32

ODESSA
A new approach to healthcare risk analysis

by [1]M.J.Warren, [2]S.M.Furnell and [2]P.W.Sanders

*[1]Business Security Group,
Plymouth Business School*

*[2]Network Research Group,
Faculty of Technology,*

*University of Plymouth,
Plymouth, UK
Email: matw@pbs.plym.ac.uk*

Abstract

The paper describes the development of a new security risk analysis methodology that can be used to determine the security requirements of organisations. The methodology has been developed for use within healthcare. but because of the generic nature of ODESSA it can be used to determine the security requirement of many types of organisation.

The paper describes the problems with existing automated risk analysis systems and how the ODESSA system can overcome the majority of these problems. The paper also presents example security scenarios.

Keywords

Security Risk Analysis. Baseline Security, Healthcare Security.

1. INTRODUCTION

The use of information technology (IT) has become more widespread in areas of business and society. and computers have now diversified into many types of applications. As a result, IT systems are used by all levels of staff within organisations. and relied upon greatly to such an extent that it would be difficult to operate without them.

The aim of risk analysis is to eliminate or reduce risks and vulnerabilities that affect the overall operation of these computer systems. Risk analysis not only looks at hardware and software, but also covers other areas such as physical security, human security, business and disaster protection.

In practice there are major problems with the use of risk analysis; the time taken to carry out a review, the cost of hiring consultants and/or training staff. To overcome these negative aspects a new methodology and operational system has been developed. This paper proposes a methodology that is able to simplify the identification of security requirements for individual systems, and to provide a means by which a system administrator or security officer can select the appropriate security countermeasures for their own system. The methodology also describes the impact that the implementation of security could have upon the organisation.

2. THE NEED FOR RISK ANALYSIS IN HEALTHCARE

Within the UK, National Health Service (NHS) there is a general lack of security awareness and security expertise, even though very sensitive and personal data is kept on computers and is communicated between computers. Medical computer security is primarily concerned with:

<u>Confidentiality</u>
Ensuring that unauthorised people (including staff) do not have access to the sensitive and/or personal healthcare data.

<u>Integrity</u>
Ensuring that the data produced by and used within a healthcare system can be trusted as being accurate and complete.

<u>Availability</u>
Ensuring that the computer systems are able to provide the necessary clinical data when and where it is needed.

From a medical point of view [1] perhaps the most important security problems are concerned with:

<u>Physical security</u>
The open nature of hospitals and clinics make them vulnerable to theft, damage and unauthorised access.

<u>Risk to the patient</u>
The failure of a healthcare computer system could affect the treatment given to patients with perhaps dire consequences.

<u>Confidentiality</u>
Medical data contains information that may be extremely sensitive to an individual, i.e. the person may be mentally ill or have the HIV virus. Disclosure of this information could be embarrassing for the individual in the extreme and could result in them being ostracised by society. Also any disclosure could destroy the trust between the clinician and the patient and possibly result in legal action being taken against the clinician or the health care organisation.

<u>Data retention</u>
Within some countries there is a legal requirement to retain healthcare data for a minimum period of many years. This raises problems concerning the long term storage of data, especially when it is converted between old and new systems, which could affect the integrity of the information.

Previous research resulted in a new medical risk analysis method being developed. The method is aimed at the enhancement of security in existing healthcare systems, with a key concept of the methodology being the use of security profiles. For example, using the assumption that a PC network system would require similar security countermeasures to be installed in similar environments. The method has been extended to develop a more generic methodology that can be used within most organisations, the major differences being the types of profile, types of data and organisational details. This generic system ODESSA (Organisational DEScriptive Security Analysis) [2], is being evaluated initially in the healthcare field to help overcome the lack of security awareness and act as a low-cost source of security expertise.

3. THE THEORY OF ODESSA

The rationale of ODESSA is that at a basic level, organisations will have similar security requirements, but beyond this basic level the security countermeasures are unique to each organisation.

Within ODESSA security is examined from the context of the whole organisation, with all factors that influence the organisation being considered, which may range from the location and age of buildings, to the sensitivity and type of data.

These elements have been incorporated into a framework as shown in figure 1. This illustrates the steps involved (at a theoretical level) in determining the security requirements for an organisation.

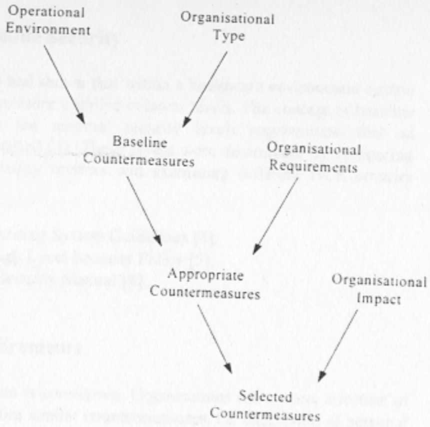

Figure 1. ODESSA methodology overview

The ODESSA system suggests three sets of security countermeasures.

- *Baseline Countermeasures*
These represent the minimally acceptable security countermeasures for any organisational type.

- *Appropriate Countermeasures*
These represent the unique organisational security countermeasures. They are based upon a series of questions from which data sensitivity profiles are formed.

- *Selected Countermeasures*
These represent the selected countermeasures from 1) and 2) that have been applied against the SIM-ETHICS (see 3.5) impact criteria and then accepted by the user.

The main elements of the methodology are now considered in more detail:

3.1 Organisational Environment

This considers the environment in which the organisation's assets are located, which may affect the level of protection required. Table 1 gives examples of environmental considerations that have to be considered for a medical environment.

Table 1. Organisational Environments

Type	*Options* .	*Comments*
Location	Inner City	Location may indicate risk of vandalism theft.
	Urban	Location may indicate risk of theft.
	Rural	Location may be many miles from emergency services. i.e. fire station.
Old / Modern		Age of building may indicate risk of fire disasters, etc.

3.2 Organisational Type

This relates to the different organisational types that exist within a business sector. The baseline security countermeasures are tailored to these different organisations. The research included a comparison of past healthcare security reviews, which helped to form the baseline security needs for the different types as shown in table 2.

Table 2. HCE Organisational Types

Type	*Description*
GP (Single)	A single doctor working among the community, location of surgery is within the community, i.e. in converted house.
GP (Practice)	A group of doctors working in the community, location of surgery is within the community, i.e. purpose built surgery, large converted house.
Community	Units used for specialist patient health care , i.e. speech therapists. Community units are based within the community, within a variety of different sites.
Hospital	Units used for the direct treatment of patients, i.e. specialised surgery, general surgery, radiotherapy, etc. These organisational types tend to be in very large units and based in one location or a variety of different sites.

3.3 Organisational Baseline Security

Previous research undertaken had shown that within a healthcare environment certain HCE's had the same countermeasure installed at lower levels. The concept of baseline within ODESSA relates to the minimal security levels requirements that an organisation should have installed [3]. These levels were determined by comparing results of different HCE security reviews and examining different HCE security guidelines:

- SEISMED Existing System Guidelines [4];
- SEISMED High Level Security Policy [5];
- NHS IM&T Security Manual [6];
- BS7799 [7].

3.4 Organisational Requirements

At this stage the use of the data is considered. Organisations use a cross selection of similar data types, which require similar countermeasures, i.e. encryption of personal data. The ODESSA system uses a set of HCE generic data types [8], as described below:

Table 3. HCE's generic data usage types

Data Use	*Description*
Patient identification	General information relating to patients.
Patient administration	Information used in patient day-to-day scheduling of non-clinical activities.
Patient care	Contains medical history, diagnosis care decisions and treatment information relating to patients.
Clinical services	Information used for planning of clinical services (not patient related).
Finance	Information relating to all aspects of finance that are involved in the operations of HCE.
Staff	Personal information relating to HCE staff.
Resource management	Information used in the management, monitoring and planning of HCEs.
Library and information	Details of existing medical knowledge that is used by clinical staff systems.
Expert Systems	Information used by decision support systems or neural networks used within the HCE.

Once the type of data has been decided, it's sensitivity has to be defined. The sensitivity impacts of the data are:

- **Denial** Denial of access to the information for different time periods.
- **Destruction** Destruction of the information.
- **Disclosure** Unauthorised disclosure of information.
- **Modification** Accidental or deliberate alteration of data.

The data impacts are determined as percentages, and rated as being low, medium or high, (low is equal to baseline security, and high the maximum protection that is offered). The sensitivity values and data types are determined from a series of questions to the appropriate staff of the organisation, which then are used to produce a security profile of the organisation under review. Figure 2, shows the steps involved in determining the organisational requirement.

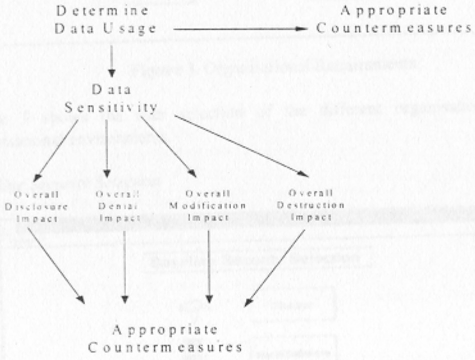
Determine Data Usage
Appropriate Countermeasures
Data Sensitivity
Overall Disclosure Impact
Overall Denial Impact
Overall Modification Impact
Overall Destruction Impact
Appropriate Countermeasures

Figure 2. Organisational Requirement

The stages involved are:

Stage 1) Determine Data Usage
The user of the system picks the data types that the organisation uses, which are associated with certain countermeasures, i.e. levels of access, encryption.

Stage 2) Data Sensitivity
The user answers a series of security related questions. The replies determine the overall impact of disclosure, denial, modification and destruction. The countermeasures are generated from the answers and the overall levels of impact.

3.5 Organisational Impact

Any security countermeasure that is being implemented will effect the organisation as a whole. The impact is determined from a set of impact criteria that has been used as part of a change control methodology, SIM-ETHICS [9] (Security Implementation Method - Effective Technical and Human Implementation of Computer-based Systems).

The use of this criteria allows management to determine the impact of introducing security. It relates to:

Ease of Implementation
How easy can new security features be added to a system and/or new security procedures added to an organisation?

Training Issues
What are the training requirements needed by the staff to use new security features?

User Impact
What is the impact that security could have upon users, i.e. how does it affect user satisfaction, efficiency or effectiveness?

Organisational Impact
What will be the effect that security features could have upon the organisation, i.e. changing of the organisational culture?

Human Issues
What is the impact that security has upon a user from the human perspective, i.e. changes of peoples jobs, creating new management roles?

4. IMPLEMENTATION OF ODESSA

The ODESSA system has been initially developed as a prototype using Visual Basic and Access and is developed to work on PC machines. Visual Basic was chosen because it offered the quickest and easiest way to create the ODESSA prototype. Visual Basic allows a system to be developed that incorporates an easy to use graphical user interface (GUI) and on-line help facilities. The prototype system contains all the features of the methodology. Some of the features of the ODESSA system are described below:

Organisation Selection

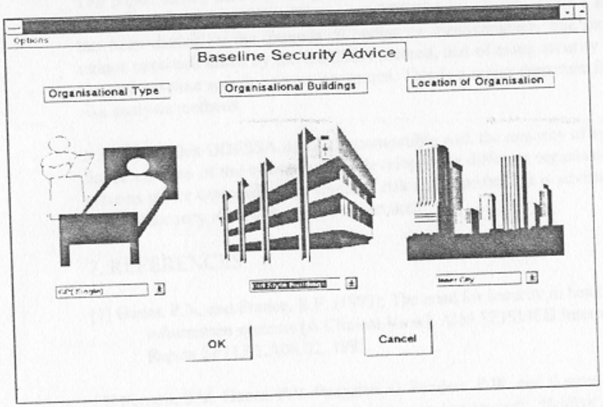

Figure 3. Organisational Requirements

Figure 3 shows the user selection of the different organisational types and organisational environments.

Baseline Security Selection

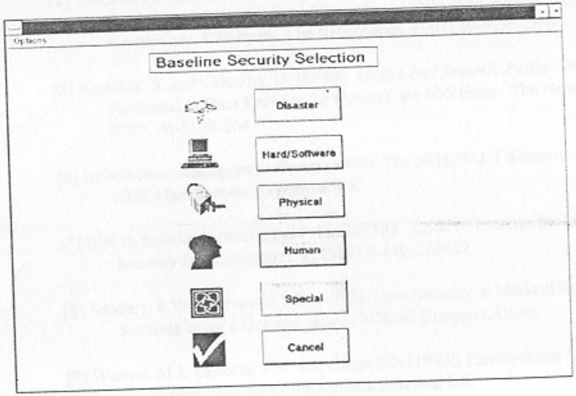

Figure 4. Countermeasure Groups

Figure 4 shows the selection option for Organisational Baseline Security. The security groups are broken down into several groups according to the aspect of protection being addressed (namely *Disaster, Hardware/Software, Physical, Human and Special*).

Organisational Impact

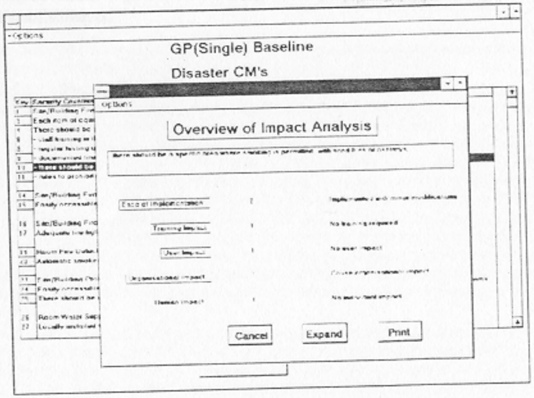

Figure 5. SIM-ETHICS analysis of countermeasure

Figure 5 shows an example of the SIM-ETHICS criteria being used in order to evaluate the selected security countermeasures.

Evaluation

The ODESSA methodology was evaluated by members of the AIM SEISMED consortium during its development. Once the prototype was developed it was sent to various healthcare security experts in order for them to evaluate the prototype. All of the results were very positive.

The SIM-ETHICS method was evaluated by a top UK soft systems expert and was also validated by using it within a HCE to help introduce security systems.

Future Development

At the moment the ODESSA system is just a prototype. The next stage is to develop it into a full system. A business prototype of ODESSA has also been developed.

6. CONCLUSION

The paper shows how by using ODESSA, the process of security reviews within healthcare can be simplified. The use of ODESSA is valuable where a security review has been denied on the grounds of budget or inconvenience. The paper shows the unique approach taken by the ODESSA method, that of using security profiling, data use and baseline security countermeasures. This is a major departure from traditional risk analysis methods.

It is the aim that ODESSA should be compatible with the majority of systems and that future versions of the system will be developed for different organisational types. In systems where extremely high levels of risk are identified, it is advisable that a more detailed security review should be undertaken.

7. REFERENCES

[1] Gaunt, P.N. and France, R.F. (1993), The need for security in health care information systems [A Clinical View], AIM SEISMED Internal Project Report SP11.02.A08.02, 1993.

[2] Furnell, S.M. Gaunt, P.N. Pangalos, G. Sanders, P.W. and Warren, M.J. (1994), A generic methodology for health care data security, *Medical Informatics*, **Vol 19, No 3**, 229 - 245, UK.

[3] Information Management Group (1992), Basic Information Systems Security, NHS Management Executive, UK.

[4] Sanders, P.W, Furnell, S.M. and Warren, M.J (1996), *Baseline Security Guidelines for Health Care Management*, Published in Data Security for Health Care, IOS Press, The Netherlands, ISBN 90-5199-264-5.

[5] Katsikas, S. and Gritzalis, D. (1996), *High Level Security Policy Guidelines*, Published in Data Security for Health Care IOS Press . The Netherlands, ISBN 90-5199-264-5

[6] Information Management Group (1996), The NHS IM&T Security Manual, NHS Management Executive, UK.

[7] British Standards Institute (1995), BS7799 - Code of Practice for Information Security Management, UK, ISBN 0-580-236420.

[8] Sanders, P.W and Furnell S.M (1993), Data Security in Medical Information Systems using a Generic Model, MIE 93 Congress, Israel.

[9] Warren, M.J, Sanders, P.W and Gaunt P.N (1995), Participional Management and the Implementation of Multimedia Systems, UK.