The ISHTAR guidelines for healthcare security

S.M. Furnell, J. Davey, P.N. Gaunt, C.P. Louwerse, K. Mavroudakis and A.H. Treacher

S.M. Furnell
Network Research Group, School of Electronic Communication and Electrical Engineering
University of Plymouth
Plymouth, UK
Tel/Fax: 01752 233520
Email: stevef@jack.see.plym.ac.uk

J. Davey
HEIMDALL Ltd
Claremont House
22/24 Claremont Road
Surbiton, UK
Tel: 0181 399 3130
Fax: 0181 3903360
Email:HEIMDALL @compuserve.com

P.N. Gaunt
Department of Healthcare Informatics
Derriford Hospital
Plymouth, UK
Tel: 01752 792371
Fax: 01752 771561
Email:nick.gaunt@phnt.swest.nhs.uk

C.P. Louwerse
Leiden University Medical Centre
Leiden, The Netherlands
Tel: +31 71 5263240
Fax: +31 71 5248240
Email: cplouwer@cdiv.azl.nl

K. Mavroudakis
University of the Aegean, Research Unit
30 Voulgaroktonon Street
Athens, GR-11472
Greece
Tel: +30 1 6442727
Fax: +30 1 8203507
Email: kmav@aegean.gr

A.H. Treacher
PO Box 231
Burton upon Trent
Staffordshire, UK
Email: 100606.2753@compuserve.com

Correspondence to:
S.M. Furnell

Data security is now recognized as an important issue in healthcare information systems and, as such, a number of relevant guidelines have been produced. However, the range of available sources means that a standardized approach to security between establishments is unlikely. In addition, the majority of known approaches are paper-based and do not lend themselves to easy reference or ad hoc queries in relation to specific issues. As a result, while appropriate guidelines are available, it is frequently the case that they are not fully utilized.

This paper focuses upon efforts that have been made to resolve these problems through the development of an electronic database of healthcare security guidelines. This aims to provide a comprehensive resource, utilizing information from a number of sources, built upon a foundation of previous guidelines developed in European research. The discussion addresses the background, implementation and advantages of the new approach. It is also recognized that the provision of a database alone will not totally overcome the issue of security awareness and training. As such, brief details of other supporting initiatives, including training programmes, an incident reporting scheme and a WWW service are also provided.

The paper is based upon work that has been conducted as part of the ISHTAR project (Implementing Secure Healthcare Telematics Applications in euRope) under the European Commission's Telematics Applications for Health research programme.

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 desktop PCs to minicomputer and mainframe installations.

The influence of information systems can 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 dependent upon the availability of systems and reliant upon the correctness of the data that they hold. This, in combination with the overall sensitivity of much of the data, dictates a requirement to preserve information security. Indeed, the provision of appropriate protection is increasingly likely to be a legislative requirement, with the European Union Directive on the protection of personal data stating that appropriate security measures should be in place within the system [1].

IT SECURITY INCIDENTS IN HEALTHCARE

A recent survey of computer crime and abuse within the UK [2] has revealed that 45% of HCEs have experienced some form of security incident within the past three years. This represents an increase of 10% when compared with the results from a previous survey conducted in 1994 – indicating that the problem of security is not only significant within healthcare, but is getting worse. However, it can be conjectured with some confidence that a significant proportion of such incidents would have been preventable if the HCEs involved were pursuing appropriate security policies. A key aspect in ensuring protection is training users about security and raising awareness of the issues [3].

Previous research has indicated the lack of security training provided for HCE staff. A survey conducted among the general user population of a large European HCE illustrated the nature of the problem that exists [4]. The survey covered a range of issues, grouped under the main headings of physical, logical and personnel-related security measures. The results revealed that, out of 75 overall respondents, 25% claimed to have received initial security-related training and only 15% indicated that they had attended ongoing security awareness seminars. Both figures are clearly low, but it is important to note the significant difference between them, which indicates that even where security training is provided, it is not always supplemented by further ongoing awareness activities. As such, staff may become less security conscious as time goes on, with less opportunity for good practice to be reinforced. The survey also highlighted some of the security

problems that had arisen from the lack of security training, including:

- poor use of passwords;
- poor use of system security features;
- unauthorized data modification;
- incidents of attempted hacking by staff;
- problems with information control.

The consideration of these points in light of the results above indicates that there is a relationship between a lack of security awareness and training, and an apparent increase in security misuse incidents.

As a result of these observations it is clear that a general need exists to improve both the level of information security within the healthcare community, as well as the training and awareness initiatives associated with it. A key factor in being able to achieve this is to ensure the availability of suitable advice and guidance on a wide scale.

THE ISHTAR PROJECT

A number of security awareness initiatives have been developed and promoted by the ISHTAR project (1996–99), under the European Commission's Telematics Applications for Health programme. The main objective was to address the problems of health data protection and information systems security within the healthcare community at a general level. The mechanism utilized to achieve this was the actioning of programmes aimed at raising the level of security awareness within HCEs across Europe.

The project involved the collaboration of partners from ten European Union countries (Belgium, France, Finland, Germany, Greece, Ireland, Italy, The Netherlands, Portugal and the UK), one EFTA country (Switzerland) and one Eastern European country (Czech Republic). Security expertise within the consortium was provided by representatives from healthcare establishments, commercial companies, standards bodies and universities from across Europe. The practicality of the resulting recommendations was ensured by the participation of ten HCEs acting as *verification centres* for the project. One of the principal deliverables of the project, and the main focus of this paper, is a database of security guidelines specifically tailored for use within the healthcare community.

SECURITY GUIDELINES FOR HEALTHCARE ESTABLISHMENTS

A comprehensive set of healthcare security guidelines had previously been produced by the SEISMED project (Secure Environment for Information Systems in MEDicine) which was the forerunner of ISHTAR under the European Commission's Advanced Informatics in Medicine (AIM) programme. As such, these represented the principal foundations for further guideline development within ISHTAR.

The SEISMED work represented a detailed treatment of the issue and sought to provide individual establishments with a key source of reference for all major security considerations. The coverage included areas such as risk analysis, high-level security policy, systems development and implementation, existing systems security and network security. This material was presented in a series of three 'handbooks', targeting general users, management and technical staff within an HCE [5].

While they represented the starting point for ISHTAR, the SEISMED handbooks are by no means the only source of security guidelines available to HCEs. Guidelines from other, non-healthcare, sources are also used on a frequent basis. An example of this can be cited in terms of the countermeasures arising from CRAMM (HM Government Risk Analysis and Management Method), which are widely used for systems within the UK National Health Service [6]. In addition, since the SEISMED work, various other guidelines have been produced that are targeted towards (or at least applicable to) healthcare. Examples include the guidelines produced by CEN (Comité Européen Normalisation [7]) and the security framework developed by the INFOSEC Business Advisory Group (IBAG [8]). While the existence of these multiple sources is good from the point of view of HCEs having wider access to useful guidance, the downside is that the advice is presented in fundamentally different ways, leading to the strong probability of a lack of harmonization in the approaches taken by different establishments.

In addition, a number of criticisms can now be levelled at the original SEISMED guidelines:

- The guidelines themselves are becoming out of date as the core information technologies used within healthcare advance. For example, the mainstream adoption of

the Internet and World Wide Web has occurred *since* the release of the guidelines, but brings with it a whole range of new security considerations that must be addressed.

- It has been determined that the presentation of guidelines according to the three audiences is restrictive – more 'views' are required to suit different personnel and circumstances.
- The original paper-based dissemination medium does not allow flexibility in terms of quick reference or topic-based searching, making them unsuited to day-to-day use within HCEs.

A fundamental difference in the ISHTAR approach is that the enhanced guidelines are presented in electronic format. This approach centres on a database containing all of the updated principles, guidelines and risk analysis countermeasures. The aim here is to increase the usability and accessibility of the material, so that a security manager (or similar) could easily extract all of the countermeasures/guidelines applicable to a particular area of concern (for example, access control).

The core material included in the database was provided by an enhancement of the SEISMED work. However, to enable the required harmonization of recommendations, reference was made to a number of other established sources to identify omissions. These included the results from the European pre-standard work of CEN PT012 (in the form of healthcare 'protection profiles') [7], the UK code of practice for information security management [9], the IBAG security framework [8] and the latest CRAMM network security countermeasures [6]. The resulting database is considered to provide the most comprehensive source of healthcare security guidance available.

The conceptual structure of the ISHTAR guidelines is shown by the entity relationship diagram in Fig. 1. At the highest level are a

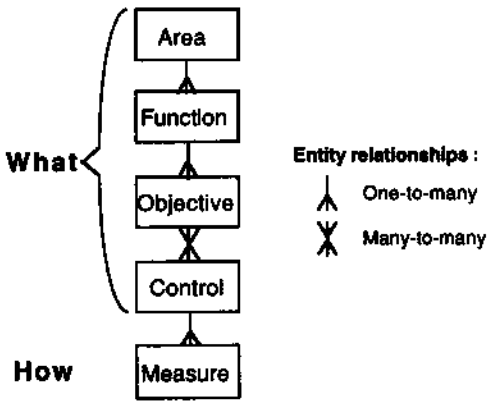

Fig. 1. Conceptual structure of guidelines.

number of *areas* of security which require control. Each of these may encompass a number of *functions*, each of which may in turn have one or more *objectives* in terms of protection. The *objectives* are realized by one or more conceptual *controls*, which may necessitate the use of one or more practical *measures*. Controls may actually apply to the realization of more than one objective, hence the many-to-many relationship indicated in Fig. 1.

The content of the database addresses the 'what' aspect (i.e. from *areas* down to *controls*). The level of *measures* is considered to be too dependent upon specific technologies/products and, as such, is not covered by the ISHTAR work as any recommendations would be too volatile.

The main control areas, and examples of the underlying functions that they encompass, are listed in Table 1.

The guidelines are presented from an organizational/functional point of view rather than from the perspective of asset protection. What this means in practice is that the issue is approached from a viewpoint such as 'These are the controls that you must consider if you are a clinician' rather than 'These are the controls that you must consider if you have a Windows 98 PC'. This approach is considered to be more appropriate to the people-based healthcare environment. With this in mind, the concept of providing tailored advice to different audiences has been retained. However, the database approach also permits more flexibility in this respect, allowing different 'views' on the core information to be provided more easily than was previously possible. As such, the ISHTAR database supports clinical and procurement views in addition to the user, management and technical views provided by the SEISMED handbooks. Further views may be defined in future if demand is evident from other distinct audiences. Consideration is also being given to the idea of supplementing the database with a simple risk analysis front-end to enable the categorization of risks within specific HCEs. This would, in turn, enable the recommendation of appropriate guidelines from the database. The approach will be based upon risk analysis work undertaken within the SEISMED project [10][11].

In addition to their comprehensive content, the ISHTAR guidelines are considered to offer a number of practical advantages:

- *Computer-based*. The electronic format sets the ISHTAR guidelines apart from most other approaches. While it can be said that CRAMM, for example, is IT-based, its original design objectives mean that coun-

Table 1 ISHTAR Control areas

Control area	Example functions
Management	Policy development Legislative obligations Business continuity, etc.
Personnel and organization	Job responsibilities and resource allocations Security awareness Recruitment, etc.
Physical access	Computing equipment Media Communications infrastructure, etc.
Logical access	Identification and authentication management Levels of access, etc.
Data security	Data confidentiality, etc.
Hardware	Planning and procurement Configuration management, etc.
Environment	Operational environment User environment, etc.
Operating systems	Maintenance Integrity of processing Malicious software, etc.
Software utilities	Procurement Restart/recovery, etc.
Operations	Management of operations Output handling and distribution Security breaches, etc.
Applications development	Quality plan Development method and tools Software design, etc.
Applications management	Procurement and implementation Training Access control, etc.
End-user computing	User management responsibilities Awareness and understanding Processing responsibilities, etc.
Communications	Data confidentiality Network availability and integrity Network management, etc.

termeasure recommendations are not structured or presented in a way that make it suitable for the delivery of the sort of ad hoc advice and enquiries that the ISHTAR database is expected to provide.

- *Flexibility.* The database makes it easy to tailor the extraction and presentation of information to the needs of a particular HCE.
- *Ease of update.* The paper-based format of guidelines such as those produced by SEISMED restricts the opportunities for producing and distributing revised versions of the material. With the database approach, new/updated versions could be made available easily (e.g. by enabling them to be downloaded via the Internet).
- *Compatibility.* The database has been implemented using Microsoft Access™ and runs on a standard Windows PC platform. As such, it is considered to be compatible with the technologies found in the majority of modern HCEs.

FURTHER AWARENESS INITIATIVES

It is recognized that the provision of guidelines alone will not resolve the problem of healthcare security. The guidelines need to be supported within a wider awareness framework to ensure that HCEs know of their existence and have the appropriate skills to implement/utilize them in practice. To this end, the ISHTAR project has also pursued a number of other initiatives that can be considered as complementary to the guidelines. Notable activities here include:

- The establishment of a range of security training courses;
- Establishment of a healthcare-specific incident reporting scheme (HIRS);
- Creation of a security dissemination service based on the World Wide Web (WWW).

These are summarized in the sub-sections that follow.

Security training courses

A series of three training courses have been established, targeting user, management and technical audiences respectively. The content of the programmes is based upon information from the guidelines, standards work from the former CEN TC251 Working Group 6 and other relevant expertise.

The suitability of the training material was validated through the conduct of a successful pilot course in The Netherlands during the ISHTAR project.

Healthcare incident reporting scheme

An Incident Reporting Scheme (IRS) is an information system responsible for gathering, evaluating and processing data relating to computer security incidents, as well as disseminating processed information to appropriate interested parties. The desirability of a healthcare-specific scheme is related both to the increased use of interconnected and highly sensitive healthcare systems, as well as the characteristics of healthcare environments that set them apart in terms of other requirements for security. The aim of the ISHTAR HIRS is to provide HCEs with facilities to

compare results, improve information quality and obtain a more accurate view of the threats and vulnerabilities that such organizations are susceptible to.

A pilot version of the HIRS has been developed for trial purposes within the ISHTAR Verification Centres (European HCEs acting as referees on the results and outcomes of the work). The current functionality encompasses the management of the database (i.e. registration, update and deletion of incident records) and the publishing of reports (based upon a variety of criteria – e.g. incidents relating to a specific type of threat).

Healthcare security WWW service

This is probably the most widely accessible aspect of the ISHTAR work and is intended to provide basic security advice and guidance to a general audience. The content of the service can be grouped into three main categories: detailed information sources, reference facilities and supporting services.

The detailed information sources represent the main areas from which security advice and guidance can be obtained. These include online links to information from the security guidelines (initially related to the original SEISMED incarnation, but ultimately reflecting the full ISHTAR set), an archive of published papers and presentations, and statistical reports and anonymized information relating to healthcare security incident reports.

The reference facilities include an online glossary of security terminology (accessible directly or via hyperlinks from the other sections) and a bibliography of healthcare security references. The supporting services relate to search and feedback facilities, as well as the provision of a comprehensive set of relevant links to external Internet sites.

CONCLUSIONS

The pervasiveness of IT within the modern healthcare environment means that information systems security will always be an important issue. However, at the most basic level, it is likely to be perceived as an overhead in relation to the core activity of care delivery. As such, HCE staff require every assistance and encouragement to enable pursuit of good practice. The ISHTAR security guidelines are considered to make a significant contribution in this respect, providing a comprehensive source of reference in an easily accessible manner. The supporting activities, such as training and the Web service, contribute further to an overall framework in which widespread security awareness may be achieved.

Having said this, it is worth noting that the ISHTAR project has principally focused efforts towards the provision of security advisory facilities and has made little contribution in terms of developing the underlying technologies that are being recommended. As such, the success is still dependent upon the existence of controls and countermeasures that can be implemented in practical terms, and are workable within the environment of an HCE.

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] European Union Directive 95/46/EC. On the protection of individuals with regard to the processing of personal data and on the free movement of such data. OJ L281/31-50, 24 October 1995.

[2] Audit Commission. *Ghost in the machine – an analysis of IT fraud and abuse*. London: HMSO, 1998.

[3] Fåk V, Hunstad A. Teaching security basics: the importance of when and how. In: Dougall E G (ed.) *Computer Security*. North-Holland: Elsevier Science, 1993.

[4] Furnell S M, Gaunt P N, Holben R F *et al*. Assessing staff attitudes towards information security in a European healthcare establishment. *Medical Informatics* 1996; 21 (2): 105-12.

[5] The SEISMED Consortium. *Data security for healthcare*, Vols. 1–3. *Studies in Health Technology and Informatics* series, Vols. 31–33. Amsterdam: IOS Press, 1996.

[6] CRAMM. The CRAMM User Guide, Issue 1.0 April 1996. CRAMM Software 3.0, The CRAMM Manager, PO Box 1028, London N1 1UX.

[7] CEN. Medical Informatics – Security categorisation and protection for healthcare information systems, TC251 WG6 [PT012] prENV 12924, CEN, Brussels, June 1997.

[8] IBAG. The IBAG Framework for Commercial IT Security, version 2. INFOSEC Business Advisory Group, European Commission INFOSEC Programme, September 1993.

[9] British Standards Institute. Code of Practice for Information Security Management, BS7799. London: British Standards Institute, 1995.

[10] Barber B and Davey J. Risk analysis in healthcare establishments. In: Barber B *et al*. (eds). *Towards security in medical telematics*. Amsterdam: IOS Press, 1995.

[11] Davey J, King S. Guidelines on IT security risk analysis. In: The SEISMED Consortium (eds). *Data security for healthcare*, Vol. 2. *Studies in Health Technology and Informatics*, Vol. 32. Amsterdam: IOS Press, 1995.