if all personnel with system access know, understand and accept the necessary precautions. Many breaches are the result of incorrect behaviour by general staff who are unaware of security basics. The provision of security training and awareness will make it possible for staff to consider the security implications of their actions and avoid creating unnecessary risks.

Most IT users are now well aware of the need for security, with the regular stream of highly publicised incidents of hacking, viruses and the like helping to underline the problems that may be encountered without it [2]. Knowledge of such cases helps to make users more accepting of the security measures that may be enforced on their systems. However, this does not necessarily mean that they fully appreciate the associated issues. For example, whilst virtually all users make use of passwords, a much lesser number pay correct attention to selecting, changing and maintaining the secrecy of them. In addition, many security breaches are of a much less dramatic nature than the cases that are highlighted in the media and, as such, it is possible for their significance to be overlooked. For example, staff may routinely breach aspects of security policy through what are (in their opinion) “minor” offences, such as failing to challenge strangers, sharing passwords with colleagues and the like (whilst both of these examples may seem relatively trivial, they offer an opportunity for a second party to perpetrate a more serious breach).

The lack of training is frequently reflected in the attitudes of HCE staff. As an example of this, it is possible to consider the results of a survey conducted amongst the general user population of a large European HCE [3]. This revealed that, out of 75 overall respondents, only 25% claimed to have received initial security-related training and only 15% indicated that they received ongoing security awareness. The consequences of this were apparent in a number of observations regarding the same staffs attitudes towards different aspects of security. Various problems were identified, including poor use of passwords, unauthorised data modification, incidents of attempted hacking and problems with information control. With these points in mind, it is useful to consider how security issues may be more effectively promoted to the healthcare community.

2. Key issues in promoting training and awareness

This section considers some basic steps that could be taken to address the training and awareness requirements within an individual HCE. This advice draw heavily upon the training and awareness recommendations that appear in the security guidelines produced by the AIM SEISMED (Secure Environment for Information Systems in MEDicine) project [4,5].

2.1. Job training *Job training*

Staff should receive instruction in how to perform their day-to-day duties as well as any specific security issues relating to their role. This should convey a clear statement of what is expected in terms of security, with well-defined bounds so that staff are not concerned when performing legitimate duties. 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. In addition, documentation should be available for general reference to supplement and re-enforce the training provided.

2.3. HCE training programmes *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 security policy and concentrate upon providing basic security awareness for all personnel. Coverage should include the key issues of confidentiality, integrity and availability as they apply in the health care environment and stress the basic security procedures that should be followed by staff using information systems (e.g. correct use of passwords, backing up of data, awareness of viruses etc.).

More specific in-house training may be provided at the departmental level, with programmes tailored to the needs of the staff within them. These schemes should make reference to the wider HCE programme so that staff can relate to their existing knowledge of general security requirements. In-house training should also highlight the relationship that exists between security and maintaining patient safety and confidentiality, underlining the importance of following the advice.

2.4. Specialist training courses

Some staff (e.g. IT managers, security staff) will require training beyond the level of that described above. 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). The way in which additional awareness is provided may vary depending upon the significance of the issue (e.g. immediate threats to security should be handled via staff briefings, whereas in more minor cases details could be communicated via memos / email). In any case it must be ensured that the message is effectively conveyed to all relevant personnel.

2.6. Training responsibilities

A Security Officer 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. However, general staff should also be able to contact the security officer to establish their individual training needs.

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 [6] :

1. formation of an expert advisory panel in legal, medical and technical aspects of healthcare data protection;
2. enhancement of the SEISMED security guidelines;
3. establishment of security training programmes for healthcare users, management and technical personnel;
4. dissemination of security-related material via the world-wide web (WWW).

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. The enhancement of the guidelines is being conducted on the basis of comments received from the ten European HCEs acting as Verification Centres within the project, along with updates to address recent developments in information security. 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 WWW service sets out to promote and supplement the work of the project in a number of areas. These include the provision of online access to security advice, healthcare incident reports, security strategies from the verification centres and a repository for security-related presentations and publications. A more detailed description of the web service can be found in [7].

It can be seen that the various initiatives seek to promote security in different ways, providing a comprehensive and complementary overall strategy. Papers from the panel will promote general awareness of the key issues facing the healthcare community, facilitating a harmonised approach. 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. However, simply promulgating the guidelines to all staff or relying upon individual initiative to read them would be unfeasible and provide no real likelihood of improved security. The sheer volume and depth of information would ensure that few people would remember or understand the complete set. Furthermore, many staff could encounter difficulties in identifying what is really relevant to them. As such, key individuals will benefit from formal instruction in the basic security concepts upon which the guidelines are based. This is where the training seminars are valuable, enabling certain staff to be established as security contacts for their colleagues and ensuring specific awareness in key roles (e.g. system administrators and departmental managers).

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 summarised 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.

4. Conclusion

The paper has outlined a range of ideas that will enable a comprehensive approach to healthcare security awareness to be established. However, it must be realised that even with these points addressed, the security issue should not be considered totally resolved. The training framework must actually be utilised and the advice it provides should be regularly reviewed in order to maintain its relevance.

The ISHTAR project is currently addressing healthcare security on many fronts and can, therefore, be considered to be making a significant contribution to the overall awareness issue. However, these initiatives are again 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.

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. Audit Commission. 1994. Opportunity Makes a Thief - An Analysis of Computer Abuse. HMSO Publications Centre, PO Box 276, London, United Kingdom.
3. 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*.
4. 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.
5. 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. 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. Furnell, S.M, Sanders, P.W. and Warren, M.J. 1996. "Provision of healthcare security information services using the World-Wide Web", in *Proceedings of Medical Informatics Europe 13th International Congress (MIE 96)* (Copenhagen, Denmark, Aug. 19-22): 98-102.