1996

A Security Advisory System for Healthcare Environments

Warren, Matthew John

http://hdl.handle.net/10026.1/1833

A Security Advisory System for

Healthcare Environments

by

Matthew John Warren
BA (Hons)

A thesis submitted to the University of Plymouth
in partial fulfilment for the degree of

DOCTOR OF PHILOSOPHY

School of Electronic, Communication and Electrical Engineering
Faculty of Technology

In collaboration with
Plymouth and Torbay Health Authority

January 1996

To Shona

A red, red Rose

O my Luve's like a red, red, rose
That's newly sprung in June.
O my Luve's like the melodie
That's sweetly play'd in tune.

As fair art thou, my bonnie lass,
So deep in luve am I;
And I will love thee still, my Dear,
Till a' the seas gang dry.

Till a' the seas gang dry, my Dear,
And the rocks melt wi' the sun:
I will love thee still, my Dear,
While the sands o' life shall run:

And fare thee weel, my only Luve!
And fare thee weel, a while!
And I will come again, my Lurve,
Tho' it were ten thousand mile!

(R.Burns 1759-96)

A Security Advisory System for Healthcare Environments

Matthew John Warren
BA (Hons)

This thesis considers the current requirements for security in European healthcare establishments. Information Technology is being used increasingly by all areas of healthcare, from administration to clinical treatment and this has resulted in increased dependence upon computer systems by healthcare staff.

The thesis looks at healthcare security requirements from the European perspective. An aim of the research was to develop security guidelines that could be used by healthcare establishments to implement a common baseline standard for security. These guidelines represent work submitted to the Commission of European Communities SEISMED (Secure Environment for Information Systems in Medicine) project, with which the research programme was closely linked. The guidelines were validated by implementing them with the Plymouth and Torbay Health Trust.

The thesis also describes the development of a new management methodology and this was developed to allow the smooth implementation of security within healthcare establishments. The methodology was validated by actually using it within the Plymouth and Torbay Health Authority to implement security countermeasures.

A major area of the research was looking at the use of risk analysis and reviewing all the known risk analysis methodologies. The use of risk analysis within healthcare was also considered and the main risk analysis methods used by UK healthcare establishments were reviewed.

The thesis explains why there is a need for a risk analysis method specially developed for healthcare. As part of the research a new risk analysis method was developed, this allows healthcare establishments to determine their own security requirements. The method was also combined with the new management methodology that would determine any implementional problems. The risk analysis methodology was developed into a computerised prototype, which demonstrated the different stages of the methodology.

Contents

Chapter 4   Development of the SIM-ETHICS method

Chapter 5   Critical Review of Risk Analysis

Chapter 6   Development of the ODESSA methodology

Chapter 7   Development of the ODESSA Prototype system

Chapter 8   Validation of Research

Chapter 9   Conclusions

List of Figures

List of Tables

Acknowledgements

I would like to express my sincere thanks to the following people:

- Peter Sanders, my Director of Studies, for his encouragement and support and for his confidence in my abilities;

- Dr Nick Gaunt, of Plymouth and Torbay Health Authority and the Department of Healthcare Informatics at Derriford Hospital, who provided valuable help and input into the research programme.

I wish to thank my Dad and Shona Leitch who have both inspired and supported me.

I would also like to acknowledge the assistance of various members of the SEISMED consortium and members of the Network Research Group who all gave help and support.
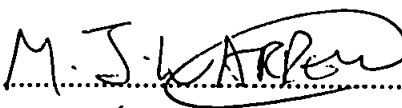
I wish also to thank Mr Wahlgren of Stockholm University and Mr John Davey for their assistance.

DECLARATION

At no time during the registration for the degree of Doctor of Philosophy has the author been registered for any other University award.

The study was financed with funding form the Commission of European Communities SEISMED project and was carried out in collaboration with the Plymouth and Torbay Health Trust.

Relevant conferences and SEISMED project meetings were regularly attended (at which work was frequently presented) and a number of external establishments were visited for consultation purposes. In addition, several papers were prepared for publication, details of which are listed in the appendices.

Signed ...... M. J. WARREN ......

Date ...... 12/3/96 ......

GLOSSARY OF ABBREVIATIONS

AIM   Advanced Informatics in Medicine

CCTA   Central Computer and Telecommunications Agency

CCTV   Close Circuit Television

CESG   Communications Electronic Security Group

CM   Countermeasure

COMECON   Council of Mutual ECONomic co-operation

CRAMM   CCTA Risk Analysis Management Methodology

DTI   Department of Trade and Industry

EFTA   European Free Trade Association

ESP   Existing Security Principles

EU   European Union

GP   General Practitioner

HCE   Healthcare Establishment

HLSP   High Level Security Policy

IBM   International Business Machines

ISHTAR   Implementing Secure Healthcare Telematics in euRope

IMG   Information Management Group

IT   Information Technology

MB   Mega Byte

MS-DOS   Microsoft Disk Operating System

NHS	National Health Service
ODESSA	Organisational DEScriptive Security Analysis
OLE	Object Linked Embedding
PC	Personal Computer (IBM compatible)
RAM	Random Access Memory
R+D	Research and Development
SEISMED	Secure Environment for Information Systems in Medicine
SIM-ETHICS	Security Implementation Method - Effective Technical and Human Implementations of Computer based Systems
VTX	Video TeXT system
WWW	World Wide Web

Chapter 1: Introduction

1.1) Introduction

During the last few decades the use of Information Technology (IT) has become more extensive throughout society (Poppel and Goldstein, 1987). There are few people today which have no contact with computer systems in modern life, whether from personal banking to buying lottery tickets. The future use of the 'Internet' for business and leisure will truly allow the globalisation of IT systems.

The advancement of IT has also resulted in an advancement of reliability of computer systems. This advancement has resulted in more trust being placed in IT systems (Barber and Davey, 1994) and an increased reliance upon computer systems in a majority of commercial sectors, i.e. banking, healthcare and within society as a whole. These computer systems handle the processing of very sensitive and confidential information which affect the lives of people. Society seems poised to tolerate greater reliance on computer system as IT restructures peoples role at work and at home and helps to improve their quality of life (Poppel and Goldstein, 1987).

The use of IT within the healthcare sector has developed at the same pace as other commercial sectors and IT systems are now in widespread use. However, healthcare information is of a very personal nature sometimes concerning very sensitive details and it is therefore of the utmost importance to protect this data. Healthcare security is primarily concerned with the following issues.

<u>Confidentiality</u>

Ensuring that unauthorised persons (including staff) do not have access to

sensitive data or personal data.

<u>Integrity</u>

Ensuring that the data produced by and used within a healthcare system can be

trusted as being accurate.

<u>Availability</u>

Ensuring that the computer systems are able to provide the necessary data

when and where it is needed.

All computer systems are at risk of their security being compromised. These risks are

defined as being (IMG, 1992):

- threats to the system - e.g. fire, theft, unauthorised system access,

system error;

- vulnerabilities of the system to threats - e.g. inadequate control of

access, poor supervision;

- impact on system assets if a threat succeeds -e.g. destruction or corruption of

data.

From a clinical point of view the most important healthcare security problems have been identified as described below (Gaunt and France, 1993).

Physical security

The open nature of hospitals and clinics make them vulnerable to theft, damage and unauthorised access.

Risk to the patient

The failure of a healthcare computer system could affect the treatment given to patients, with potentially dire results.

Confidentiality

Medical data contains information that may be extremely sensitive to an individual, i.e. the person may be mentally ill or have HIV. 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 either the clinician or the health care organisation.

The consequence of security breaches vary enormously between sectors, systems and the use of those systems. Various consequences may result from security breaches, as indicated below:

- financial loss;

- disruption of organisational activities;

- infringement of privacy;

- personal safety;

- failure to meet legal obligations;

- embarrassment or loss of business goodwill.

(Barber and Davey, 1994)

All of the above points suggest a real need for security within the healthcare environment and highlights its complex nature in terms of threats, requirements and consequences.

Information security is primarily concerned with protecting data stored on computer systems, but other factors such as physical security, disaster protection and staff security must also be considered. Information security is also a human issue and is concerned with educating users and making them aware of the issues (Warren and Gaunt, 1993).

The European Union (EU) believes that fragmented national approaches to IT research and development (R&D) results in duplicated efforts and do not allow for cross-fertilisation (Poppel and Goldstein, 1987). This perception, combined with the need for European IT Standards, has resulted in the development of extensive European IT research programmes (including countries from EU, EFTA (European Free Trade Association) and former COMECON (Council of Mutual ECONomic co-operation) countries). The increased concern about computer security has resulted in several research and development programmes specifically looking at the area of HCE security, such as SEISMED (Secure Environment for Information Systems in MEDicine) (SEISMED, 1994). It has been recognised that the production of European-wide security standards and guidelines will help address the HCE security problems currently present, as well as ensuring that security levels are standardised across the whole of the EU.

A key issue within the EU is how to transfer knowledge about security to the HCE staff and educate users about computer security. This forms the basis of a new EU project called ISHTAR (Implementing Secure Healthcare Telematics Applications in euRope), which aims to increase computer security awareness in HCEs.

A overview of information security and the issues affecting HCE organisations is presented in chapter 2.

1.2) Aims and Objectives of Research

This research is concerned with the issues of implementing security within HCEs and

providing security knowledge within computerised systems. The research

demonstrates the importance of proving security knowledge to HCE staff and

establishing security standards within the EU.

The overall research program can be divided into the following areas:

1. developing security guidelines, then validating these

guidelines with HCEs acting as validation centres;

2. developing a method for the implementation of security with an HCE;

3. developing a risk analysis method to enable HCEs to carry out their own

security reviews.

A principal objective of the first phase was the validation of security guidelines. This

involved working extensively with the staff of the Plymouth and Torbay Health

Authority in determining their applicability. The second phase concerned the

validation of the new method (called SIM-ETHICS) to be used for the implementation

of security. The validation process consisted of using the method to help implement

new security measures within the HCE and determining the impact that these would

have upon staff. The main aim of the third stage was the development of a working

prototype, embodying the risk analysis methodology that was developed.

The full objectives of the present research programme can be listed as follows:

1. to assess the general need for information security within various types of

    HCE;

2. to assist in the production and validation of security guidelines which would

    help improve the levels of security that exist within HCEs;

3. to develop and validate a new methodology that could be used in the

    implementation of security within various HCEs;

4. to assess the current use of security risk analysis packages and whether they

    can be applied to healthcare;

5. to develop a new security risk analysis method which allows HCEs

    to determine their own security requirements;

6. to implement the above method into a fully working prototype

    computer system.

The above points are reflected by appropriate chapters of the thesis, which will be discussed in the next section.

The research has involved significant liaison with HCE staff from Plymouth and Torbay Health Authority, Plymouth Community Trust and various General Practitioners (GPs). This liaison has occurred in the context of the AIM SEISMED project, which was concerned within improving healthcare security within HCEs. The research has also involved liaison and correspondence with security experts from the following countries:

- Canada;	- Netherlands;
- Denmark;	- Serbia;
- Eire;	- Slovenia;
- France;	- Sweden;
- Germany;	- UK;
- Greece;	- USA.
- Israel;	

1.3) Thesis Structure

This thesis describes the research that has resulted in the formulation of a complete system that can be used to assist HCE security. The research helps HCEs to determine their organisational security requirements and allows the smooth implementation of security measures within HCEs.

Chapter 2 begins by explaining the need for security within HCEs. The chapter also highlights the steps that can be taken to improve security within HCEs. The AIM SEISMED project is described, as well as the major security guidelines which the project has produced. Finally, the more recent ISHTAR project is described as a way

of enabling the transfer of security knowledge to HCE staff throughout the EU and indeed the rest of the world via the use of the Internet.

Chapter 3 describes the role of security management within HCEs. It includes descriptions of several surveys that have been undertaken at Plymouth and Torbay Health Trust, as part of a study of security awareness of managers and users. The chapter also looks at security culture and the impacts that this has upon management, staff and the HCE establishment as a whole.

Chapter 4 describes the managerial concept of participational management. It explains what it is, the countries where it is used and the experiences that they have had. The future of participational management in general is also discussed. The development of a new method called SIM-ETHICS is considered, which may be used for implementing security. This chapter also includes real life examples of the use of participational management within the Plymouth and Torbay Trust.

Chapter 5 is concerned with security risk analysis. The chapter considers the nature of risk analysis and the different fundamental types followed by an evaluation of various different methods. The use of risk analysis within healthcare is also examined. The chapter ends with a suggestion as to the future of security risk analysis methods.

Chapter 6 then proceeds to present a major area of the research, namely a new risk analysis methodology specifically developed for use within the healthcare environment. It explains the need for a simplified system to be used by HCE staff to

evaluate their security requirements, rather than undertaking extensive risk analysis reviews. The development of the ODESSA (Organisational DEScriptive Security Analysis) methodology is described in detail, as well as the underlying theoretical points. The methodology is based upon the concept of classification of systems and offers baseline security advice for those systems. It also uses techniques such as determination of data sensitivity, organisational profiling to enable specific countermeasures to be offered and incorporates the use of the SIM-ETHICS method (see chapter 4). The perceived advantages and disadvantages of the ODESSA methodology are also described.

Chapter 7 explains how the new methodology was embodied in a working prototype computer system written in Visual Basic. The chapter describes different parts of the system and finally looks at the areas where the prototype could be improved. This serves to increase the potential usefulness of the method and show its applicability for HCEs.

Having described the main areas of research, chapter 8 describes the validation of the research programme. It describes how SIM-ETHICS was validated by using it within the Plymouth and Torbay Health Trust and how ODESSA was validated by experts throughout Europe.

Finally, chapter 9 presents the main conclusions of the research programme, highlighting the principal achievements of the work as well as suggesting areas for potential further investigation.

The thesis also include a number of appendices which contain additional information to support the research, as well as a bibliography of references used for the thesis. Copies of published papers relating to the research undertaken are also appended.

Chapter 2: An overview of security within Healthcare

2.1) Introduction

Healthcare within the EU is important since its affects the entire population. The following summary shown in table 2.1 relates to the state of the EU healthcare system, this was based upon 1990 figures (Acosta, 1994).

Population of EU

344,000,000

Healthcare Workers

Doctors	800,000
Dentists	156,000
Nurses	1,600,000
Other (technicians, administrators, cleaners, etc)	3,860,000

Healthcare Resources

Hospitals	15,000
Beds	2,600,000

Table 2.1. The size of healthcare within the EU

The above figures excludes data relating to Austria, Finland and Sweden which have subsequently joined the EU in 1995. The tables shows the population of the EU, for each person shown a unquantifiable amount of computerised data is kept. The table also shows the extensive number of HCEs and HCE workers within the EU, they also produce extensive quantity of data. There is therefore a unquantifiable amount of information that potentially needs to be protected.

2.2) The need for security within healthcare

The need for security with healthcare has been explained in chapter 1. The sections that follow will now consider two specific areas:

- past problems of security within healthcare;

- steps taken to improve security within healthcare.

2.2.1) Past problems of security within healthcare

Within the UK there has been no detailed study relating to incidents of healthcare security breaches. There have however been attempts to study computer fraud within the UK, notably the Audit commission. In the 1991 report, 327 organisations in the NHS responded to the Audit commission, of these 18 (5%) recorded some form of security incident (Manuel, 1991). In the 1994 report, 334 organisations in the NHS responded, of these 127 (38%) recorded some form of security incident (Audit, 1994). This shows that breaches of computer security within HCEs is on the increase.

In France there have been studies of healthcare security undertaken by insurance companies breaches These studies provide a comprehensive review of healthcare security breaches that have occurred in France, as shown below (APASAIRD and CLUSIF, 1988).

• Hardware (accidents, breakdowns, vandalism)

Twelve day breakdown of a minicomputer managing beds in a ward caused errors, over and under allocation for two months. Loss of profit and adverse publicity was valued at £400,000.

Explosion of a minicomputer used for the control and analysis of an imaging system caused by the indirect spread of lightning into a comms link joining the machine to another for access to a database. Hardware loss was put at £200,000 and consequential losses at £300,000.

A series of acts of vandalism and thefts perpetrated on small items of specialised and vital hardware amounted to £80,000.

- Fraud

Creation of false invoices in a hospital by an employee who has noticed that the access key to an application was the date. The employee obtained money from the so-called suppliers who disappeared after a year. The embezzlement was in the region of £150,000.

Fraudulent use of a utility to change fields in a file containing allocations of invitations to tender. The total loss was £200,000.

- Theft of Goods

Modification of dosage tables for certain patients taking opiate derivatives and also of tables of anaesthetic dosages. Over a year the value of drugs stolen amounted to £100,000.

- Sabotage of Programs and Data

£50,000 blackmail relating to a logic bomb on a system essentially dedicated to physical security control/monitoring, the management of alarm calls and liquid food in a hospital.

- System Development Errors

During migration from one system to another, certain buffer areas were truncated. When programs dealing with medical analysis were run, incorrect results were obtained and the consequences, although not measurable, were very serious.

- Operating Errors

Disks left on top of a laser printer in a computer room were damaged. The disks were very difficult to read and it was necessary to reinput large volumes of data. Supplementary costs came to £200,000.

- Personnel Problems

After the departure of the person running a small data centre in a hospital, the state of the documentation did not allow him to be satisfactorily replaced (there were only three people in the department). The main functions has to be moved to another centre. Adapting to the change took six months and cost £600,000.

Within the National Health Services (NHS) there are concerns about future IT projects, there is growing concern about the NHS network that is being implemented

and its minimal security features (Sunday Times, 1995). In 1992 the Department of Health decided that data encryption was not necessary because the risk of hacking was minimal (Davies, 1995). Because of this stance the British Medical Association (BMA) is urging the government to make breaching confidential health information a statutory offence (Milton, 1995).

2.3) Steps taken to address the problems of security within healthcare

Steps are being taken to address the problems of security at a local, national and a European level.

At the local level steps are being taken to address the problems of physical security. The Royal Devon and Exeter Healthcare NHS Trust is paying Devon and Cornwall police £60,000 a year for round-the-clock protection (Guardian, 1995). This protection takes the form of two police officers being permanently based at a Exeter hospital.

Within the UK, the Information Management Group (IMG), part of the NHS Management Executive, are addressing this problem. As part of this initiative they have developed a Security Policy for use by the NHS. Some of the issues put forward by the policy are governed by legislation and steps must be take to ensure compliance (IMG, 1992). The most notable UK acts are:

- the Data Protection Act, 1984;

- the Copyright, Designs and Patents Act, 1988;

- the Computer Misuse Act, 1990.

The IMG run a series of training seminars for NHS staff looking at the various IT security and data protection issues. It has also produced documentation relating to IT security, which can be distributed to all NHS staff.

At the European Level, the Advanced Informatics In Medicine (AIM) research programme is concerned with applying information and communication technologies to medicine and healthcare. The exploratory phase of AIM lasted from 1989 to 1990, with 20 million ECU funding from the European commission. The main phase was for three years (1992 - 94) with 97 million ECU backing (Rossing, 1994). One of the research and development projects was entitled SEISMED and this was specifically concerned with European HCE IT security.

2.3.1) The Role of SEISMED

The objective aims of the AIM SEISMED project (SEISMED, 1994) were:

- to examine across Europe, the legal issues of data protection within

healthcare IT systems in order to develop a common code of ethics;

- to develop a High Level Security Policy to enable organisations using

information systems to follow a consistent path;

- to perform risk analysis at four healthcare centres to identify the

   opportunities and needs for improved security;

- to develop specific guidelines to enhance security looking at:

   - existing systems;

   - design and implementation of future systems;

   - the use of networks.

- to develop an encryption prototype for use by HCEs.

The partners for the SEISMED project came from Czech Republic, Belgium, France,

Germany, Greece, Ireland, Netherlands, Switzerland and the UK, as shown in figure

2.1.

Key

BE = Belgium
CR = Czech Republic
GR = Greece
HO = Holland
UK = United Kingdom
SW = Switzerland
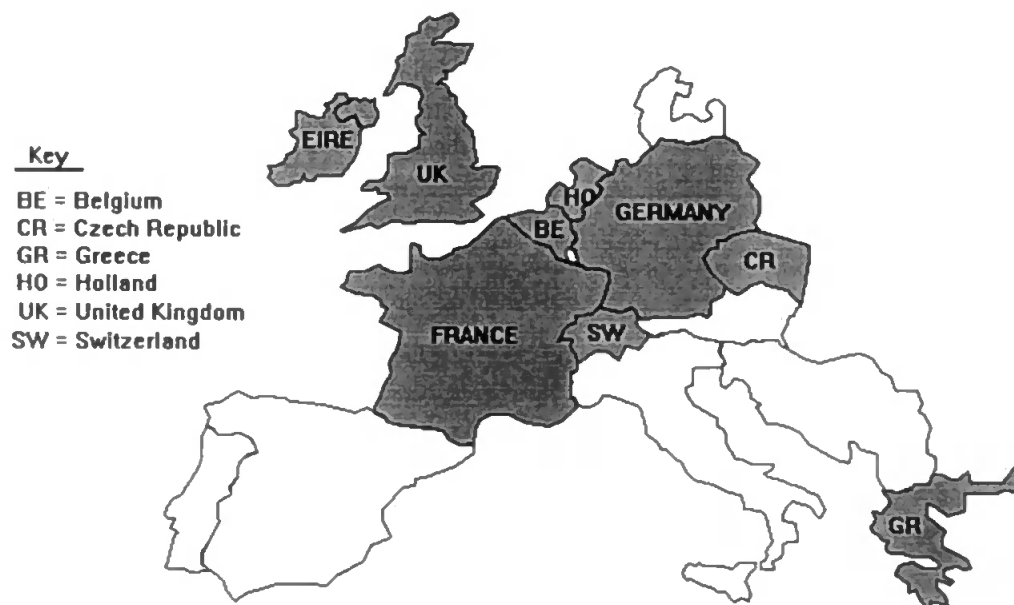
Figure 2.1.The countries involved in the SEISMED Project.

There were five reference centres within the project, which provided medical knowledge and allowed for the validation of the research. These reference centres were:

- Plymouth and Torbay NHS Trust (UK);

- The Royal London Hospital NHS Trust (UK);

- Leiden University Hospital (The Netherlands);

- GEN Hospital Cantonal Universitaire de Genenve (Switzerland);

- Institute for Clinical and Experimental Medicine (Czech Republic).

A major aspect of the project was the development of security guidelines. These guidelines allow a harmonised approach to be taken to security through the EU and provide the same level of protection. Two of the most important guidelines produced by the project were:

- the High Level Security Policy;

- the Existing Systems guidelines.

The author was personally involved in developing the existing system guidelines. The author was also involved in validating the above guidelines within the Plymouth and Torbay NHS Trust.

2.3.3.1) The High Level Security Policy

The High Level Security Policy (HLSP) is a policy that a HCE should use in order to implement security efficiently and indicating to management how a HCE should be run (Katsikas and Gritzalis, 1993). The HLSP aims at protecting human rights of patients, ensuring the confidentiality and quality of personal health data (Katsikas and Gritzalis, 1994).

The HLSP for SEISMED was developed by:

- an attitude survey of healthcare professionals in Europe;

- results of risk analysis reviews carried out at reference centres;

- the results of the analysis of existing and emerging data protection legislation throughout Europe;

- relevant international literature, i.e. US Department of Health Automated Information Systems Security Program Handbook.

The SEISMED HLSP consists of a set of nine principles, with each principle further detailed by a set of guidelines. The principles of the HLSP are shown in table 2.2:

Code	Principle
P100	Code of good Practice
P200	Contractual Regulations
P300	Data Protection Authority
P400	Education - Awareness
P500	Limited data circulation
P600	Patient Rights
P700	Quality of health data
P800	Medical research
P900	Security regulations

Table 2.2. HLSP Principles

The development of the HLSP was helpful to form the basis of a consistent, harmonised and transferable framework which can be used to efficiently implement security and privacy in automated Health Information Systems throughout Europe (Katsikas and Gritzalis, 1993). The HLSP does not suggest security guidelines but rather a set of mandatory conditions to ensure adequate security of information processed by HCEs.

2.3.3.2) Existing System Guidelines

The problem of securing existing systems was also addressed by the SEISMED Project. Whilst various guidelines and standards for IT security have previously been developed, none have specifically targeted the needs of the medical community at a European level. The new guidelines are intended to provide a common source of reference for European healthcare establishments and are relevant to (and will affect) all categories of personnel.

The existing system recommendations were developed to satisfy the following aims:

- to represent a minimum acceptable standard for the security of operational

healthcare systems and their associated environments;

- to be usable by all HCEs and staff within Europe;

-to allow a straightforward means of validating existing systems security to

ensure compliance.

The development of the resulting guidelines was based upon an interactive approach, in close co-operation with the SEISMED Reference Centres and in consultation with other independent healthcare professionals.

2.3.3.3.1) An Overview of Existing Systems Guidelines

The final Security Guidelines for Existing Healthcare Systems (Furnell and Sanders, 1994) are grouped under 10 key principles of protection, representing the main elements governing the security of existing healthcare information systems (having been agreed in detail with the Reference Centres). The principles are denoted by ESP followed by a unique reference code, as listed in table 2.3:

Code	Title
ESP0100	Security Policy and Administration
ESP0200	Physical and Environmental Security
ESP0300	Disaster Planning and Recovery
ESP0400	Personnel Security
ESP0500	Training and Awareness
ESP0600	Information Technology Facilities Management
ESP0700	Authentication and Access Control
ESP0800	Database Security
ESP0900	System Maintenance
ESP1000	Legislation Compliance

Table 2.3. Existing Systems Security Principles

Each of the principles has a number of associated guidelines. These represent the specific security concepts or countermeasures that should be considered by the HCE to meet the requirements of a given principle. As established earlier, the consideration

of existing systems encompasses a very broad range of issues and the overall coverage consequently extends from general concepts to specific technical measures.

The 10 protection principles are described in more detail below (Furnell et al., 1995). In each case the general purpose of the principle is stated, along with a list of the main issues that are covered by the underlying guidelines (the overall number of guidelines pertaining to each principle is given alongside its title).

1. **Security Policy and Administration** (5 guidelines)

   General Principle

   A formal policy will provide clear direction and support for security within the HCE. Policy is formulated from the senior managerial level, with subsequent guidance provided to all levels of staff. Correct administration of and adherence to the policy should ensure the effectiveness of HCE security controls.

   Main issues :

   - the need for a security policy;

   - policy awareness issues;

   - co-ordination and administration of security;

   - use of specialist security personnel.

2. **Physical and Environmental Security** (22 guidelines)

General Principle

The generally open nature of HCEs and their high degree of public access dictates that physical security measures are a vital first stage of protection to prevent unauthorised access to computing equipment and facilities. Systems must also be safeguarded against a variety of environmental hazards that may adversely affect operation.

Main issues :

- physical access control;

- security of HCE equipment;

- protection against natural disasters;

- environmental controls;

- various procedural measures.

3. **Disaster Planning and Recovery** (7 guidelines)

General Principle

The continuous availability of Information Systems is essential to the operation of a modern HCE. It is essential that adequate plans are made to ensure the level of availability needed by the HCE can be maintained in the event of any catastrophe. Recovery of IT systems should be a component of an overall HCE disaster / recovery plan.

Main issues :

- continuity planning (development, testing and update);

- fallback arrangements;

- post-disaster procedures and controls.

4. Personnel Security (8 guidelines)

General Principle

The major security weakness of many systems is not the technology but the people involved. Many organisations are extremely vulnerable to threats from their own staff and, as a result, even the most comprehensive technical controls will not guarantee absolute security. There are, however, a number of personnel-related measures that can be introduced to help reduce the risks.

Main issues :

- staff recruitment;

- contractual agreements promoting security;

- security during normal working practices;

- staff appraisal and monitoring;

- termination of employment.

5. Training and Awareness (6 guidelines)

General Principle

Information systems security can only be maintained if all personnel involved in their use 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.

Main issues :

- the need for general security awareness;

- specific areas that must be addressed (job training, use of information

systems);

- recommendations for internal / HCE training and awareness initiatives;

- use of specialist training courses;

- assignment of responsibilities for training.

6. Information Technology Facilities Management (31 guidelines)

General Principle

A variety of activities can be identified that are related to the normal day-to-day use and administration of information systems. All categories of HCE personnel (management, technical and general users) have responsibilities that must be addressed in order to maintain security in this area.

Main issues :

- system planning and control;

- the importance of maintaining back-ups;

- media controls;

- auditing and system monitoring;

- virus controls;

- documentation issues.

7. **Authentication and Access Control** (28 guidelines)

General Principle

It is essential that IT systems are protected by comprehensive logical access controls. Access should be guaranteed for legitimate users and denied to all others. All classes of user must be identified and authenticated before any access is granted and further mechanisms must control subsequent reading, writing, modification and deletion of applications and data. There should be no method for by-passing any authentication or access controls. HCE users are unlikely to be satisfied with controls that intrude upon working practices and chosen schemes should be transparent and convenient in order to gain acceptance.

Main issues :

- requirements for user identification and authentication;

- password issues;

- system and object access restrictions;

- methods of control;

- access in special cases (e.g. system management, third parties, temporary

staff).

8. **Database Security** (21 guidelines)

General Principle

Database security is concerned with the enforcement of the security policy concerning the disclosure, modification or destruction of a database system's data. Databases are fast becoming very important for HCEs. Over 90% of today's IT systems contain some kind of database and the value of information stored is now widely recognised as a major asset, far more important than any other software. However, databases also introduce additional security concerns (e.g. granularity, inference, aggregation, filtering, journaling etc.) and therefore warrant specific consideration.

Main issues :

- control of medical database software;

- organisation and administration of HCE database systems;

- database operation issues.

9. **System Maintenance** (5 guidelines)

General Principle

System maintenance activities merit special consideration given the opportunities that exist to affect the operation of the system. Unauthorised or uncontrolled changes to any aspect of an operational system could potentially compromise security and, in some cases, endanger life. Maintenance must therefore be carried out in accordance with well-defined procedures.

Main issues :

   - controls to prevent unauthorised changes to and upgrades of HCE software,

      vendor software and operating systems;

   - requirements for testing and acceptance.

10. Legislation Compliance (5 guidelines)

General Principle

Specific levels of protection may be demanded in order to comply with national

and European legislative requirements, as well to satisfy internal HCE policy.

Whilst the guidelines highlight the most basic requirements, this principle

represents an ongoing process which must take account of any new legislation

that may be relevant, as well as ensuring compliance with existing standards.

Main issues :

   - data protection;

   - abuse of information systems;

   - prohibition of "pirated" software;

   - compliance with internal security standards;

   - retention and protection of business records.

It should be evident that many of the issues covered are not relevant to all HCE staff.

Therefore the guidelines are broken down into following groups (Furnell, et al, 1995).

• A general guideline set, aimed at the majority of HCE staff, including

clinicians, administrators and general system users. Guidelines are presented

for user reference during day-to-day use of HCE information systems,

highlighting what they can do to safeguard security.

• A management guideline set, primarily targeting the senior decision makers

within the HCE, who will be responsible for defining security policy

(although a significant number of points will also be relevant at department /

line management level). This set is intended to highlight areas in which

management should be directly involved and also improve management

security awareness by explaining / justifying the importance of other more

technical guidelines (for which management approval will be required).

• An IT and security personnel set, aimed at IT staff, system administrators,

security officers and other support staff who will be most likely to have the

lower level responsibilities for implementing security. This is the most

detailed of the guideline subsets and should be a key source of reference for

implementation and validation of security.

2.3.3.3.2) Implementing the Guidelines

The Security Guidelines for Existing Healthcare Systems could be applied in any

European Healthcare Establishment with existing operational information systems

(where the term Healthcare Establishment refers to any establishment providing

medical services, research, training or health education). They will be relevant even where systems are thought to include security provision, so that the level of protection can be validated against the recommendations.

As for the implementation strategy itself, it would obviously be impractical to attempt to address all of the suggestions at once due to constraints of cost and likely disruption to services. A phased approach is, therefore, advised in which each principle is considered in turn to identify the areas in which the HCE / department is currently deficient. The individual guidelines may then be assessed to determine implementation priorities based upon local requirements.

Whilst the new recommendations are intended to provide a simple and straightforward means of addressing healthcare security issues, it is recognised that problems may exist.

Firstly, many establishments may currently be operating with security significantly below the recommended level and progression to the required level may be a non-trivial task. As mentioned in the discussion of implementation, HCEs may face a number of constraints that affect their ability to address security requirements. For example, cost (in terms of finance, performance and practicality) will be a significant factor in determining acceptability (Fagen, 1993). Financial cost will be particularly relevant, given that expenditure for direct care activities is likely to receive higher priority than security.

Conversely, some environments and / or applications may demand a level of security significantly higher than the proposed baseline. In these cases a risk analysis review is recommended in order to determine the level of additional protection that is necessary.

2.2.3) The Role of ISHTAR

As mentioned in previous sections there is a problem ensuring that security information can be properly disseminated to reach the HCE staff that it is intended for. The use of the Internet will allow vast amounts of information to be transferred efficiently and economically effectively.

This objective has formed the basis a forthcoming EU project to be called ISHTAR (Implementing Secure Healthcare Telematics Applications in euRope) which intends to use the WWW as a dissemination mechanism for healthcare security knowledge.

The main aims of ISHTAR are (Furnell et al, 1996):

- to allow on-line access to healthcare security guidelines and related security papers (including SEISMED documents and guidelines);

- to develop an on-line healthcare security discussion forum;

- to act as a repository for automated security demonstrators and security programs, i.e. risk analysis systems;

- to act as a link to other security WWW sites;

- to advertise any healthcare security training seminars or healthcare security

conferences.

The use of the Internet will allow a new dimension in the area of healthcare security and will allow for the globalisation of EU security guidelines (which may help in the development of world-wide security standards).

2.4) Conclusion

In conclusion this chapter has explained the need for security within healthcare, it shows within the UK there has been an increase of computer fraud and misuse within HCEs.

The chapter has shown the steps that are being taken at a local, national and European level to address these security problems through:

- development of security guidelines;

- the use of new technologies to transfer security knowledge.

These new security guidelines form a basis by which a HCE can implement a certain security level. Once this basic security level has been implemented, a risk analysis

can be undertaken by using a new healthcare risk analysis method (see chapter 6).

This will then determine the HCE need for security. By the use of a new management

method (see chapter 4) the organisational impacts of implementing security can also

be determined.

Chapter 3: Overview of Security Management

3.1) Introduction

Security management can be defined as viewing and managing risks in terms of the cause, effects, and therefore costs, of a loss of security (Robson, 1994). From this statement it is clear that organisations need to manage the risk exposure of every IT element and this may be carried out by using risk analysis (see Chapter 5). In 1992 a Department of Trade and Industry (DTI) sponsored survey suggested that the true level of UK losses from computer fraud and misuse is around £1.1 billion a year (Robson, 1994).

There are distinct differences between security management goals in different sectors. In a commercial environment, the aim is to introduce security controls at the most cost effective basis. The aim of military security is to minimise losses, irrespective of the costs associated (Von Solms et al, 1990). The aim of commercial security is to primarily ensure the integrity of data to prevent fraud and errors (Clark and Wilson, 1987).

3.2) The need for security management

Security management is an issue affecting all countries. Of particular importance is computer fraud, usually undertaken by the companies employees (Audit, 1994). The risk from employees is due to:

- staff being familiar with systems;

- staff being familiar with security procedures;

- staff holding a grudge against their employer.

The level of computer fraud and misuse is indicated by the following studies.

United Kingdom (Audit, 1994)

     Total losses to computer misuse   £3,822,213

     Total losses to computer fraud   £3,042,318 (79.5%)

Australia (Kamey and Adams, 1992)

     Total losses to computer misuse   (A$)16,908,029

     Total losses to computer fraud   (A$) 13,660,543 (80.8%)

Security management is primarily concerned with protecting the organisation against outside and inside threats, e.g. hackers or unhappy employees. The main areas for security management can be broken down into:

        - risk assessment (See Chapter 5);

        - implementing security;

        - developing corporate security policies;

        - security awareness and training.

3.2.1) Managing Security

To manage computer security there should be appropriate management duties and responsibility allocated within the whole organisation. Typically, organisations will appoint a single, central IT security manager. In many instances, IT security is combined with responsibilities for other aspects of IT management, and the role may well be part time (Fagen, 1993).

Only a limited amount of research has been conducted in this area, but that which has been done identified the following national characteristics.

Germany

Who is responsible for IT Security ?

Information Manager	78%
Executive Manager	10.5%
Data Security Commissioner	8.5%
Data Protection Commissioner	8%
Security Manager	3%

(Gliss, 1990)

(Note: The data which totals 108% shows that some organisations have more than one person concerned with security).

Slovenia

Is there someone directly responsible for computer security?

No person	23.3%
One Person	31.5%
More than One Person	8.2%
Without Answer	37%

(Hudoklin and Smitek, 1992)

These limited studies suggest that a more structured approach to security management was taken by countries with an already developed use of using IT. This area has to be researched even further to explore more of the national issues.

3.2.2) Implementing Security

Any new technology that is being implemented, including security would cause an organisational impact. The impact would be top down and would affect the organisation as a whole. Security is a human issue and should therefore be considered in the context of the staff and the organisation. It is important to ensure that the introduction of the new security systems and procedures does not hinder the staff (Warren and Gaunt, 1993). Any implementation plan should take into account the life cycle of the security system as described below (Wylder, 1992).

The Introductory Phase

This is when the security features are initially introduced and is important because it establishes the organisational emphasis on security. This stage affects few users.

The Early Growth Phase

This is when security features are added to a limited number of systems, This stage affects some users.

The Rapid Growth Phase

This is when security features are added to all existing systems. This stage consequently affects all the users of the systems.

The Maturity Phase

This is when the system is fully developed, so that post development features will be added, affecting a varying number of users.

The importance in determining the impact of security suggests that some methodology should be used, such as SIM-ETHICS (See Chapter 4).

3.2.3) Developing Corporate Security Policies

A security policy is a statement of belief that the organisation adheres to, and a series of objectives that the organisation strives to comply with. The security policy also states the responsibilities that staff have (directly and indirectly) for organisational security. The assignment of security responsibility is dependent upon the structure of the organisation. The purpose of a computer security policy has been defined as follows.

> A computer security policy serves as a vehicle to demonstrate senior management's involvement in introducing, implementing and maintaining a secure computer systems environment throughout the organisation.

<div align="right">(Eloff and Badenhorst, 1990)</div>

Computer security is only obtainable by having a corporate security policy, as without it no cohesive and cost effective security can be achieved (Smith, 1989). The content of an organisations security policy will have a significant affect upon its management's attitude to security (Plant, 1993) and also upon its workforce.

There are various ways of developing a security policy. Formalised methods have been developed, which allow for policy development and installation. An example of this is the CS-methodology (Eloff and Badenhorst, 1990), which describes the main steps in compiling a computer security policy as given below.

Determine common framework of terminology

Agree on a common framework of terminology that can be understood by all members of the organisation.

Determine purpose for computer security

Determining the security requirements of the organisation:

- identifying areas of the organisation that are dependant on computer

    systems;

- identification and protection of data which is considered an asset;

- ensuring continuation of business operations;

- establishing the relationship between computer and other policies

    already in existence.

Defining the scope of computer security

Senior management and IT staff have to determine the scope of applicability of computer security to their business organisations.

Agree accountability and responsibility

To define the responsibilities of parties involved in the computer security policy. Accountability lies with line management, whereas responsibility should be in the hands of experts, e.g. IT staff.

3.2.4) Security Awareness and Training

Within the new workplace protection of information is a new skill which many employees do not understand or accept (Lafleur, 1992). To ensure that staff are given these skills there are two approaches.

Training

To give new staff basic computer security skills and an understanding of the wider security issues.

Awareness

To remind staff of the security issues and also to educate them about new security issues.

This process has to be on-going to ensure that once staff are given these new skills that they do not lose them because of lack of awareness or continued training.

3.3) Studies undertaken for Plymouth and Torbay Health Authority

Plymouth and Torbay Health Authority was established by the amalgamation of Plymouth Health Authority and Torbay Health Authority in 1993. The main collaboration was with Plymouth Hospitals NHS Trust based at Derriford Hospital, Plymouth.

As previously mentioned in chapter 2, the work conducted by the SEISMED project identified three principal divisions of HCE staff that should be considered when introducing security (Furnell and Sanders, 1994) :

- general HCE staff (e.g. clinicians, nurses, administrators);
- HCE management;
- IT and Security personnel.

It was decided that the most effective way of eliciting information from staff was by the use of surveys. It was considered most important for the first survey to assess the attitudes of the general users and IT staff, so that management would then be able to determine which security concepts needed to be promoted to their staff and where resistance or problems would be likely to occur. It was also considered important to specifically look at the attitudes of system managers as it was thought that if their knowledge of security was limited then so would that of the system users.

It was anticipated that the staff within Derriford Hospital would possibly be more security aware than those within many other European HCEs, given that the establishment participated as a reference centre in the SEISMED project, involving many of them in the implementation and validation of the recommended guidelines.

3.3.1) General Users Study

The first investigation attempted to determine the attitudes of the general staff within the reference environment. The survey document contained four pages and included a

total of 37 questions ([1]Furnell et al 1995). This survey formed the basis of a final year project at Plymouth University (Holben, 1995), the author was involved in its supervision and provided input into the design of the questionnaire.

These were divided into four sections, which obtained general background information followed by responses to questions in three key areas of security awareness, as summarised below.

1. General

   Obtained information on general computer usage (in terms of system, application and data access) and opinions on basic aspects of security.

2. Physical

   A small section which collected basic information concerning attitudes towards the physical protection measures employed within the HCE.

3. Logical / Computer system security

   This section concentrated upon respondents awareness of security breaches and their use of passwords (the latter being the prime method of authentication and access control used in operational systems at the time and, therefore, expected to be well understood by the staff).

4. Personnel

Assessed staff security awareness in respect of their own role within the HCE, including specific security and data protection responsibilities and their attitudes towards the level of security training provided.

Although it would have been desirable to explore some areas in more detail, it was considered that the inclusion of too many questions would serve to make the questionnaire appear daunting and consequently reduce the potential response rate. Amongst the staff targeted were consultants, doctors, nurses, administrators and secretaries, with respondents being asked to identify their discipline to allow potential for subdivision of the final results.

A total of 200 questionnaires were distributed and responses were gathered over a period of about a fortnight. At the end of this time, a total of 75 usable responses had been received. The distribution of responses from within the individual staff categories was rather uneven and, in some cases, the number of responses was too low to allow any confident analysis (for example only 4 responses were received from doctors, whilst a more healthy 18 responses were obtained from nurses). For this reason it is difficult to assess attitude differences between the staff groups and so analysis was restricted to the general domain.

From the basic introductory questions there was a general consensus amongst the respondents that information security was of most importance to help preserve patient

safety and confidentiality. Only 10% of staff felt that the current levels of security restricted them in their work. Respondents were generally more confident in the effectiveness of the HCEs logical security controls than the physical and personnel measures, but even in these cases the consensus appeared to be that the measures were at least adequate.

From the responses to the physical security questions, it was established that almost a third of staff do not wear their identity badges. However, some 83% claimed that they would challenge someone not wearing a badge - indicating that many staff do not follow the practice that they expect others to observe. Some 16% of respondents were unaware that areas of the HCE were monitored/under surveillance - which provided a first indication that security awareness was not all that it could be.

In terms of logical security the results firstly established that only 5% of staff were aware of security breaches within the HCE. However, this figure is still worrying in that it represents violations perpetrated by HCE staff. The results relating to the use of passwords and general observance of system security were of even more concern. Some 59% of respondents admitted to leaving their terminals logged in and unsupervised, whilst an even greater proportion (65%) claimed to have used someone else's system when left in such a condition. These factors indicate lax attitudes towards the protection and privacy of individual accounts.

Proceeding from the basis that a password is supposed to represent secret knowledge known only to the legitimate user, the survey proceeded to assess how carefully the

HCE users attempted to abide by this concept. The responses established that some 21% of respondents legitimately shared a group password with other users. However, a further 18% admitted that their password had been shared with other users without authorisation and 15% claimed to know other peoples passwords illegitimately, again indicating scant regard for the purpose of the controls.

Other statistics were that 18% of staff felt that their password could potentially be guessed (on the basis that it was related to their name, hobbies or a dictionary word) and almost a third of respondents admitted to keeping a written record of their password (which further defeats the point of having one - especially if the information is left around for others to read).

Finally, respondents were asked what they considered would be a reasonable length of time between password changes. Opinions here varied dramatically, as indicated in figure 3.1 below, and it should be noted that only 26% of users concurred with the view of 30 days that is advocated (Smith, 1989).
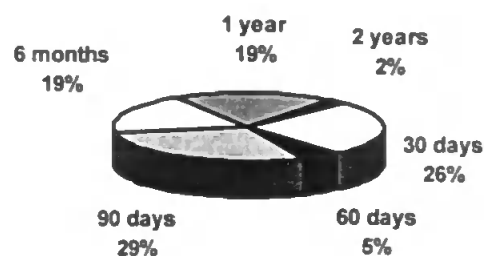
Fig 3.1. Respondents opinion of password changes

The responses to the final section, personnel security, were also rather mixed. Some 64% of staff were aware of security-related clauses in their contracts of employment (this would appear to be quite encouraging in the sense that, at the time of the study, the reference centre was still in the process of revising contracts to incorporate such clauses and, therefore, a fair proportion would genuinely not have incorporated them). Also encouraging was that almost all staff (92%) claimed to be aware of the Data Protection Act and how it applied to their information.

However, problems were still apparent in that approximately two thirds of staff were unaware of the existence of local or general HCE security documentation. This represents a problem irrespective of whether the views were actually correct or not, as it means that the HCE is either failing to provide the documentation or promote sufficient awareness of its existence.

The final questions in the survey actually concerned the issues of security training and on-going awareness initiatives. Unfortunately, the indications in both cases were disappointing, with only 25% of staff having received security training and 15% claiming to receive adequate security awareness. These figures would tend to explain some of the significant weaknesses observed elsewhere (e.g. the poor use of passwords).

3.3.2) System Managers Survey

This element of the investigation concentrated on the HCEs technical personnel, obtaining information regarding the security awareness and attitudes of the local

system administrators. The potential response base in this case was obviously somewhat smaller than that of the general user population. The survey was sent to all twenty system managers, who collectively run 36 computer systems in operation within Derriford Hospital. After a period of three weeks, a total of 14 responses had been received (i.e. a successful return of 70%).

The content of this survey was considerably different in that it was intended to elicit information from those who were responsible for selecting and implementing security, as opposed to those who were ultimately affected by it. As such, the prime issues covered were the respondents confidence in their own knowledge of security and the factors that they considered important when trying to incorporate it into their systems. As a result, few opportunities existed for direct comparison with the general staff responses.

The survey intended to determine:

- managers level of computers security knowledge;

- organisational level of security training;

- identification of security cost components;

- human impact of introducing security;

- departmental security set-up.

(\[1\]Furnell et al, 1995)

The first questions of the survey related to security knowledge. In these 64% of system managers felt confident in their security knowledge and 71% of managers would like specific training relating to security. This seems strange as it implies that system managers require specific security training in order to improve their security knowledge and that of their users.

The next section was concerned with costs and this section showed that 50% of system managers felt that consultants costs were very important when implementing security and 30% of system managers thought that training costs were irrelevant. This is important since it shows that more emphasis is placed on the cost of implementing security by outsiders, rather than the issue of training several hundred staff in how to use the security features.

When it comes to implementing security, the most important issues is that of ease of implementation and here 85% stated that this was very important. The level of training required by staff was also considered to be very important (but not financially important) by 77% of system managers.

When it came to training itself, 75% of managers felt that the level of training given and the cost of training was important and 50% of managers felt that the number of staff to be trained was important. This is shown in fig 3.2:
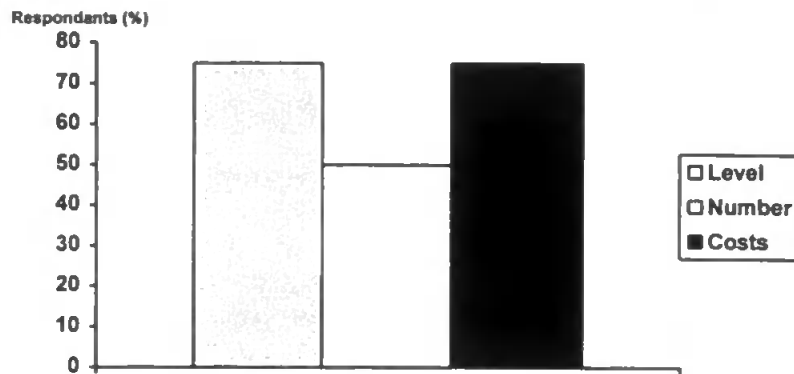
Fig 3.2. Training Costs

This implies that managers are more concerned with training costs, i.e. in-depth training is expensive and the time lost through training, rather than the number of people being trained.

When the issue of the user impact of introducing security was considered, it was found that 92% of system managers were concerned if it would affect the way users use the system. Some 61.5% were concerned that the security would change the users job and 30% were concerned if new security features created new jobs or responsibilities. This shows that managers were concerned to ensure that any change would not put users off using the system.

This section of the questionnaire was concerned with departmental security set-up. The survey found that 77% of departments had a person concerned with security, 46% of departments has a general computer security policy and 20% had a policy dealing with portable PCs. The use of portable PCs was considered because they are the only

items of IT that are regularly taken off site. The response to these questions are shown in figure 3.3:

Respondants (%)
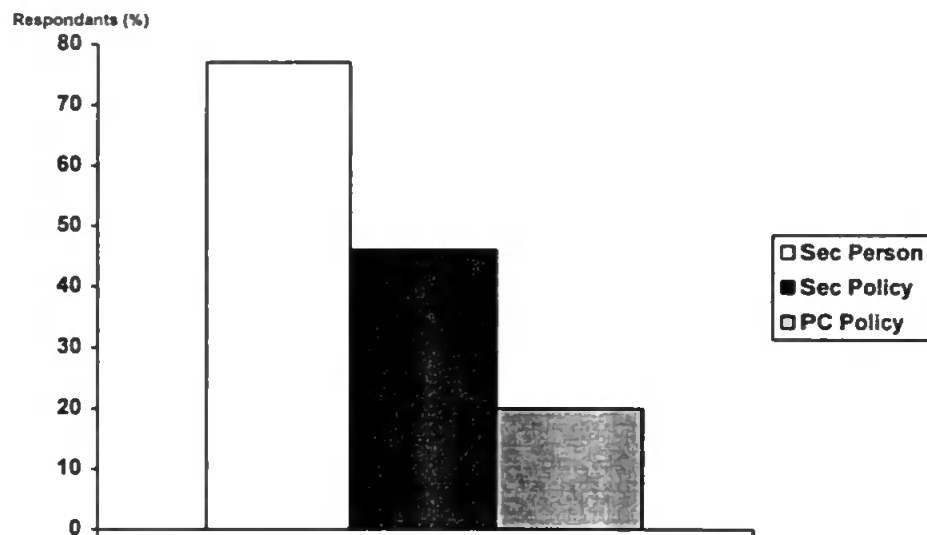
Fig 3.3. Levels of Security

The chart shows even though 77% of the departments have a person concerned with security, these persons do not have the appropriate knowledge to develop departmental security policies or specific security policies. This implies the people concerned with security should be given further training to assist them.

The final section of the questionnaire was concerned with users security training. This found that 71% of user were given initial security training but only 23% undertook regular security awareness programs. This is shown in fig: 3.4:

Respondants (%)
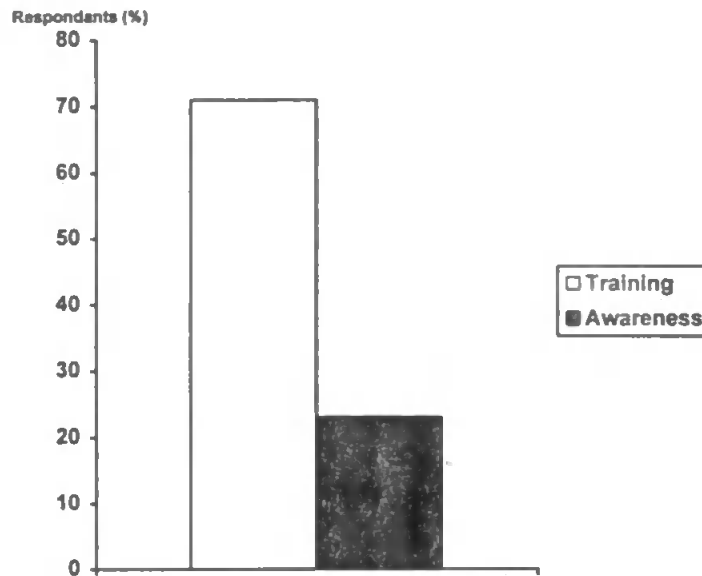
Fig 3.4. User Security Training

This chart implies that after staff are given their initial security training they are not given any other security training. Hence staff may become less security conscious because they are not as aware or reminded about the security issues.

3.4) Solutions to Problems Identified

Within the Plymouth and Torbay Health Authority there are 36 main systems in operation (including radiology, ward nursing, pharmacy, library) from a number of suppliers. The users of the different systems seek guidance from the system managers about security and the quality of the advice that they are given varies. The lack of security knowledge within the system managers can be related to their non IT background. The trust personal has a good understanding of data protection principles and have a Data Protection Officer to help enforce the Data Protection Act (DTI, 1993).

:xisting problems within the Plymouth and Torbay Health Authority

)wing points have been determined by the two surveys, interviews with all the

nanagers and interviews with a cross section of users:

:)wing describes the problems that **existed** within the Plymouth and Torbay

\uthority and within **some** systems:

- no formal policy relating to IT security;

- no formal policy relating to PC security;

- no formal training directly related to security;

 :: complete lack of any procedures relating to security matters;

 no formal source of knowledge relating to security within the

> organisation, i.e. an IT security officer;

poor use of passwords, e.g.;

> - the passwords are never changed;

> - passwords are shared between users;

> - a written record of passwords is kept by users;

 · ·)r use of levels of access;

> levels of access once set are never changed or checked;

 : ·)r use of audit trials on systems;

 : ·)r use of VAX security features;

 ' :: orical problems with physical security, i.e. equipment being stolen;

 :: storical incidents of 'attempted hacking' by members of staff and outsiders

> using remote links;

- historical incidents of unauthorised data modification by members of staff;

- historical incidents of virus infection on PC computers;

- historical problem of data duplication effecting the accuracy of the data on

    the computer systems;

- no formal virus checking procedure on most PCs;

- problem with information control, staff able to down load

    information from the main computer onto floppy disc.

3.4.2) Steps towards improving security

The following steps were taken to improve security within the Plymouth and Torbay
Health Authority.

SEISMED Project

The role of the SEISMED has been mentioned in previous chapters.

IT Security Committee

A special committee was formed to look at issues of IT security. This committee has
produced an IT security policy for the whole organisation (using the high level policy
produced by the SEISMED project as a basis) and will also be looking at producing a
PC security policy. Some members of this committee will also produce and run
security awareness seminars for system managers and users.

Trust Status

As mentioned before Plymouth Health Authority were given independent trust status, becoming Plymouth and Torbay Health Authority. This meant that staff had to sign new contracts. In these new contracts are clauses relating to IT security and these would help to increase staff awareness, i.e. staff being held responsible for their actions.

3.5) Security Culture

Culture is defined as being values and beliefs which provide people with a 'programmed way of seeing' (Pheysey, 1992). The function of culture within an organisation changes as the group matures. When a group first forms, its evolving culture creates a stable, predictable environment and provides meaning and identity. That same organisation many generations later may find that its culture has become so embedded that its serves only to reinforce the values of the older elements of the organisation (Schein, 1985). In these conditions counterculture is created by younger elements of the organisation, these countercultures are then absorbed into the main culture. A security culture is an example of one of these countercultures and is driven by both the dependence upon IT and by younger elements of the organisation who have greater understanding of IT.

At a general level culture is defined by following (Pheysey, 1992):

- national cultures;

- value, goals and behaviours.

National Culture

National culture relates to different national management styles, the management of

IT varies from country to country. Research into the impact of culture and security is

extremely limited. An example of Saudi Arabian national culture and security is

described in Appendix E.

Value, goals and behaviours

In terms of security culture the use of an appropriate type of power encourages a

certain type of behaviour, see fig 3.5:

Organisational Goals

Protection of Data

Order Goals   Ideological Goals

Legality   Involvement
Conforming   Understanding
Control
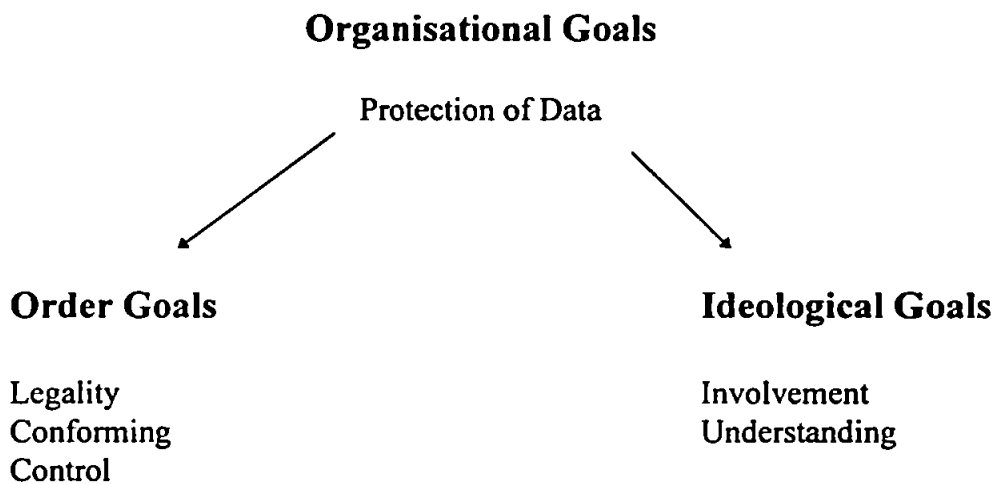
Fig 3.5. Security culture goals

The diagrams show that there are different reasons for the protection of data. The data

can be protected for legal reasons and also for the data can be protected because it is

understood that disclosure of data is wrong.

Security culture can be defined as being a set of goals, i.e. understanding security, confirming to security guidelines in support of an overall goal, i.e. protection of data held by the organisation.

3.5.1) Security Culture within the British NHS

There are major security problems within the NHS (Barber, 1992), which are summarised below.

Trends in NHS Systems

The trends in NHS computing are leading to more extensive use of IT systems. Within the NHS there are now more:

- systems and terminals;

- networks and database;

- non-expert use of IT systems;

- clinical systems;

- safety clinical systems.

Assets at Risk

Systems used by the NHS are vital to its operation and they represents assets that need to be protected against all possible risks.

<u>NHS Reforms</u>

The NHS reforms require IT in order to achieve the desired goals in a wide variety of areas:

- registration of NHS trusts;

- contracting and field maintenance;

- data protection compliance.

<u>Security Concerns</u>

There are a number of reasons within healthcare why security is beginning to become important:

- data protection;

- draft EU directive on data protection;

- health care evidence of security lapses;

- audit commission reports.

Security culture with the NHS is aimed primary at ensuring that staff are aware of security and what their responsibilities are in accordance to it. The NHS IMG (Information Management Group) suggests a framework by which a security culture can be established within an HCE. The steps are shown below (Barber, 1992).

Establish Security Awareness and Responsibility

The steps are:

- determine the responsibility of senior management;

- increase staff awareness of security issues;

- review threats to data security and data protection.

Establish Computer Security Policy

The steps are:

- implement NHS top level policy;

- make security a component of overall IT strategy;

- specify an approach to security management;

- produce an organisational security policy;

- produce local systems security policies.

Address the Computer Security Issue

Look at ways of improving technical, physical, procedural and staff

security.

Address Staff Aspects

Look at areas of :

- staff selection;

- security training;

- security awareness;

- motivation and leadership.

Address Risk Assessment

Undertake CRAMM (CCTA Risk Analysis Management Method)

security review and develop security expertise.

Appoint staff for security management

Appoint:

- data protection officer;

- computer security officer.

Systems Development

During development:

- design in IT Security;

- use formal development methods;

- undertake software quality assurance.

The IMG approach is being promoted within the NHS to help develop a security culture. But the main problem within the NHS is that it has a culture of co-operation and sharing information. Many staff find the concept of restricting data use and data access an alien concept and they are hostile to the introduction of security. There has to be a greater understanding of the NHS culture to ensure that it is easier for staff to accept the introduction of IT and security. Further research into this area is needed to help in the introduction of large NHS IT projects, e.g. the national NHS network (Sunday Times, 1995).

Chapter 4: Development of the SIM-ETHICS Method

4.1) Introduction

An area of security management that has been considered is the implementation of security and the effect that this has upon staff, but thishas not been resolved. It became apparent during the SEISMED project that this issue needed to be resolved. The authors interviews at the Plymouth and Torbay Health Authority showed an alienation between users and newly implemented computer systems. The reason for this was that users were not involved in the decision making or the design stage of the systems (Warren and Gaunt, 1994). It then became apparent that users would feel exactly the same about new security features that were being implemented.

Research into the problem looked specially at two areas:

- the use of different participational management techniques;

- development of a methodology that could be used for the

participational implementation of security.

4.2) Participational Management

At a theoretical level participational management is co-operation between management and staff. The advantages of such an approach are:

- staff have ideas which can be useful;

- effective upwards communications are essential to effective decision

making at the top;

- staff may better accept decisions if they participate in them;

- staff may work harder if they share in decisions that affect them;

      - workers participation develops a more co-operative attitude amongst

workers and management;

      - staff participation may act as a spur to managerial efficiency.

(Adams, 1984)

Participational management can be used to manage small organisations or run national economies and the method has been used throughout the world.

4.2.1) Example uses of Participational Management

Co-operatives

Co-operatives started in the UK in about the 1850s and they were formed by artisans to provide particular services, e.g. food retailing, printing. Typically within a co-operative there are three levels of participation:

      - workers;

      - other individuals (e.g. former workers);

      - other organisations (e.g. trade unions).

(Jones and Svejnar, 1982)

Each member has a equal vote when it come to decision making (usually committee based) and each member has an equal share of the profit. The co-operatives allowed for shared resources, experiences, skills and profits.

Co-operatives are common throughout the world, e.g.:

- France (e.g. farming co-operatives);

- Italy (e.g. engineering co-operatives);

- Spain (Mondragon co-operatives (started and based in the Basque

    region of Spain));

- Israel (Kibbutzim);

- former Soviet Union (Collective farms).

The former Yugoslavia

In the 1950's a law was passed entitled 'Basic Law on the Management of State Enterprises by Working Collectives'. This law allowed the workers to participate in running the organisations for which they work. Further reforms in 1965 and 1970 allowed for greater decentralised control of organisations by workers. Workers within the organisations were involved in decision making at every level via the use of worker committees. Within small organisations the system of self-management was effective (Stanic, 1988) but within the large state-run organisations the result was chaos. The organisation structure is shown in fig 4.1.:
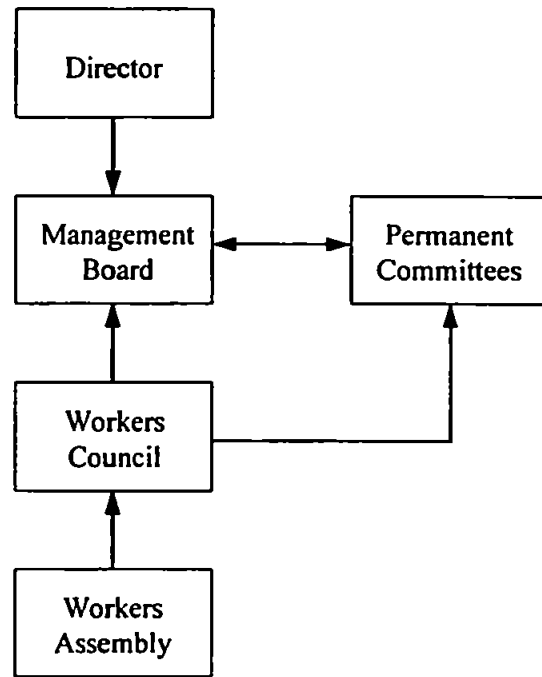
Fig 4.1. Yugoslavia Model of Self-Management (Zeffane, 1988)

Self management implemented across the whole country has caused problems, this can be seen in table 4.1.

	1953-64	1965-73	1974-79	1980-90
Industrial Production	12.7	6.9	7.6	2.4
Labour Productivity	2.2	3.2	1.7	-1.3
Unemployment Rate	5.2	7.9	12.5	15.3
Consumer Prices	4.0	14.2	18.2	208.7

Table 4.1. The Decline of the Yugoslavia Economy (Average annual Growth rate %)

(Zizmond, 1992)

The table shows that between the period 1950-90 industrial production had collapsed, labour productivity also collapsed and the unemployment rate increased as consumer prices increased. The problems that self-management caused within organisations were due to:

- bureaucrats and managers having privileged status;

- inter-organisational relations and external contracts being

 handled by bureaucrats and managers;

- workers having a lack of understanding and skill in handling

 and understanding decision making;

- decisions being put forward without alternatives solutions;

- rampant bureaucracy within organisations;

- increased strikes concerned primary with wages;

- increased corruption.

(Stanic, 1988, Rojek and Wilson, 1987)

4.2.2) Conclusion

After study of different participational management techniques it may be concluded that it would only work within small organisations or departments (Stanic, 1988) . The future of self-management is certain and the co-operative method will continue to be used and is successful in areas where it has been used. The national use of self-management seems limited to the countries of the former Yugoslavia but even this will change.

4.3) Development of SIM-ETHICS

In order to combat the alienation between users and newly implemented computer systems, a new methodology was developed based on ETHICS (Effective Technical and Human Implementations of Computer based Systems) (Mumford, 1985). ETHICS had only been used for designing computing systems. Therefore a new methodology had to be developed, to handle the implementation of security and IT within organisations. The resulting methodology is called SIM-ETHICS where SIM stands for Security Implementation Method.

The philosophy behind SIM-ETHICS is that the development of new technology is not only a technical problem but also an organisational issue. This issue is concerned with the effect that the process of change could have upon the organisation as a whole.

The use of the SIM-ETHICS method allows for the hypothetical implementation of security countermeasures. This allows for the assessment of certain factors:

- organisational impact of security;

- technical problems of implementing security within the organisation;

- training issues related to security;

- SIM-ETHICS grading of security countermeasures by a set criteria.

SIM-ETHICS works through the use of committees to discuss group issues. Fig 4.2 shows how the SIM-ETHICS committee fits into the existing healthcare managerial structure:
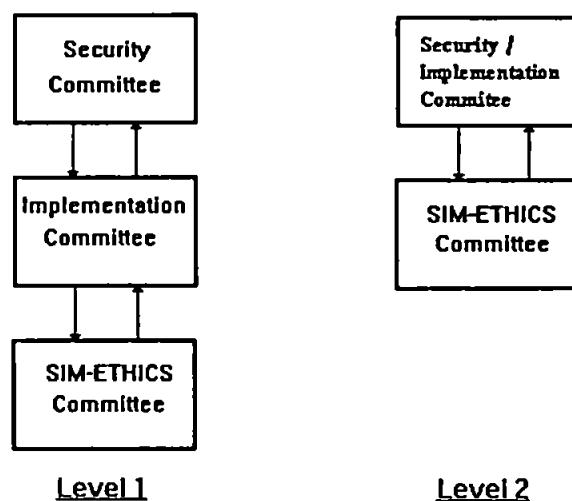
Fig 4.2. Participational Management Models

Level 1 represents a comprehensive managerial method of implementing security. Where a series of committees consider different aspects of security implementation.

Security Committee

The aim of this committee is to consider security at an organisational level and then oversee the implementation.

Implementation Committee

The role of this committee is to implement a particular security project, e.g. findings of a security review.

SIM-ETHICS Committee

The aim of this committee is to allow for user participation in the implementation of security.

Level 2 represents a less rigid organisational structure as the role of the security committee and the implementation committee have been combined. The role of the SIM-ETHICS committee stays the same.

4.3.1) The SIM-ETHICS method

The following are the steps used by the SIM-ETHICS method.

1) Initial Committee Consultation

The committee will be made up of a cross section of staff directly involved or affected by the implementation of the new security features. e.g.:

- representatives of staff from the different departments affected by

    the change;

- representatives of the IT department;

- representatives of the other users who will be using the new security

    countermeasures.

The SIM-ETHICS method uses the participational approach in order to allow user input into the process of change. There are various levels of participation.

Consultative

This is when an existing body, e.g. security committee, is used to implement the change process. This will then consult users on the effect that change will have upon them.

Representative

This is when a cross selection of users effected by change are brought together into a design group. This ensures that representatives effected by change have the same powers in the committee as those bringing about change.

<u>Consensus</u>

This is when all the staff effected by the change are involved in the design process. Representatives of the staff effected are elected to form the design committee.

(Mumford, 1983)

The committee will decide initially on what should be considered the major impacts, e.g.:

- the impacts of introducing security countermeasures;

- training of users;

- cost of new equipment;

- compatibility with existing clinical and administrative computer systems.

Areas of consideration within the SIM-ETHICS method at this stage are as follows.

<u>Job Satisfaction</u>

Job satisfaction is defined as the attainment of a good "fit" between what employees are seeking from their work (their job needs, expectations and aspirations) and what they are required to do in their work; their organisational job requirement.

Effectiveness

This is defined as ensuring that tasks already being carried could be carried out in a more effective manner.

Efficiency

Efficiency is a set of support services which help individuals to work in a organised way with all the necessary back-up facilities which they require. These will include information, materials, technical aids, specialist knowledge and supervisory help. Employees who do not receive support services which they regard as essential to their job performance are likely to become frustrated and dissatisfied.

(Mumford, 1993)

2) Managerial consultation

The intended security countermeasures are evaluated against the SIM-ETHICS criteria (see Appendix A) to determine the level of impact its implementation will have. The criteria relate 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 these new security features?

User Impact

What is the impact that security could have upon users, e.g. how does it affect

user satisfaction, efficiency or effectiveness?

Organisational Impact

What will be the affect that security features could have upon the organisation,

e.g. changing of the organisational culture?

Human Issues

What is the impact that security has upon a user from the human perspective,

e.g. changes of peoples jobs, creating new management roles?

A representative of the committee would meet the following people:

- system managers of existing clinical systems;

- specialist IT managers, e.g. network managers;

- managers and staff involved in implementing the

new security features.

At these meetings, issues relating to the introduction of the security countermeasures

are discussed (as determined in Stage 1) as well as any other possible problems that

managers could foresee.

3) Committee Stage

The views of the managers are discussed within the committee. It is now that initial problems are discussed, e.g. problems of introducing new security swipe cards (see chapter 8).

The committee decides on how to approach the user consultation stage, such as:

- what questions to ask;

  e.g. how do you feel about having to use new security swipe cards.

- the type of user to be questioned;

  e.g. ward clerk.

- the number of users to ask;

  e.g. every ward clerk.

4) Users consultation

A representative of the committee then meets the users to explain the proposed security countermeasures and then ask them a series of predecided questions.

The security countermeasures are then re-evaluated against the SIM-ETHICS criteria to take into account the newly raised user issues.

5) Committee Stage

The views of the users are discussed. If problems are found concerning the system, ways would be discussed on how to overcome the problem, e.g. increase the level of training.

6) Post implementation review

This meeting takes place after the implementation to determine if any unforeseen problems have occurred and if so discuss ways in which to rectify them.

4.3.2) The use of SIM-ETHICS

SIM-ETHICS was used to determine the impact of two new security countermeasures and a new computer information system at Plymouth and Torbay Health Authority.

The new security countermeasures and IT system implemented were as follows.

Countermeasures

Physical Access Control Cards

This considered the use of 'Swipe Cards' (see chapter 8) to control access of staff and visitors within the hospital. These will be used mainly after working hours and in sensitive areas, e.g. maternity wards.

Passwords

Users perception of the need for and use of passwords as a form of access control for computer systems.

IT System

Information Display System

A universal information display system that can be used by all users. The information that will be displayed relates to:

- general administration notices;

- general guidelines, e.g. what to do in case of fire?;

- clinical practices and protocols;

- clinical guidelines, e.g. nationally produced guidelines.

SIM-ETHICS was used to evaluate the security countermeasures and new computer system against a pre-defined criteria (see Appendix A for the full set). These looked at the following issues:

- ease of implementation;

- training issues;

- user impact;

- organisational impact;

- human issues.

A full description of how the SIM-ETHICS methodology was used to evaluate the previously mentioned countermeasures and IT system can be found in Chapter 8.

Multimedia Healthcare Record System

SIM-ETHICS was also used to suggest problems with the implementation of a new multimedia system that was being developed as part of an NHS research project. The aim was to develop electronic health care records for all patients treated within the Plymouth and Torbay Health Authority for certain types of cancers (Plymouth and Torbay Health Authority, 1994). The medical record is the most important repository for information covering patient's healthcare. The traditional paper-based system suffers from serious drawbacks, relating to factors such as duplication of information and illegible handwriting (Ceustres, 1993). The system will be PC based to allow for integration with existing medical computer systems.

The perceived advantages of the system are that it:

- is simple to use, so any member of staff should be able to use it;

- allows for more accurate and complete storage of patient details during their treatment in different areas of the hospital;

- allows for greater access to patient details by staff involved in the treatment, e.g. by general practitioners, community nurses;

- improves the quality of patient data records, e.g. by reducing duplication and improving illegibly;

- improves the working relationship that exists between the clinical teams

providing cancer services;

- allows long term follow up of patients;

- allows for instant access to medical records, 24 hours a day.

(Warren et al, 1995)

Fig 4.3 shows an overview of the system, including the main functional areas and illustrating the different types of data that exists. This data will be contained within the new multimedia health record.

The diagram shows that, although the system is being designed for the treatment of certain cancers, it will have a direct effect upon general practitioners, neighbouring trusts and several departments within Plymouth and Torbay Health Authority. The users could number several hundred staff with different requirements and needs from the system.
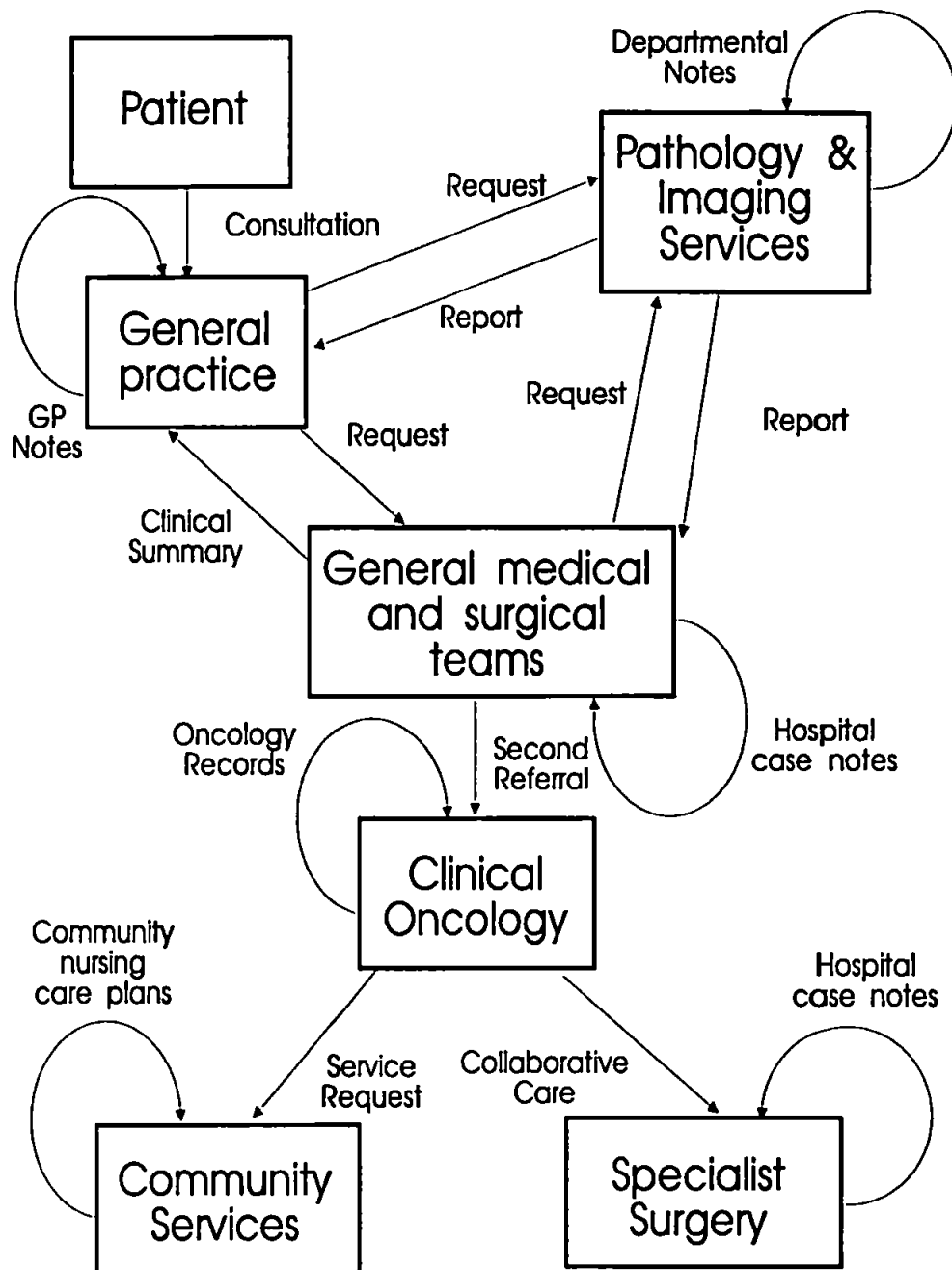
Fig 4.3. Medical Multimedia System

Problems with implementation

The main problems identified through using SIM-ETHICS to analyse the system specification are listed below.

1. Designing a system that meets user requirements and can be used by many

   different types of staff e.g.,

   - doctors;

   - nurses;

   - laboratory staff;

   - radiographers;

   - community nursing staff;

   - general practitioners.

2. Designing a multimedia record that incorporates data from the following

   information sources:

   - general practitioners;

   - hospital clinics and wards;

   - pathology and radiology departments;

   - oncology department;

   - community nurses.

3. Determining the training requirements of users, such as:

   - determining the level of training needed;

   - number of staff to be trained.

4. Initiating awareness programs to educate staff about multimedia and its

   implications.

5. Integrating with various existing computer systems.

(Warren et al, 1995)

4.3.3) Future use of SIM-ETHICS

SIM-ETHICS has been combined with a risk analysis methodology to produce a new security advisory system (see chapter 6). The SIM-ETHICS stages of the system determines the impacts of the suggested security countermeasures. The security advisory system will allow non-security staff to carry out risk analysis reviews and then determine the impact that the security countermeasures could have. This new combination is at the forefront of risk analysis development, it is fully explained in chapter 6.

Chapter 5: Critical Review of Risk Analysis

5.1) Introduction

Risk analysis is often the first step that is taken in developing an organisational computer security policy. Risk analysis also determines the threats to IT systems, the vulnerabilities of IT systems and the countermeasures needed to protect them. It provides the justification for management in order to invest money in security. The aim of risk analysis is to help management strike an economic balance between the impact of risks and the costs of protective measures (FIPS 65, 1979).

Risk analysis is also concerned with protecting the information contained on the computer systems, especially the following aspects (explained in earlier chapters):

- confidentiality;

- integrity;

- availability.

An issue that has to be considered is the management of risk. This is concerned with selecting the best mix of security in order to achieve the greatest risk reduction for the lowest cost.

5.2) The Theory of Risk Analysis

Risk analysis is based upon certain basic principles that are defined as follows (Pursall, 1992):

Asset

Any resources, item or information of value to an organisation, which if compromised in some manner, would result in a loss.

Threat

A potential action manifested by a natural act, or an accident that could result in loss.

Vulnerability

Any weakness in security and controls which provides an opportunity for a threat to manifest itself in the form of a loss.

Loss

The undesirable product of a threat that has occurred resulting in one or any combination of the following.

Denial.

Denial of access to information or systems for different time periods.

Destruction.

Destruction of information or systems.

Disclosure

Unauthorised disclosure of information.

Modification

Accidental or deliberate alteration of data.

Risk

The measurable uncertainty of loss, expressed in terms of both the number of occurrences over a given unit of time, and the amount of potential loss to the identified assets.

Safeguard/Countermeasure

A protective measure designed to reduce the possibility of a loss of an asset.

Risk analysis methods tend to be structured in a similar manner and are broken down into the following stages (Pursall, 1992).

Asset Identification and Valuation

This is concerned with identifying the assets of the organisation, e.g. IT hardware, systems etc. These assets are analysed to produce a prioritised list according to the criticality to the organisation. This prioritisation is based upon the loss of the system to the organisation, for example:

vital system - its loss will be vital to the organisation;

important system - its loss would cause severe disruption;

minor system - inconvenient but having no major impact.

Threat Assessment

In order to determine the potential threats to the organisation, the threats are classified as natural, accidental or deliberate. The threats are then separated by their probability of occurring and the seriousness of their impact. An example is shown in table 5.1, in relation to a hospital organisation.

Threat	Impact	Probability
Aircrash	High	Low
PC Virus Outbreak	Low/Medium	High/Medium
Burglary	Low	High

Table 5.1 Example Threat Assessment of Hospital

Vulnerability Analysis

This is an analysis of vulnerabilities, highlighting flaws and weakness in existing and planned security, e.g. users share passwords.

Safeguard\Countermeasure Selection

Existing or proposed countermeasures are selected based upon their effectiveness against the threats and vulnerabilities that they are trying to combat, e.g. installing CCTV (Close Circuit Television) to protect

against a high risk of burglary. These countermeasures should also be evaluated against the cost/benefits, e.g. it may be cheaper to install improved physical security than a CCTV system.

There are two types of risk analysis methods, as suggested by Anderson and Shain (1991).

- **Quantitative Risk Analysis Methods**

These risk analysis methods use data and also produce data expressed as a level of severity, e.g. high to low, or a scale of one to ten. These type of methods can also model other losses, i.e. damage to morale, political embarrassment.

- **Qualitative Risk Analysis Methods**

The risk analysis method uses and produces data via known quantities, e.g. monetary values, numeric estimates, frequencies of occurrences. These methods can only be used to model certain types of losses.

Risk analysis systems have developed through several stages, including the following.

Checklists

These are a list of security options from which the reviewer would select the options appropriate for their organisation. At the end of the review the aggregated scores would be calculated and, from this, a list of appropriate countermeasures determined.

The advantage of using this method is that reviewers do not have to be specially trained and also the reviews are cheaper to undertake (Baskerville, 1993).

Elementary Information Security Risk Analysis

The development of risk analysis provide a formal basis for evaluating vulnerabilities of computer systems and was attractive because the need for countermeasures could be justified. During this stage of risk analysis development, elements of risk were defined. Courtney (1977) defined two major elements of risk R: where P, the probability of an exposure occurring a given number of times per year, and C, the cost of loss attributed to such as exposure. Risk is then calculated as:

$$R = P * C$$

The probability P is determined with the aid of Probability Range Tables which provide various subjective frequency times and an equivalent annual loss multiplier (Baskerville, 1993). These methods have been implemented as computerised decision support systems, e.g. LRAM and SPAN (see section 5.4). These methods oversimplify more complex information systems and also require a level of maintenance to make them current. The methods suggest the 'best-fit' solution to the problem, which may be not be the actually required solution. (Baskerville, 1993)

Mechanistic Engineering Methods

These methods focus very much on the system requirements, (e.g. taking into account existing physical security) and they also focus on the security project life cycle (Baskerville, 1993), as shown in table 5.2.

Stage 1 Asset Identification and Valuation

Stage 2 Threat Assessment

Stage 3 Vulnerability Analysis

Stage 4 Countermeasure Selection

Stage 5 Implement and maintain countermeasures

Table 5.2: Security Project Life Cycle

These methods are also computerised and the systems are more advanced containing, databases of threats, assets and countermeasures. Such methods include CRAMM and RiskPAC (See section 5.3). These methods are very comprehensive and are useful for carrying out reviews of very complex systems. The different impacts, (e.g. modification, disclosure) are easily determined. The drawback is that the methods are very complex. Teams of staff are needed to carry out reviews and these require a high level of training. The software and licences needed to carry out the reviews can also be very expensive (Baskerville, 1993).

Logical Transformation Models

The aim of these models is to show the security problems and the solutions. The 'logical' aspects of these models relate to the security process, whilst the 'transformation' aspect relates to how the security process can be transformed in the work place. Examples of these models include ODESSA (See chapter 6) which was developed as part of this research programme. This method determines the security requirement of the organisation and then determines the various organisational impacts, (e.g. user impact, training requirements) by using SIM-ETHICS. Models

such as ODESSA are very new and, as such, research is still on going (Baskerville, 1993). The perceived advantages are that they allow a more flexible approach of security design and there is less conflict between security and system usability. Disadvantages are that because they are still new, there is a general lack of experience about them. Because of the 'Transformation' aspect of the models, cost benefit evaluation is more difficult to carry out (Baskerville, 1993).

5.3) Critical review of Risk Analysis methodologies

A complete critique of the main risk analysis methods could not be carried out for a number of reasons. These were:

- risk analysis methods are very expensive so that, it would be expensive even to buy a few risk analysis methods to evaluate;

- the developers of the risk analysis methods would not provide information since it was commercially confidential information;

- companies which have used the methods would not disclose information since it could undermine their security.

Previous research into the area of comparing risk analysis reviews is extremely limited, with the only notable exception being the work undertaken by Wahlgren of Stockholm University, Sweden. He evaluated twelve of the most widely used risk analysis methods using the following criteria (Wahlgren, 1990).

5.3.1) Background

This is the area for which the system was developed, e.g. government, military, consultancy etc.

5.3.2) Type of System

This describes the type of approach that the risk analysis system uses. As previously mentioned, there are two different types:

- quantitative approach;

- qualitative approach (both approaches are explained on page 90

earlier in this chapter).

5.3.3) Supported by a method

As a risk analysis review is very time consuming and rather complicated, it is important that the system is supported by a method informing the user of which steps they should take.

5.3.4) Size of System

The size of the system relates to how extensive the systems are in terms of factors such as the number of questions etc.

5.3.5) Automated Cost/Benefit

One of the main purposes of systems using the quantitative approach is to find out if new proposed countermeasures can be motivated in terms of cost benefit.

5.3.6) Degree of Automation

Some of the described systems are simply tools to help the analyst undertake a risk analysis reviews and this requires a lot of work by the reviewer. Some of the systems already contain a considerable amount of knowledge built into them. This occurs typically when expert systems are used to build systems using the qualitative approach.

5.3.7) Possibilities to change the systems

Some risk analysis methods check the system under analysis to see if they have any countermeasures in place, but these countermeasures can differ between organisations. Some methods allow the countermeasures to be remodelled to reflect a particular organisation.

5.3.8) Gathering of Input Information

For systems that use the quantitative approach to risk analysis, a vast amount of information is gathered (relating to asset values, threat frequencies etc.). This can be very difficult to find within the system. It is important that the system models threats and assets in such a way that it is possible for the user to find accurate information easily.

5.3.9) Reduction of processed information

While undertaking a risk analysis review, a lot of information such as threats, assets, threat-asset pairs etc. is obtained. The majority of this information has little

significance for the final results of the analysis. Some systems can reduce the level of information that is produced for the final analysis.

5.3.10) Degree of Completeness

Systems using the qualitative approach may have a set of required countermeasures for the system under review. These countermeasures should cover all aspects of security, e.g. physical, logical, disaster.

5.3.11) "What if" Functions

When a new system is developed, risk analysis is used to ensure it has the right level of security. In such cases it is important that the risk analysis system has a "What-if" function, so the analyst can model different security solutions on different scenarios.

5.3.12) Why function

The results of a risk analysis can be very confusing for the user. When a rule-based expert system is used an important feature of the system is the ability to explain why it reached certain decisions.

5.3.13) Dynamic threats

Most systems model all threats in a static way, which means that a threat always has the same frequency of occurrence. Some systems use a more dynamic way to model a threat, by taking into account such factors as the motivation and the capability of the perpetrator.

5.3.14) Multi valued loss

Many systems not only use money to measure expected losses, but also qualitative values like loss of morale, political embarrassment etc.

5.3.15) Recommendation of safeguards

One of the main purposes of the quantitative system is to find weaknesses in the system being reviewed. If a weakness is found, it is possible to recommend new countermeasures to reduce it.

5.3.16) Evaluation of Risk Analysis Methods

The most widely used risk analysis methods are shown below

	Number of users	Area of Application
MARION	15,000	Consultancy
RiskPAC	1,000	Consultancy
RiskWatch	800	Consultancy
Rank-IT	600	Consultancy
Predict	350	Consultancy
Control - IT	300	Consultancy
CRAMM	200	Government
Melisa	200	Military
Risiko	100	Consultancy
Buddy System	80	Consultancy
Risan	55	Consultancy
BDSS	25	General
Feros	17	Consultancy
AnalyZ	15	Consultancy
Analyes des Risqué Programmes	11	Consultancy
Arome+	10	Consultancy
DAFI	10	Consultancy
XRM (eXpert Risk Management)	10	Consultancy
BIS Risk Assessor	7	Consultancy
SBA	5	Military
SISSI	4	Consultancy

Table 5.3. The most commonly used Risk Analysis Methods

References: (S2014, 1993), (Computer Select, 1995)

The above shows that most risk analysis methods are used in a consultancy role and are not specially used for healthcare. It is the general case that most consultancy methods are used within a business environment (Wahlgren, 1990). A comparison of the criteria used in the evaluation is given in table 5.4. The above methods are fully described within the appendices.

	Cossac	CRAMM	Expert Auditor	IST/ RAMP	LAVA	LRAM	MARION	MELISA	Control Matrix	RISK CALC	RISK PAC	Xsec
1 Background	Consult	Gov.	Consult	Consult	Gov.	Military	Consult	Military	Consult	Consult	Consult	Consult
2 Type of System	Qual.	Qual.	Qual.	Quant	Both	Quant	Both	Qual.	Qual.	Quant	Qual.	Qual.
3 Method Support	Low	High	Medium	Medium	High	Medium	High	High	Low	Low	Low	Low
4 Size	Medium	Large	Medium	Medium	Large	Medium	Medium	Medium	Small	Small	Medium	Medium
5 Cost/benefit	No	No	No	No	No	Yes	Yes	No	No	Yes	No	No
6 Automation	High	Medium	High	Low	Medium	Low	Low	High	Medium	Low	High	High
7 Change	Yes	No	No	n/a	No	n/a	No	No	Yes	n/a	Yes	No
8 Input	Low	Medium	Low	High	Low	Medium	Medium	Medium	Low	Low	Low	Low
9 Reduction	n/a	High	n/a	Low	n/a	High	n/a	n/a	n/a	Low	n/a	n/a
10 Completeness	High	High	Low	n/a	High	n/a	High	High	Medium	n/a	Low	High
11 What/if	No	Yes	No	n/a	No	n/a	Yes	Yes	No	n/a	No	Yes
12 Why	Yes	Yes	No	n/a	No	n/a	No	No	No	n/a	No	Yes
13 Dynamic Threat	n/a	Yes	n/a	No	Yes	No	No	Yes	n/a	n/a	n/a	n/a
14 Multival. losses	n/a	Yes	n/a	No	Yes	No	No	No	n/a	No	n/a	n/a
15 Safeguard Rec	Yes	Yes	Yes	n/a	Yes	n/a	n/a	Yes	Yes	n/a	Yes	Yes

Table 5.4 Comparison of Risk Analysis Methods

Recommendations

Wahlgren makes no recommendations about the use of a particular method for undertaking security reviews. The main reason for this is that the methods are developed for particular uses and cannot be used properly in domains other than those intended. For this reason, the methods are largely inappropriate to healthcare which has its own unique problems (as defined in chapter 1).

The reasons why each of the above methods are inapplicable to healthcare are examined more specifically below.

● <u>CRAMM, LAVA, LRAM, MELISA</u>

These methods have been developed specially for use by the military and government. The problem is that they were developed for their own particular data usage, e.g. CRAMM was developed to handle the following data groups (CESG, 1992):

- Official Information   Undefined.

- Restricted   The compromise of this information would be likely to : affect diplomatic relations; make it more difficult to maintain the operational effectiveness of security organisations, etc.

- Confidential   The compromise of this information would be likely to : damage diplomatic relations; damage the effectiveness of valuable security or intelligence operation, etc.

- Secret   The compromise of this information would be likely to : raise international tension; seriously prejudice public order, etc.

- Top Secret   The compromise of this information would be

likely to: lead directly to widespread loss of

life; to cause severe long-term damage to the

UK economy.

CRAMM (CCTA Risk Analysis Management Method) was developed by the CCTA (Central Computer and Telecommunications Agency) in 1985. The system was designed to be used by central government departments (CCTA, 1992). Whilst CRAMM has been adopted for use within healthcare by the UK Department of Health. This may have been due to government departmental pressure and not the healthcare applicability of CRAMM (the use of CRAMM is discussed within the appendices).

- **COSSAC**

This system is extremely limited in its application and has not been developed fully. The versions of COSSAC that have been developed have been aimed at US governmental departments (this method is fully explained within the appendices).

- **Expert Auditor, Xsec**

These systems are auditor tools they are used to check the consistence and quality of existing countermeasures. These methods are not applicable for healthcare (these methods are fully explained within the appendices).

- <u>IST/RAMP, RISKCALC</u>

These systems use a quantitative approach to determine the impact loss. Although RISKCALC was used during the SEISMED project to evaluate its performance (Kantzavelou, et al, 1993) the results were unconvincing. The main reason for this was the way RISKCALC expressed loss of healthcare data in monetary terms, it did not look at other implications, e.g. would loss of data affect patients treatment (these methods are fully explained within Appendix F).

- <u>MARION</u>

This method uses data produced by French insurance companies to determine risk levels and impacts. The majority of this data comes from non-healthcare organisations, which means that the method is not healthcare specific (this method is fully explained within the appendices).

- <u>Control Matrix, RiskPAC</u>

These methods are used by consultants to determine the basic security requirements of the organisation. This systems are very basic and determine loss e.g. loss of patient data by monetary means. Because of their general nature these methods are not suitable for use within healthcare (these methods are fully explained within the appendices).

<u>Conclusion</u>

None of the main risk analysis methods evaluated are suitable for use within healthcare. The reason for this is the special nature of healthcare and the data used within its environment (the use of risk analysis within UK HCEs is described in section 5.5). The majority of the risk analysis methods discussed in table 5.4 are of a very general nature and not suitable for healthcare. The risk analysis methods developed for the military and government are not suitable for healthcare because of their data requirements.

5.4) Risk Analysis Methods

This section presents an extensive and unique study of all the known risk analysis methods. This methods are grouped by their area of origin.

Companies Own

These methods have been uniquely developed for particular

company's needs to carry out risk analysis reviews. Sometimes

the method is also used by the company's customers (see table 5.5).

Consultants

These methods have been developed as generic methodologies that can

be used by any organisation to carry out security risk reviews (see table

5.6).

General

These methods are general risk methods, not specifically designed for security. However security systems can be reviewed by using these systems, but the problem first must be modelled (see table 5.7).

Government

Methodologies developed for the government tend to reflect their high requirements for national security (see table 5.8).

Healthcare

Methodologies developed specially for use within healthcare (see table 5.9).

Military

Military risk analysis methods are designed to protect the highest level of data security classification (see table 5.10).

Research

These are methods that are still under development (see table 5.11).

The methods are as follows.

Companies Own

Risk Analysis Name	Country of Origin	Type of Method
ASIS	Germany	Paper
BULLRAM	France	Computer
Citicorp Operations Risk Assessment	USA	Computer
Data Center Evaluation Checklist	UK	Paper
IBM Methodology (Spain)	Spain	Computer
Bureau IFAL Insurance Technical	USA	Computer
PSICHE	France	Computer
REASSURE	Canada	Computer
Sofine	Netherlands	Computer

Table 5.5 Companies own Risk Analysis Methods

(The above methods are fully described in Appendix F).

Consultants

Risk Analysis Name	Country of Origin	Type of Method
Analyse des Risqués Programmes	France	Computer
AnalyZ	UK	Computer
AROME+	France	Computer
BIS Risk Assessor	UK	Computer
Buddy System	USA	Computer
COBRA	UK	Computer
Control Matrix Methodology for Microcomputers	USA	Computer
Control - IT	USA	Computer
COSSAC	Canada	Computer
CRITI-CALC	USA	Computer
DAFI	France	Computer
DDIS	Germany	Computer
EDV-Sicherheits-Check	Germany	Computer
Expert Auditor	USA	Computer
Feros	France	Paper
GRA/SYS	USA	Computer
IST/RAMP	USA	Computer

IS Case	France	Computer
Janber	USA	Computer
MACS	France	Computer
MARION	France	Computer
MicroSecure Self Assessment	USA	Computer
MINIRISK	USA	Computer
Predict!	USA	Computer
QuikRisk	USA	Computer
RA/SYS	USA	Computer
RANK-IT	USA	Computer
RISAN	Netherlands	Computer
Risiko	France	Computer
RiskCALC	USA	Computer
RiskPAC	USA	Computer
RiskWatch	USA	Computer
SISSI	France	Computer
SOS	USA	Computer
SPAN	USA	Computer
X.R.M (eXpert Risk Management)	France	Computer
Xsec	Sweden	Computer

Table 5.6 Consultants Risk Analysis Methods

(The above methods are fully described in Appendix F).

General

Risk Analysis Name	Country of Origin	Type of Method
@Risk	USA	Computer
BDSS	USA	Computer
PRISM	USA	Computer
Risk	USA	Computer

Table 5.7 General Risk Analysis Methods

(The above methods are fully described in Appendix F).

Government

Risk Analysis Name	Country of Origin	Type of Method
Baseline Security	UK	Paper/Computer
CRAMM	UK	Computer
FIPS PUB 65	USA	Paper
LAVA	USA	Computer
PARIS	UK	Paper
RiskPAC (Federal)	USA	Computer

Table 5.8 Government Risk Analysis Methods

(The above methods are fully described in Appendix F).

Healthcare

Risk Analysis Name	Country of Origin	Type of Method
ZIP	UK	Paper

Table 5.9 Healthcare Risk Analysis Methods

(The above methods are fully described in Appendix F).

Military

Risk Analysis Name	Country of Origin	Type of Method
ANSSR	USA	Computer
ARES	USA	Computer
LRAM	USA	Computer
Melisa	France	Computer
SDC US Navy Risk Assessment Methodology	USA	Paper
Security by Analysis (SBA)	Sweden	Computer

Table 5.10 Military Risk Analysis Methods

(The above methods are fully described in Appendix F).

Research

Risk Analysis Name	Country of Origin	Type of Method
SARA	European Union	Paper
SEISMED Risk Analysis Method	European Union	Paper
SESAME HYPERVIEW	France	Paper/Computer

Table 5.11 Research Risk Analysis Methods

(The above methods are fully described in Appendix F).

5.5) Use of Risk Analysis within UK Healthcare

Within the UK, the NHS use two main risk analysis methods (described in 5.4). These

are:

5.5.1) CRAMM

CRAMM has been adopted by the NHS IMG (Information Management Group) as the

'de facto' standard for risk analysis. The reason for this is that it has been developed

for civil service use. The IMG suggested that when organisations carry out risk

analysis reviews they should use CRAMM (IMG, 1992). The method is computer

based and runs on an IBM PC.

The advantages of using CRAMM are:

- allows for extensive security risk analysis reviews to be undertaken;

- allows "What - If" facilities to allow reviewer change the data values and

    determine the impact that this has;

- CRAMM allows for backtracking, in that a review can backtrack

    any earlier stage in order to determine the reasons for the findings.

- produces cost-benefits details.

The disadvantages of using CRAMM are (O'Connell and Patel, 1992):

- that it was designed for use within a government/commercial environment

    and it may not really be suited for healthcare environment. It does not

    take into account specific security problems within the healthcare

    environments in the following ways:

    - does not suggest how the countermeasures may be

        implemented;

    - CRAMM was designed as a consultants tool;

    - in order to use CRAMM staff have to go on training courses;

    - some of the countermeasures produced by the system are not

        very descriptive;

    - the impact analysis of assets is designed for a civil service

        perspective,

        e.g. an example question asked relating to political

        embarrassment

"Would disclosure of data cause civil unrest or cause

the government to resign?"

- if the skills do not exist within the organisation already to

carry out a CRAMM review then expensive

consultants have to be hired;

- reports produced by CRAMM are not easy for staff to

understand.

5.5.2) ZIP

ZIP has been adopted by the NHS Information Centre as a standard risk analysis security method. The aim of ZIP is that it is used in security reviews of small PC systems (less than 8 machines). The ZIP methodology is based upon the principles of CRAMM.

The actual methodology is paper based and is contained within a single booklet. simplistic Also contained is a questionnaire that is used to value the system assets.

The advantages of using ZIP it is;

- cheap to use;

- simple to use;

- no training required to use method;

- quicker then undertaking a full security review;

- covers a area that CRAMM neglects such as PCs.

The disadvantages of using ZIP are:

- the method is limited due to the fact that it is contained in a single booklet
  and due to its size does not address the healthcare issues (mentioned in
  previous chapters);

- designed for use within a government/commercial environment may not
  really be suited for healthcare environment. It does not take into
  account specific security problems within the healthcare environment;

- does not suggest how the countermeasures may be implemented;

- problems with determining impact values e.g. applying the same figure to
  determine general security, local area network and financial system;

- does not contain cost benefit details.

5.5.3) SEISMED Risk Analysis Method

Work within the AIM SEISMED Project has produced a risk analysis method that may in the future be used within the NHS. The risk analysis method was developed specifically for healthcare (Davey and King, 1995) but is at the moment not widely used.

The advantage of using this method are:

- designed specifically for use within healthcare;

- cheap to use;

- simple to use;

- no training required to use method;

- quicker then undertaking a full security review.

The method also has disadvantages, which are;

- the method is paper based;

- the method is a cut down version of CRAMM and so includes the

weaknesses of CRAMM and amplifies them;

- does not suggest how the countermeasures may be implemented;

- some of the countermeasures produced by the system are not very

descriptive;

- determination of impacts and threats is very simplistic;

- limited number of countermeasures.

5.6) Problems of Using Risk Analysis

The biggest problem of risks analysis is that staff have to be specially trained in order

to use the method. The major resource required for risk analysis is man power - highly

skilled manpower. If management want meaningful results they must be willing to

commit the resources necessary for such an undertaking (Pursall, 1992).

Research into the use of risk analysis has shown that industry needs 'smart' risk

analysis tools, capable of modelling the system environment in a few broad strokes

(Anderson and Shain, 1991). In short what is a needed is a risk analysis tool that is:

- 'user friendly', so that general management and technical staff can

use the system;

- able to produce easy to understand reports;

- complete with an extensive on-line help facilities;

- inexpensive to buy;

- able to run on a standard PC machine.

(Warren et al, 1996)

5.7) Conclusion

This chapter has explained what risk analysis is, why it is used and the problems that can occur. This chapter has also evaluated twelve of the most widely used risk analysis methods and has shown that none of them were suitable for use within healthcare. The current state of risk analysis within the UK NHS was also reviewed and again it was found that current methods used were not really suitable for healthcare.

In conclusion the use of risk analysis allows the identification of problems within an organisation and also suggests countermeasures that can be used to reduce risk. It is still the job of management to decide what to do with the information that they are given; poor security is often linked to poor management. The next chapter describes a new risk analysis methodology developed for use within healthcare.

Chapter 6: Development of the ODESSA

(Organisational DEScriptive Security Analysis)

Method

6.1) A new risk analysis method for healthcare

Chapter 5 has demonstrated that there is a need for a computerised risk analysis method that is healthcare specific.

The development of this healthcare methodology and computerised system proceeded in two main phases.

Stage 1 Development of a generic risk analysis method for HCEs

This paper based method was developed as part of the SEISMED Project (Furnell et al, 1993) and is explained fully in section 6.2.

Stage 2 Development of the ODESSA method

This method was developed as a progression of the HCE generic risk method. Some problem associated with the HCE method was corrected and major new concepts added. The method is described in section 6.3 and the prototype computer system is described in chapter 7.

6.2) The Generic Risk Analysis method for HCEs

As stated in 6.1 there was a need for a methodology that could be used for the identification of security requirements in healthcare computer systems. The method developed was an attempt to allow system administrators or computer security staff to carry out a security review of their own system (Furnell et al, 1994).

6.2.1) The HCE method

The major rationale behind developing the method was that security-relevant elements of existing systems are (Furnell et al, 1994):

$$\textbf{Information}_{\textbf{System}} = \text{Computer Configuration} + \text{Operational Environment} + \text{Data Sensitivity}$$

The rationale of the methodology is that similar organisations/systems will have similar security requirements and a key factor in the approach was to devise a number of predetermined security "profiles" for each element of existing systems.

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

Computer Configuration

This refers to the IT assets (both hardware and software) of the organisation. At a high level it is possible to identify a relatively small number of elements which may be included in any given computer configuration, as shown in figure 6.1. Individual systems would be considered to determine which elements are applicable, and countermeasures selected accordingly.
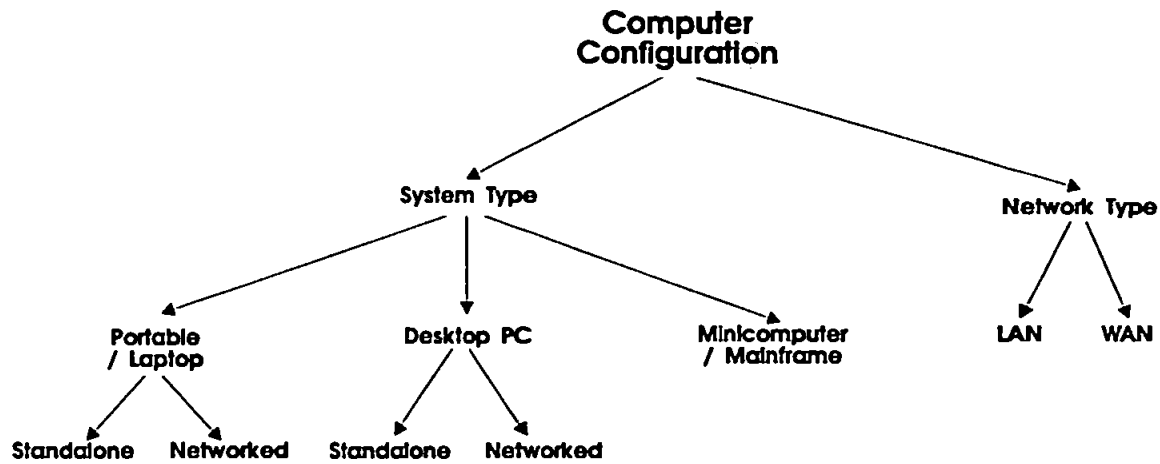
Fig 6.1 : Computer Configuration group

Examples of associated baseline countermeasures were identified for each configuration and are grouped around the following areas:

- physical;
- disaster planning;
- system;
- procedural;
- personnel.

Operational Environment

This considers the nature of the environment in which the IT assets are actually located and used. It has a significant effect on the types and levels of protection that are required. The factors relate to the location of the site, the type of buildings and the people who have access to the site. Appropriate combinations of these factors can be used to describe the majority of health care establishments (i.e. from GPs to general hospitals).

Data Sensitivity

The sensitivity of data is determined by its type and the way that it is used.

• Data type

In consultation with a number of HCEs within Europe, the general care activities carried out by hospitals, general practitioners, community health care centres, and various other support services were examined. This enabled a generic model of medical data to be developed as the basis for further investigation (Sanders and Furnell, 1993). The model is comprised of 12 main data groups, as described in table 6.1. The purpose is to allow a simple means of specifying what data is available within a system and help in the allocation of appropriate sensitivities, thus simplifying the process of identifying how and where data is located in different computer systems and networks.

The information used by the HCE may be of varying levels of sensitivity and this will again be highly dependent upon the cases involved, i.e. data ranging from information about to HIV/AIDS patients to information relating to book loans from a hospital library.

The model groups are of a (necessarily) broad nature (see section 6.3.1), but they may be divided into further levels of detail as required. For example :

Patient Care

Episode information   Specific needs

Dates of admissions / discharges   Health Care Delivered

Staff Involved   Drug Therapy

Diagnosis including clinical coding/s Outcome of the treatment

Care Plan   Consultants and anaesthetists reports

The model provides a generic framework that should encompass all data required by a HCE. Specific medical applications may store and communicate information from all of the data groups, or a particular subset of them. It is consequently possible to map such applications onto the model, indicating the data groups that are involved and from this derive the basic sensitivity of the information.

○ Data use

Incorporating this factor of data sensitivity into the methodology demands that an appropriate range of general uses can be identified. Related work within the SEISMED project (Gaunt and France, 1993) has determined a high level set of data uses that are appropriate for our purposes. A total of 9 categories are considered, as described in table 6.1.

Data Use	Description
Operational Clinical	Used in the planning, delivery and monitoring of patient healthcare.
Emergency Care	Provision of care in a clinical emergency, where optimal conditions and / or information cannot be guaranteed. Therefore, only a minimum set of essential data is required, with HCE's relying on their own training and experience.
Critical Clinical	Control of instrumentation / systems in direct feedback loops (e.g. control of radiation dose administration to cancer patients). Data availability and integrity essential in such contexts.

Expert Systems	Use in decision support tools or neural networks, which aid clinical diagnosis and interpretation or general management of HCE.
Operational non-clinical	Use of information that supports the HCE infrastructure, but does not directly influence the care of individuals.
Financial	Use of data in financial systems for contract management, purchasing and patient billing.
Planning & resource management	Systems used for aggregation of patient data for planning and clinical review purposes.
Quality Management	Systems using data for clinical audit, assessment of care efficiency and outcome.
Clinical Research	Identifiable or anonymised data used for research purposes. Normally utilises aggregated data.

Table 6.1 : General categories of medical data usage

Sensitivity rating

Sensitivity is quantified in terms of several different types of impact that may relate to the data in the system. As previously identified in chapter 5 four main types of impact can be used, with appropriate countermeasures being given in each case.

Disclosure Unauthorised disclosure of information to HCE staff or outsiders.

Denial Denial of access to the information for varying periods.

Modification Accidental or deliberate alteration of the information.

Destruction Destruction of the system or information. An extreme form of unavailability.

The type and use of the data will have different influences over the protection requirements in each of these cases.

Disclosure

Data type is the most significant factor in determining the confidentiality requirement, as data will generally portray the same information in all contexts. The protection afforded should, therefore, remain constant regardless of which application uses it. However, data usage may still have some effect as it can influence problems arising through data aggregation. It is conceivable that if certain data elements are combined, then the impact of disclosure may be greater than that of any one element in isolation.

Denial, Modification and Destruction

The requirements for these are primarily determined by the data usage, as the context will determine the seriousness of the impact, e.g. modification of medical treatment notes could seriously harm a patient.

Impacts are rated low, medium or high (where low indicates that the baseline countermeasure level is satisfactory, and high is the maximum protection that can be provided). The level is determined by considering a number of potential influencing factors :

- confidentiality (both personal and commercial);
- disruption;
- embarrassment;
- financial loss;
- legal;
- personal safety.

For example, the disclosure of sensitive patient care information to HCE outsiders could be seen as a serious risk in terms of legal action, patient personal privacy and

embarrassment to both the patient and the HCE. The level of impact will in turn determine the level of countermeasure.

Countermeasures

Actual security countermeasures are identified and refined at various stages within the methodology, they are categorised under three headings. These are distinguished as shown below :

- baseline countermeasures;

- appropriate countermeasures;

- selected countermeasures.

(These are explained fully in section 6.3.1).

Methodology Implementation

The following describes the specific steps by which the methodology would be implemented when considering individual existing systems. In order to apply the method the following factors would need to be identified for the specific system / application being considered :

- computer configuration involved;

- type of operational environment(s);

- data groups involved;

- purpose of application (data use).

Countermeasures would then be derived as shown in figure 6.2.
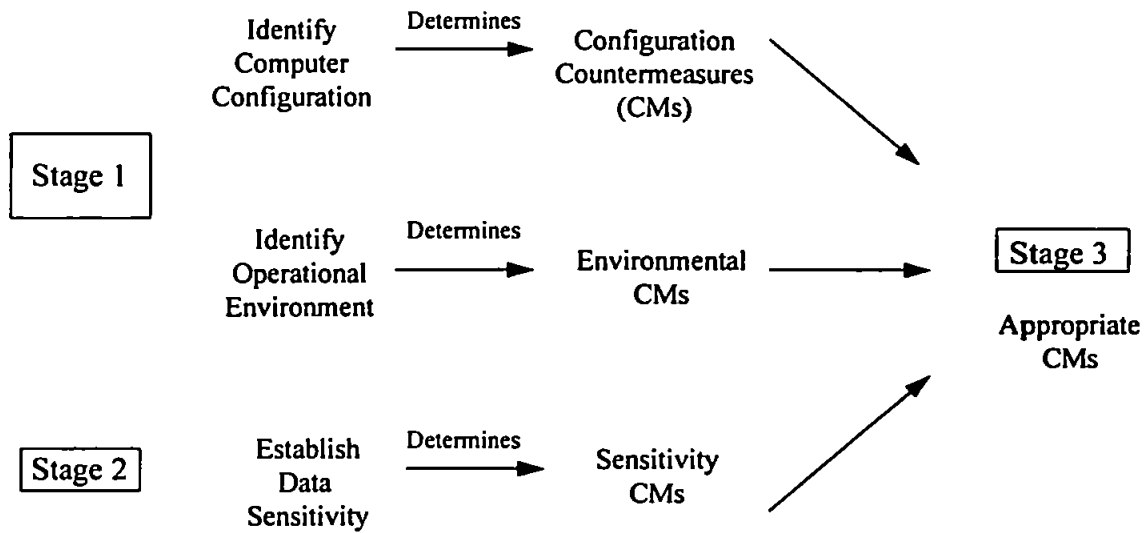
Fig 6.2 Methodology Implementation Steps

At each stage appropriate countermeasures would be selected from corresponding categories (NB: it is likely that some duplication may occur in terms of the countermeasures suggested within different categories).

The stages of the methodology are expanded as follows :

Stage 1   :   Determine basic system profile;

Inputs   :   None;

Output   :   Baseline Countermeasures;

Description   :   Categorise computer configuration and operational environment of the existing system according to pre-determined profile categories.

For computer configuration choose appropriate elements from :

- laptop / portable;
- desktop PC ;
- mini / mainframe;
- network.

For operational environment categorise elements of :

- location;
- buildings;
- people.

Stage 2   : Determine Data Sensitivity;

Inputs   : None;

Output   : Data-related countermeasures;

Description   : Establish data types and uses, Select countermeasures based upon

sensitivities encompassed.

Choose appropriate level from each of (as shown below):

- disclosure countermeasures;
- denial countermeasures;
- modification countermeasures;
- destruction countermeasures.

Stage 3   : Determine appropriate system countermeasures;

Inputs   : Baseline Countermeasures, Data-related Countermeasures;

Output   : Appropriate System Countermeasures;

Description   : Generate countermeasure set that would satisfy the requirements of

the existing system.

Stage 4   : Select system countermeasures;

Input   : Appropriate Countermeasures;

Output   : Selected (final) System Countermeasures;.

Description   : Refine countermeasure set by considering any HCE specific factors

                   / constraints that may apply.

6.2.2) Problems with HCE method

Developed as a paper based method, it was only when the method was being assessed

for use as a possible model for a computerised system that the following problems

were found:

- the "Data Sensitivity" concept was weak when tested, the combination of

    data type and data use would not in practice since there are too similar;

- the concept of generic group "mapping" for particular systems would not

    work in practice;

- the use of the disclosure, denial, modification and destruction impacts

    within the method would be difficult to use in real life;

- the countermeasures groups needed to be amended;

- some of the operational environment categories would be difficult to

    implement, i.e. people factors;

- no specific section of the methodology relating to threat assessment.

6.3) The ODESSA Methodology

The ODESSA methodology was the continuation of the work carried out on the HCE generic risk analysis model. The rationale of ODESSA (Organisational DEScriptive Security Analysis), 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. These may range from the location and age of buildings, to the sensitivity and type of data. The method was developed as a generic methodology that could be used within most organisations, but initially it was developed for use within healthcare.

6.3.1) The Method

The key elements have been incorporated into a framework as shown in figure 6.3.

Operational   Organisational
Environment   Type

Baseline   Organisational
Countermeasures   Requirements

Appropriate   Organisational
Countermeasures   Impact

Selected
Countermeasures

Figure 6.3. ODESSA methodology overview

This illustrates the steps involved (at a theoretical level) in determining the security

requirements for an organisation. The ODESSA system suggests three sets of security

countermeasures.

1) Baseline Countermeasures.

These represent the minimally acceptable security countermeasures that an

organisation should have implemented. These countermeasures are applied in

a generic manner, e.g. every hospital should have the same baseline security

countermeasures.

2) Appropriate Countermeasures

These represent the unique organisational security countermeasures. They are based upon of questions from which data sensitivity profiles are formed. The countermeasures reflect the type of organisation, e.g. a GP would not have the same countermeasures as a hospital.

3) Selected Countermeasures

These represent the selected countermeasures from 1) and 2) that have been applied against the SIM-ETHICS impact criteria and then accepted by the user. The impact varies between organisations, e.g. the impacts of a countermeasure would be different between a GP and a hospital.

The relationship of the countermeasures are shown in fig 6.4.
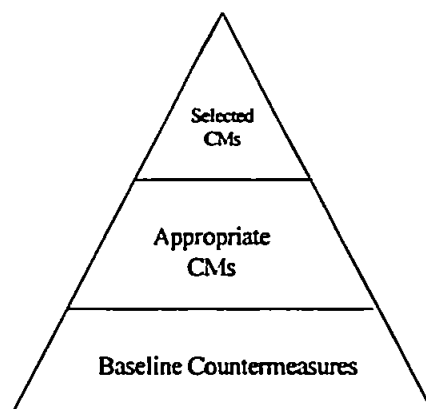
Fig 6.4: Relationships of the Countermeasures

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

Organisational Environment

This considers the environment in which the organisation's assets are located, which may affect the level of protection required. Table 6.2 gives examples of environmental considerations that have to be considered for a medical environment.

Type	Options	Comments
Location	Inner City	Location may indicate risk of vandalism, theft. - may result in a need for increased physical security.
	Urban	Location may indicate risk of theft. - may result in a need for a CCTV system.
	Rural	Location may be many miles from emergency services, i.e. fire station. - may result in increased fire drills, fire awareness schemes, automated fire fighting system, etc.
Building	Old / Modern	Age of building may indicate risk of fire, disasters, etc. - may result in a review of buildings, looking at electricity wires, water pipes, etc.

Table 6.2. Organisational Environments

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. Within the SEISMED project a comparison was made of past healthcare security reviews, which helped to form the baseline security needs for the different types as shown in table 6.3.

Type	Description
GP (Single)	A single doctor working amongst 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. special home nursing, 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 within a variety of different sites.

Table 6.3. HCE Organisational Types

Organisational Baseline Security

Work on the SEISMED project has shown that within a healthcare environment that certain HCEs have the same countermeasure installed at lower levels. The concept of baseline within ODESSA relates to the minimal security levels requirements that a HCE organisation should have installed. These levels were determined by comparing results of different HCE security reviews and examining different HCE security guidelines, such as:

- AIM SEISMED Guidelines for Information Systems Security in Existing

Systems (Sanders and Furnell, 1993);

- AIM SEISMED High Level Security Policy for Healthcare Establishments

(Katsikas and Gritzalis, 1993);

- CCTA Baseline Security for IT Systems (CCTA, 1993);

- DTI (Department of Trade and Industry) A code of practice for Information

Security Management (DTI, 1993);

- IMG Basic Information Systems Security ([1]IMG, 1992).

The ODESSA baseline security countermeasures are divided into particular groups, as shown in table 6.4.

Security Type	Sub groups	Description
Disaster	7	Relates to disaster prevention, contingency planning.
Physical	5	Relates to physical protection of sites and assets.
Hardware /Software	10	Relates to protection of computer systems and the data contained within them.
Human	8	Relates to training, procedural issues, etc.

Table 6.4. Security Groups

The countermeasures are defined as being physical, procedural, programmable or communicational countermeasures.

Organisational Requirements

At this stage the use of the data is considered. Organisations use similar data types, which require similar countermeasures, e.g. encryption of personal data. The ODESSA system uses a set of HCE generic data types (Sanders and Furnell, 1993), as described in table 6.5.

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 and planning	Information used in the management, monitoring and planning of HCE.
Library and information systems	Details of existing medical knowledge that is used by clinical . staff.
Expert Systems	Information used by decision support systems or neural networks used within the HCE.

Table 6.5 HCEs generic data types

Once the type of data has been decided, its sensitivity has to be defined. The sensitivity impacts of the data are as follows:

- denial;

- destruction;

- disclosure;

- modification.

The data impacts are also determined as percentages, in addition as being rated low, medium and high. 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 6.5 shows the steps involved in determining the organisational requirement

Determine
Data Usage ——————► Appropriate Countermeasures

Data
Sensitivity

Overall	Overall	Overall	Overall
Disclosure	Denial	Modification	Destruction
Impact	Impact	Impact	Impact

Appropriate
Countermeasures
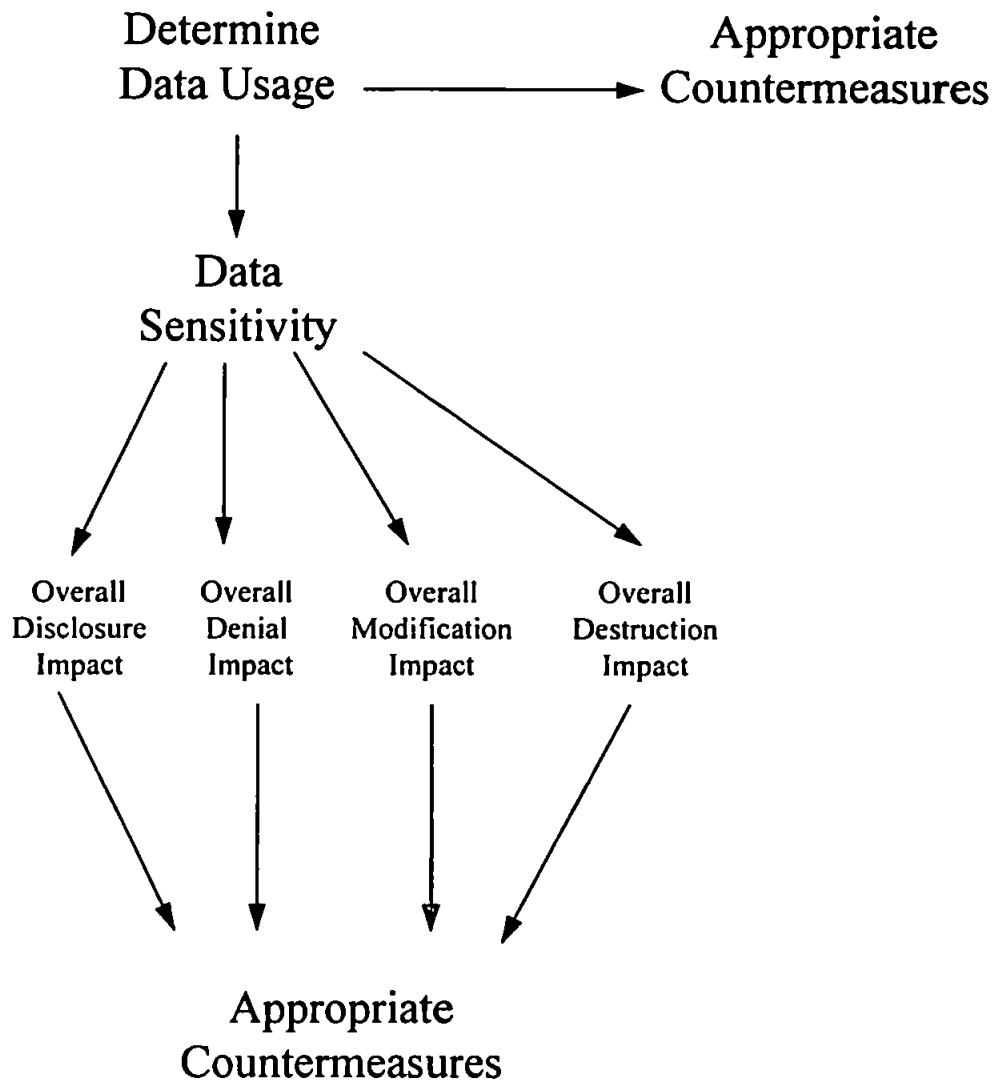
Figure 6.5 Organisational Requirement

The stages involved are detailed below.

Stage 1 Determine Data Usage

The user of the system picks the data types that the organisation uses, which are associated with certain countermeasures, e.g. 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. The questions relate to possible threats that could affect the organisation.

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 SIM-ETHICS (See chapter 4).

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

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 these 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 affect 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?

Example Scenario

The scenario is that of a single GP (General Practitioner - primary community care provider), based in an old building located in an inner city.

Stage 1: Determine Baseline Countermeasures

Stage 1.1 Determine Organisational Criteria

Determine baseline security criteria from the above information.

Organisation type: GP Single

Building Type :   Old

Location: Inner City

Stage 1.2 Determine Baseline Countermeasures

Summary of some of the baseline countermeasures identified for the GP.

Disaster and Damage Protection

Physical Countermeasure

Adequate site fire protection.

Fitting of smoke detectors.

Hardware/Software

Programmable Features

Use of passwords to protect systems.

Software Training/Use

Procedural Countermeasures

Offence to use unauthorised software.

All users should be trained in the packages which they will use.

Special Consideration

Inner City

Physical Access Control

Physical Countermeasures

To counter an increased risk of theft and vandalism improved

physical security should be introduced, i.e. window locks,

secure locks on doors.

Stage 2: Determine Organisational Requirement

Stage 2.1 Determine Data usage

The data types are selected from a list of nine data types (see table 6.5). In this

example the GP uses the following data types :

- patient identification;

- patient administration;

- patient care.

Stage 2.2 Determine Data Sensitivity

The data sensitivity impacts are determined by answering a series of questions related

to the sensitivity impacts.

i.e. If there were problems with your system, would the delay cause any of the

following:

a) patients may be kept waiting for treatment;

b) patients may receive inappropriate treatment;

c) patients may receive inappropriate treatment resulting in additional time

spent in hospital;

d) patients may suffer immediate harmful problems due to lack of treatment.

The hypothetical sensitivity impacts for the scenario are as follows.

- Denial	Medium
- Destruction	Medium
- Disclosure	High
- Modification	Medium

Stage 2.3 Determine Appropriate Countermeasures

Certain countermeasures are specific to the type of data used and its function, i.e.

Data Usage	Example Countermeasures
Patient Identification	Encryption of data
Patient Administration	Use of levels of access to ensure only authorised staff have access.
Patient Care	" "

The next step is to determine the countermeasures for data sensitivity. The type of countermeasures for a particular sensitivity would be dependant upon the impact level.

The following are examples of some countermeasures.

Data Sensitivity	Level	Example Countermeasures
Denial	Medium	Disk shadowing.
		Resource control.
Destruction	Medium	Alternative process arrangements.
		Contingency plan development.
Disclosure	High	Encrypted storage.
		Secure disposal of media/paper.
Modification	Medium	Checksums of data.
		Audit of modifications.

Stage 2.4 Determine Security Profile

The next stage is to determine countermeasures which are unique to the organisation.

These are determined by having the user answer a series of questions. For example:

Question

Hardware/Software Related Questions

Are special provisions made for the use of portable PC's?

Countermeasures

Hardware and Software Related

PC Protection

Physical Countermeasure

Ensure portable PC is secured when in transit.

Procedural Countermeasure

Removed important information when portable PC is in transit.

Programmable Countermeasure

Encrypt the contents of the hard disc.

Implement password protection system.

Stage 3: Determine Organisational Impact

The countermeasures are reviewed and the appropriate SIM-ETHICS criteria selected. The impacts are dependant upon the type of organisation and each countermeasure would have a unique impact description.

Example use of SIM-ETHICS criteria

Sample Countermeasure

> Introducing security awareness program.

Criteria

> Ease of Implementation
>
> Once the basic program framework has been determined it can be repeatedly
>
> used.
>
> Training Issues
>
> Awareness program may be included as part of initial computer training for
>
> new staff.
>
> Training seminars should be held on a regular basis, i.e. once every two
>
> months.
>
> User Impact
>
> Users will be more aware about security, therefore security problems should
>
> be reduced, i.e. virus outbreaks, passwords naming conventions.
>
> Organisational Impact
>
> The program will help raise security awareness amongst all staff and help
>
> establish a security culture within the organisation.

<u>Human Issues</u>

Expertise for such a training scheme might not exist with the GP's staff,

therefore outside help would be needed in setting up the awareness program.

6.3.2) Analysis of the ODESSA method

<u>ODESSA as a Logical Transformational System</u>

The concept of "Logical Transformational Risk Analysis" system is explained in chapter 5. ODESSA is one of these systems since it determine the security requirement of the organisation and then determines the various organisational impact, i.e. user impact, training requirements by using SIM-ETHICS.

<u>Security Expertise</u>

The knowledge used for the ODESSA system were acquired from a number of sources, these were:

- formal risk analysis security reviews of major systems within Plymouth

  and Torbay Health Authority and Plymouth Community Trust;

- personal experience of implementing security and interviewing staff

  within the Plymouth and Torbay Health Authority and Plymouth

  Community Trust;

- knowledge gained from research undertaken within the EU (European

  Union) SEISMED Medical Security Research Program;

- discussions with commercial organisations about security issues;

- discussions with security consultants about security issues;

- knowledge obtained from literature review of security guidelines;

- results obtained from security questionnaires;

- SIM-ETHICS criteria evaluation of security countermeasures lists

    produced by various security risk analysis methodologies, i.e.

    CRAMM.

(Warren, Sanders and Gaunt, 1994)

Advantages of ODESSA

The advantages of the ODESSA system are:

- designed for use with healthcare by healthcare personnel;

- designed to be easy to use;

- overcomes the problems of the HCE generic risk analysis method (as

    described in 6.2.2);

- incorporates the SIM-ETHICS "change control" methodology.

Disadvantage of ODESSA

Because of the Logical 'Transformation' aspect of the method, cost benefit evaluation

is more difficult to carry out, but this problem has to be resolved in order to give

management the information that they require.

6.4) Conclusion

The chapter has described the development of risk analysis method that has been designed specifically for use within healthcare. The chapter also describes in detail the development of:

- HCE Generic Risk analysis method;

- ODESSA.

ODESSA was not designed as a paper based method, it was designed to be computerised so that HCE staff could easily use the system. This logical continuation is described in Chapter 7, which describes the development of the ODESSA computer prototype.

Chapter 7: Development of the ODESSA Prototype System

7.1) Introduction

Chapter 6 described the development of the paper based ODESSA methodology. However it was considered that the method should also be computerised in order for it to be effectively used by HCE staff. It was therefore decided to develop a prototype computer system that would encapsulate the ODESSA methodology. The ODESSA prototype, was designed :

- to be 'user friendly', so that general management and technical staff can use the system;

- to be able to produce easy to understand reports;

- to have extensive on-line help facilities;

- to be inexpensive to buy;

- to be used on a standard PC machine (see below).

(Warren, et al 1996)

To run the ODESSA system the user needs the following minimum PC requirements:

- 486SX PC or better;

- 4MB main RAM;

- 4MB free hard disc space;

- 1MB video card running at 1024 x 768 screen resolution.

ODESSA will run on a lower screen resolution, but some text may be missing or not aligned correctly. This is because the layout of the screens will change between different screen resolutions.

7.2) Design Considerations

During the development of the ODESSA system the following areas were considered.

Expert System

At the early stages of the system development it was envisaged that an expert system would be developed (Warren et al, 1994) (see chapter 8). Later it became apparent that ODESSA would not have to be an expert system but a system that gave "expert" advice. During this time several system design methodologies were assessed but known were suitable for developing ODESSA.

Visual Basic

Visual Basic was chosen as the language in which to develop the system because it:

- allowed for the development of PC windows based systems;

- allowed for the development of powerful user interfaces;

- was able to produce independent stand alone systems;

- was compatible with other packages being was using, e.g.

Microsoft Access;

- was easy to use.

Prototyping

A prototype is defined as being:

- a working model of an information system, which emphasises aspects of the

system.

(Vonk, 1990)

A prototype approach to developing the ODESSA system was selected because of the advantages this method gives, as summarised below:

- it allows for the quick development of computer systems

(especially when using a languages such as Visual

Basic);

- it reduces uncertainty about the nature of the problem;

- the testing phase of system development would be shorter;

- it is easier to develop the full system with skills learned from

prototype development.

(Vonk, 1990, Avison and Fitzgerald, 1989)

The inherent problems of developing a prototype were accepted, but it was decided that the problems would not have a major impact on the work. These problems are that:

- prototyping is inefficient for developing large systems;

- the prototype model is not complete and only performs certain

tasks;

- the prototype would be unsuitable for integrating with other

systems or packages.

(Avison and Fitzgerald, 1989)

7.3) Explanation of ODESSA System

The ODESSA system is split into three mains sections:

- stage 1   - baseline security determination;

- stage 2   - security impact/profiling determination;

- stage 3   - impact analysis.

The system was designed so that the separate stages can be run independently. The

ODESSA system interfaces with the following packages;

- Microsoft Access (a database system);

- Microsoft help creation system.

The sections of the ODESSA system are described using the following format:

Screen   - relates to the name of the screen within the system;

Function   - relates to the function of the screen within the system;

ODESSA Function   - relates to the function of the screen in terms of the

ODESSA methodology.

7.3.1) ODESSA Stage 1

This stage of ODESSA is concerned with determining the baseline security requirements for an organisation and is made up of the following screens.

Screen: Introductory Screen

Function :   This screen is the opening title page for the system.
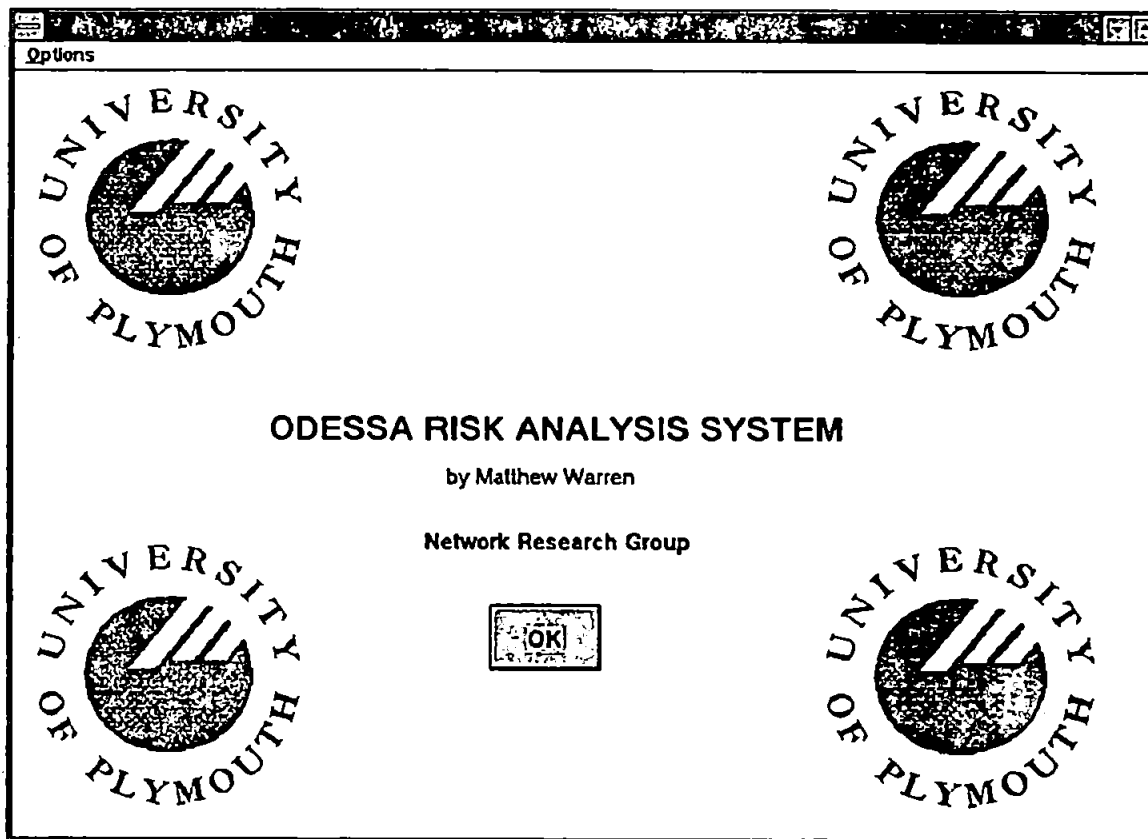
Fig 7.1. Introductory Screen

ODESSA function: None

Screen: Choice Selection

Function: The screen allows the user to decide which options they wish to

use:

Baseline review	- goes to baseline security review;
Overview	- goes to CM overview area;
End	- ends program.
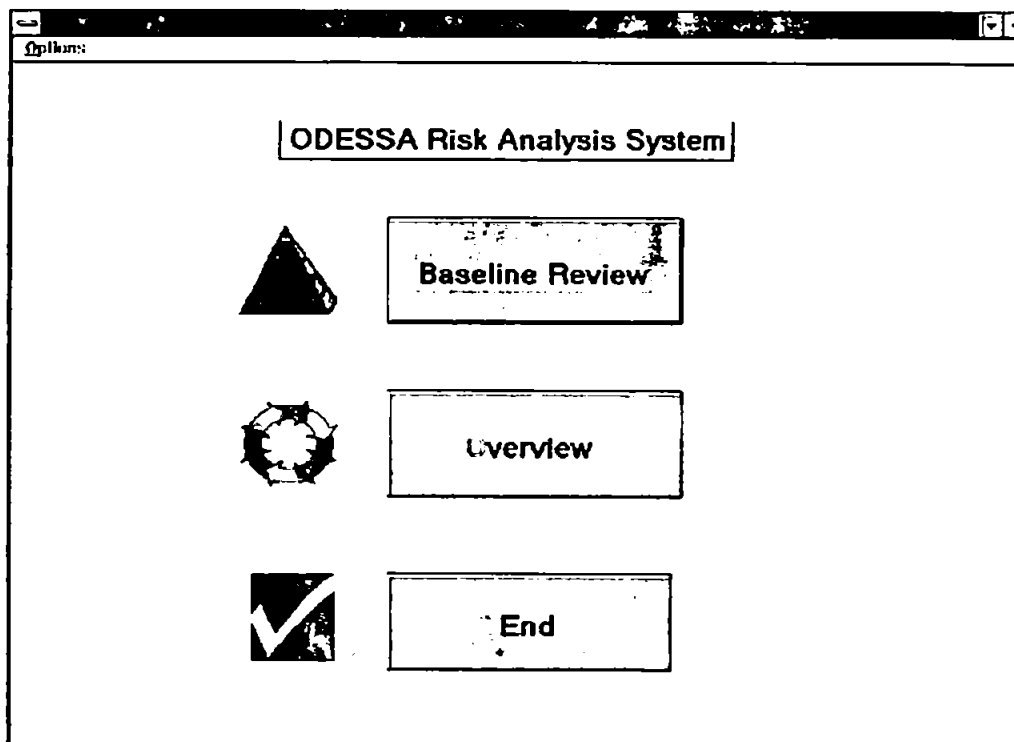
Fig 7.2. Choice Selection

ODESSA Function: None

Screen: Baseline Review Selection

Function: User has to select options from the criteria below in order to determine

the organisations security requirement.

Organisation type: GP(Single);

GP(Practice);

community;

hospital.

Organisational Buildings: old style;

new style;

mixture.

Location of organisation: inner City;

urban;

rural.
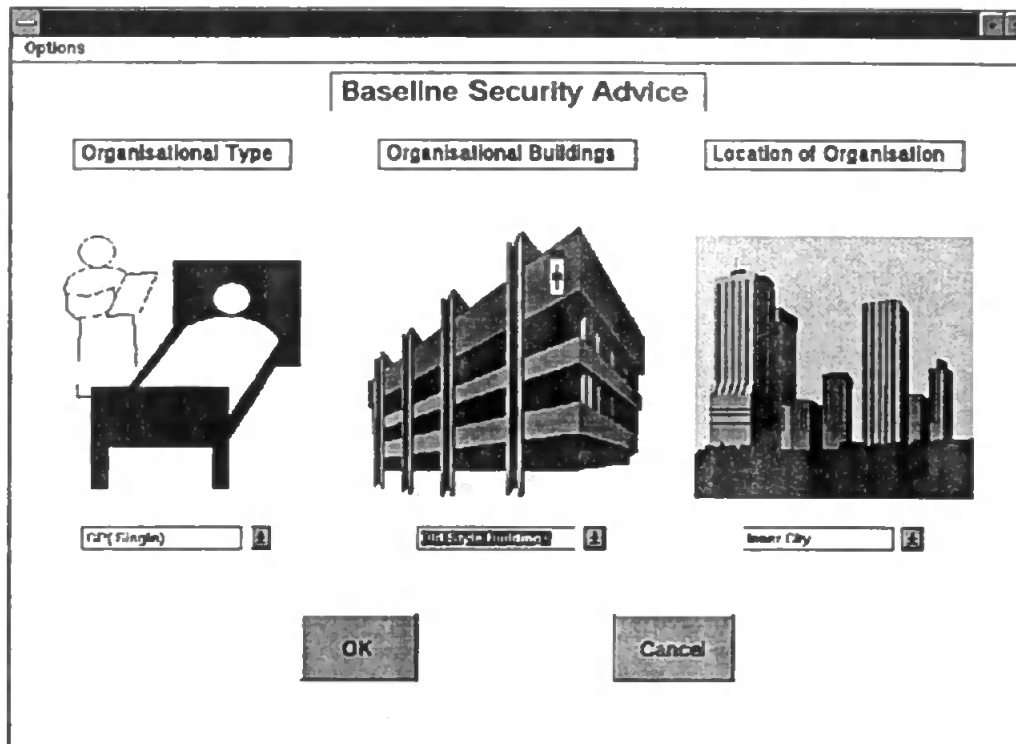
Fig 7.3. Baseline Security Requirements

ODESSA Function: Selections from this screen determine the organisational criteria

for selecting baseline security countermeasures.

Screen: Baseline Security Selection

Commands: The user can look at selected Countermeasures (CMs) by selecting:

Disaster	- shows baseline disaster CMs;
Hard/Software	- shows baseline hard/software CMs;
Physical	- shows baseline physical CMs;
Human	- shows baseline human CMs;
Special	- shows special CMs relating to the
	organisation.
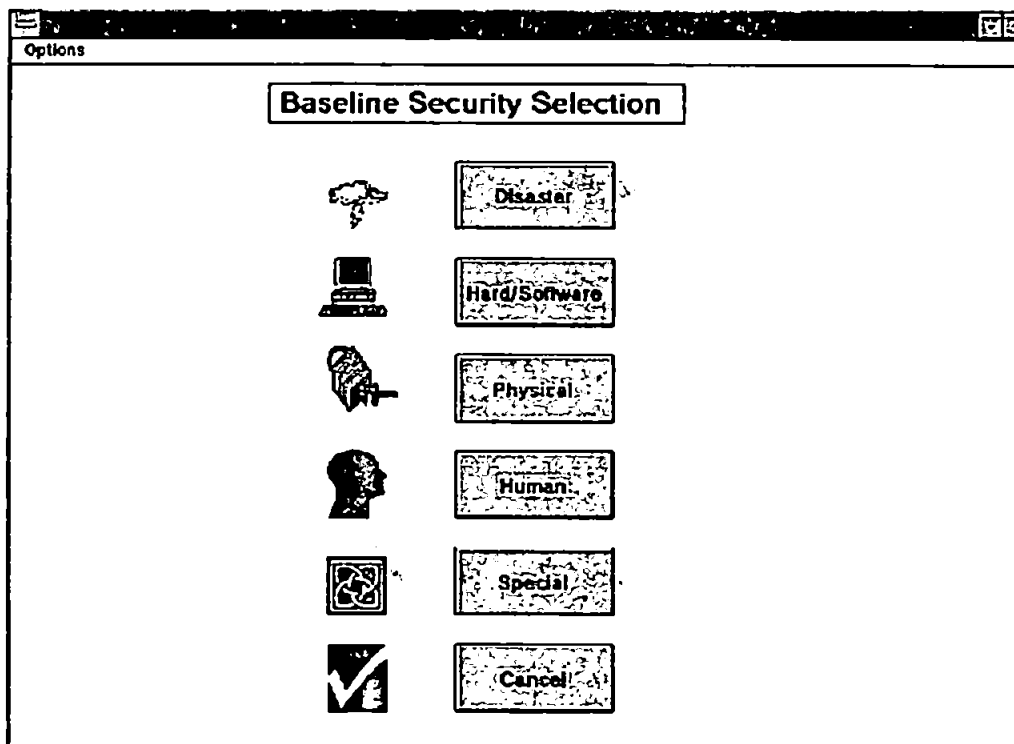
Fig 7.4. CM Selection

ODESSA Function: By viewing the CMs the user can select the ODESSA baseline

CM details for future use.

Screens: Baseline countermeasures for:

                        Disaster;

                        Hard/Software;

                        Physical;

                        Human;

                        Special screens.

Function: The user can interrogate the baseline countermeasures they

                        have selected. They can also print the CM details.

Fig 7.5. CM details

ODESSA Function: The user can look at the results of the baseline review.

Screen: Countermeasure overview screens (selected from main screen).

Function: The user can view all the baselines security CMs, e.g. look at

all disaster countermeasures groups.

Disaster Planning

Countermeasure Groups

☒ Fire Protection
☐ Water Protection
☐ Disaster + Damage Protection
☐ Continuity of Operation
☐ Equipment Failure Protection
☒ Power Protection
☐ Contingency Planning

OK   Cancel
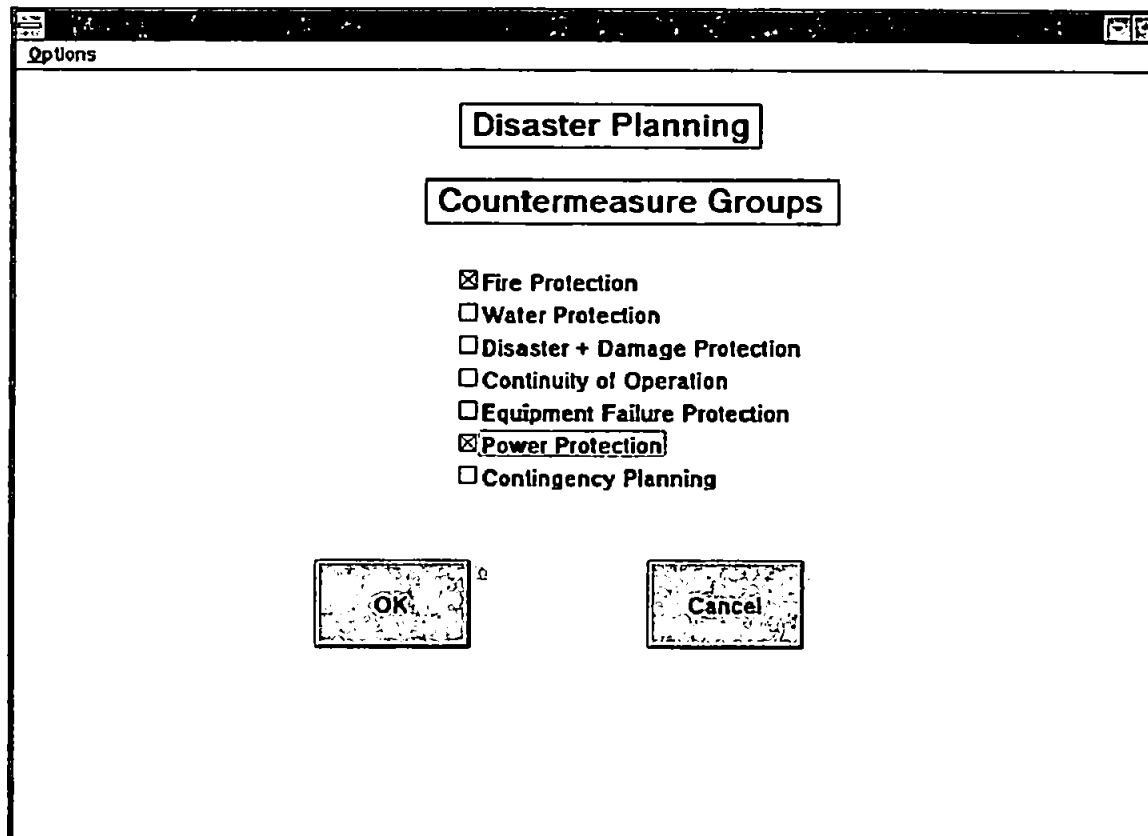
Fig 7.6. CM Groups

ODESSA Function: None.

7.3.2) ODESSA Stage 2

This stage is concerned with suggesting countermeasures which are unique to the

organisation. The unique countermeasures are defined by determining:

- organisations data usage;

- organisations data sensitivity;

- organisations security profile.

Screen: Organisational Selection

Function: This informs the user of their organisational type that they choose in a

              previous stage (useful if the user is running stage2 again).
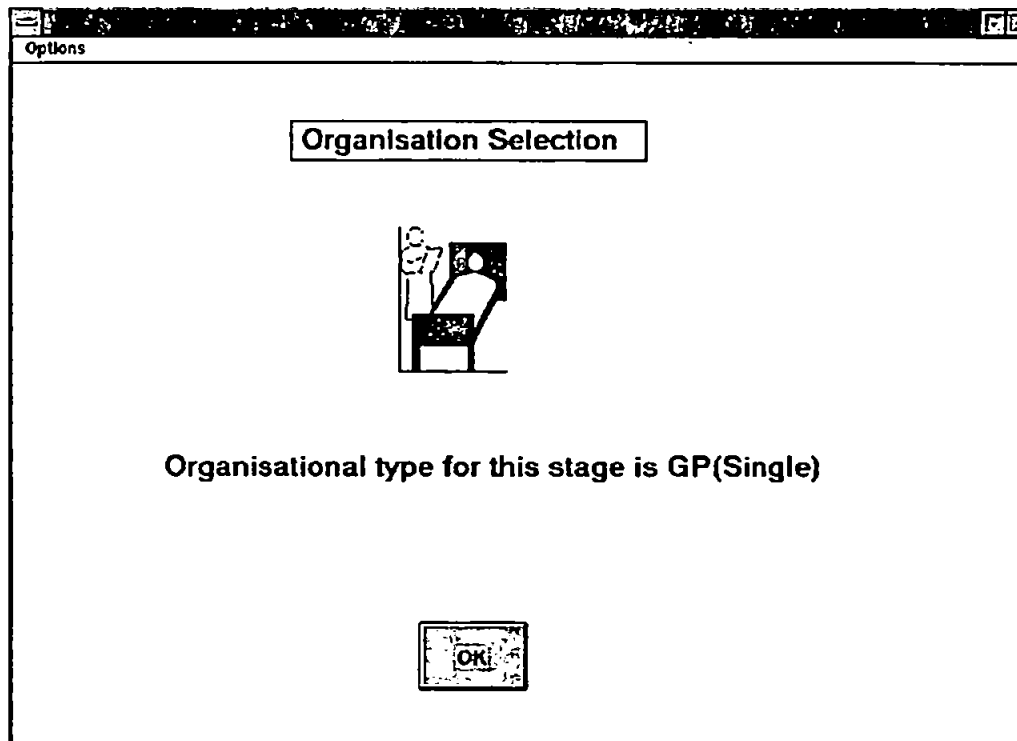
Fig 7.7. Organisational Selection

ODESSA function: None

Screen: Data Usage

Functions: This section of the prototype is not fully implemented (due to

                      time constraints). In the complete system the user would select

                      the data types and this would result in certain countermeasures

                      and predefined risk levels being set.
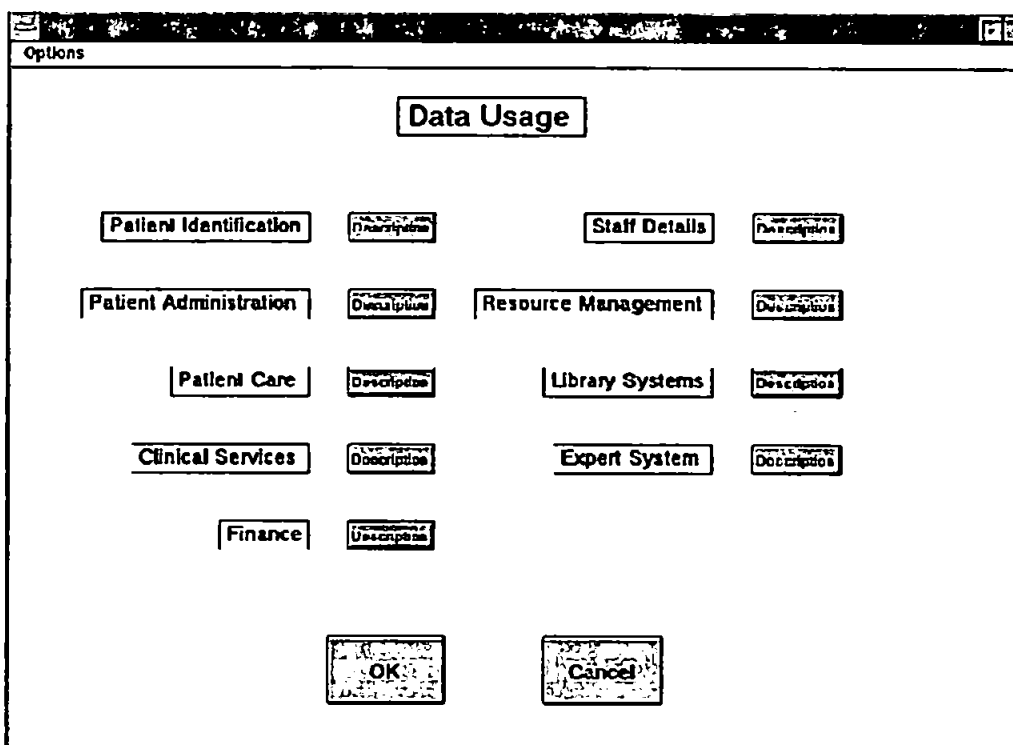
Fig. 7.8. Data Usage

ODESSA function: This determine the data use of the organisation. From this data

                   security countermeasure and risk levels can be defined, e.g.

                   data used for clinical decisions would be regarded as more

                   important then administration data, since clinical data is used

                   for the treatment of patients.

Screen: Data Sensitivity

Function: The user must answer a series of questions. The questions relate

                            to responses to different considerations and scenarios, such as:

- embarrassment;
- safety;
- privacy;
- legal;
- commercial confidentiality;
- financial loss;
- destruction of physical components.

The user must answer the questions relating to the scenario and

its impact on the following:

- denial of service;
- destruction of equipment;
- disclosure of data;
- modification of data.

Fig 7.9 Data Sensitivity Screen

ODESSA function: This stage of ODESSA determines the risk levels that are used

later within the system to allocate the level of required

countermeasures.

Chapter 7: Development of the ODESSA Prototype System

Screen:	Summary of Risk levels

Functions:	Once all of the questions have been answered a summary of risk levels are shown. These are rated as low, medium or high and as percentages.
	The user also has the option of viewing the risk levels as a graph.

Summary of GP(Single) Risk Level

	Risk Score %	Risk Level
Denial Level	60	Medium
Destruction Level	63	Medium
Disclosure Level	60	Medium
Modification Level	60	Medium
Overall Level	61	Medium

OK   Cancel   Graph   Print

Fig 7.10. Summary of risk levels

ODESSA function:	This informs the user of the risk levels, so when the countermeasure are suggested they have an idea of their magnitude.

Screen: Impact countermeasures

Function: User has the option to look at impact countermeasures relating

to:

                          - denial;

                          - destruction;

                          - disclosure;

                          - modification.

ODESSA function: Allows the user to look at the countermeasures determined by

the data sensitivity.

Screen:	Security Profile Selection
Function:	In order to determine a unique security profile, the user must

answer a series of questions. The questions relate to the

following areas:

- disaster;

- hardware/software;

- physical;

- human.
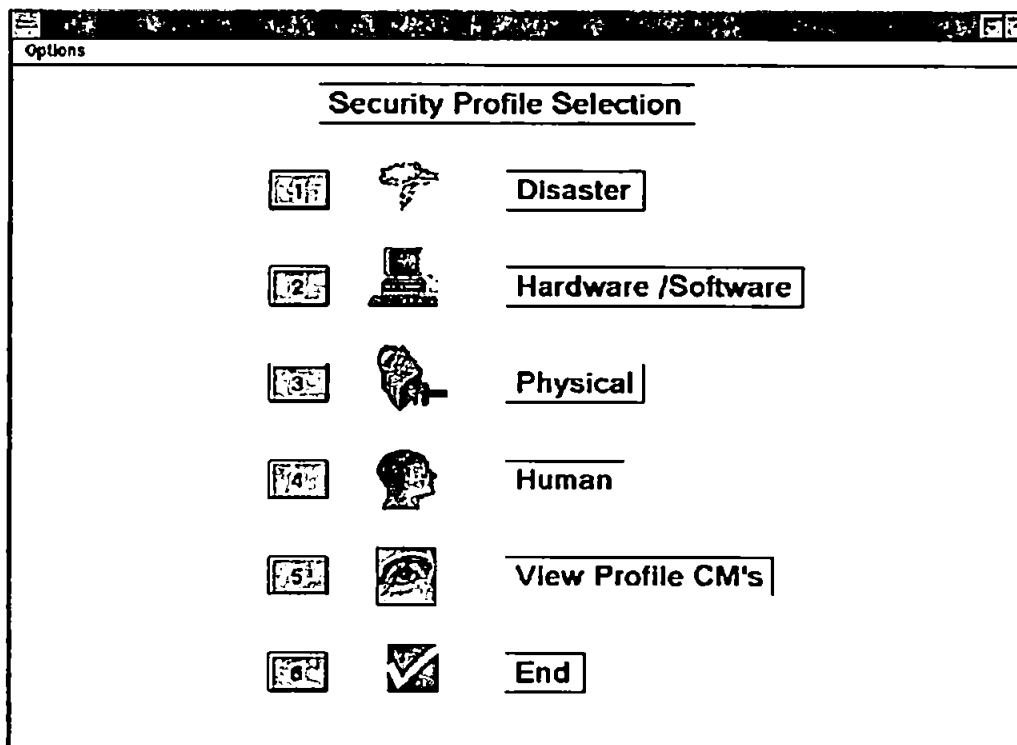
Fig: 7.11. Security Profile Choice

ODESSA function:	The user must answer a series of questions that are unique to

their organisation. Countermeasures recommened are

dependant upon their replies.

Screen: Disaster, Hardware/Software, Physical and Human Profile

           questions.

Functions: The user must answer a series of questions by selecting 'Yes'

           or 'No'.
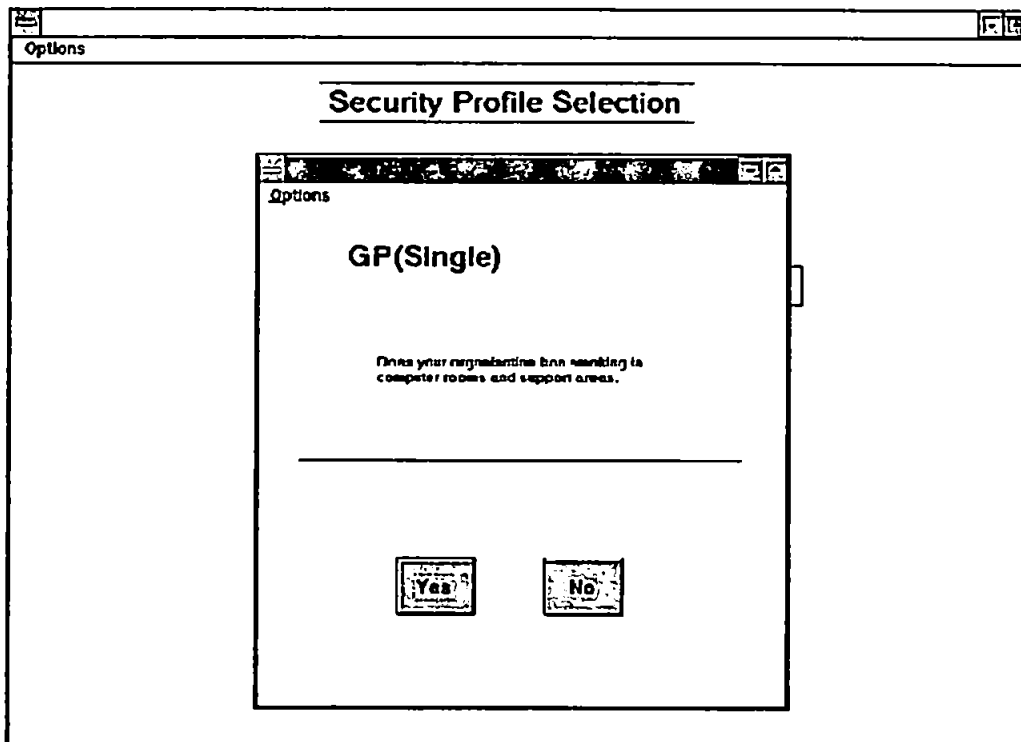
Fig 7.12. Security profile questions

ODESSA function: This part of ODESSA produces countermeasures that are

         unique to the organisation. This is because they are asked about

         existing equipment or procedures.

Screen: Profile Countermeasure Selection

Function: The user can select which profile countermeasure groups they

wish to see. The groups are:

- disaster;

- hardware/software;

- physical;

- human.

ODESSA function.   The user can look at the countermeasures which have been

produced via the profiling section of ODESSA2.

7.3.3) ODESSA Stage 3

The stage is used to review the countermeasures organisational impact. The SIM-ETHICS methodology is used to evaluate the impact of the countermeasures. This stage will currently only work GP (single) and GP (Practice) because of time constraints during the development of the prototype.

Screen: ODESSA Impact Analysis Screen

Function: The user can select the following:

     - view baseline countermeasures;

     - view ODESSA stage 2 countermeasures.
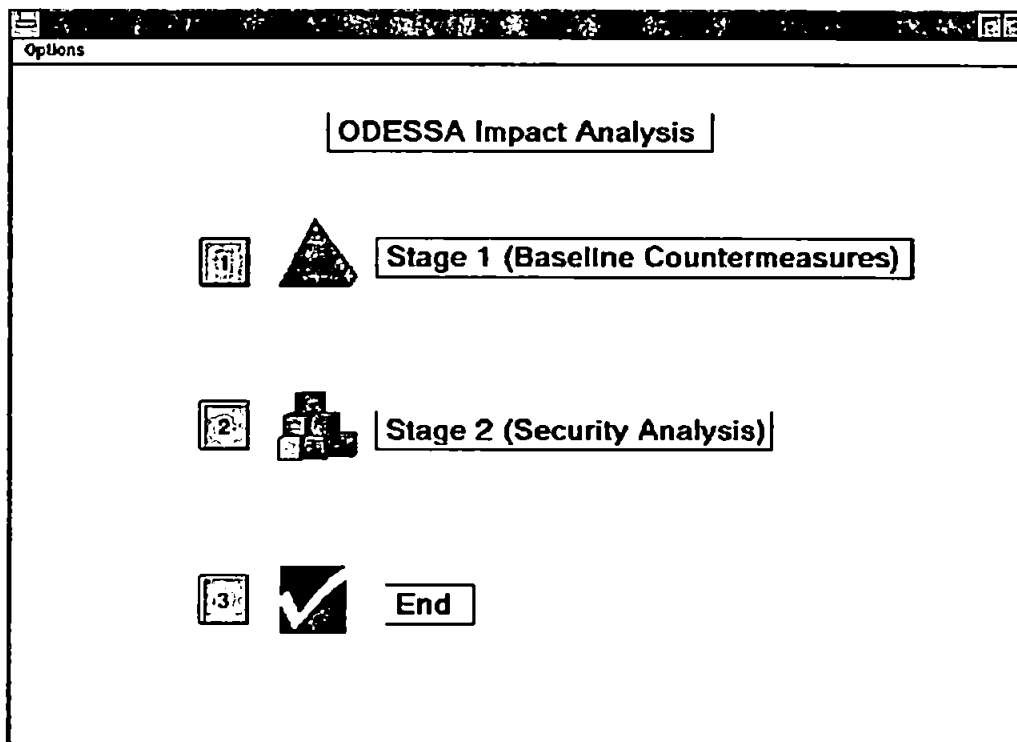
Fig 7.13. Impact Analysis Choices

ODESSA Function: None.

Screen:	Baseline countermeasure screen

Function:	The countermeasures groups selected from ODESSA stage 1 are displayed. If a group cannot be selected, a message appears informing the user of this fact (the screen is displayed over the previous screen).
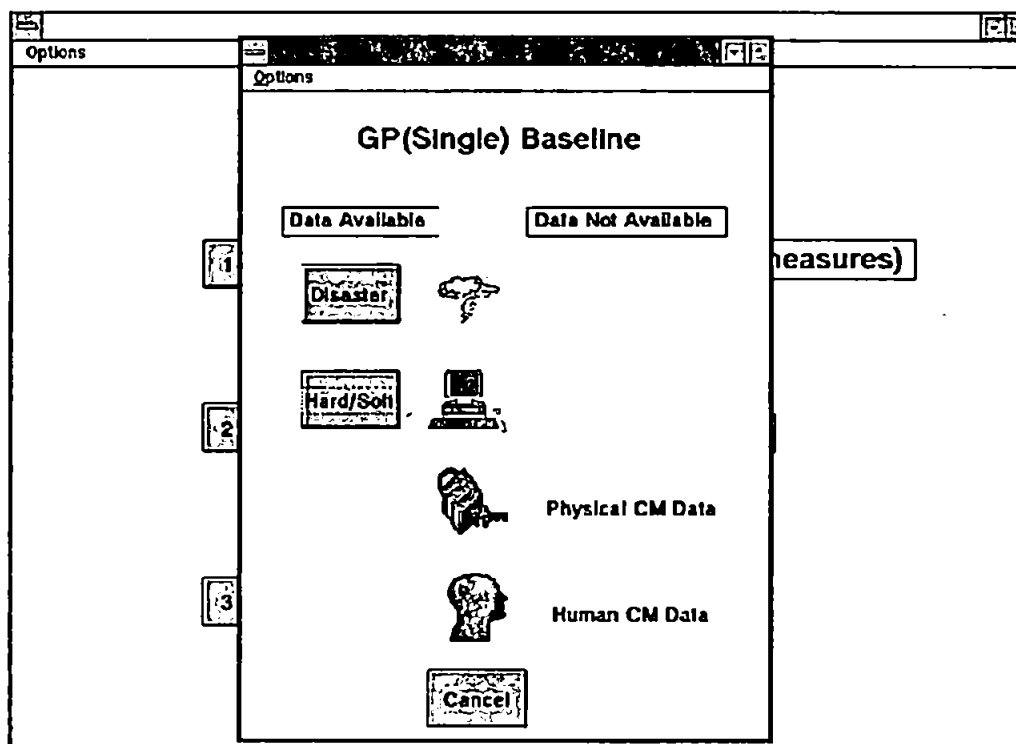
Fig 7.14. Baseline Countermeasure Groups

ODESSA function:	None.

Screens   Disaster, Hard/Software, Physical, Human countermeasures screens.

Functions: Shows baseline countermeasures. By clicking on a countermeasure the

               SIM-ETHICS impact is described (the screen is displayed over the

               previous screen).
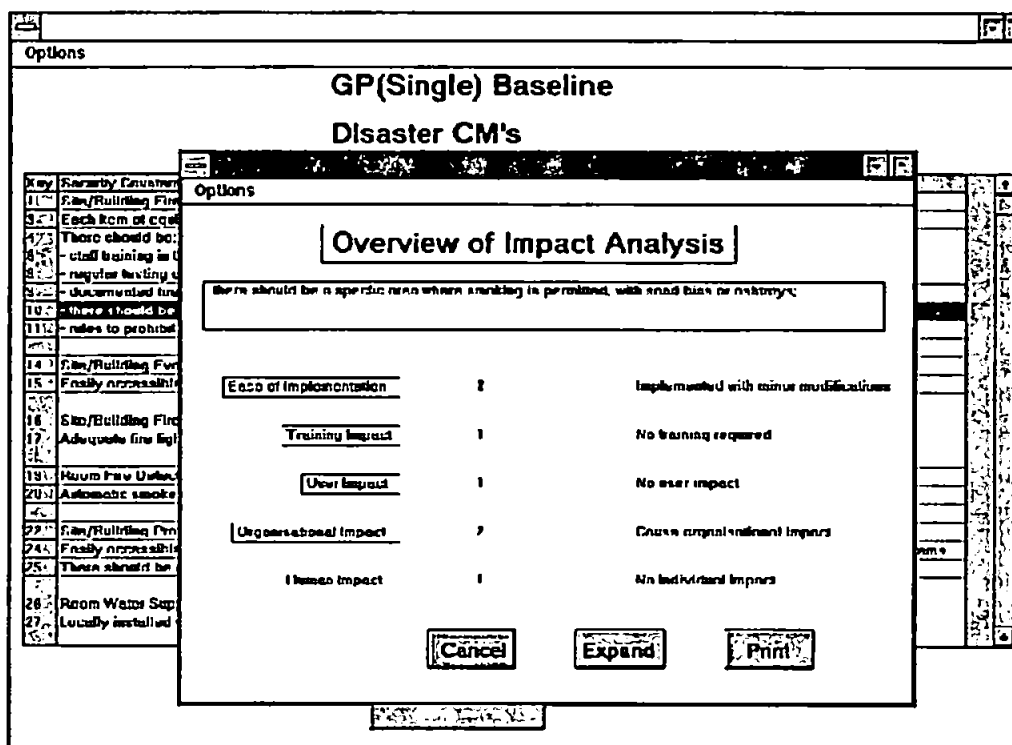
Fig 7.15. Impact analysis of countermeasure

The user can expand the impact analysis details by clicking on the

expand button. This gives a more descriptive analysis of the

countermeasures impact, as shown next.

Fig 7.16. Expanded Impact Analysis

ODESSA Functions: This part of the system demonstrates the SIM-ETHICS

analysis of the data. The analysis determines the organisational

impact of introducing baseline security.

Screen:	ODESSA Stage 2 Countermeasure details

Functions	The user can select which countermeasure to look at. The countermeasures are:
	
	    - sensitivity countermeasures;
	
	    - profile countermeasures.
	
	This screen is displayed over the ODESSA Impact Analysis Screen.
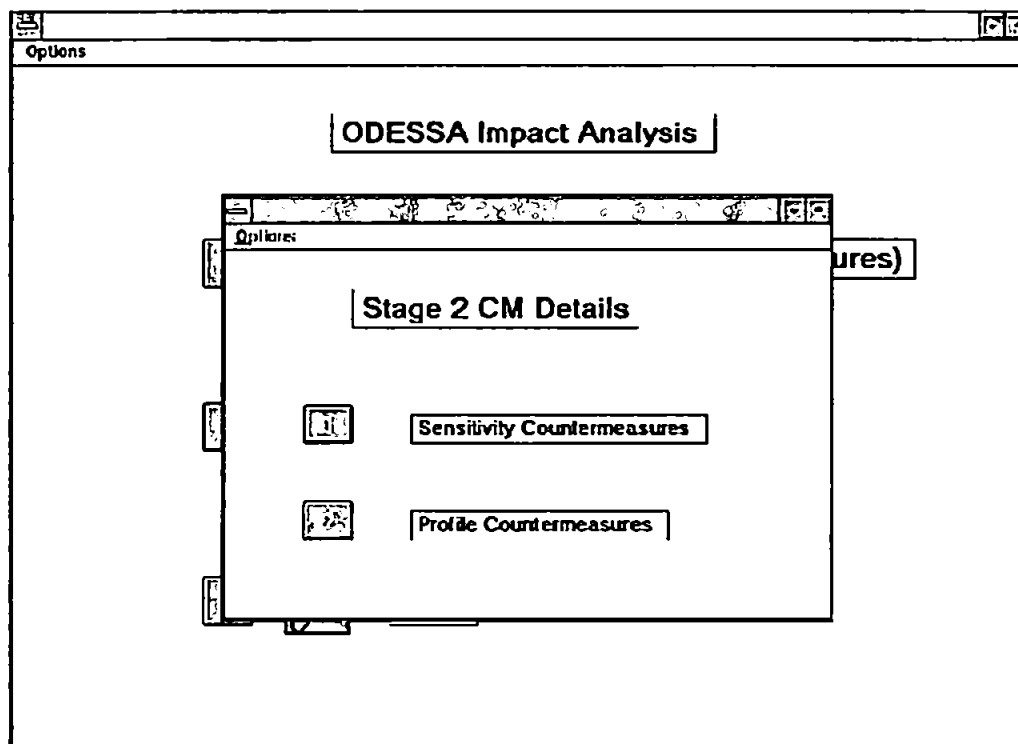
Fig 7.17. ODESSA Stage 2 Countermeasure Selection

Screen:	Sensitivity countermeasure screen
Function:	The user can look at the different sensitivity countermeasures that were chosen. The countermeasures relate to the following impact areas: denial; destruction; disclosure; modification.
	The user can select a countermeasure which then summarises its organisational impact. The user can expand this to a more descriptive analysis.
ODESSA function :	This part of the system demonstrates the SIM-ETHICS analysis of the data. The analysis determines the organisational impact of introducing impact security countermeasures (the screen is identical to Fig 7.15).

Screen: Profile countermeasures screen

Function: The user can look at the different profile countermeasures

that were chosen. The countermeasures relate to the following

profile groups:

- disaster;

- hardware/software;

- physical;

- human.

The user can select a countermeasure which then summarises

its organisational impact. The user can expand this to a more

descriptive analysis.

ODESSA function :   This part of the system demonstrates the SIM-ETHICS analysis

of the data. The analysis determines the organisational impact

of introducing the unique profile countermeasures (the screen is

identical to Fig 7.16).

7.4) Limitations of the ODESSA system

As described earlier the system was designed as a prototype. This means that the system is not fully developed and the following issues will have to be resolved to develop a complete system:

- stage 3 of ODESSA will currently only work for GPs and new data will have to be created to extend stage 3. The system will then be able to determine the impact analysis for community healthcare units and hospitals as well;

- a full set of countermeasures will have to be developed;

- the help facilities will have to be extended;

- certain features of the system have yet to be implemented (e.g. data usage in ODESSA stage 2);

- some print routines are not fully implemented.

7.5) Conclusion

This chapter has explained the development of the ODESSA prototype, it explained:

- the design considerations;

- analysis of the separate stages of the ODESSA system;

- limitations of the ODESSA prototype.

Future areas of development are explained in chapter 9, which presents the conclusions of the research.

Chapter 8: Validation of Research

8.1) Introduction

The development of new methodologies as the solution to a problem is insufficient in itself. The solution must be validated in order to determine its quality and worth. The validation of the new methodologies previously described took the following form:

- the SIM-ETHICS methodology was validated by using it within a

    HCE environment;

- the ODESSA methodology was validated by sending details and in some

    cases the prototype system to security experts for evaluation.

8.2) Validation of the SIM-ETHICS method

The following countermeasures were being implemented within the Plymouth and Torbay Health Authority. It was decided to use the maternity ward as a pilot study area to elicit views from users via the use of SIM-ETHICS regarding the following (as described in chapter 4).

1.   A new access control system;

2.   A new password procedure;

    (this was changed to the concept of password use

    and the users were only approached about this matter)

3.   A new computerised information system.

In total 15 users were interviewed from the maternity department representing a cross section of users within a very small department. These are broken down into the following groups;

Management 2

Administration Staff 4

Medical Staff 9

The questions asked in the review can be found in the Appendix.

8.2.1) SIM-ETHICS Review

The maternity managers were interviewed relating to the introduction of:

- access cards;

- computerised information system.

The aim of the review was for the users to raise concerns which the management could resolve.

8.2.2) Managers view of Access Cards

Overview

These cards will have dual use as they will be used to enforce access control of selected areas and will also be used as identification cards.

Access control systems are being implemented in the following areas:

- child health;

- maternity units;

- certain external doors.

At the moment access card control systems are used in:

- pharmacy;

- hospitals main computer suite.

The access control cards will be controlled by a central computer system based in the main security office. This system will record details of which areas staff have access to and where staff are present.

Training

Training will consist of a talk to a number of users. This talk will explain the basic operation of the system and how the cards work.

Problems

Ensuring that staff are made aware of wider issues, e.g. the fact that the card expires if it is not used for 30 days.

The number of people being trained could cause problems, e.g. child health directorate has around 1000 staff. If the access control system is implemented across the whole organisation, around 4000 staff will have to be trained. This excludes the

use of cards by visitors. It is planned that all 15 external doors would be controlled by the use of access cards.

Comments

The system managers have to inform security about new staff so that they can be given a card.

Problems may occur in the future if all the access card systems are not standardised.

8.2.3) SIM-ETHICS evaluation of Access Cards

Ease of Implementation

Implemented with an extensive amount of effort. Therefore certain areas of the hospital will have access control before others.

Training

Training is needed on one of two levels, departmental or the whole organisation.

Training could be implemented by a mixture of:

- demonstration of cards to certain staff, e.g. system managers within the

department, so these staff can train the rest of the department;

- circulation of leaflets explaining how to use the cards and what to do in

unusual circumstances, e.g. staff losing their card.

Organisational Impact

The countermeasure could affect the way minor tasks, e.g. cleaning staff may feel it is inconvenient to use an access card.

The countermeasure will change the culture of the organisation. It will help to enforce the 'Security Culture' concept to staff and may be combined with security awareness programs to promote this even further.

8.2.4) Users view of Access Cards

Overall

Access cards were accepted as being needed and there was overall support for implementation. It was also accepted that it would help raise security awareness amongst staff.

Training

It was the general consensus that managers should be trained on how to use the system. They could then train the remaining staff and help with any problems, e.g. loss of cards.

Issues Raised by Users

Users would like the following:

- procedures should be in place to quickly cater (i.e. in and out of normal working hours) for staff replacement of cards;

- procedures to quickly change individual access rights within the wards.

General questions raised by users were;

- how reliable is the access card equipment?

- how easily could be the card be damaged accidentally or just through general

use?

Operational Questions raised by users:

-how would access cards be issued to visitors and how should they be held

accountable for these cards?

- how can staff verify that visitors are related to children, e.g. an uncle?

- would there be an override facility on the access control system in case of

emergency?

- would the access cards system become inoperative during a fire or large

medical emergency?

Other Points

The use of access cards could help to stop children leaving the wards and wandering

around the hospital.

Some staff were concerned about the time it may take them to realise that their card has been stolen, during which time the thief would have their access privileges.

Staff were in favour of having access control mechanisms on the drug dispensing units. Staff felt that the use of the system would stop any thefts that might otherwise occur.

Staff felt that they initially would have to be reminded about wearing their ID badges, since it acts as the access card.

8.2.5) Managers view of VTX (Video TeXT system)

Overview

VTX is a system that is used to display various types of HCE information, e.g. hazard notices, clinical information, ward procedures or urgent information. The aim is to ensure that users are given the information that is relevant to them.

The notices will be sent out via a distribution list. Once a notice has been read a message will be automatically returned to the system to signify this event.

Another aim of VTX is to use the system within clinical departments to circulate details relating to practice guidelines, surgeon protocols, and the like.

Pilot Stage

This stage will be used for the transmission of safety and hazard notices to business managers, clinicians and departmental heads. The pilot stage will then be extended to cover clinical procedures for haematology.

Training

Users will be given a simple instruction guide and there will also be open days explaining how to use the system. The system itself is designed to be simple to use. Training within clinical departments should be top down to ensure that common procedures are used in each department. This is important in clinical teams where non-IT staff (e.g. nurse) would be the main users.

Problems

Accuracy of the information entered on the system is very important, e.g. is the intended drug dosage data relevant for children. It is important to control which people have the right to put information onto the system.

If the system becomes very successful it could 'snowball', with the systems original aims being forgotten and non-relevant information being entered on the system.

Comments

The system is what the users want rather then something that is being forced upon them. The system is likely to grow as a result of the users demanding more from it..

8.2.6) SIM-ETHICS evaluation of VTX

Ease of Implementation

Implemented with an extensive amount of effort. Implementation will be based upon user types and areas, e.g. system managers, business managers, clinical areas.

Training

Training needs to be given to a few people (e.g. system managers) who can then train others. Because the system is designed to be user friendly, it is assumed that staff would not have difficulty using it. If users have problems they should be able to contact their system managers.

User Impact

VTX should help to improve user satisfaction through the use of the computer system. VTX should also improve users job efficiency and effectiveness.

Organisational Impact

The use of VTX will dramatically change the way notices and guidelines are distributed within the organisation.

The culture of the organisation may change in the following ways:

- the organisation moves towards a greater acceptance of IT;

- the organisation accepts IT in ways that were not planned for, e.g. VTX

    expands to cover new areas such as Community Health;

- the system 'snowballs' and similar systems are developed, e.g. notice boards;

- the development continues until it is out of control and problems

occur, e.g. inaccurate information being entered on the system.

Human Issues

Certain jobs may be restructured, e.g. the person who currently photocopies staff notices may have this duty taken away.

8.2.7) Users view of VTX

Overall

It was felt that the VTX system would help to overcome the problem of large numbers of memos being sent within the organisation.

Training

User made it clear that any training information sent with monthly paycheques would be ignored.

The users expect a comprehensive VTX training manual to be produced.

Users expect key staff to be fully trained so that they could train the remainder of the staff.

Any training conducted during dinner break would not be acceptable to staff.

<u>Issues Raised by Users</u>

<u>Practical problems</u>

The following points were raised by users.

> - What would happen if the system fails?
>
> - There is a problem due to lack of terminals in wards, existing terminals are
>
>   heavily used for clinical systems.
>
> - Which members of staff would get the task of entering the information on
>
>   the system?

<u>Technical Problems</u>

The users enquired about the following:

> - is it possible to determine who sent the memo?
>
> - is there an option to print the memos?
>
> - would there be a facility to save and retrieve memos?
>
> - how would the system prove that staff have read memos sent?

<u>Other Points</u>

Some staff (e.g. nurses) would not fully trust all the information displayed on the terminal, this is because they are not confident in the use of IT.

There was some concern about the type of information that could be entered on the system, e.g. confidential information.

Some staff had worries relating to the fact that information displayed on screen is not legally treated the same as written information.

Some staff suggested that the VTX system may cut down human interaction, which they see as being very important.

8.2.8) Users View of Passwords

Overall

Users see the overall need for passwords on computer systems.

Issues Raised

Users wonder if the frequency of password changes should be related to their individual usage of a system.

Users would prefer to define their own passwords rather then be given computer generated passwords.

Problems

Users were unhappy about having one password for each system, especially when they use three or four systems. They would prefer one password that would give them access to all systems.

Some users have never changed their passwords (in some case for as long as four years).

Users are unhappy about certain systems because they have to change passwords every three months.

Some users have a written record of their passwords, e.g. written on the back of their ID card.

8.3) Findings of SIM-ETHICS review

The appropriate managers were given a series of problems that the users raised, the now had to overcome these before the actual implementation of the countermeasures and computer systems. The review raised many points which management had not considered.

The findings of the review were given to :

- the appropriate system managers concerned with implementation;

- the Plymouth and Torbay Health Authority security forum.

The SIM-ETHICS review provided impetus in the production of an authority wide security policy. The results of the SIM-ETHICS review were cited to show a need for a security policy.

8.4) Validation of the ODESSA method

The ODESSA method was validated by experts during its development from paper based methodology to computer prototype. The validation took the form of correspondence, direct meetings and questionnaires. The findings of the validation process are presented in the pages that follow, citing feedback from specific individuals who were consulted.

Name: Professor Enid Mumford (Manchester Business School)

Country: UK

Expertise: Developer of the ETHICS methodology

Medium: Correspondence

Comments:

> She was sent a copy of a paper (Warren, Sanders and Gaunt, 1994) relating to ODESSA. She thought that the system seemed an excellent way of securing user co-operation and identification with a new computer system. She thought one of its major objectives would be to give future users a sense of ownership. She was sure there must be a large market for the kind of system that was being developed.

Name: Mr Avraham Hayam

Country: Israel

Expertise: Security Consultant

            Co-chairman of MIE 93 Security session

Medium: Correspondence

Comments:

Mr Hayam considers himself to be a pioneer of IT security in Israel, he

is trying to introduce the use of expert systems in risk analysis and

audit evaluation. Mr Hayam was sent the initial model of ODESSA.

He thought that the model could be improved by adding data

sensitivity (which it was). He liked the model of classification relating

to disclosure, denial, modification and destruction.

Name: Mr John Davey

Country: UK

Expertise: Security consultant

            Project manager of SEISMED project

            Help developed CRAMM

Medium: Direct Meetings

Comments:

Mr Davey assisted with various problems that occurred relating to

the use of CRAMM. Mr Davey also assisted by validating the early

conceptual design of the ODESSA method. The original ideas were

based upon the production of an expert system, as shown in fig 8.1.
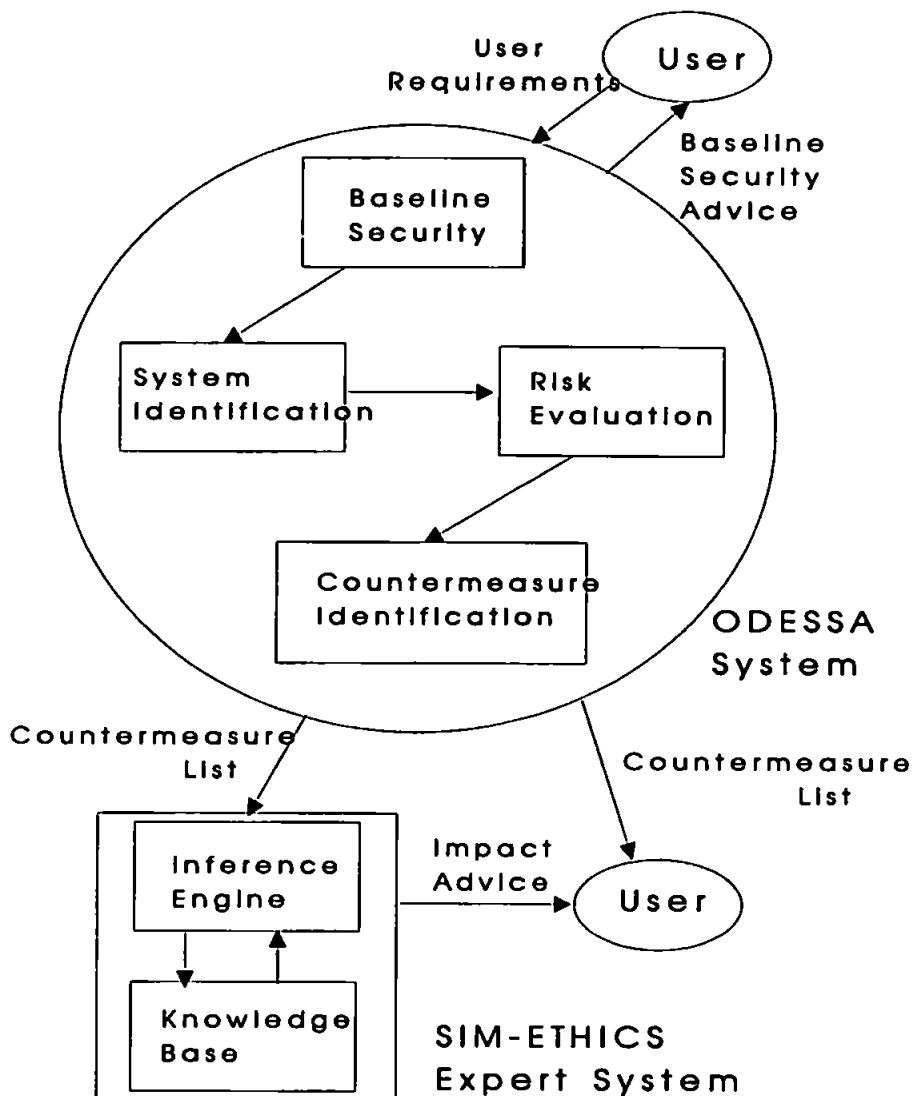
Fig 8.1. Early Conceptual view of ODESSA

Figure 8.1 is explained as follows.

The ODESSA system is broken down into the following:

1) Baseline Security   - the user is given basic security advice for their

                                     organisation;

2) System Identification   - system assets are evaluated;

3) Risk Evaluation   - risks and vulnerabilities are determined;

4) Countermeasure   - appropriate countermeasures are produced.

      Identification

SIM-ETHICS Expert System

The expert system takes the countermeasure lists produced by the ODESSA system and determine the impact that their implementation could have.

Name: Mr John Fowler

Country: UK

Expertise: Head of IT at Royal Hospitals Trust, London.

            Member of SEISMED project

Medium: Direct Meetings and questionnaires.

Comments:

Mr Fowler was sent a copy of the ODESSA prototype to evaluate. He thought " I was on to a potential winner". He liked the idea of an overview impact analysis (Stage 3 of ODESSA), something that is missing from CRAMM. He would like to see OLE (object linked embedding) added to allow the use of word processing packages. The printing was considered slow, although he felt that this was a fault of Windows rather than ODESSA. The data produced by the system was useful and he found the system beneficial as a source of security advice.

Name: Mr Erik Flikkenschild

Country: Netherlands

Expertise: IT manager at Leiden University Hospital

Member of SEISMED Project

Medium: Direct Meetings and questionnaires.

Comments:

Mr Flikkenschild was sent a copy of the ODESSA prototype to

evaluate. He found the system simple to install and set up, he also

found the user guide very helpful. He found the system easy to use

and found the data produced by the system useful. Mr Flikkenschild

particularly liked the graphics, but would have liked to seen healthcare

related icons (this will be added at a later stage).

8.5) Conclusion

This chapter has proven the worth of the methodologies that were developed. SIM-
ETHICS has been proven by actually using it in real life situations to determine the
problems of implementing security and IT systems. ODESSA has been validated
though its developmental life cycle by experts and, as such, has proven itself in terms
of its applicability and quality. In addition, the fact that people were so enthusiastic
about the methods proves that there is a genuine need for them.

Chapter 9: Conclusions

9.1) Achievements of the Research Program

The research programme has met all of the objectives originally specified in chapter 1. New conceptual and practical work has been developed in a number of areas, as listed below.

1. The project helped to determine the need for information security for HCEs. This took the form of working extensively within HCEs, meeting users and seeing their requirements for security at first hand.

2. The work within the AIM SEISMED project allowed the production of new security guidelines. These guidelines were validated by meeting users within HCEs and discussing the issues.

3. A new management method was developed that could be used to assist with the implementation of security within healthcare. This method was proven by using it within a HCE during the implementation of 'real world' security features and computer systems.

4. The current use of risk analysis security packages was assessed. The resulting list of methods represents one of the most comprehensive lists of its kind.

5. A new risk analysis methodology was developed specifically for use within healthcare. This will allow HCE staff to carry out security reviews of their own systems (i.e. without requiring external consultants).

6. A security prototype was developed that fully encapsulated the new risk analysis management method.

7. By combining the use of SIM-ETHICS and ODESSA a new method of handling the life cycle of security has been developed, as shown below:

- identification of organisational security needs;

- assessment of an organisation to determine needed security

features;

- implementation of security features;

- determination of organisational impacts.

Several papers relating to the research have been presented at referred conferences, with favourable comments being received from other delegates. Several papers have also been published in refereed journals. As such, it is believed that the research has made valid contributions to the IT security field in terms of the healthcare field, as well as at a more general level.

9.2) Limitations of the Research

Despite having met the overall objectives of the research, it is possible to identify a number of limitations associated with the work. These points are presented below.

1. The ODESSA methodology, whilst complete in terms of the overall framework and associated prototype, cannot be considered viable until it is developed into a full working system. However, due to time constraints it was not possible to do this.

2. The review of risk analysis method was limited by the fact that organisations are reluctant to give any significant information about their products. This is because it could indicate the type of security countermeasures that they have installed.

9.3) Suggestions and scope for future work

It is possible to identify a number of areas in which further work could be conducted to build upon the research already undertaken. There are a number of areas where direct continuation of research could take place as follows.

1. Development of the ODESSA prototype into a full working system, which would potentially produce a marketable commercial product. As part of the development, extensive studies within HCEs should be

undertaken to look at the applicability of countermeasures. These reviews would further enhance the applicability of the system.

2. Further research into the use of ODESSA and SIM-ETHICS within other commercial sectors (although they originally developed for healthcare). This would help determine if the methods can be used in a more generic manner.

3. More extensive research into the known risk analysis methods. This information is very scare so any further research will enlighten the risk analysis practitioners.

4. More research is needed into the human aspect of security . This research is required because security is a human issue (Warren and Gaunt, 1993) and the most advanced security mechanism will fail if users do not wish to use it.

5. The area of security management has not been extensively researched and new work in this area is therefore desirable.

9.4) Conclusion

The development of the ODESSA method is at the forefront of research in its area. Further work will be needed in developing this "logical transformation" style of risk analysis method.

The work described is the product of real world experiences. This was carried out by working within a HCE and looking at the real life requirements for security, which help to validate its applicability.

There is always going to be a need for security within healthcare. A main reason for this is that technology changes and therefore the way that technology is implemented will change. The improved technology would have even greater impact to staff and their job functions.

The future use of the 'Internet' for business and leisure will truly allow the globalisation of IT systems. These new network technologies will have a major impact on all aspects of society including healthcare. It is for this reason that the role of healthcare will change in the next millennium. The future ISHTAR project will help to develop the use of these new technologies by healthcare.

References

1. ACOSTA. 1994. *Telematics for Healthcare: Its impact ? Its future ?,*

   Produced by for the Commission of the European Union AIM programme,

   France.

2. Adams R. 1984. *Participation Today,* The Industrial Participation

   Association, UK, ISBN 0-9503090-36.

3. Addison S. 1991. *Cobra Risk Consultant - "The next generation of Risk*

   Management Software ", C & A Systems Security Limited, UK.

4. Al-Hahhah M and Bamgboye E. 1992. "Attitudes and opinions of medical

   staff towards computers", *Computer Biological Medicine,* Vol 22, No 4, UK.

5. Anderson A and Shain M. 1991. *Information Security Handbook,*

   Stockton Press, UK, ISBN 0-333-51172-7.

6. Audit. 1994. Audit Commission Report - *Opportunity makes a Thief,*

   (An analysis of computer abuse), HMSO, UK, ISBN 011-886137-9.

7. APSAIRD and CLUSIF. 1988. *Marion - Examples of Major Computer*

   Security Breaches, Coopers and Lybrand, UK.

8.   Avison D.E and Fitzgerald G. 1989. *Information Systems Development,*

Blackwell Scientific Publications, UK, ISBN 0-632-01645-0.

9.   Barber B. 1992. *Information Management Group Security,*

IMG Marketing Document, UK.

10.   Baratte E. 1989. "Marion: A method for measuring and improving security in

EDP systems",*Proceeding of IFIP Conference,* Elsevier Science Publishers,

The Netherlands.

11.   Baskerville R. 1993. "Information System Security Design Methods:

Implications for Information Systems Development", *ACM Computing

Surveys,* Vol 25, No 4, USA.

12.   Barber B and Davey J. 1994. "Approaching Safe and secure health

information systems in Europe", *Guidelines for the Security of Health

Information,* University of Thessalonkiki, Greece.

13.   Bodeau D. 1992. "A conceptual model for computer security risk analysis",

Proceeding 8th Annual Computer Security Application Conference,

IEEE Computer Society Press, USA.

14.   Carroll J and Mac Iver W. 1985. "COSSAC: A framework for analysing and configuring secure computer facilities", *Computers and Security*, Issue 4, UK.

15.   CCTA. 1992. *An Overview of CRAMM*, CCTA, UK.

16.   CCTA. 1993. *Baseline Security for IT Systems*, CCTA, UK.

17.   CESG. 1992. *CESG (Communications Electronic Security Group), Memorandum Number 10*, UK.

18.   Ceustres W. 1993. The aim of the nineties bringing multimedia records to life, *Proceeding of MIE 93 Conference*, Israel.

19.   Clark D.D and Wilson D.R. 1987. A Comparison of commercial and military computer security policies, *IEEE Symposium on security and privacy*, Computer Society Press, USA, ISBN 0-8186-0771-8.

20.   Computer Select. 1995. *Computer Select CD* (Software Product Specification), USA.

21.   Coverson R. 1991. Report of Computer Security Review, *Securities and Investments Board (SIB)*, UK.

22. Coopers and Lybrand. 1989. *"Marion (Information Systems Security)"*, UK.

23. Courtney R . 1977. "Security risk assessment in electronic data processing", *AFIPS Conference Proceeding of the National Computer Conference*, USA.

24. Digital. 1991. *Data Center Evaluation Checklist*, Digital Equipment Corporation, UK.

25. Davey J and King S. 1995. *Guidelines for Health Care Security Risk Analysis for Healthcare IT and Security Personnel*, AIM SEISMED Deliverable SP05.5, HEIMDALL, UK.

26. Davies S. 1995, "Doctors oppose NHS database", Sunday Times, 4th June, UK.

27. DTI (Department of Trade and Industry). 1993. *A code of practice for Information Security Management*, British Standards Institution, UK, ISBN 0-580-22536-4.

28. Eloff J and Badenhorst K P. 1990. "Managing computer security: Methodology and Policy", *Information Age*, Volume 12, No 4, UK.

29. Fagen P. 1993. Organisational Issues in IT Security, *Computers and Security*, Volume 12, No 8, UK.

30. FIPS 65. 1979. *Federal Information Processing Standards (FIPS) Publication 65*, Department of Commerce, USA.

31. Fitzgerald K. 1993. "Risk Analysis: Ten Years on", *Information Management and Computer Security*, Vol 1, No 5, UK.

32. Furnell S.M, Gaunt P.N, Sanders P.W and Warren M.J. 1993. *Generic Data Model Methodology Refinements*, AIM SEISMED SP07.0.8, UK.

33. Furnell S.M and Sanders P.W. 1994. *Security Guidelines for Existing Healthcare Systems*, AIM SEISMED, Deliverable 26, UK.

34. 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, UK.

35. Furnell S.M, Sanders P.W and Warren M.J. 1995. Development of Security Guidelines for Existing Healthcare Systems, *Medical Informatics*, Vol 20, No 2, UK.

36.   [1]Furnell S.M, Gaunt P.N, Holben R.F, Sanders P.W, Stockel C.T

and Warren M.J. 1995. "Assessing staff attitudes to information security in a

European healthcare establishment", *Awaiting publication in Medical*

Informatics, UK.

37.   Furnell S.M, Sanders P.W and Warren M.J. 1996.

"Provision of healthcare security information services using the World-Wide

Web", *Awaiting acceptance to MIE 96.*

38.   Gaunt P.N, and. France R.F. 1993. "The need for security in health care

information systems [A Clinical View]" , *SP11.02.A08.02,*

AIM SEISMED Internal Project Report, UK.

39.   Gliss H. 1990, "A Survey of Computer Abuse (Germany)",

Proceeding of CompSec Conference, UK.

40.   Guardian. 1995. "Hospital 'buys in' Police", 4th September, UK.

41.   Guarro S.B. 1987. "Principles and Procedures of the LRAM Approach to

information system risk analysis and management", *Computers and Security*,

Issue 6, UK.

42. Holben R. 1995. "Attitudes to information security in healthcare establishments", *BSc(Hons) (Business Information Management Systems) Final Year Project*, Plymouth University, UK.

43. Hudoklin A and Smitek B. 1992. "Security of Computer Supported Information Systems - State in Slovenia", *Proceeding of International Conferences on Organisational and Information Systems*, Slovenia.

44. IMG (Information Management Group). 1992. *Information Systems Security: Top Level Policy for the NHS*, NHS Management Executive, UK.

45. [1]IMG (Information Management Group). 1992. *Basic Information Systems Security*, NHS Management Executive, UK.

46. Jones D and Svejnar J. 1982. *Participatory and Self-Managed Firms*, Lexington Books, USA, ISBN 0-669-04328-1.

47. Kamey V and Adams T. 1992. "1992 Profile of Computer Abuse in Australia", *Computer Control Quarterly*, Vol 10, No 4, UK.

48. Kantzavelou I, Clissman C and Patel A. 1993. "Finalisation of network guidelines for implementation", *AIM SEISMED Report SP09-090993*, University College Dublin, Eire.

49. Katsikas S and Gritzalis D. 1993. "A High Level Security Policy for

     Healthcare Establishments", *AIM SEISMED SP 04 Deliverable No 15*,

     Greece.

50. Katsikas S and Gritzalis D. 1994. "The need for a security policy in health care

     institutions", *International Journal of Bio-Medical Computing*, Issue 34,

     Eire.

51. Lafleur L. 1992. "Training as part of a security awareness program",

     Computer Control Quarterly, Vol 10, No 4, UK.

52. Lee T. 1992. "A Study of Risk Assessment Packages",

     Midland Bank, UK.

53. Manuel G. 1991. "Computing - Disasters, Security and Patient

     Confidentiality", *The Health Service Journal*, 25th July, UK.

54. Milton C. 1995. "NHS network 'a hackers' dream", *Sunday Times*, 2nd June,

     UK.

55. Mumford E. 1983. *Designing Participatively,*Manchester Business School,

     UK, ISBN 0-903808-29-3.

56.   Mumford E. 1985. "Defining System Requirements to meet Business needs: a case study example", *The Computer Journal*, Vol 28, No 2, UK.

57.   Mumford E. 1993. *Designing Human Systems For Health Care*, 4C Corporation, The Netherlands, ISBN 90-74687-01-6.

58.   Neugent W. 1985. "Technology Assessment: Methods of measuring levels of Computer Security", Special Publication: 500 - 133, *US Department of Defence*, USA.

59.   NIST. 1991. *"Description of Automated Risk Management Packages"*, NIST Risk Management Research Laboratory, USA.

60.   O'Connel S and Patel A. 1992. *"Limitations of CRAMM"* AIM SEISMED Internal Paper SP09 - 1.02, Eire.

61.   Pheysey D. 1992. *Organisational Cultures*, Routledge, UK, ISBN 0-415-08292-7.

62.   Plant M. 1993. "Getting Management Buy-In to IT Security", *Computers and Security*, Volume 12, No 7, UK.

63.   Plymouth and Torbay Health Authority. 1994. The Plymouth EPHR (Electronic Patient Health record) Project Specification, UK.

64.   Poppel H and Goldstein G. 1987. *Information Technology - The Trillion*

Dollar Opportunity, McGraw-Hill Inc, USA, ISBN 0-07-050511-X.

65.   Pursall K. 1992. *Computer Risk Management (3rd Edition)*,

Elsevier Science Publishers Ltd, UK, ISBN 1-85617-172-8.

66.   Robbins S. 1992. *Essentials of Organisational Behaviour*,

Prentice-Hall International, USA, ISBN 0-13-287954-9.

67.   Robson W. 1994. *Strategic Management and Information Systems*,

Longman, UK, ISBN 0-273-60042-7.

68.   Rojek C and Wilson D. 1987. "Workers Self-Management in the World

System: The Yugoslav Case", *Organisation Studies*, Vol 8, Issue 4, USA.

69.   Rossing N. 1994. "Presentation note of AIM Program",

EU AIM SEISMED Booklet, Belgium.

70.   S2014 EU Security Investigation Project - Risk Analysis. 1993.

WP08 Risk Analysis Methods Database, UK.

71.   Sanders P.W and Furnell S.M. 1993. "Data Security in medical information systems using a generic model", *Proceeding of MIE 93 Conference*, Israel.

72.   Schein E.H. 1985. *Organisational Culture and Leadership*, Jossey-Bass Limited, USA, ISBN 0-87589-639-1.

73.   SCOLL. 1992. *NHS Small Systems Security Review System*, UK.

74.   SEISMED. 1994. "Presentation note of AIM Program", *EU AIM SEISMED Booklet*, Belgium.

75.   Smith M.R. 1989. *Common-sense Computer Security*, McGraw-Hill Book Company, UK, ISBN 0-07-707162-X.

76.   Smith S and Jalbert M (1990), "LAVA: A Software System for vulnerability and risk assessment", *Proceeding of the 13th National Computer Security Conference*, USA.

77.   Sunday Times. 1995. "Doctors oppose NHS database", 4th June, 1992,UK.

78.   Stanic N. 1988. "Yugoslavia Self-Managed Crisis",

       International Management, Vol 43, No 1, January, UK.

79.   Vonk R. 1990. *Prototyping*, Prentice Hall, UK,

       ISBN 0-13-731589-9.

80.   Vons Solm R, Eloff J.H.P and Von Solms S.H. 1990.

       "Computer Security Management: a framework for effective management

       involvement", *Information Age*, Volume 12, Number 4, UK.

81.   Voutilainen R. 1989. "Experiences of the use of the SBA vulnerability

       analysis for improving computer security in Finland", *Proceeding of IFIP*

       Conference, Elsevier Science Publishers, The Netherlands.

82.   Yavis U and Yasin M. 1993. "Computing environment in an Arabian Gulf

       Country", *Information Management and Computer Security*, Vol 1, No 1,

       USA.

83.   Wahlgren G. 1990. "Survey of Computer Aided Risk Analysis Packages for

       Computer Security", Stockholm University and the Royal Institute of

       Technology, Sweden.

84.   Warren M.J and Gaunt P.N. 1993. "Impact of Security on a Healthcare

environment and how to overcome it ", *IMIA WG4 "Caring for Health

Information"*, Heemskerk, The Netherlands.

85.   Warren M.J and Gaunt P.N. 1994. "The use of SIM-ETHICS at Plymouth

Health Authority", *AIM SEISMED Report SP11-06*, UK.

86.   Warren M.J, Gaunt P.N and Sanders P.W. 1995. "Particaptional Management

and the Implementation of Multimedia Systems", *Proceedings of Mediacomm

Conference*, UK.

87.   Warren M.J, Sanders P.W and Gaunt P.N. 1994. "Security Criteria Expert

System - The Medical Application", *Proceeding of Neural Networks and

Expert Systems in Medicine and Healthcare (NNESMED) Conference*,

UK.

88.   Warren M.J , Sanders P.W and Gaunt P.N. 1996. *"ODESSA - A new risk

analysis method"*, To be published.

89.   Wrede R. 1984. "SBA Method - A method for testing vulnerability",

Proceeding of IFIP Conference, Elsevier Science Publishers,

The Netherlands.

90.   Wylder J. 1992. "The Life Cycle of Security Managers",

        Information System Management, Winter, UK.

91.   Zeffane R. 1988. "Participative Management in Centrally Planned

        Economies", *Organisation Studies*, Vol 9, Issue 3, USA.

92.   Zizmond E. 1992. "The Collapse of the Yugoslav Economy",

        Soviet Studies, Vol 44, No 1, USA.

Appendix A SIM-ETHICS Criteria

SIM-ETHICS Criteria

Ease of Implementation
1) Easily implemented.
2) Implemented with minor modifications to existing systems or with the minimal amount of effort.
3) Implemented with major modifications to existing systems or with an extensive amount of effort.
4) Implemented with the development of a new system or redevelopment of an existing system.

Training Issues
1) No training requirements.
2) Some training needed, i.e. a few people.
3) Some training/retraining needed, i.e. a department.
4) Extensive training needed, i.e. the whole organisation.

User Impact (Related to users Job function)
1) No user impact.
2) Countermeasure affects user satisfaction.
   a) Causes a minor impact.
   b) Causes a major impact.
3) Countermeasure affects users efficiency, effectiveness.
   a) Causes a minor impact.
   b) Causes a major impact.

Organisational Impact
1) No organisational impact.
2) Effect the way tasks are carries out.
   a) Causes a minor impact.
   b) Causes a major impact.
3) Effect Organisational Culture.
   a) Culture changed through planned change.
   b) Culture changed through unplanned change.
   c) Culture changed through technical seduction.

Human Issues
1) No individual impact.
2) Results in restructuring a persons job or changing a persons individual power.
3) Results in restructuring of management techniques or creation of new management techniques.

Appendix B Questions asked in SIM-ETHICS Review

Access Control Cards

1. How do you feel about having to use access cards.

2. Do you mind having to use a dual ID card and access control card.

3. Can you think of any practical problems of using access control cards.

4. To what extent do you think access cards should be used within the hospital.

5. What training will you feel that you need in order to use the access control cards.

6. Do you think access control cards will help promote a "security" culture and security awareness.

7. Would you feel that 'Big Brother' is watching you since the access control system can be used to monitor where you are in the hospital.

VTX

1. Can you see any problems with using VTX.

2. What would you use the information provided by VTX for and how important is the accuracy of that information.

3. Can you think of any practical problems of using VTX.

4. What do you think will be the best method of training.

5 How do you feel VTX will improve our job.

6 Do you think VTX will change the culture of the organisation.

7. How do you feel that VTX may affect your job.

PASSWORDS

1) How many password do you use and how do you feel about it.

2) How often do you change your passwords, how often would you actually like ((i.e. 30 - 90 days).

3) How do you feel having passwords structured, i.e. so many characters.

4) Do you think there should be restrictions on names used as passwords, i.e. secret, a persons name.

5) How do you feel about being forced to change your password.

Appendix C Questionnaires sent to System Managers

System Managers Security Questionnaire

Name :

Directorate :

Computer System :

(Please tick the appropriate boxes)

Question 1

Do your feel confident in your knowledge of computer security?

a) Yes ☐

b) No ☐

Question 2

Would you like specific training relating to security?

a) Yes ☐

b) No ☐

Question 3

Are you aware of any specific security features on your system?

a) Yes ☐

b) No ☐

Question 4

Please enter the appropriate value:

    1) Cost is very important   2) Cost is important

    3) Cost is relevent   4) Cost is irrelavent

Please identify which cost components are considered when implementing security.

    a) Direct Costs, i.e. cost of security   ☐

    b) Associated Costs, i.e. training   ☐

    c) Indirect Costs, i.e. extra equipment   ☐

    d) Consultancy, i.e. externally hired staff   ☐

    e) Upgrade costs, i.e. extra equipment costs   ☐

(Please tick the appropriate boxes and expand any anwers in the space provided)

Question 5

Which of the following factors have you considered when deciding how to secure your system.

    a) Ease of Implementation   ☐

    b) Whether the existing system needs to be modified   ☐

    c) The amount of training needed   ☐

Question 6

Which of the following factors are taken into account regarding training:

a) The level of training that is required by users ☐

b) The number of people to be trained ☐

c) The cost of training, i.e. time lost through training ☐

Question 7

When implementing security are any of the following considered:

a) User Satisfaction, i.e. would security features effect their system use ☐

b) User Efficiency, i.e. would security features effect their effiency ☐

c) Group Effectiveness, i.e. how security influences clinical care ☐

Question 8

Are any of the following user issues considered when introducing security:

a) How security features change the users jobs ☐

b) Whether the security requires new jobs or responsibilities ☐

c) Would the security measures affect the way users use the system ☐

(Please tick the appropraite boxes)

Question 9

Does your department have a person responsible for security matters. ☐

    a) Yes ☐

    b) No

Question 10

Does your department have a general computer security policy.

    a) Yes ☐

    b) No ☐

Question 11

Does your department have a special security policy for the use of portable PC's.

    a) Yes   ☐

    b) No   ☐

Question 12

Are your users given computer security training.

    a) Yes   ☐

    b) No   ☐

If so by whom:

```
┌────────────────────────────────────────────────────────────┐
│                                                            │
│                                                            │
│                                                            │
│                                                            │
└────────────────────────────────────────────────────────────┘
```

Question 13

Are your users given regular security awareness programs.

    a) Yes   ☐

    b) No   ☐

If so by whom:

```
┌────────────────────────────────────────────────────────────┐
│                                                            │
│                                                            │
│                                                            │
└────────────────────────────────────────────────────────────┘
```

Thank you for completing this questionnaire

(All answers given will be held in strictest confidentiality)

Dr Nick Gaunt

Appendix D - Results of System Managers Security Questionnaire

Questionnaire Results

Questionnaire Overall Rate of Return 70%

Questions

Q1) Do you feel confident in your knowledge of computer security?

a) Yes	64
b) No	36

(% Replies - 100%)

Q2) Would you like specific training relating to security?

a) Yes	71
b) No	29

(% Replies - 100%)

Q3) Are you aware of any specific security features on your system

a) Yes	93
b) No	7

(% Replies - 100%)

Q4) Please identify which cost components are considered when implementing security

	(Very Important)			(Irrelevant)
	1	2	3	4
a) Direct Cost (Cost of security)		27	55	18

(% Replies - 78.5%)

	1	2	3	4
b) Associated cost (Training)	10	20	40	30

(% Replies - 71.5%)

	(Very Important)			(Irrelevant)
	1	2	3	4
c) Indirect Costs (extra equipment)	22.2	33.3	44.4	

(% Replies - 64%)

d) Consultancy	50	25	25	

(% Replies - 57%)

e)Upgrade Costs	20	30	40	10

(% Replies - 71.5%)

Q5) Which of the following factors have you considered when deciding how to secure your system?

      a) Ease of Implementation   85

      b) Whether the existing system needs to be modified   69

      c) The amount of training needed   77

(% Replies - 93%)

Q6) Which of the following factors are taken into account regarding training

      a) The level of training that is required by users   75

      b) The number of people to be trained   50

      c) The cost of training, i.e. time lost though training   75

(% Replies - 86%)

Q7) When implementing security are any of the following considered:

      a) User Satisfaction   66

      b) User Efficiency   66

      c) Group Effectiveness   66

(% Replies - 86%)

Q8) Are any of the following user issues considered when introducing security

a) How security features change the users jobs   61.5

b) Whether the security requires new jobs or responsibilities   30

c) Would the security measures affect the way users   92
     use the system

(% Replies - 93%)

Q9) Does your department have a person responsible for security matters

   a) Yes   77
   b) No   23

(% Replies - 93%)

Q10) Does your department have a general computer security policy

   a) Yes   46
   b) No   54

(% Replies - 93%)

Q11) Does your department have a special security policy for the use of portable PC's

   a) Yes   20
   b) No   80

(% Replies - 86%)

Q12) Are your users given computer security training

   a) Yes   71
   b) No   29

(% Replies - 100%)

Q13) Are your users given regular security awareness programs

    a) Yes   23
    b) No   77

(% Replies - 93%)

Overview

Two thirds of system managers are confident in their knowledge of computer security but just over 70% would like specific training relating to security.

Managers consider ease of implementation and the training required by users very important when implementing security. When it comes to training, managers are concerned about the level of training required by users and the time that staff lose through training.

Managers are also concerned about how security features would affect the users use of individual systems.

Nearly all departments have a person responsible for IT security, but less than half of these departments have IT security polices. About 70% of system mangers said that users are given security training, but less than 25% go on security awareness programs after their initial training.

Appendix E - Security Culture in Saudi Arabia

Taking Saudi Arabia as an example of the following national characteristic are found:

National Culture

Saudi Arabia is defined as being a Power Distance culture. Society accepts the fact that power in organisations is distributed unequally. Employees show respect for those in authority, titles, rank and status being important.

General use of IT

Saudi Arabia has developed a five year plan with the aim of using labour-saving technology as a result of a severe shortage of indigenous manpower. Research has shown (Yavis and Yasin, 1993) that IT is implemented mainly for business expansion and replacing manual operations. This research also shows that employees are considered as the main security risk.

Medical use of IT

Surveys undertook at a Saudi Arabian hospital on the use of IT systems found:

> Males (39%) used the IT systems more than females (30%);
>
> Non Saudi Consultants (31%) made the most use of IT systems;
>
> The Saudis which used IT the most were consultants (29%);
>
> 67% of staff had poor computer skills or none at all;

46% of Consultants has computers,

44% of Physicians thought computers were useful but not

necessary.

(Al-Hahhah and Bamgboye, 1992)

Appendix F: Comprehensive list of Risk Analysis

Methods

Companies Own

Method Name: ASIS

Country of Origin: Germany

Description: During 1991 a major German IT manufacturer designed an

overall framework for risk management. The scope of the

project comprised the development of a conceptual model for

an object oriented risk analysis tool.

References: (S2014, 1993)

Method Name: BULLRAM

Country Of Origin: France

System: Computer based

Description:

BULLRAM was developed by BULL for its internal use and

for use by its customers. The model is broken down into the

following stages.

Incident Scenario Model

Phase 1 - Aggression

An aggression threatens to trigger a attack against a

resource ("the Primary Target"). The aggression will use a set

path or series of paths of attack, the attributes of these give a

measure of the targets vulnerability to attack.

Phase 2 - Degradation

This stage determines the level of damage caused by the attack.

The estimated damage to physical and logical resources is

carried out and especially loss in confidentiality, integrity and

availability.

Phase 3 - Recovery

The aim of this stage is to recovery from any damage that has

occurred to the organisations business functions.

Safeguards Scenario Model

BULLRAM uses classes of safeguards, each class coping with

various adverse actions occurring in the incident scenario.

These safeguards are suggested as certain incidents occur.

Risk Assessment Metrics

Risk is measure by a combination of two major parameters,

"potentiality" of threat and incident and "gravity" (seriousness)

of business impact. This is the estimated residual losses related

to the businesses functions.

References: (S2014, 1993)

Method Name: Citicorp Operations Risk Assessment

Country Of Origin: USA

System: Computer based

Description: This method is an impact analysis method used to determine

which operations and services are of critical, high or medium

risk. The method is concerned with ensuring availability and

continuation of services. The method consists of the following

steps:

          - designate business functions, products and services;

          - determine impact of product/service loss;

          - asses loss of dependent resources;

          - apply the results of review in a contingency plan that

               would incorporate 'containment measures'.

This method is not commercially available.

References: (S2014, 1993)

Method Name: Data Center Evaluation Checklist

Country Of Origin: UK

Required Experience: None

System: Paper based

Description:

        This checklist is used by Digital to determine if their computing

        resources meet their minimum suggested security levels.

References: (Digital, 1991)

Method Name: IBM Methodology (Spain)

Country Of Origin: Spain

Description:

        This method is designed for use in producing contingency plans

        for organisation computing centers and it can be used within

        other organisational environments. The evaluation of risk is

        carried out via the use of scenarios that considers the

        disruption that could occur as a result of security breaches. The

        risks relate to destruction of assets, corruption of data,

        disclosure of information and interruption of IT service. This

        method is not commercially available.

References: (S2014, 1993)

Method Name: Insurance Technical Bureau IFAL

Country Of Origin: USA

System: Computer based

Description:

This was developed to provide risk assessment for oil, gas and petrochemical plants. IFAL assumes that the risk is influenced by three elements: the process risk, the quality of design and construction and the quality of management and operation. IFAL only considers protecting IT assets, staff etc. from explosions. This package is highly specialised and is concerned only with the oil, gas and petrochemical industries.

References: (S2014, 1993)

Method Name: PSICHE

Country Of Origin: France

System: Computer based

Description:

PSICHE is a vulnerability and risk management method developed for EDF/GDF (National Electricity and Gas companies of France) for their internal use as aid to the development and implementation of IT security plans. The method is broken into three major steps.

Intrinsic Vulnerability Analysis

Vital and sensitive systems are identified, then quantified and measured in terms of relative value.

Effective vulnerability and management

The organisational functions are analysed and expressed in terms of information systems and applications, each of which is represented by a vulnerability chain (the vulnerability of hardware, software, organisational and human elements). The system rates the average and maximum vulnerability of a chain link.

The overall effective vulnerability level of the information systems is obtained by combining the risk values of the chains. If this level is considered too high then security countermeasures are suggested.

Specification of the Security Plan

A detailed analysis of the safeguards suggested in stage 2 is carried out in order to take into account the financial, technical, organisational and time constraints.

References: (S2014, 1993)

Method Name: REASSURE

Country Of Origin: Canada

System: Computer based

Description:

This system was the result of a Canadian academic research project. The system includes an expert system and is concerned about the security issues of implementing networks and standards, e.g. US Yellow Book.

References: (S2014, 1993)

Method Name: Sofine

Country Of Origin: The Netherlands

System: Computer based

Description:

This system is highly specialised and it used by financial instructions to undertake security risk analysis reviews.

References: (S2014, 1993)

Consultants

Method Name: Analyse des Risqués Programmes

Country Of Origin: France

Required Experience: IT security experience and specific method training required

System: Computer based

Description:

Assets Protection:	Extensive
Impact Analysis:	Extensive

Threat/Vulnerability Analysis:	Extensive
Level Countermeasures:	Extensive

The method expresses risks, threat and vulnerability levels by using a quantitative approach. The system can also given justification for the security suggested.

References: (S2014, 1993)

Method Name: AnalyZ

Country Of Origin: UK

Required Experience: Specific method training required.

System: Computer based

Description:

Assets Protection:	Extensive
Impact Analysis:	Extensive
Threat/Vulnerability Analysis:	Extensive
Level Countermeasures:	Extensive

The method expresses risks by using a quantitative approach. AnalyZ has been designed to take risk analysis to the user, e.g. a project manager or business manager. AnalyZ is data driven

and therefore it can changed to suit any organisation by simply

changing the contents of the database. AnalyZ database

contains a set of baseline security measures, which are changed

to reflect the organisation requirements. AnalyZ is menu driven

and allows the user to:

- build a risk model of the system through a question and

    answer session;

- establish the target level of acceptable risk based on the type

    of business for which the system is being used;

- review the risk profile of the systems against the target level

    for the business;

- perform 'what-if' scenarios on the initial model.

References: (S2014, 1993)

Method Name: AROME+

Country Of Origin: France

Required Experience: IT security experience and experience of the MARION method

System: Computer based

Description:

Assets Protection:	Extensive
Impact Analysis:	Extensive
Threat/Vulnerability	Extensive

Analysis:

Level Countermeasures: Extensive

The method expresses risks, threat and vulnerability levels by using a quantitative and qualitative approach. The system can also give justification for the security countermeasures suggested. The method allows the use of scenarios as a way of allow the user carry out risk analysis reviews. The system produces its own questionnaires for the user to answer as a way of measuring vulnerability levels. The system in only available in French.

References: (S2014, 1993)

Method Name: BIS Risk Assessor

Country Of Origin: UK

Required Experience: Limited

System: Computer based

Description:

Assets Protection: Moderate

Impact Analysis: Extensive

Threat/Vulnerability   Extensive

Analysis:

Level Countermeasures: None

BIS Risk Assessor does not produce countermeasures but the data produced from it can be imported into CRAMM for future use. The method expresses threat and vulnerability levels by using a quantitative approach. The method expresses risk levels by a qualitative method.

The BIS risk assessor is conceived as being a high-level risk evaluation product. The system evaluates risk according to approximately 30 threat categories. The BIS risk assessor calculates a conceptual level of risk, that is risk levels without taking into account any existing or potential countermeasures that the organisation is considering. The objective of the BIS risk assessor is limited to obtaining global indications of risk for consideration by the organisations management. Any further risk analysis should be carried out using another method, which is the reason for the link to the CRAMM method.

References: (S2014, 1993)

Method Name: Buddy System

Country Of Origin: USA

Required Experience: None for general use

IT security knowledge needed for the maintenance utility

System: Computer based

Description:

Assets Protection: Moderate

Impact Analysis: Extensive

Threat/Vulnerability Extensive

Analysis:

Level Countermeasures: Extensive

The method expresses risks, threat and vulnerability levels by using a quantitative approach. The Buddy system can justify any security recommendations that its make.

The Buddy System derives its name from the concept of two separate individuals being involved in the security process; the end user and the security analyst. The end users completes the security survey and the security analysis loads the survey information into a central database and performs the risk analysis. The end user survey can be completed by users with little knowledge of computer security. It collects baseline information about the system and identifies countermeasures that are already in place. The security analysis loads the results into a risk management system. This software determines the vulnerability level, and uses "what-if" scenarios to model the vulnerabilities and provide additional countermeasures.

References: (S2014, 1993), (NIST, 1991)

Method Name: COBRA (Consultative, Objective and Bi-functional Risk

Analysis)

Country Of Origin: UK

Required Experience: None

System: Computer based

Description:

Assets Protection:		Extensive
Impact Analysis:		Extensive
Threat/Vulnerability Analysis:		Extensive
Level Countermeasures:		Extensive

The method expresses risks, threat and vulnerability levels by

using a qualitative approach. The method can justify its security

recommendations. The system can be used with two different

approaches. The first is to target a specific area, e.g.

contingency planning for a specific area. The second approach

is for a business manager to complete a business impact survey

that will quantify security breaches. The system makes use of

computer generated questions in order to elicit user

information.

References: (S2014, 1993), (Lee, 1992), (Addison, 1991)

Method Name: Control Matrix Methodology for Microcomputers

Country Of Origin: USA

System: Computer based

Description:

This method use a matrix approach for designing controls into microcomputer environments. It identifies which controls are needed to ensure adequate security in business or scientific systems. The main package is a control matrix development package that contains a database of controls plus separate database of threats and computer system components. There is also a graphical package which draws the final matrix representing threats, components and controls. The package also comes with two training programs.

References: (S2014, 1993), (NIST, 1991)

Method Name: Control - IT

Country Of Origin: USA

System: Computer based

Description:

This system identifies potential threats related to a computer system as well as identifying the controls that are necessary to protect the system. The main software package contains a spreadsheet development package that contains three databases

of potential threats, components and controls. The package draws a matrix showing risk regions and their rankings. This system comes with automated teaching packages.

References: (S2014, 1993), (NIST, 1991)

Method Name: COSSAC (Computer Systems Security Analyser and

                   Configurator)

Country Of Origin: Canada

Required Experience: None

System: Computer based

Description:

COSSAC is an automated checklist system that consists of 400 questions. All the questions can be modified and more questions can be added by the user. The questions are structured into the following groups, which are:

- general (parameter security, fire protection, hardware and

  software security features etc.);

- financial (accounting, auditing, fund transfer etc.);

- virus (deals with threats from computer viruses);

- classified and sensitive (deals with classified and sensitive

  material as defined by US law and regulations, e.g. US

  Orange Book).

At the end of each section COSSAC suggest simple hints and

countermeasures to improve security.

References: (S2014, 1993), (Wahlgren, 1990), (Carroll and Mac Iver, 1985)

Method Name: CRITI-CALC

Country Of Origin: USA

System: Computer based

Description:

The system uses the concept of ALE (Annual Loss Expectancy)

to quantify the criticality of risk exposure for applications. The

criticality of each system is determined by the potential for loss

caused by a processing interruption. This system is menu

driven with a built in "major threats" database and a "fill-in-

the-blank" application database. The system uses the user input

to determine the optimum off-site recovery time for

applications. CRITI-CALC allows the user to carry out "what if

analysis" on their input data and this is used as a way of

verifying the effectiveness of certain countermeasures.

References: (S2014, 1993), (NIST, 1991)

Method Name: DAFI

Country Of Origin: France

Required Experience: IT security, Method relating training, auditor skills.

System: Computer based

Description:

                Assets Protection: Extensive

                Impact Analysis: Extensive

                Threat/Vulnerability   Extensive

                Analysis:

                Level Countermeasures: Extensive

                The method expresses risks, threat and vulnerability levels by using a quantitative and qualitative approach. DAFT can also justify its security recommendations. This method provides either a high level view of the security requirements or a detailed report.

References: (S2014, 1993)

Method Name: DDIS (Datenschutz-und-datensicherheits (Data Protection and Data Security) Information System)

Country Of Origin: Germany

Required Experience: None

System: Computer based

Description:

                Assets Protection: Extensive

                Impact Analysis: Extensive

Threat/Vulnerability   Extensive

Analysis:

Level Countermeasures: Extensive

The method expresses risks, threat levels by using a

quantitative and qualitative approach. Users can tailor the

system to their own requirements by defining new questions for

the system. The system uses a questionnaire to determine user

requirements and these results can be aggregated and shown as

graphs. The system can justify the countermeasures its

suggests. The system produces a high level report of the

organisational security requirements. The system is only

available in German.

References: (S2014, 1993)

Method Name: EDV-Sicherheits-Check

Country Of Origin: Germany

System: Computer based

Description:

The system is used to analysis the consequence resulting from

the unavailability of IT systems or system components. The

method is comprised of two stages.

Stage 1

Analysis of dependencies upon systems, data, effectiveness of existing countermeasures. At the end of stage 1 the critical dependence of the business should be determined - that is which business functions would be hindered if the IT system were not available.

Stage 2

A quantitative simulation of business functions is carried out. The simulation represents the use of different threats and countermeasures. This stage also produces other simulations relating to production and costs. At the end of this stage a security profile for the organisation is produced.
This method is used as a consultancy tool and is not commercially available.

References: (S2014, 1993)

Method Name: Expert Auditor

Country of Origin: USA

Description:

This system is an automated checklist used for auditing. The main function of the system is to ensure that the system under review meets certain criteria. This criteria relates to

environmental issues, e.g. type of building, where the data centre is placed.

References: (Wahlgren, 1990)

Method Name: Feros

Country Of Origin: France

Required Experience: None

System: Paper based

Description:

Assets Protection:	Extensive
Impact Analysis:	Extensive
Threat/Vulnerability Analysis:	Moderate
Level Countermeasures:	Extensive

The method expresses risks, threat and vulnerability levels by using a qualitative approach. This method is used to identify the requirements, security objectives and the system then produces a high level report. This method should be used before a detailed risk analysis review is carried out.

References: (S2014, 1993)

Method Name: GRA/SYS

Country Of Origin: USA

System: Computer based

Description:

This system performs a qualitative risk assessment of multi-organisational units. The method is designed to assist auditors and security personnel in developing a work priority plan for reviewing organisational risks.

References: (S2014, 1993), (NIST, 1991)

Method Name: IST/RAMP

Country Of Origin: USA

System: Computer based

Description:

This system supports an automated model of a computer security environment. This is used to estimate loss to determine the benefits of introducing security measures. The model evaluates against five loss categories, which are unavailability, physical damage, fraud, disclosure of data and physical theft.

References: (S2014, 1993), (NIST, 1991), (Wahlgren, 1990)

Method Name: IS Case

Country Of Origin: France

Required Experience: Software design

System: Computer based

Description:

    Assets Protection: Extensive

    Impact Analysis: Extensive

    Threat/Vulnerability   Extensive

    Analysis:

    Level Countermeasures: Extensive

The method expresses risks, threat and vulnerability levels by

using a quantitative and qualitative approach. IS Case can also

justify the reason for suggesting security countermeasures.

IS Case suggests ways in which security can be designed into

new systems. The system produces reports relating to:

        - maximum risk analysis results;

        - audit results;

        - economic issues reports, e.g. cost benefit reports;

        - simulation reports;

        - suggested countermeasures.

The system uses a simulation to determine the major risks and then the simulation reduces the risks by use of appropriate countermeasures.

References: (S2014, 1993)

Method Name: JANBER

Country Of Origin: USA

System: Computer based

Description:

This is a qualitative risk analysis package that is customised to fit an organisations requirement. JANBER uses a yes/no questionnaire and checklist for collecting information about existing security controls. The system records information relating to current systems, countermeasures and data classification of systems.

The review determines the level of vulnerability for the organisation by using a vulnerability level of between 2 - 28 (28 being worse case scenario). The system contains a database of all the information collected, which is then used to suggest future countermeasures.

References: (S2014, 1993)

Method Name: MACS

Country Of Origin: France

System: Computer based

Description:

This method allows a project manager to include security

concepts from the initiation of any programming project in

order to implement efficient security at a minimal cost.

The method is concerned mainly with logical systems security,

but takes into account all cause of unavailability, e.g. hardware

failure. The software comes complete with a database

containing risk scenarios and countermeasures.

References: (S2014, 1993)

Method Name: MARION

Country Of Origin: France

Required Experience: IT security experience

System: Computer based

Description:

Assets Protection:	Extensive
Impact Analysis:	Extensive
Threat/Vulnerability Analysis:	Extensive
Level Countermeasures:	Extensive

The method expresses risk, threat and vulnerability levels by using a quantitative and qualitative approach. MARION can also justify the reason for suggesting security countermeasures. MARION uses data complied from the French Insurance Companies as a method of determining risks.

The MARION method consist of six stages.

Stage 1

At this stage the level of risk is determined for the organisation. This is determined by using staff from the different departments to complete a questionnaire.

Stage 2,3 and 4

In these stages the maximum risk (losses that the organisation can accept) are determined. The calculation is carried out for each of the different risk types. During the third stage a security audit is undertaken to determine the quality of the suggested countermeasures.

Stages 5 and 6

In stage 5 the new countermeasures are selected relating to different aspects of security, e.g. prevention, recovery. In stage

6 an implementational plan is produced which suggests how the

countermeasures can be implemented over a three year plan.

References: (S2014, 1993), (Wahlgren, 1990), (Baratte, 1989), (Coopers

and Lybrand, 1989)

Method Name: MicroSecure Self Assessment

Country Of Origin: USA

System: Computer based

Description:

This is a menu driven qualitative risk analysis package that

allows PC users to conduct their own security self assessments.

The system contains an expert system which analyses a

companies computing environment and gives advice about

security weakness and how to improve it.

References: (S2014, 1993), (NIST, 1991)

Method Name: MINIRISK

Country Of Origin: USA

System: Computer based

Description:

MINIRISK is a tool to assess security vulnerabilities in a
microcomputer environment. A vulnerability assessment allows
the organisation to evaluate the adequacy of their
countermeasures. The absence of certain safeguards determines
the level of vulnerability between 0 (best case) and 9 (worse).

References: (S2014, 1993), (NIST, 1991)

Method Name: Predict!

Country Of Origin: USA

Required Experience: Understanding of Risk Analysis

System: Computer based

Description:

Assets Protection:	Extensive
Impact Analysis:	Extensive
Threat/Vulnerability Analysis:	Extensive
Level Countermeasures:	Extensive

The method expresses risk, threat and vulnerability levels by
using a quantitative and qualitative approach. The system
makes extensive use of user models of computer systems. This
package contains a number of models that can be used.

References: (S2014, 1993)

Method Name: QuikRisk

Country Of Origin: USA

System: Computer based

Description:

QuikRisk is a system that can be used to determine the impact

of security breaches. This system requires the user to enter

information about their system on a computerised scenario

form. This form relates to potential threats, current

countermeasures and assets. Once all the information has been

entered the annual loss exposure is determined.

References: (S2014, 1993)

Method Name: RA/SYS

Country Of Origin: USA

System: Computer based

Description:

The system works by getting the user to answer questions on

four subsets of risk, these are:

- corporate risk;

- PC risk;

- mini-computer risk;

- generic risks (e.g. physical).

The system then determines the threat, vulnerability ratings, asset valuations, annual loss expectancy. From this the system produces a list of countermeasures and cost benefit analysis.

References: (S2014, 1993), (NIST, 1991)

Method Name: RANK-IT

Country Of Origin: USA

System: Computer based

Description:

This is an automated risk analysis tool that uses Delphi techniques. Delphi is an expert system approach to risk ranking. The system automates Delphi by adding comparison risk ranking to obtain a list of ranked events. These events relates to threat scenarios, disaster recovery, etc. Each ranked item has a number that can be used as a weighting factor to determine its importance.

References: (S2014, 1993), (NIST, 1991), (Wahlgren, 1990), (Fitzgerald, 1993)

Method Name: RISAN

Country Of Origin: The Netherlands

Required Experience: Method related training course

System: Computer Based

Description:

            Assets Protection: Extensive

            Impact Analysis: Extensive

            Threat/Vulnerability   Extensive

            Analysis:

            Level Countermeasures: Extensive

            The method expresses risk, threat and vulnerability levels by

            using a quantitative approach. RISAN can also justify the

            reason for suggesting security countermeasures.

            The system determines the vulnerability of design options and

            it presents the risk to the user and assists in selecting

            countermeasures for the user.

References: (S2014, 1993)

Method Name: Risiko

Country Of Origin: France

Required Experience: Method specific training

System: Computer based

Description:

            Assets Protection: Extensive

Impact Analysis:	Extensive
Threat/Vulnerability Analysis:	Extensive
Level Countermeasures:	Extensive

The method expresses risk, threat and vulnerability levels by using a quantitative and qualitative approach. Risiko can also justify the reason for suggesting security countermeasures. This method is very similar to the Marion method (Wahlgren, 1990)

References:	(S2014, 1993)

Method Name:	RiskCALC
Country Of Origin:	USA
System:	Computer based
Description:	

RiskCALC has two separate parts; one for the system manager and one for the user. The system manager section is used to develop different security models and determine the risk factors. The user section is used to elicit information about the users system. RiskCALC uses the annual loss expectancy (ALE) to determine the impact of security breaches. The system then determines the organisations most significant risks and determines the ALE. The system comes complete

with a risk minimizer section and this is used to find areas of

high risk and reduce that risk level. In essence, RiskCALC is a

tool for building risk analysis models.

References: (S2014, 1993), (NIST, 1991), (Wahlgren, 1990)

Method Name: RiskPAC

Country Of Origin: USA

Required Experience: No experience required

System: Computer based

Description:

Assets Protection:	Extensive
Impact Analysis:	Extensive
Threat/Vulnerability Analysis:	Extensive
Level Countermeasures:	Extensive

The method expresses risk, threat and vulnerability levels by

using a qualitative approach. RiskPAC can also justify the

reason for suggesting security countermeasures.

RiskPAC is a knowledge based system that uses questionnaires

to obtain user information, there are questionnaires for

determining risks, business impact analysis and evaluating

disaster recovery plans. RiskPAC evaluates user answers and

then determines the level of risks from this data,

countermeasures are then suggested. RiskPAC includes a ALE

calculator, this is used to identify the level of loss for loss of

systems.

References: (S2014, 1993), (NIST, 1991), (Wahlgren, 1990)

Method Name: RiskWatch

Country Of Origin: USA

Required Experience: No experience required

System: Computer based

Description:

Assets Protection:	Extensive
Impact Analysis:	Moderate
Threat/Vulnerability Analysis:	Extensive
Level Countermeasures:	Extensive

The method expresses risk, threat and vulnerability levels by

using a quantitative and qualitative approach. RiskWatch can

also justify the reason for suggesting security countermeasures.

RiskWatch makes use of questionnaire to elicit information

from users and these questionnaires can be altered for any

organisation. This method contains a re-usable security

database so that information from the risk analysis can be used to generate security and contingency plans automatically. RiskWatch contains a module that evaluates the "Orange Book Level". This evaluates the highest classification of data used against the levels of staff who use the data.

References: (S2014, 1993), (NIST, 1991)

Method Name: SISSI

Country Of Origin: France

Required Experience: Method specific training

System: Computer based

Description:

Assets Protection:	Extensive
Impact Analysis:	Extensive
Threat/Vulnerability Analysis:	Extensive
Level Countermeasures:	Extensive

The method expresses risk, threat and vulnerability levels by using a quantitative and qualitative approach. The system uses questionnaires to obtain information from users.

References: (S2014, 1993)

Method Name: SOS (Security On-line System)

Country Of Origin: USA

System: Computer based

Description:

This system was designed for use by security management.

The user defines their security requirements and the system

then carries out a risk assessment, looking at factors

such as data loss, modification. The user then has to

complete computer generated questionnaires, from this data the

system produces lists of threats, vulnerabilities and

countermeasures. This data can be used in developing a

contingency plan.

References: (NIST, 1991)

Method Name :   SPAN

Country of Origin: USA

Description:

This decision support system (DSS) provides suggestions to

assist Security Plan Analysis (SPAN). The DSS includes a

relational database that details the interaction of resources,

threats, risks and countermeasures. Resources and

countermeasures are associated with particular locations.

References: (Baskerville, 1993)

Method Name: X.R.M (eXpert Risk Management)

Country Of Origin: France

Required Experience: Method specific training

System: Computer based

Description:

         Assets Protection: Extensive

         Impact Analysis: Extensive

         Threat/Vulnerability   Extensive

         Analysis:

         Level Countermeasures: Extensive

         The method expresses risk, threat and vulnerability levels by using a quantitative and qualitative approach. This system can also justify the reason for suggesting security countermeasures.

References: (S2014, 1993)

Method Name: Xsec

Country Of Origin: Sweden

System: Computer based

Description:

         Xsec is a system that is used for auditing countermeasures for an organisation. There are two versions of Xsec, there are:

Xsec-Base - covers areas such as physical security, data

security.

Xsec-Di - covers areas such as data confidentiality.

Xsec is an expert system, the system consists of 18 knowledge

bases, these relate to a specific area of security, e.g. physical

security, disaster and recovery planning. Each area consists of

control points, e.g. water and fire damage control. For each area

there are between 10 and 20 different control points covering

different aspects of computer security. The current level of

security for a control points depends on what countermeasure

are implemented. There are 6 different levels of security on a

scale from low to very high. The method has the following

steps:

- determine the security levels of specific computer centres.

This is done by determines the systems that are operated in

these centres, this information is obtained through the use of

questionnaires. Xsec uses this information to produce a security

profile for the organisation.

- evaluation of countermeasures. This stage is concerned with

determining the current level of security for all control points.

This information is determined by the use of questionnaires, these are completed by the users.

- security comparison. In this stage a comparison of the security demand profile and security level profile for all control points is undertaken. If the security demand is higher than the security level then a security weakness occurs.

References: (Wahlgren, 1990)

General

Method Name: @Risk

Country Of Origin: USA

Required Experience: Specialist knowledge required

System: Computer based

Description: @Risk is an add-in for either Lotus 1-2-3 or Microsoft Excel software package. This package is a general purpose risk analysis and simulation modelling package. The package has been designed as a general risk analysis tool but it is possible to determine and simulate the risk of implementing computer systems.

Assets Protection:	Limited
Impact Analysis:	None
Threat/Vulnerability Analysis:	None
Level Countermeasures:	None

References: (S2014, 1993)

Method Name: BDSS (Bayesain Decision Support System)

Country Of Origin: USA

Required Experience: None

System: Computer based

Description:

Assets Protection:	Extensive
Impact Analysis:	Extensive
Threat/Vulnerability Analysis:	Extensive
Level Countermeasures:	Extensive

The method expresses risks, threat and vulnerability levels by using both quantitative and qualitative approaches. BDSS qualitatively identifies assets and supports valuation as bounded ranges within an associated confidence factor to accommodate uncertainty.

References: (S2014, 1993), (NIST, 1991)

Method Name: PRISM

Country Of Origin: USA

System: Computer based

Description:

PRISM supports development of risk modelling, simulation,

sensitivity analysis and graphical presentation of results. This

method allows the use of BASIC-like statements to model more

complex applications.

References: (S2014, 1993), (NIST, 1991)

Method Name: Risk

Country Of Origin: USA

System: Computer based

Description:

RISK is a LOTUS 123/ Microsoft Excel add-in for general risk

analysis. The software uses Monte Carlo simulation to

determine uncertainly. The system includes output routine for

displaying the information graphically and also providing

detailed statistics.

References: (S2014, 1993)

Government

Method Name: Baseline Security

Country of Origin: UK

Required Experience: None

System: Computer based and paper based

Description:

This system is a cut down version of CRAMM and it was

developed in 1991. The aim of its development was to suggest

basic security measure ("Baseline") that should be installed on

IT systems. It is used by UK governmental departments in

order to carry out security reviews on small systems

References: (CCTA, 1993)

Method Name: CRAMM (CCTA Risk Analysis and Management Method)

Country Of Origin: UK

Required Experience: IT security and method related training

System: Computer based

Description:

Assets Protection:	Extensive
Impact Analysis:	Extensive
Threat/Vulnerability Analysis:	Extensive
Level Countermeasures:	Extensive

The method expresses risks, threat and vulnerability levels by using a quantitative and qualitative approach. The system can justify its security recommendations. The method was developed for use by UK government agencies. CRAMM is developed as a tool to assist staff or consultants undertaking a security review.

CRAMM is broken into 3 main stages, which are as follows.

Stage 1

This stage is concerned with:

- agreeing the boundaries of the review;

- identifying and valuing the assets, e.g.:

> physical assets;

> software assets;

> data.

Stage 2

This stage is concerned with:

- evaluating the dependence of a system or group of assets. Each group is made up of assets which are considered for the assessment of threats and vulnerabilities.

- assessing threats and vulnerabilities. The CRAMM system

generates questionnaires in order to determine the level

of threats and vulnerabilities for each asset group.

- calculating risk levels. The system automatically generates

the risk for each asset group.

Stage 3

This stage is concerned with:

- countermeasure selection. The system selects appropriate

countermeasures from a library containing 1100

countermeasures.

- unjustified countermeasures. If an existing system is being

reviewed there may be some countermeasures which are

not required.

A new version of CRAMM is being released in 1996. The

stages of this new method are slightly different from the stages

described.

References: (S2014, 1993), (NIST, 1991), (Wahlgren, 1990), (CCTA, 1992)

Method Name: FIPS PUB 65

Country Of Origin: USA

System: Paper based

Description:

The system was developed for the US Department of

Standards. One of the main objectives of its development was

to inform governmental staff how to undertake a risk

assessment.

The method is broken down into three main stages.

Preliminary Examination

This is concerned with initially examining the system that has

to be reviewed, e.g. the type of system, the type of data is

processes, special considerations, etc.

Risk Analysis

The risk analysis process requires the estimation of two

quantities:

- frequency of occurrence of a threat;

- the impact of when a threat materialises and how it

affects an asset.

Multiplication of these factors results in the annual loss which
can be expected from the threat.

Selection of Countermeasures

This stage is concerned with selecting countermeasures for the
organisation, an important aspect of the selection is the cost
benefit of the countermeasures.

The advantages of the FIPS method is that it produces
financial figures, e.g. annual loss expectancies which is
easier for management to understand. The main disadvantage of
the system is that because it is paper based its very staff
intensive.

References: (FIPS 65, 1979), (Neugent, 1985)

Method Name: LAVA (Los Alamos Vulnerability Analysis)

Country Of Origin: USA

System: Computer based

Description:

The structure of LAVA is broken into three stages.

Vulnerability Assessment

Information is gathered about the organisations. This information takes the form of asset and threat determination. These threats and assets are combined into threat - asset pairs, the result of these pairing are then determined, e.g. modification of data. Countermeasure are then suggested on relating to the threat - asset pairing. The vulnerability assessment measures the relative weakness of the countermeasures and uses the assumption that all attacks are equally likely to occur and that the consequences of these attacks will be extreme.

Threat Analysis

The threat analysis takes into account possible threat agents, e.g. terrorists, employees and their potential attack goals, e.g. sabotage, theft, fraud. The threat analysis uses the following.

- asset attractiveness, e.g. how attractive the asset is to a threat
    agent;
- motivation, e.g. how much effort would a threat agent be
    willing to expand to attack an asset;
- capability, e.g. this is the measure of the resources that the
    threat agent has at their disposal;
- opportunity is a measure of how easy it is for the threat agent
    to carry out an attack.

The threat analysis provides a score for each possible threat, these scores are combined to produce an overall score.

Consequence Analysis

The object of this analysis is to determine the effect that an outcome of a successful attack would have upon an organisation. The consequence measures the potential costs in both monetary and non-monetary terms. The types of consequences are obtained from using interactive questionnaires. The potential loss is determined by calculating and combining the results from the previous analysis. Then the system suggests possible countermeasures. This system was developed for the US government.

References: (S2014, 1993), (Wahlgren, 1990), (Smith and Jalbert, 1990)

Method Name: PARIS (Pragmatic Assessment RISk methodology)

Country Of Origin: UK

Required Experience: None

System: Paper based

Description:

This system is a cut down version of CRAMM. Its used by the UK government department, The Home Office to carry out

security reviews on existing or new computer systems. PARIS

uses a tabulated questionnaire. The method identifies the

following:

     - assets to be protected;

     - threats to those assets;

     - likelihood of the threat occurring and the

       impact it causes.

Having determine these facts, it then poses questions regarding

possible methods of countering the threat or reducing its

likelihood.

References: (Coverson, 1991)

Method Name: RiskPAC (Federal)

Country Of Origin: USA

System: Computer based

Description:

This system meets the USA regulation requirement for risk

analysis that is used on classified and unclassified critical

government computer systems. The system is particularly

focused by US government documents, e.g. Orange Book,

National Computer Security Act (1987), etc.

References: (S2014, 1993)

Healthcare

Method Name: ZIP

Country Of Origin: UK

Required Experience: None

System: Paper based

Description:

This system is a cut down version of CRAMM. It is used by the

UK National Health Services (NHS). The NHS use it to carry

out security reviews of small systems.

References: (SCOLL, 1992)

Military

Product Name: ANSSR (Analysis of Networked Systems Security Risks)

Country Of Origin: USA

System: Computer based

Description:

The method is aimed at carrying out risk analysis reviews for

networked systems. The work was sponsored by the US Navy.

The system works by the reviewer entering descriptive

information via a set of menus. This information helps to

produce a system model. Other factors can also be modelled,

such as existing countermeasures. ANSSR performs a

simulation of human attacks against systems with the goal of gaining access. These attacks are modelled as threat scenarios and the likelihood of success depends upon the attackers capabilities and the systems countermeasures. If a system is compromised by a threat scenario, then the system can be remodelled with new countermeasures and the simulation run again.

References: (Bodeau, 1992)

Method Name: ARES (Automated Risk Evaluation System)

Country Of Origin: USA

System: Computer based

Description:

This method is a quantitative system. ARES uses a rule based interference engine and a menu driven checklist system to perform a risk analysis. The system collects information from user and from this information the risk analysis process is carried out. This process shows where the potentials risks are and the system then suggests countermeasures. The system was developed for the US Air Force.

References: (NIST, 1991)

Method Name: LRAM (Livermore Risk Analysis Methodology)

Country Of Origin:	USA
System:	Computer based
Description:	

The method was developed for the US Air Force Logistics Command by Lawrence National Laboratory in 1985.

The system is structured to allow screening of asset/threat event combinations so only high impact risks are reviewed. The system looks at proposed and present security features. LRAM is structured in three stages.

Scoping of Analysis

This phase defines the scope of the analysis and identifies needed resources and personnel.

Risk Identification

Risk elements are identified by establishing corresponding threats, countermeasure and assets.

Decision Support

This process is concerned with selecting and listing in priority each recommended countermeasure on the basis of cost benefits estimates.

References:	(S2014, 1993), (Wahlgren, 1990), (Guarro, 1987)

Method Name: Melisa

Country Of Origin: France

Required Experience: None

System: Computer based

Description:

Assets Protection:	Extensive
Impact Analysis:	Extensive
Threat/Vulnerability	Extensive
Analysis:	
Level Countermeasures:	Extensive

Melisa was developed for the French Navy in 1985. The method expresses threat and vulnerability levels by using a quantitative and qualitative approach. Risk is expressed by using a quantitative approach. The threat levels are measured is terms of its seriousness and vulnerability levels are presented by grades. Risk levels are presented by a score of between 0 (no risk) and 100 (absolute risk).

References: (S2014, 1993), (Wahlgren, 1990)

Method Name: SDC US Navy Risk Assessment Methodology

Country Of Origin: USA

System: Paper based

Description:

The system was developed in 1979 for the US Navy. The
method consist of six phases. The first three are concerned with
identifying the system to be evaluated, identifying the threats
and then the vulnerabilities. The identification of threats and
vulnerabilities using a qualitative approach, e.g. low, medium.
The fourth stage is concerned with matching threats and
vulnerabilities to determine areas of possible attacks and
impacts. The fifth stage is concerned with expanding the
impacts and this is determined by multiplying the impact
against the frequency of attack (using supplied mathematical
tables) to determine the annual loss expectancy (ALE). The
sixth stage is concerned with selecting the countermeasures.

References: (Neugent, 1985)

Method Name: Security by Analysis (SBA)

Country Of Origin: Sweden

Required Experience: Method specific training and IT security knowledge

System: Computer based

Description:

Assets Protection:	Extensive
Impact Analysis:	Extensive
Threat/Vulnerability	Extensive

Analysis:

Level Countermeasures: None

The method expresses risk, threat and vulnerability levels by
using a quantitative and qualitative approach. The method was
originally developed in Sweden for their Ministry of Defence,
but is now used by all commercial sectors. The method
describes the principles an analyst should adopt to examine
threats in a business area. The SBA method is based on
the analysis of three factors which affect the vulnerability of
computer systems, these are:

       - interruptions in information processing systems;

       - unauthorised use of information;

       - poor information quality.

The SBA method consists of various modules that can be used
independently of each other, these modules are:

SBA Start   - this module relates to managers
                      judgements of their present security
                      situation, e.g. how serious would the
                      consequence, be if something
                      happened;

SBA Dependence	- reveals the functions that the organisation is more dependant upon and the information systems supporting these functions;
SBA System	- analyses how the systems behave under the influence of various vulnerability factors;
SBA Scenario	- assesses the data risks by means of imagined future events, e.g. worse case scenarios;
SBA Report	- an assessment of the current state of information security within the organisation;
SBA Project	- estimates the risk of a project;
SBA Development	- eliminates risk factors of system developments;
SBA Key Personnel	- analyses the organisations dependence of key staff.

References: (S2014, 1993), (Wrede, 1984), (Voutilainen, 1989)

Research

Method Name: SARA (Simple to Apply Risk Analysis)

Country Of Origin: Europe

System: Paper based

Description:

The method was developed by the European Security Forum.

Due to the fact that I have signed a non-disclosure agreement

relating to this method, I cannot expand upon it any further.

Method Name: SEISMED Risk Analysis Method

Country of Origin: Europe

System: Paper Based

Description:

The method was developed as part of the SEISMED project,

it is a development of the ZIP methodology. The method has

not been used within healthcare and it has not been adopted

by any official organisations.

References: (Davey and King, 1995)

Method Name:	SESAME HYPERVIEW
Country Of Origin:	France
System:	Still in development
Description:	

Assets Protection:	Extensive
Impact Analysis:	Extensive
Threat/Vulnerability Analysis:	Moderate
Level Countermeasures:	Extensive

The method expresses risk, threat and vulnerability levels by using a quantitative and qualitative approach. Risk is expressed by using a qualitative approach. The system is still been developed and it is one of the few methods developed for use by UNIX systems.

References:	(S2014, 1993)

Other methods

The following are a list of known risk analysis method that exists but no information was found relating to them:

> BP Methodology (not commercially available);
>
> Chase Manhattan Bank;
>
> CSAEP (Computer Security Assessment and Evaluation
>
> > Package);
>
> CVRP;
>
> DHSS Methodology (not commercially available);
>
> DIAPASON;
>
> EBP;
>
> GRAM;
>
> ICI Methodology (not commercially available);
>
> M2 Risk;
>
> Risk Manager;
>
> PARI/AEROSPATIALE;
>
> Predictor.

References: (S2014, 1993)

Appendix G Published Papers

Published Papers

Conferences

Particaptional Management and the Implementation of Multimedia Systems,

by M.J.Warren, P.W.Sanders and P.N.Gaunt,

MEDIACOMM 95 - International Conference on Multimedia

Communications.

Southampton, England, April, 1995.

Secure Multimedia Systems in Healthcare and Medicine

by S.M.Furnell, N.J.Salmons, P.W.Sanders, C.T.Stockel and M.J.Warren,

MEDIACOMM 95 - International Conference on Multimedia

Communications.

Southampton, England, April, 1995.

Security Criteria Expert System - the medical application,

by M.J.Warren, P.W.Sanders and P.N.Gaunt

International Conference on Neural Networks and Expert Systems in Medicine

and Healthcare Conference,(NNESMED 94),

Plymouth, England, August, 1994.

Impact of Security on a healthcare environment and how to overcome it,

by M.J.Warren and P.N.Gaunt,

IMIA (International Medical Informatics Association) WG4,

Caring for Health Information Conference,

Heemskerk, The Netherlands, November, 1993.

Journals

Development of Security Guidelines for Existing Healthcare Systems

by S.M.Furnell, P.W.Sanders and M.J.Warren,

Published 'Medical Informatics', Vol 20, no 2, 1995.

A Generic Methodology for Health Care Data Security,

by S.M.Furnell, P.N.Gaunt, G.Pangalos, P.W.Sanders and M.J.Warren,

Published 'Medical Informatics', Vol 19, no 3, 1994.

Awaiting Publication

Conferences

ODESSA - Baseline Security Risk Analysis,

by M.J.Warren, P.W.Sanders and P.N.Gaunt,

To be published.

Provision of healthcare security information using the World-Wide-Web,

by S.M.Furnell, P.W.Sanders and M.J.Warren,

MIE 96, Denmark, August, 1996.

Journals

Assessing staff attitudes to information security in a European healthcare

establishment,

by S.M.Furnell, P.N.Gaunt, R.F.Holben, P.W.Sanders, C.T.Stockel and M.J

Warren,

Medical Informatics, UK.

PARTICIPATIONAL MANAGEMENT AND THE IMPLEMENTATION OF MULTIMEDIA SYSTEMS

M.J.Warren[1] & P.W.Sanders[1] & Dr P.N.Gaunt[2]

[1]Network Research Group, SECEE,
University of Plymouth,
United Kingdom
E-mail: Matw@soc.plym.ac.uk

[2]Division of Health Care Informatics,
Faculty of Medicine, University of Plymouth, United Kingdom

ABSTRACT

Multimedia is the latest development in user information presentation systems. In certain sectors there will be an increasing dependency upon the quality of data that is delivered by multimedia systems. Acceptance of the computer systems by users is of utmost importance, and without this acceptance a whole series of problems can occur relating to the user and the organisation.

The paper describes a methodology that can be used for the process of implementing multimedia systems and determining the problems that could occur during the implementation stage This is the first step in the UK towards developing a complete approach that can be used for change control management in respect to multimedia systems.

INTRODUCTION

The use of this new type of presentation will have a major impact across many different sectors, that range from business to healthcare. The use of multimedia systems will be major component of the information age, but there are problems; technological innovations by themselves are not enough for the development of systems that users require and need[1]. Other considerations relate to availability and reliability of the systems once they have been introduced.

The introduction of new technology into an organisation is not only a technical but also a human issue the following should be considered:

Human Issues
The main impact areas are:

- User requirements
New technology directly affects users. There is little evidence that managers have recognised the need of using IT (including multimedia) to change the way they do business [2].

Users requirements should be incorporated fully into the system design from the start so that the system that is designed actually complies with user requirements.

- User job satisfaction
The way in which the multimedia system operates usually has a direct affect upon the user and the way they use the system. If the user is unsatisfied with the system they will become less motivated and users will take longer to carry out tasks; or might not even use the system at all. It is important to determine how users will react to the visual style of data that will be contained within the multimedia system

Organisational Issues

The introduction of new technology is a method by which organisations can gain a competitive edge by increasing their efficiency. The main organisational issues are:

- Technical Impact

The introduction of new technology often has a technical impact within the organisation. Computer system should be phased in gradually in order to smooth out compatibility problems that could arise.

- Training

The introduction of new computer systems will require the training of users in order to use it effectively. Training considerations would relate to the level of training required, the number of staff requiring training and the amount of time lost by staff because of training. A particular consideration will be making users aware of the limitations and advantages of using multimedia information.

- Costs

An important organisational issue is that of cost. Any new technology being introduced will be more expensive then existing available technology. User costs also have to be considered, such as the cost of training.

- Culture

The introduction of new types of technology could have a direct or indirect impact upon the culture of the organisation, i.e. new technology being seen as status symbols, jobs being redesigned around the new technology.

WHAT IS SIM-ETHICS?

SIM stands for Security Implementation Methodology and ETHICS stands for Effective Technical and Human Implementation of Computer based Systems. ETHICS was originally developed by Professor Enid Mumford of the Manchester Business School.

SIM-ETHICS is a methodology that manages the implementation of IT technology, i.e. from multimedia to organisational IT policies. It allows for the assessment of factors relating to:

-determining the impact of technology in terms of user job satisfaction and system efficiency and effectiveness.

-determining problems that could occur when implementing new technical systems within an organisation.

-determining the training required to use the implemented technology.

SIM-ETHICS is based upon the concept of participational management, and uses a selection of committees as a basis to discuss organisational issues [3].

Part of SIM-ETHICS is used to evaluate multimedia applications against a pre-defined set of criteria. These criteria relates to:

- Ease of Implementation
- Training Issues
- User Impact of multimedia
- Organisational Impact
- Human Issues regarding the use of multimedia

The criteria means that major problems could be foreseen and overcome before the actual implementation of the system occurs.

THE USE OF SIM-ETHICS

SIM-ETHICS has been successfully used in Plymouth NHS Hospital Trust, UK to determine:

- the impact of a security physical swipe card system.
- the impact of a computer system that will be used for sending memos and office notices ; internally via e-mail.
- users perceptions of passwords.
- security training needs for users and system managers.

SIM-ETHICS is intended to be used in the future to determine:

- the organisational impact of a new IT security policy.

- the impact of various new computer systems, including multimedia systems.

CASE STUDY

The case study relates to a new multimedia system that is being considered within the Plymouth NHS Hospital Trust. The aim is to develop electronic health care records for all patients that are treated within the Trust for certain cancers. The medical record is the most important repository for information covering patient's healthcare. The traditional paper-based system suffers from serious drawbacks [4]. The drawbacks relate to factors such as duplication of information, illegible handwriting.

The electronic health record system would contain a mixture of text and multimedia and will help to overcome some of the problems of paper-based medical records.

The system will be PC based to allow for integration with existing medical computer systems.

The perceived advantages of such a system are:

- simple to use, so any member of staff should be able to use it;

- allows for more accurate and complete storage of patient details during their treatment in different areas of the hospital;

- allows for greater access to patient details by staff involved in the treatment, e.g. by general practitioners, community nurses;

- improves the quality of patient data records, i.e. by reducing duplication and improving illegibly;

- improve the working relationship that exists between the clinical teams providing cancer services;

- allows long term follow up of patients;

- allows for instant access to medical records, 24 hours a day.

Problems with implementation

The main problems with implementation will be:

- designing a system that meets user requirements and can be used by many different types of staff:
    - doctors
    - nurses
    - laboratory staff
    - radiographers
    - community nursing staff
    - general practitioners

- Designing a multimedia record that incorporates data from the following information sources:
    - general practitioners
    - hospital clinics and wards
    - pathology and radiology departments
    - oncology department
    - community nurses

- Determining the training requirements of users.

- Initiating awareness programs to educate staff about multimedia and it's implications.

- Problems of integrating with various existing comput systems.

Case study Diagram

The diagram on the next page shows an overview of the system. It shows the main function areas of the system and shows the different types of data that exists within the system. This data will be contained within the new multimedia health record.

The diagram shows that, though the system is being designed for the treatment of certain cancers, it will have a direct effect on general practitioners, neighbouring trusts and several departments within Plymouth Hospital Trust. The users could number several hundred staff with different requireme and needs from the system.
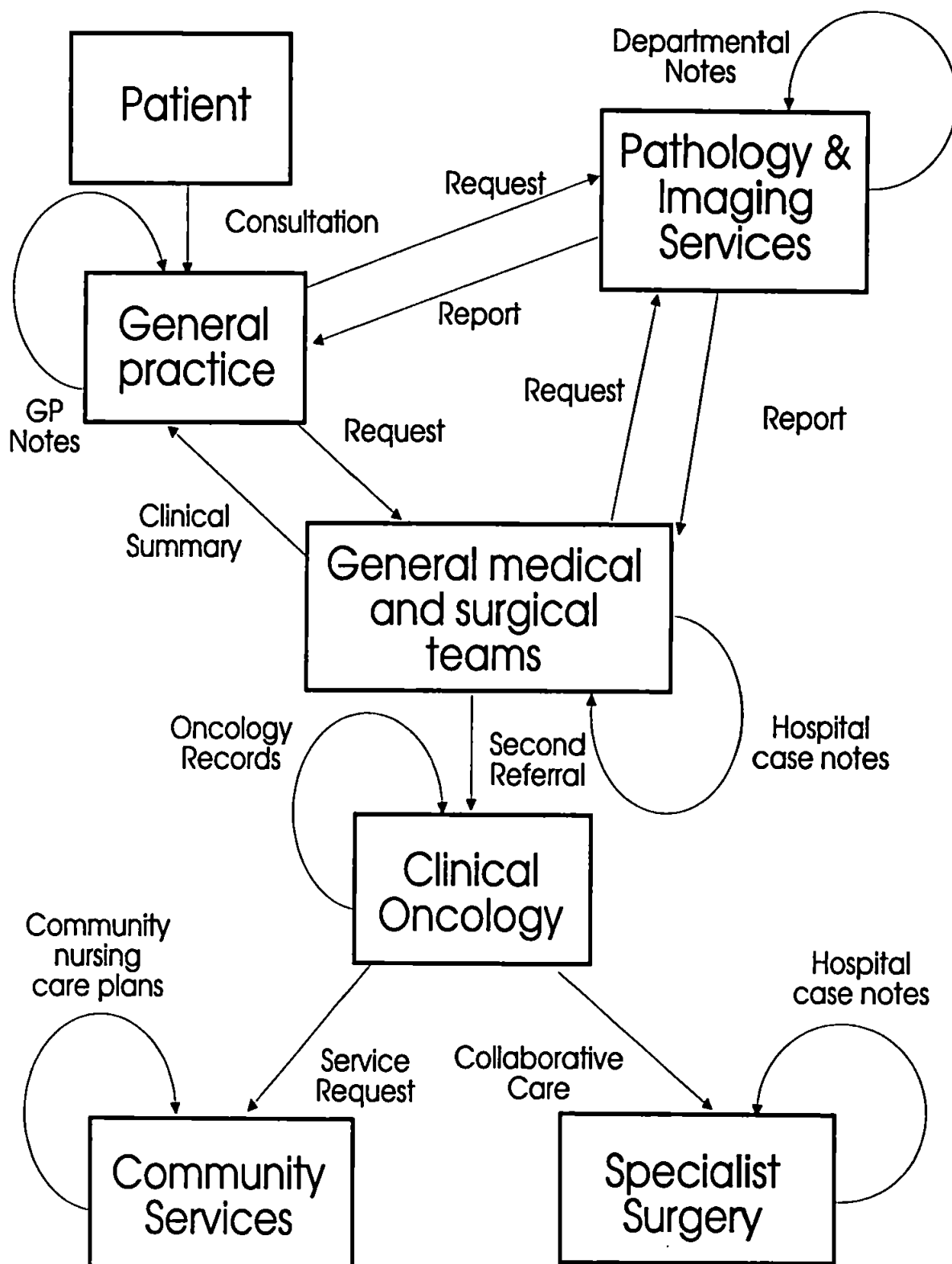
System Overview

Intended use of SIM-ETHICS

The following indicates the framework that is intended to be used for the introduction of the new multimedia medical record system.

1) Initial Committee Consultation

The committee will be made up of a cross section of staff directly involved or affected by the implementation of the new computer system. i.e.:

- representatives of clinical staff from the different departments affected by the change
- representatives of the IT department
- representatives of the GP's who will be working with the system

The committee will decide initially on what should be considered the major impacts:

- the impacts of introducing multimedia
- training of users
- cost of new equipment
- compatibility with existing clinical and administrative computer systems

2) Managerial consultation

The intended computer system is evaluated against the SIM-ETHICS criteria to determine the level of impact it's implementation will have.

A representative of the committee would meet the following

- system managers of existing clinical systems
- specialist IT managers, i.e. network managers
- managers and staff involved in implementing the new multimedia system.

At these meetings issues relating to the introduction of the system are discussed (as determined in Stage 1) as well as any other possible problems that managers could see.

3) Committee Stage

The views of the managers are discussed within the committee. It is now that initial problems are discussed, i.e. problems of changing existing paper based medical records into the new required format.

The committee decides on:

- What questions to ask,
  i.e. How do you feel about having to use a new type of medical record.
- The type of user to ask,
  i.e. Ward clerk
- The number of users to ask
  i.e. Every ward clerk

4) Users consultation

A representative of the committee then meets the users to explain the proposed system and then ask them a series of questions.

The multimedia system is then re-evaluated against the criteria to take into account the newly raised issues.

5) Committee Stage

The views of the users are discussed. If problems are found concerning the system, ways would be discussed on how to overcome the problem, i.e. increase the amount of training.

6) Post implementational review

This meeting takes place after the implementation to determine if any unforeseen problems have occurred and discuss ways in which to rectify the problems.

CONCLUSION

The key to successfully implementation of new computer systems is an participational approach involving the staff directly affected ensuring their acceptance of the system The work being carried out is a step towards developing a generic methodology that could be used for the implementation of multimedia systems.

References

JOURNAL
[1] P.F.Chatterton. 1991. "Multimedia computing in the retail industry", *Information Services & Use,* Volume 11: 337 - 344,

[2] I.Gretton, 1994. "The Promise of IT", *Professional Manager,* Volume 3, no.3(July): 20 - 21

BOOK
[3] E.Mumford, 1983, " Designing Participatively," Manchester Business School, UK, ISBN 0-903808-29-3

PROCEEDINGS
[4] W.Ceustres(et al) "The aim of the nineties bringing multimedia records to life" In Proceedings of MIE 93, (Jerusalem, Israel Apr. 18 -22), Freund Publishing House Limited, London, UK

SECURE MULTIMEDIA SYSTEMS IN HEALTHCARE AND MEDICINE

Steven M Furnell, Nichola J Salmons, Peter W Sanders, Colin T Stockel and Matthew J Warren
Network Research Group
Faculty of Technology
University of Plymouth
Plymouth, United Kingdom
E-mail : nichola@soc.plym.ac.uk

ABSTRACT

The aim of this paper is to examine the increasing potential for applying multimedia technology within the medical community. Multimedia is considered to be a particularly appropriate means for information delivery within Healthcare Establishments (HCEs), especially for that relating to patient care, and the paper considers the principal advantages in this area. The discussion then proceeds to highlight the fact that adoption of multimedia dictates new requirements for information security and, by the nature of the technology involved, also allows new approaches to be explored. On this premise, the outline of a security strategy for future multimedia healthcare networks is proposed. The discussion is supported by an example scenario and a brief examination of our own research groups efforts in this area.

INTRODUCTION - MULTIMEDIA IN MODERN MEDICAL CARE

Over the past twenty years computerised information systems have gradually been introduced to, and utilised within, a large number of healthcare establishments (HCEs). Information Technology (IT) now enables modern HCEs to provide more comprehensive medical care, comprising more numerous and more complex procedures. As such, HCE systems now process and handle information beyond simple text and graphics and more advanced medical applications may also generate digital images, full motion video and audio. The use of this multimedia information can considerably aid patient diagnosis and treatment (Ceusters et al. 1993).

As a result of recent advances in desktop processing power, the large scale use of multimedia-based healthcare systems is closer to being an achievable goal, with the presentation and delivery of multimedia information becoming possible at a viable price. This is largely due to the fact that PC-based systems can now represent a realistic platform for multimedia and can be found in numbers in most HCEs. In addition, telecommunications networks are now capable of handling the high speeds necessary to transfer large amounts of multimedia data,

allowing further improvements to the speed of information delivery within and between HCEs.

In terms of advantages, the presentation of medical data in a multimedia format is considered to be ideally suited to the healthcare field as it inherently provides more information (Orozco-Barbosa et al. 1992), and in a form that is more easily comprehended than traditional text-based reports. This should indirectly help to improve the quality of care, as clinical decisions are made on the basis that the clinician has direct access to the most comprehensive information possible. In addition, it will allow the seamless integration of existing operational systems, with the ability to maintain a standardised viewing structure. As such, the potential applications of multimedia in healthcare are wide-ranging. For example, an area of significant potential will be the establishment of composite electronic health records, bringing together various types of multimedia patient data into a single entity (Arnold and Peter 1993). Such electronic multimedia record systems have the potential to significantly improve care delivery as they will allow immediate access to *full* patient data at any time, with flexible options for retrieval (whereas the same data may currently be held in several different places, making it difficult for clinicians to obtain all of the information that may be available).

REQUIREMENTS FOR SECURITY

It is important to recognise that a major consequence of the progression to multimedia will be an extension of the already significant reliance upon IT in healthcare establishments. This reliance stems from the increasing number of healthcare IT applications, particularly those relating to clinical care, that are now fundamental to routine clinical practice (Barber 1991). A number of future trends are predicted (European Commission 1994), with European project sponsorship (in the 4th Framework) under way, that will further increase this dependency. These include :

- increased intra and inter-HCE networking;
- increased exchange of data between HCEs;

- increased potential for sharing of facilities between HCEs;
- establishment and adoption of the composite electronic health record.

Due to the comprehensive nature of the information presented, it is envisaged that there is likely to be a even greater level of implicit trust in the correctness of the system. As such reliance upon IT increases, so too does the potential impact of any system unavailability or erroneous data. This, therefore, heightens the requirement to ensure that the availability and integrity of medical systems can be maintained.

In addition, further considerations arising from the increasing variety and complexity of data dictate a greater need for confidentiality controls. Firstly, the amalgamation of different forms of data into the composite record may potentially increase the sensitivity of the information beyond that of any of the component parts. Secondly, information that would previously have been held (and potentially secured) by separate applications would now be placed together, and thus the impact of a security breach would be significantly higher. The use of multimedia can, therefore, be seen to affect all three main principles of information security (i.e. confidentiality, integrity and availability).

As a result of these considerations, the authors believe that a different approach may be necessary to integrate security into multimedia systems and that the environment may also allow new opportunities to be explored.

A SECURITY STRATEGY FOR MULTIMEDIA HEALTHCARE SYSTEMS

Whilst many areas of security (e.g. physical, environmental and personnel considerations) will not be directly affected by the multimedia context, there will be noticeable effects in others; some significant, some less so (e.g. the quantity of data involved will affect the backup process in terms of increased storage requirements and, potentially, the time required to perform the task). The paper concentrates upon two aspects in particular which should be re-examined in light of the trends predicted above; namely *user authentication* and *data communications*. In both of these cases, an important issue will be the transparency of protection mechanisms employed. One of the main advantages of multimedia systems is that data can be presented in a more natural and "user-friendly" context. As such, there is a dilemma that whilst the systems must be easy to use and effective, they must at the same time be made secure. This does not necessarily mean that users should be totally unaware of security (indeed, it will probably increase trust in the system if some security is seen to be present), but it must not interfere with their work and should be compatible with the general "feel" of the system.

User Authentication

User authentication mechanisms will still be required to prevent impostors masquerading at local terminals and workstations. However, two factors suggest that traditional password-based methods alone will no longer be sufficient protection :

- multimedia systems will significantly reduce the role of keyboard input in some contexts (e.g. information retrieval), such that it may not be required at all HCE terminals. As having to retain a keyboard simply for user authentication purposes would hardly constitute transparent security, an authentication mechanism not requiring this aspect would be desirable;

- the increased data sensitivity that could potentially result from the composite record context adds weight to the argument that passwords (which often provide a weak / unreliable basis for authentication anyway (Jobusch and Oldehoeft 1989)) should be supplemented by other mechanisms.

The use of smart card systems may have a place in overcoming these problems, but may not be practical as a compulsory measure as this would introduce an immediate financial burden across the whole system (which most HCEs would not be able to tolerate at the present time).

A appropriate alternative would be to utilise advanced user supervision systems which could operate transparently and in real-time throughout each session (Lunt 1993). A number of factors could potentially be encompassed by the supervision, including :

- times and locations of system usage;
- typical applications used;
- types of data accessed and how it is used;
- analysis of the users typing style (if a keyboard is still used).

The use of neural network techniques could allow appropriate information on these (and other factors) to be gathered automatically, with subtle behaviour patterns being learnt in order to develop *profiles* for legitimate system users. Current user activity could then be

continuously compared against the profile for the users claimed identity (with significant departures causing an alert to be generated).

In addition to the above, multimedia systems may allow many new options to be introduced for improving authentication. For example, appropriate hardware for implementing several biometric identification methods may already be present "as standard" in a multimedia configuration (e.g. cameras which may be used for image / "faceprint" recognition, microphones and audio processing facilities for voice recognition). These techniques have been successfully implemented elsewhere, delivering adequate authentication performance and gaining a high degree of user acceptance (Sherman 1992). As such they should integrate well with multimedia systems. However, the presence of such hardware enhancements should not be a prerequisite of the authentication strategy for the same reasons as smart cards. Nevertheless, some mechanism should be incorporated to allow extra facilities to be utilised if they are present.

Future multimedia systems may, therefore, demand that a variety of authentication technologies are actually employed, based around an approach that is primarily software-oriented. These may then be linked / managed by an intelligent supervision system which can select the most appropriate mechanism to be invoked at any given point according to the current user activity and the type of system being used (e.g. keystroke analysis could be used in any text-intensive activity; facial recognition could be used if the host system is equipped with a camera). Note that once authentication has been conducted, any underlying data / application access and auditing controls could still be implemented in a traditional manner to restrict and monitor the activities of different classes of user.

Data Communications

One of the trends likely to result from the availability of more and better information is the increased sharing and exchange of data between HCEs. In the UK, the National Health Service (NHS) already plans to bring all aspects of voice and data communications together into a common framework, with all major HCEs having the facility to communicate electronically by 1996 (NHS Management Executive 1992). However, the transmission of composite records again raises the concerns of confidentiality and integrity (i.e. the need to protect messages against unauthorised interception, modification and falsification). Hence the requirement to have secure data communications will also be correspondingly greater. A strategy is proposed that would introduce layered

security at local, national and international levels with encryption of data between different security *domains* (based upon a Trusted Third Party (TTP) approach as shown in figure 1).
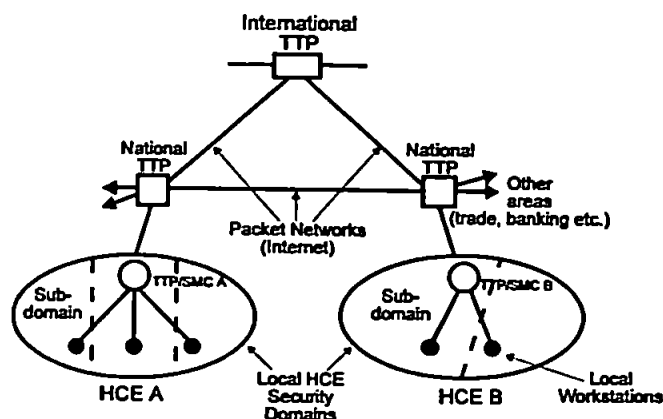

Fig. 1 : Secure Data Communications using a TTP hierarchy

The TTP would be capable of providing three main types of security service in relation to data transmission :

- integrity (e.g. checksums);
- non-repudiation (e.g. digital signatures);
- confidentiality (e.g. encryption).

These services would be applied, as appropriate, to communications at all levels of the TTP hierarchy. In addition, encryption could be used to protect stored data where workstations in the local domains cannot be physically secured. However, it should be noted that whilst the facility for encryption would exist, its use in healthcare is currently restricted in some EC countries. The operation of all data communications services could theoretically be made completely transparent to the end user (although in some cases, such as the use of digital signatures, users should be given some indication that a security service is being provided).

As can be seen from the figure, the Security Management Centre (SMC) introduced to handle the authentication system will also assume responsibility for securing communications in each local domain. The SMC facilities could be incorporated as part of an overall Network Management Centre.

This strategy would increase the importance of maintaining availability, with a reliance upon the availability of interconnected systems as opposed to earlier isolated ones. The hierarchy would, therefore, be designed to be fault tolerant to enable secure operations to continue even in the event of individual TTP failure.

However, this strategy obviously depends upon the overall TTP infrastructure being in place before it can be realised. Therefore, in the short to medium term, individual HCEs and co-operating establishments will require alternative means by which their communications can be secured (AIM SEISMED 1994). In addition, due to the enormous volume of data involved in multimedia data communications, there are also questions that must be addressed regarding the need for compression and how Message Authentication Codes (MACs) may then be used. In the longer term, the fact that uses of the TTP would not be restricted to the healthcare domain could aid its introduction and acceptance at the national and international levels. The use of TTPs in the healthcare context is described in more detail in (Furnell and Sanders 1995).

EXAMPLE SCENARIO

This section presents an example scenario to illustrate how future multimedia data exchange would be likely to function within and between HCEs. This is, in turn, used to highlight the need for security at the various stages involved. To this end, the information flows involved in a potential multimedia healthcare system are illustrated in figure 2 and explained in the description below.
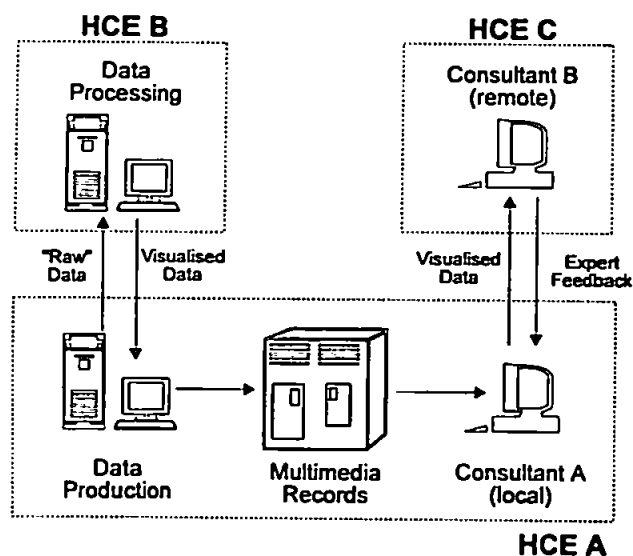

Fig. 2 : Multimedia Healthcare Application

The neurology department in one establishment (HCE A) performs a series of tests which produce a set of "raw" results data. However, HCE A lacks the equipment required to process and visualise the data, making it necessary to involve another site (HCE B). Once visualisation has been performed the results are transmitted back and stored in a database, from where they are subsequently accessed by a consultant at HCE A. However, further expert opinion is required and advice is, therefore, sought from another neurological consultant located at HCE C. Hence, the data is exchanged further, with the additional interpretation finally coming back to the originating consultant (allowing a more informed care decision to be made at HCE A). The consultants at HCEs A and C have access to a video conferencing link from their camera-equipped workstations, whilst the other parties in the scenario use standard workstations without such a facility.

From this basic outline, a general security specification can be given based upon the strategy described earlier. The different HCEs would communicate via local and national level TTPs, with all parties being authenticated by their local SMCs. Given that their workstations are equipped with cameras, the two consultants could potentially be authenticated by an image recognition system. However, the data production and data processing centres, utilising standard workstations, would have no facility for multimedia-enhanced authentication methods. Authentication of these parties would, therefore, be reliant upon the SMC facilities for activity supervision (possibly alongside traditional methods). The example is heavily communications oriented and the SMCs would communicate via the TTP hierarchy to authenticate and validate the various data exchanges and messages. The principal services required between HCEs A and B would be data integrity and confidentiality, whereas the HCE A / HCE C link would also require that the consultants were unable to repudiate information messages added to the system.

The example primarily illustrates the types of information exchange and consultations that the use of multimedia in healthcare will make possible. It also serves to underline the need for secure data communications between the various parties involved. The use of the TTP / SMC hierarchy would ensure that security was consistent across the three sites involved; a factor that considerably reduces the potential problems of sharing data and facilities as discussed.

CONCLUSION

The need for security is not unique to multimedia-based systems - indeed, similar demands already exist in many operational healthcare applications. However, the important point is that introduction of multimedia will serve to increase the demands significantly. Neither is the proposed security strategy restricted to applications within healthcare establishments. However, the primary reliance

upon software methods makes it particularly suited to HCEs, which are often more significantly financially constrained in relation to security than other types of organisation.

Our group is currently involved in the development, implementation and evaluation of a prototype multimedia patient records system in co-operation with a local HCE. Security is being considered as a key issue the project, with elements of the proposed strategy being addressed. It is hoped that the research will also help to identify other considerations that arise from the practical implementation of multimedia in healthcare.

The adoption and utilisation of multimedia technologies in healthcare is accelerating and it is likely that there will be a period of transition as research projects and pilot programmes (such as the EC 4th Framework) proceed in this area and produce their recommendations. From these, the principal uses and benefits of multimedia within healthcare will be established. We believe that it will be important for security issues to be considered during the planning and development of future systems, as the nature of the environment could well make it more difficult to securely integrate suitable protection later (or at least without it appearing to be an obvious afterthought).

REFERENCES

Arnold, U. and G. Peter. 1993. "A computer-based, distributed multimedia patient record : Use of new technologies for computer-based medical records", In *Proceedings of MIE 93 - 11th International Congress of the European Federation for Medical Informatics* (Jerusalem, Israel, Apr. 18-22), 585-590.

Barber, B. 1991. "Towards an information technology security policy for the NHS", *British Journal of Healthcare Computing*, British Computer Society.

Ceusters, W.; R.Bonneu; G. De Moor; R. Lapeer; and G. Thienpont. 1993. "The challenge of the nineties: bringing multimedia healthcare records to life", In *Proceedings of MIE 93 - 11th International Congress of the European Federation for Medical Informatics* (Jerusalem, Israel, Apr. 18-22), 594-599.

European Commission - DG XIII. 1994. *Telematics Applications Programme (1994-1998), Healthcare (area c, sector 7).* (Sep).

Furnell, S.M. and P.W.Sanders. 1995. "Security Management in the Healthcare Environment", to appear

in *Proceedings of MedInfo 95 - 8th World Congress on Medical Informatics* (Vancouver, Canada, Jul. 23-27).

Jobusch, D.L. and A.E.Oldehoeft. 1989. "A Survey of Password Mechanisms : Part 1", *Computers & Security* 8, no. 7: 587-604.

Lunt, T.F. 1993. "A survey of intrusion detection techniques", *Computers & Security* 12, no. 4: 405-418.

NHS Management Executive Information Management Group. 1992. *Handbook for IM&T Specialists*, Department of Health, United Kingdom (Dec).

Orozco-Barbosa, L.; A.Karmouch; N.D.Georganas; and M.Goldberg. 1992. "A Multimedia Interhospital Communications System for Medical Consultations", *IEEE Journal on Selected Areas in Communications* 10, no.7: 1145-1156.

AIM SEISMED Project. 1994. *Guideline for Cryptographic Mechanisms*, Secure Environment for Information Systems in MEDicine, SEISMED (A2033).

Sherman, R.L. 1992. "Biometric Futures", *Computers & Security* 11, no. 2: 128-133.

SECURITY CRITERIA EXPERT SYSTEM CONCEPT: THE MEDICAL APPLICATION

M.J.Warren[1,2], P.W.Sanders[1] and Dr P.N.Gaunt[2]

[1]Security Research Group, Faculty of Technology, University of Plymouth
United Kingdom
[2]Department of Health Care Informatics, Faculty of Medicine, University of
Plymouth, United Kingdom

ABSTRACT

In many Health Care Establishments (HCEs) there is an increasing dependency upon computer systems and the data contained within these systems. The importance of this data dictates that computer systems have to be properly protected. Within the NHS there is generally a low understanding of computer security and the problems of implementing security.

This paper describes a methodology that can be used for the process of implementing security and determining the problems that could occur during the implementation stage. This is the first step within the UK towards developing a complete approach that can be used for change control management regarding security.

The paper describes how the methodology will be developed as an expert system and used in conjunction with a newly developed risk analysis methodology.

The work contained in the paper was developed as part of the European Union SEISMED (Secure Environment for Information Systems in MEDicine) research project, the aim of which is to provide recommendations and guidelines for European HCEs.

INTRODUCTION

Security is a human issue and should be considered in the context of the health care staff. A problem with introducing security into HCE's is that it is not only a technical

problem but also an organisational issue. There is a requirement for a method to control the introduction of security and determining the different impacts that this introduction could have upon the HCE or a wider range of organisations, SIM-ETHICS was developed because of this.

WHAT IS SIM-ETHICS?

SIM stands for Security Implementation Methodology and ETHICS stands for Effective Technical and Human Implementation of Computer based Systems. ETHICS was originally developed by Professor Enid Mumford of the Manchester Business School.

This is a methodology that managers the implementation of security countermeasures. It allows for the assessment of factors related to:

> -determining the impact of security in terms of
>> user job satisfaction and system efficiency and effectiveness
> -determining technical problems that could occur when implementing
>> security within an organisation.
> -determining the training required to use the implemented security
>> countermeasures.

A more detailed breakdown of these factors are found in [1].

SIM-ETHICS is based upon the concept of participational management, and uses a selection of committees as a basis to discuss organisational issues [2].

SIM-ETHICS is used to evaluate security countermeasures against a pre-defined set of criteria.
> - Ease of Implementation
> - Training Issues
> - User Impact
> - Organisational Impact
> - Human Issues

A more detailed explanation of the criteria can be found in [3].

The use of the SIM-ETHICS security criteria allows countermeasures to be evaluated and suggest impacts that their introduction could cause, the use of this criteria will form a major component of the knowledge base of the expert system.

The steps of SIM-ETHICS

The following framework is used to implement SIM-ETHICS. The stages of the process are:

> 1) Initial Committee Consultation
> The committee decides which countermeasures to look at, taking into account issues such as training of users and the number of users affected by the proposed countermeasure.

A representative of the committee meets the managers concerned with implementing the countermeasures. Issues relating to the introduction of the countermeasures are discussed as well as any other possible problems that could occur. The countermeasures are evaluated against the SIM-ETHICS criteria.

3) Committee Stage
The views of the managers are discussed. It is then decided which users to interview, i.e. staff nurses and how many of them.

4) Users consultation
A representative of the committee then meets the users to explain the proposed countermeasures and the problems that they may cause. The representative will ask the users for their views about the countermeasures and possible problems that their implementation could cause The countermeasures are then re-evaluated against the SIM-ETHICS criteria

5) Committee Stage
The views of the users are discussed. If problems are found concerning the countermeasures, ways would be discussed on how to modify them, i.e. increase the amount of training, reduce the scope of implementation.

6) Post implementational review
Once the countermeasures have been implemented, a meeting will take place with the users to determine if any unforeseen problems have occurred and try to discuss ways to try and overcome them, i.e. arranging more training for certain staff.

The use of SIM-ETHICS

It is being used at Derriford Hospital, Plymouth, UK to determine the impact of new security countermeasures and a new computer information systems. The security areas being looked at are:

a new physical access control system for the whole hospital
a new method of assigning levels of access for all computer users
a new Information Computer Systems

THE EXPERT SYSTEM

The lack of security awareness within the NHS generates a requirement for a low cost source of appropriate expertise. The answer maybe an expert system. The SIM-ETHICS methodology will be combined with a new risk analysis methodology, ODESSA (Organisational Descriptive Security Analysis) to produce such a system. This expert system should allow staff instructed on risk analysis techniques to review a system and then determine the impact that recommended security countermeasures could have upon their department or organisation.

ODESSA is a newly developed risk analysis methodology, which operates by determining baseline security countermeasures, these countermeasures are then

modified to fit the organisational requirements by the use of risk analysis techniques. ODESSA is an extension of a theoretical risk analysis modal developed for HCE's [4], many new features have been added to this theoretical modal to produce a fully working method.

The expert system will be designed using a formal methodology such as KADS [5], to promote the benefits of:

- easier planning
- a structured approach for the design of expert systems
- an improved requirement analysis

KADS itself is a design methodology that can be adjusted to fit the scale of the problem. It is not envisaged that the full KADS methodology will be used in the design of the expert system but rather a cut down version, the reason for this is that KADS was originally developed for developing large expert systems, this explains why there are seven steps just in the feasibility stage [5].
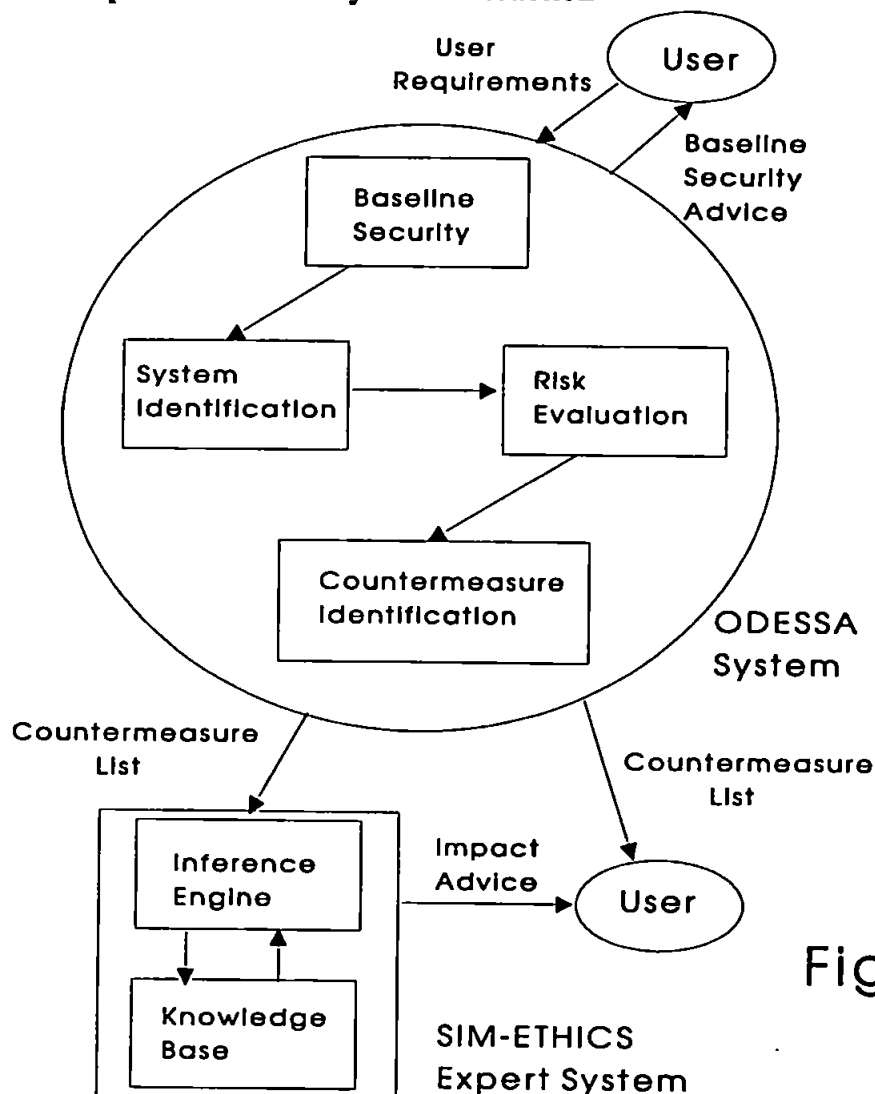
Conceptional View of System Interaction

Figure 1

ODESSA System

The ODESSA system is broken down into four main stages:

1) Baseline Security - The user is given basic security advice for their
   organisation.
2) System Identification - System assets are evaluated
3) Risk Evaluation - Risks and vulnerabilities are determined
4) Countermeasure Identification - Appropriate countermeasures are produced

SIM-ETHICS Expert System

The expert system takes the countermeasure lists produced by the ODESSA
system and determine the impact that their implementation could have.

Environment in which the expert system will operate

The SIM-ETHICS expert system will work as part of the ODESSA program suite. The
ODESSA prototype will be written in Visual Basic. The interface facilities of Visual
Basic means that a language such as C++ could be used as the host language of the
expert system. The advantage of using C++ is its portability, the speed at which it
operates and the fact that it allows the use of object orientation.

Knowledge Analysis for the expert system

Knowledge analysis is an important stage in the development of any expert system. This
analysis determines the rules which would populate the knowledge domain and
therefore structure the behaviour of the expert system.

As part of the knowledge analysis process the following areas will be looked at:

Environmental Analysis
This analysis is concerned with determining the need for and value of
knowledge within the health care environments. Particular importance is placed
upon analysing the cultural environment of HCE's, i.e. staff interaction, staff
patient interaction.

User Analysis
This analysis is concerned with analysing the way in which staff carry out their
job functions and determining their attitudes toward security issues. Other areas
that will be examined are; which key records staff used to aid their job function
i.e. how patient records were used for the treatment of a patients. Consideration
will be made of how important records are developing, i.e. Electronic Health
Care Record (EHCR) [6] and the impact that this development would have on
security.

The security knowledge for the expert system will be acquired from a number of sources, these will be:

> Formal risk analysis security reviews of major systems within Plymouth Health Authority and Plymouth Community Trust
>
> Personal experience of implementing security and interviewing staff within the Plymouth Health Authority and Plymouth Community Trust
>
> Knowledge gained from research undertaken within the EU (European Union) SESIMED Medical Security Research Program
>
> Discussions with commercial organisations about security issues
>
> Discussions with security consultants about security issues
>
> Knowledge obtained from literature review of security guidelines
>
> Results obtained from security questionnaires
>
> SIM-ETHICS criteria evaluation of security countermeasures lists produced by various security risk analysis methodologies, i.e. COBRA, CRAMM

Expert System Design

The input for the expert system will take the form of a list of security countermeasures produced by the ODESSA system, the expert system will be designed to 'bolt' onto an as a separate software package.

An aim of the expert system is to evaluate suggested security countermeasures produced by the ODESSA system and inform the user about the impact of implementing these suggested measures. The inference engine will draw conclusions using the knowledge contained in the knowledge domain.

The expert system rule set will be based around production rules. The advantage of using production rules is that they follow natural thinking, they are simple to develop, they allow for intensive knowledge to be stored and they also allow the expert system to be easily developed in modules. But, there are disadvantages with using production rules; it can be hard to keep track of them all, they are sometimes inefficient and they do not allow the expert system to learn and give the users the answers they require.

The following is an example production rule that could be contained with the expert system:

> IF security countermeasure = E123 (Introduction of identification passes)
>
> AND   large organisation (Environmental Issue)
>   based in inner city ("   ")
>
> THEN Ease of Implementation Impact 3
>   (Implemented with Extensive amount of effort)
>   Training Impact 4
>   (Extensive training needed)
>   User Impact 2b
>   (Countermeasures cause minor impact to user satisfaction)

Organisational impact 3a
(Effect culture through planned changed)
Human Issues 1
(No Human Impact)
The user would be given the following advice about countermeasure E123:

E123 Introduction of identification passes

<u>Organisational Impact</u>
The countermeasure can be implemented with an extensive amount of effort.

The intended countermeasure may have a minor impact on user satisfaction within the organisation.

<u>Training Impact</u>
The whole organisation will have to be taught about the use of identification cards and procedures relating to them.

<u>Culture Impact</u>
The countermeasure will cause a planned culture change to the organisation.

<u>Special Advice</u>

<u>Large Organisation</u>
It may not feasible to implement identification cards at the same time, it may be more feasible to stagger the implementation of identification cards within the organisation..

<u>Inner City Location</u>
Ensure that staff wear identification cards at all time, even out of office hours. Anyone without a identification card should be challenged immediately.

CONCLUSION

The work being carried out on the expert system is the first step towards combining a risk analysis system and security management expert system in the same package. The resulting system will fulfil a requirement that exists for a universal security consultation system that can be used to assess the security requirements for different types of HCEs .

ACKNOWLEDGEMENTS

REFERENCES

[1] Impact of Security on a healthcare environment and how to overcome it,
   by M.J.Warren and Dr P.N.Gaunt,
   IMIA (International Medical Informatics Association),
   Caring for Health Information Conference,
   Heemskerk, The Netherlands, 1993

[2] Designing Human Systems for Healthcare,
   The ETHICS Method,
   by E.Mumford,
   4C Corporation, The Netherlands,
   1992, ISBN 90-74687-01-6

[3] The use of SIM-ETHICS,
   by M.J.Warren and Dr P.N.Gaunt,
   EU SEISMED Project Internal Paper,
   SP11-04, 1993

[4] A Generic Methodology for Health Care Data Security,
   by S.M.Furnell, P.N.Gaunt, G.Pangalos, P.W.Sanders & M.J.Warren,
   awaiting publications in 'Medical Informatics'

[5] KADS (Analysis of Knowledge Based Systems),
   A Guide to KADS,
   Editor R.M.Taylor,
   Ellis Horwood Limited, UK,
   1989, ISBN 0-7458-0689-9

[6] The Good European Health Record,
   by Professor Lesley Southgate,
   AIM Internal project paper (Publicly released), 1993

Impact of security on a healthcare environment and how to overcome it.

by M.J.Warren and Dr P.N.Gaunt

Security Research Group, School of Electrical, Electronic and Communication Engineering, University of Plymouth, Plymouth, UK

1) Security Healthcare

Any new technology that is being implemented, i.e. security would cause an organisational impact. The impact would be top down, it would affect the healthcare organisation as a whole. Security is a human issue and should therefore be considered in the context of the staff and the organisation. Therefore the implementation of security within a healthcare environment would affect the hospital managers down to the doctors and nurses on the individual wards.

2) Major components of security

Within the NHS there is a growing dependency on computer systems and the data contained within the systems. Therefore the computer system and data contained within the system have to be protected.

Computer security is concerned with:

Confidentiality
The aim is to ensure that unauthorised people (including staff) do not have access to healthcare data unless they are authorised.

Integrity
To ensure that data produced by a healthcare system can be trusted as being accurate and complete.

Availability
To ensure that computer systems should be able to provide data when and where it is needed.

3) Issues of Medical security
From a medical clinician point of view [6] some of the major medical security problems are:

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

Risk to the patient
The failure of a healthcare computer system could affect the health care treatment given to a patient, this could ultimately result in the death of the patient.

Confidentiality
Medical data contains information that may be extremely sensitive to an individual, i.e. the person may be mentally ill or have HIV. Disclosure of information could be embarrassing for an individual and could result in that person being ostracised by society.

Any disclosure would also destroy the trust between the clinician and the patient. Any disclosure could result in legal action being taken against a clinician or health care organisation.

Data retention
Within some countries there is a legal requirement to retain health care data for a minimum period. This raises problem concerning the long term storage of data especially when data is converted between old and new machines, this could affect the integrity of the data.

4) The effect of implementing security
It is important to ensure that the introduction of the new security systems and procedures does not hinder the staffs work, it is also important to ensure that systems still stay 'user friendly' after they have been modified to cater for the new security features.

An important issue for healthcare IT users is job satisfaction. If a member of staff uses a badly designed system they will quickly become demotivated and become less efficient. If a badly designed security system is implemented across all the systems it would affect users efficiency and operational costs will go up as tasks take longer to carry out.

Another issue is the implementation of the security policy. This should be done in a structured manner using a project plan or by using a structured methodology, e.g. CS-Methodology[1] or Corporate Security Model[2]. Any plan should take into account the life cycle of the security system, as defined by J.Wylder[3]:

The Introductory Phase
This is when the plan is initially introduced. This is an important step because it establishes the healthcare organisational emphasis on security. This stage affects few users.

The Early Growth Phase
This is when security features are added to a limited number of systems, affecting some users.

The Rapid Growth Phase
This is when security features are added to all existing systems, affecting all the users.

The Maturity Phase
This is when the system is fully developed, then post development features will be added affecting a varying number of users.

5) Organisational problem of implementing security
In the UK within the national health service there is an organisation called the Information Management Group (IMG). The aim of this group is to promote security awareness and advise on security issues. They have produced documentation[5] detailing the minimum security countermeasures that should be in place within a UK healthcare organisation. Some of the countermeasures put forward by the booklet could have important organisational implications upon the organisation. One of the countermeasures recommended was the introduction of an IT security officer. This single countermeasure would have a major impact upon the organisation and raises a number of organisational questions:

- What managerial responsibilities would this person have?

- Within the organisation structure what seniority would this person have to carry out the tasks required of them?

- Would the security officer be solely responsible for the introduction of security or would he have the assistance of suitable mangers, i.e. network managers?

- What would happen if the health care organisation couldn't afford to appoint an IT security manager, who would carry out the countermeasures specified for the security officer from the security review?

The introduction of a security officer could result in other problems. There is a problem that the IT security officer may be seen as an 'agent of change', therefore an awareness scheme is needed to ensure staff are aware of his responsibilities and his aims and therefore don't perceive him as a threat.

The importance in determining the impact of security suggests that some type of methodology or model should be used, i.e. SIM-ETHICS.

6) What is SIM-ETHICS

SIM stands for Security Implementation Method and ETHICS stands for Effective Technical and Human Implementation of Computer based System.

The work on SIM is being undertaken by Plymouth University and the Plymouth Health Authority as part of the SEISMED project. The work on ETHICS was undertaken by Professor Enid Mumford of the Manchester Business School.

The use of the SIM method allows for the hypothetical implementation of security countermeasures. This allows for the assessment of certain factors:

-Determination of the organisational impact of security.

-Determination of any technical problems of implementing security within the organisation.

-Determination of the training issues related to security.

6.1) How SIM-ETHICS works

The philosophy behind SIM-ETHICS is that the development of new technology, i.e. a computer system is not only a technical problem but also an organisational issue. This organisational issue is concerned with the effect that the process of change could have upon the organisation as a whole.

SIM-ETHICS will work through the use of committees to discuss group issues. Some committee members will then interview key staff in order to determine their views about the introduction of security.

6.2) Why use SIM-ETHICS within healthcare environment?

The principle aim of SIM-ETHICS is to determine the impact of any technology, i.e. security could have upon the organisation as a whole. The impact is looked at from the point of view of:

>User job satisfaction.
>Existing system efficiency and ways to improve it.
>Determining ways to improve effectiveness.
>Allowing for the management of future change.

6.3) The use of SIM-ETHICS within an healthcare environment.

The following are the steps used in the SIM-ETHICS method:

Step 1) Initial Requirements
Theory:
The list of the prioritised countermeasures is used for discussion and is produced by the implementation group. The implementation group is the body actually concerned with the implementation of the security countermeasures. They are therefore interested in all aspects of the implementation including the technical issues, training issues and the human issues.

Process:
To obtain appropriate documents, these will act as a source of discussion within the various stages of the method.

Example:
The implementional group will be sent a list of prioritised CRAMM countermeasures. This will act as a source of discussion for the committee.

Step 2) Convening the committee
Theory:
The SIM-ETHICS method uses the participational approach in order to allow user input into the process of change. There are various levels of participation [1], these are:

Consultative
This is when an existing body, i.e. the Security Group is used to implement the change process. They will then consult users on the effect that change will have upon them.

Representative
This is when a cross selection of users effected by change are brought together into a design group. This ensures that representatives effected by change have the same powers in the group as those bringing about change.

Consensus
This is when all the staff effected by changed are involved in the design process. Representatives of the staff effected are elected to form the design group.

Part of this stage is concerned with informing the committee members about security and it's possible impact. This helps to ensure that all members have an understanding about security.

Process:
To set up a committee to carry out the participational process. This committee should reflect a cross section of managers and users, this committee should not be that large that it becomes unworkable. This process should be carried out by key staff of the committee, i.e. IT experts. The first meeting should contain a presentation about security explaining the issues related to it. The

aim of this is to educate the members of the committee who are unfamiliar with security.

Example:
Based upon the participational concept the following seems appropriate for the Plymouth Health Authority to act as the committee:

System Managers or Users	(two - six)
IT experts	(two)
Internal expert	(one)

Within this committee the role of the internal expert is to act as the security expert for the group and also to head the committee.

Step 3) Committee design questionnaire and interview script
Theory:
The aim of these stages is to determine users reaction to the implementation of the security countermeasures. This also covers thinking of questions to ask on the questionnaire or to ask at the interviews.

The ETHICS related questions of SIM-ETHICS are concerned with:

Job Satisfaction
Effectiveness
Efficiency

Mumford [2] has defined these as being :

Job Satisfaction
Job satisfaction is defined as the attainment of a good "fit" between what employees are seeking from their work(their job needs, expectations and aspirations) and what they are required to do in their work - their organisational job requirement.

Effectiveness
This is defined as ensuring that tasks already being carried could be carried out in a more effective manner.

Efficiency
Efficiency is a set of support services which help individuals to work in a well organised way with all the necessary back-up facilities which they require. These will include information, materials, technical aids, specialist knowledge and supervisory help. Employees who do not receive the support services which they regard as essential to the efficient performance of their jobs are likely to become frustrated and dissatisfied.

Process:
The committee will determine questions for the questionnaire and the user interviews. Questions will be related to the organisational impact of security, training requirements and the SIM-ETHICS approach. These questions would related to user job satisfaction, efficiency requirements and effectiveness requirements.

Example:
The committee reviews the security countermeasures produced from the review and:

> Determine the importance of particular security areas in relation to the users.

> Determine which questions will be asked on the questionnaire. These questions will help to find out about the organisational impact of security, training requirements and problems shown through the use of SIM-ETHICS.

> Determine which people, i.e. users, system managers will receive questionnaires.

> Determine questions to ask at the interviews. These interview questions will be based on the need to find out about the organisational impact of security, training requirements and the SIM-ETHICS approach.

> Determine key users to interview.

Step 4) Questionnaire phase
Theory:
The aim of the survey is to determine user job satisfaction. Questions will also be asked about other topics, i.e. organisational impact, organisational culture, efficiency and effectiveness matters.

Process:
Sending out questionnaires to determine user satisfaction and collating the results.

Example:
External advisor and other committee members will:

> Produce the questionnaires as agreed by the committee.

> Send out the questionnaires.

> Collate results for the other committee members.

Step 5) Interview Phase
Theory:
The interviews determine the organisational impact of implementing countermeasures. Questions will also be asked about other topics, i.e. efficiency and effectiveness matters.

Process:
Interview key staff in order to determine their response to the implementation of security.

Example:
Members carrying out the interview will:

> Decide on any extra questions that may be needed.

> Interview key personnel about the impact of security.

> Write up interview notes for the other committee members.

Step 6) Committee discuss results
Theory:
This is part of the participational process. The aim is to discuss results from the interviews and questionnaires and determine problems connected with the security countermeasures.

Process:
The aim is to discuss results from the questionnaires and interviews and then draw appropriate conclusions. These discussions will be based upon the results of the interviews and questionnaires.

Example:
The committee will:

> Discuss the results from the questionnaires and interviews, drawing conclusions.

> Determine potential problems of implementing security (in terms of organisational impact, threat/risk levels, technical problems, cost benefit problems)

Step 7) Committee advises on impact of implementation
Theory:
This is part of the participational process. The aim is to finalise a plan containing details about the selected countermeasures and their priority. The plan would also contain details about which countermeasures could be implemented immediately and which countermeasures could be implemented after training took place.

Process:
Committee decides on appropriate countermeasures taking into consideration the comments made. The decision is based upon the organisational impact of the countermeasure (based on views of the committee and conclusions drawn from the interviews and questionnaires).

Example:
The committee will:

     Pick appropriate countermeasures.

     Prioritise countermeasures and training.

     Consider appropriate countermeasures in the following terms:

          If countermeasures cause no organisational impact and there
          are no training problems then the countermeasures should
          be implemented.

          If countermeasure causes an organisational impact then
          training should be carried out and following this the
          countermeasures should be implemented.

Step 8) Post implementional stage (Optional)

Theory:
The aim of this stage is to consider post implementional changes by using a participational approach. This stage is optional and should be used if problems occur.

Process:
The committee would review the implementation of the security countermeasures. The committee should discuss any problems that have arisen and suggest ways to overcome these problems.

Example:
A newly implemented security countermeasure may have caused an unforeseen impact to the organisation. Therefore the committee will decide either to modify the countermeasure or find a way to overcome the organisational impact, i.e. training.

7) Future Work

The work carried out with SIM-ETHICS is part of the EEC SEISMED project (part of the AIM project). Once the SIM-ETHICS methodology has been developed for the healthcare security environment it will be implemented by other partners within the project. This would mean that SIM-ETHICS would be used within the healthcare organisations of Holland, Switzerland and the UK to determine the impact of security. The use of SIM-ETHICS would help to

ensure that healthcare workers fully understand the impact of implementing security.

Bibliography

[1] Managing Computer Security: methodology and Policy,
     by J.H.P. Eloff and K.P.Badenhorst,
     Information Age, Volume 12, No 4, October 1990, UK

[2] SP11.AZL.TRP.016,
     Information Security Management,
     by Erik Flikkenschild,
     SEISMED Project Report, EEC

[3] The Life Cycle of Security Managers,
     by J.Wylder,
     Information Systems Management, 1992, UK

[4] Defining System Requirements to meet Business needs: a case study
     example,
     by E.Mumford,
     The Computer Journal,
     Vol 28, No 2, 1985, Pages 97 - 104, UK

[5] Basic Information System Security,
     'Baseline Security',
     by the NHS Information Management Group, 1992, UK

[6] SP11.02.A08.02
     The need for security in health care information systems
          [A Clinical View],
     by Dr P.N.Gaunt and Prof. F.R.France,
     SEISMED Project Report, EEC

[7] Designing Human Systems for Health Care,
     The ETHICS Method,
     by E.Mumford,
     4C Corporation, ISBN 90-74687-01-06,
     1993, Netherlands

[8] Designing Participatively,
     by E.Mumford,
     Manchester Business School,
     ISBN 0-903808-29-3,
     1983, UK

Development of
Security Guidelines for Existing Healthcare Systems

S M Furnell, P W Sanders and M J Warren

Network Research Group, Faculty of Technology, University of Plymouth,
Plymouth, United Kingdom.
E-mail : stevef@soc.plym.ac.uk

Abstract

As modern healthcare establishments become increasingly dependent upon information systems it is vital to ensure that adequate security is present to safeguard the confidentiality and integrity of data and the availability of systems. Whilst this is now generally recognised in the design of new systems, many existing operational systems have been implemented without security in mind. This paper describes the need for a standardised approach in the protection of existing healthcare systems within Europe and presents an overview of a new set of information security guidelines that have been developed specifically for the medical community.

The guidelines discussed have been produced as a deliverable of the Commission of European Communities (CEC) SEISMED (Secure Environment for Information Systems in Medicine) project, under the Advanced Informatics in Medicine (AIM) programme.

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 and the information they store. Healthcare systems may be vulnerable to a variety of accidental or deliberate threats and, as such, it is now recognised that security issues must be considered during the development and implementation of new health information systems to maintain the confidentiality,

integrity and availability of the data held. Unfortunately, a significant proportion of operational healthcare systems were originally designed and implemented with inadequate security and, as a result, security must also be added or enhanced in many existing systems.

2 The AIM SEISMED Project

The issue of information security in healthcare has been addressed by the CEC SEISMED (Secure Environment for Information Systems in Medicine) project, part of the Advanced Informatics in Medicine (AIM) programme [1].

The objective of SEISMED is to provide practical security advice and guidance to all members of the healthcare community who are involved in the management, development, operation or maintenance of information systems. The eventual aim is to establish a consistent framework for the protection of medical data across the European Union.

The project commenced at the beginning of 1992 with an original duration of 3 years, but this was subsequently extended for a further 6 months (until mid-1995). A total of 14 workpackages were established, each addressing a separate aspect of healthcare security. Five European HCEs (located in the UK, the Netherlands, Switzerland and the Czech Republic) were selected to act as *Reference Centres* for the project, commenting upon and ensuring the viability of the recommendations made.

The problem of securing existing systems was addressed by workpackage SP07, the scope of which was to produce a comprehensive set of recommendations for the addition (or enhancement) of security in operational healthcare systems and environments. The principal objectives of this workpackage were :

- to produce guidelines on the level of protection that should be attached to existing operational healthcare systems;
- to provide guidance as to how this level of security may be achieved;
- to revise the approach based upon Reference Centre feedback.

Whilst various guidelines and standards for IT security have previously been developed, none have specifically targeted the needs of the medical community at a European level. The new guidelines are intended to provide a common source of reference for European healthcare establishments and are relevant to (and will affect) all categories of personnel.

3 Baseline Security Recommendations for Healthcare Establishments

In order to assess current security practice and attitudes within European establishments a survey was distributed to HCEs in 11 community countries [2].

Amongst other things, this allowed a broad assessment of existing systems to be made and revealed a significant variety in both the types of system in use (i.e. hardware, operating systems and applications) and the levels of security provided. For example, whilst virtually all systems included some form of user authentication mechanism (even if only a simple password in some cases), the attention given to other aspects of security (e.g. disaster recovery, physical protection and auditing) was, in general, significantly less. Furthermore, the variety of techniques used to address a single aspect of protection indicated anything but a standardised approach (e.g. the types of authentication mechanisms variously utilised include individual passwords, shared passwords, challenge-response mechanisms and other methods - with likely inconsistency between similar systems).

It was considered that, in many cases, the disparity indicated by the survey had resulted from the lack of appropriate standards and guidance, with HCEs being unclear over both general security issues and the level they should aim for. The most appropriate strategy for improving the situation was, therefore, considered to be the definition of *baseline* recommendations for security, to provide a common foundation for all HCEs.

This immediately raises the question of what level of security should be specified. The nature of the healthcare environment, with the inherent requirements to maintain patient safety and confidentiality, demands that protection should generally be higher than in many other domains. As a result, the security requirements extend beyond the levels proposed by many existing standards.

The new baseline recommendations have been developed to satisfy the following aims :

- to represent a minimum acceptable standard for the security of operational healthcare systems and their associated environments;
- to be usable by all HCEs and staff within Europe;
- to allow a straightforward means of validating existing systems security to ensure compliance.

The development of the resulting guidelines was based upon an *interactive* approach, in close co-operation with the SEISMED Reference Centres and in consultation with other independent healthcare professionals.

From the outset it was established that the recommendations should address more than the just the host system in isolation. Indeed, to provide comprehensive protection, several aspects of security must be considered :

- logical / system-based controls;
- physical and environmental protection;
- personnel procedures;
- policy and administration issues.

On the basis of these high level requirements, existing IT security guidelines and standards [3,4,5] were used in conjunction with suggestions from within the project to formulate initial recommendations. These were progressively refined and enhanced over time on the basis of Reference Centre feedback and comments from independent healthcare personnel. This procedure provided the principal criteria for retention, addition or removal of guideline recommendations.

4 An Overview of Existing Systems Guidelines

The final *Security Guidelines for Existing Healthcare Systems* [6] are grouped under 10 key *principles* of protection, representing the main elements governing the security of existing healthcare information systems (having been agreed in detail with the Reference Centres). The principles are denoted by ESP followed by a unique reference code, as listed in table 1 below.

Code	Title
ESP0100	Security Policy & Administration
ESP0200	Physical & Environmental Security
ESP0300	Disaster Planning & Recovery
ESP0400	Personnel Security
ESP0500	Training and Awareness
ESP0600	Information Technology Facilities Management
ESP0700	Authentication & Access Control
ESP0800	Database Security
ESP0900	System Maintenance
ESP1000	Legislation Compliance

Table 1 : Existing Systems Security Principles

Each of the principles has a number of associated *guidelines*. These represent the specific security concepts or countermeasures that should be considered by the HCE to meet the requirements of a given principle. As established earlier, the consideration of existing systems encompasses a very broad range of issues and the overall coverage consequently extends from general concepts to specific technical measures.

The 10 protection principles are described in more detail below. In each case the general purpose of the principle is stated, along with a list of the main issues that are covered by the underlying guidelines (the overall number of guidelines pertaining to each principle is given alongside its title).

1. **Security Policy & Administration** (*5 guidelines*)

General Principle
A formal policy will provide clear direction and support for security within the HCE. Policy is formulated from the senior managerial level, with subsequent guidance provided to all levels of staff. Correct administration of and adherence to the policy should ensure the effectiveness of HCE security controls.

Main issues :
- the need for a security policy;
- policy awareness issues;
- co-ordination and administration of security;
- use of specialist security personnel.

2. Physical & Environmental Security (*22 guidelines*)

General Principle
The generally open nature of HCEs and their high degree of public access dictates that physical security measures are a vital first stage of protection to prevent unauthorised access to computing equipment and facilities. Systems must also be safeguarded against a variety of environmental hazards that may adversely affect operation.

Main issues :
- physical access control;
- security of HCE equipment;
- protection against natural disasters;
- environmental controls;
- various procedural measures.

3. Disaster Planning & Recovery (*7 guidelines*)

General Principle
The continuous availability of Information Systems is essential to the operation of a modern HCE. It is essential that adequate plans are made to ensure the level of availability needed by the HCE can be maintained in the event of any catastrophe. Recovery of IT systems should be a component of an overall HCE disaster / recovery plan.

Main issues :
- continuity planning (development, testing and update);
- fallback arrangements;
- post-disaster procedures and controls.

4. Personnel Security (*8 guidelines*)

General Principle

The major security weakness of many systems is not the technology but the people involved. Many organisations are extremely vulnerable to threats from their own staff and, as a result, even the most comprehensive technical controls will not guarantee absolute security. There are, however, a number of personnel-related measures that can be introduced to help reduce the risks.

Main issues :
- staff recruitment;
- contractual agreements promoting security;
- security during normal working practices;
- staff appraisal and monitoring;
- termination of employment.

5. Training & Awareness (*6 guidelines*)

General Principle
Information systems security can only be maintained if all personnel involved in their use 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.

Main issues :
- the need for general security awareness;
- specific areas that must be addressed (job training, use of information systems);
- recommendations for internal / HCE training and awareness initiatives;
- use of specialist training courses;
- assignment of responsibilities for training.

6. Information Technology Facilities Management (*31 guidelines*)

General Principle
A variety of activities can be identified that are related to the normal day-to-day use and administration of information systems. All categories of HCE personnel (management, technical and general users) have responsibilities that must be addressed in order to maintain security in this area.

Main issues :
- system planning and control;
- the importance of maintaining back-ups;
- media controls;
- auditing and system monitoring;
- virus controls;
- documentation issues.

7. Authentication & Access Control (*28 guidelines*)

General Principle

It is essential that IT systems are protected by comprehensive logical access controls. Access should be guaranteed for legitimate users and denied to all others. *All* classes of user must be identified and authenticated before *any* access is granted and further mechanisms must control subsequent reading, writing, modification and deletion of applications and data. There should be no method for bypassing any authentication or access controls. HCE users are unlikely to be satisfied with controls that intrude upon working practices and chosen schemes should be transparent and convenient in order to gain acceptance.

Main issues :

- requirements for user identification and authentication;
- password issues;
- system and object access restrictions;
- methods of control;
- access in special cases (e.g. system management, third parties, temporary staff).

8. Database Security (*21 guidelines*)

General Principle

Database security is concerned with the enforcement of the security policy concerning the disclosure, modification or destruction of a database system's data. Databases are fast becoming very important for HCEs. Over 90% of today's IT systems contain some kind of database and the value of information stored is now widely recognised as a major asset, far more important than any other software. However, databases also introduce additional security concerns (e.g. granularity, inference, aggregation, filtering, journaling etc.) and therefore warrant specific consideration.

Main issues :

- control of medical database software;
- organisation and administration of HCE database systems;
- database operation issues.

9. System Maintenance (*5 guidelines*)

General Principle

System maintenance activities merit special consideration given the opportunities that exist to affect the operation of the system. Unauthorised or uncontrolled changes to any aspect of an operational system could potentially compromise

security and, in some cases, endanger life. Maintenance must therefore be carried out in accordance with well-defined procedures.

Main issues :

- controls to prevent unauthorised changes to and upgrades of HCE software, vendor software and operating systems;
- requirements for testing and acceptance.

10. Legislation Compliance (*5 guidelines*)

General Principle
Specific levels of protection may be demanded in order to comply with national and European legislative requirements, as well to satisfy internal HCE policy. Whilst the guidelines highlight the most basic requirements, this principle represents an ongoing process which must take account of any new legislation that may be relevant, as well as ensuring compliance with existing standards.

Main issues :
- data protection;
- abuse of information systems;
- prohibition of "pirated" software;
- compliance with internal security standards;
- retention and protection of business records.

5 HCE Target Audiences

It should be evident that many of the issues covered are not relevant to all HCE staff. As such, the *Security Guidelines for Existing Healthcare Systems* are targeted at three main staff groups (as shown in figure 1), with separate guideline sets having been developed for each audience.
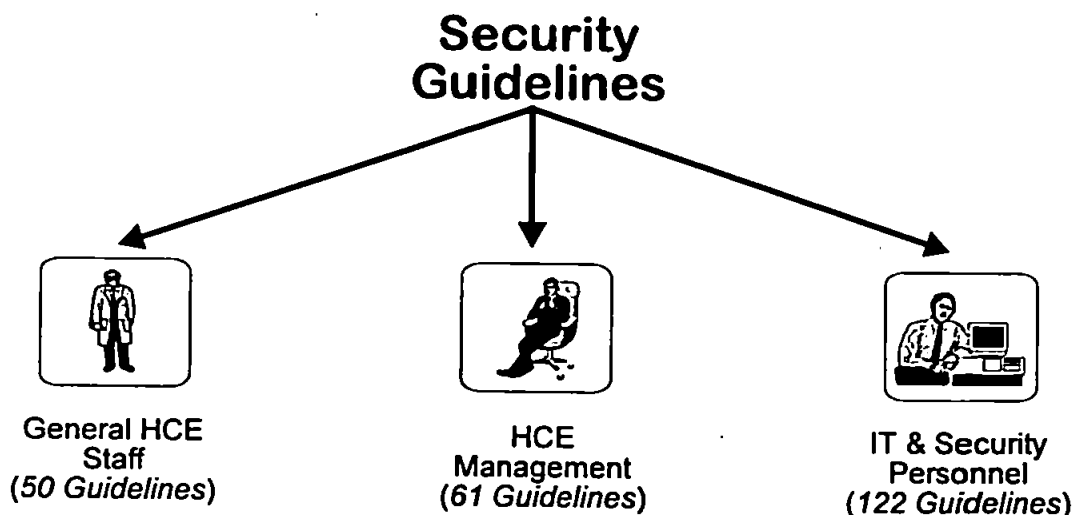
Security
Guidelines

General HCE
Staff
(*50 Guidelines*)

HCE
Management
(*61 Guidelines*)

IT & Security
Personnel
(*122 Guidelines*)

Fig. 1 : HCE target audiences

Whilst all three sets draw upon the same core principles, they nevertheless differ dramatically in terms of the type and quantity of information presented. The anticipated readership and general content of each set is as follows :

- The *General* guideline set is aimed at the majority of HCE staff, including clinicians, administrators and general system users. Guidelines are presented for user reference during day-to-day use of HCE information systems, highlighting what they can do to safeguard security.

- The *Management* set primarily targets the senior decision makers within the HCE, who will be responsible for defining security policy (although a significant number of points will also be relevant at department / line management level). This set is intended to highlight areas in which management should be directly involved and also improve management security awareness by explaining / justifying the importance of other more technical guidelines (for which management approval will be required).

- The *IT & Security Personnel* set is aimed at IT staff, system administrators, security officers and other support staff who will be most likely to have the lower level responsibilities for implementing security. This is the most detailed of the subsets and should be a key source of reference for implementation and validation of security.

The *Management* and *IT & Security* audiences would also be expected to read and observe the *General* guideline set.

6 Implementing the recommendations

The *Security Guidelines for Existing Healthcare Systems* should be applied in any European Healthcare Establishment with existing operational information systems (where the term *Healthcare Establishment* refers to any establishment providing medical services, research, training or health education). They will be relevant even where systems are thought to include security provision, so that the level of protection can be validated against the recommendations.

However, given the diverse nature of European healthcare environments and systems, it is impossible to specify precise guidelines for implementation. Establishments will differ in terms of both the information systems used, as well as financial, operational and other constraints that may apply. These issues will all have bearing on the applicability of the recommendations and the guidelines therefore concentrate more on describing *what* aspects of security should be considered rather than *how* they may be best implemented (with broad recommendations that should be compatible, to at least some degree, with the majority of systems and environments)

Despite these attempts to ensure applicability, it is still conceivable that some guidelines may not be suitable for all systems. As such, implementors must use their discretion in cases where guidelines are genuinely inappropriate to the environment. However, recommendations should be followed as closely as possible and in some cases the implementation of a guideline *will* depend upon others already being in place (which is made clear from the guideline context and / or cross-references to other points).

As for the implementation strategy itself, it would obviously be impractical to attempt to address all of the suggestions at once due to constraints of cost and likely disruption to services. A phased approach is, therefore, advised in which each principle is considered in turn to identify the areas in which the HCE / department is currently deficient. The individual guidelines may then be assessed to determine implementation priorities based upon local requirements.

Further work within the SEISMED project has resulted in the development of the methodology SIM-ETHICS (Security Implementation Methodology - Effective Technical and Human Implementation of Computer based Systems) which may be used to assist with the implementation of these and other SEISMED guidelines [7]. The methodology is based upon the concept of participational management, using groups of users and managers to carry out a hypothetical implementation of chosen security countermeasures. This provides a means of highlighting any problems which may occur, which may then be overcome in advance of the actual implementation.

Finally, the *Security Guidelines for Existing Healthcare Systems* should not be considered in isolation and a number of the other SEISMED guideline deliverables are also relevant in the context of existing systems. These include specific guidelines relating to high-level security policy, system development and implementation, network security and data encryption.

7 Potential Problems

Whilst the new recommendations are intended to provide a simple and straightforward means of addressing healthcare security issues, it is recognised that problems may exist.

Firstly, many establishments may currently be operating with security significantly below the recommended level and progression to the required level may be a non-trivial task. As mentioned in the discussion of implementation, HCEs may face a number of constraints that affect their ability to address security requirements. For example, cost (in terms of finance, performance and practicality) will be a significant factor in determining acceptability. Financial cost will be particularly relevant, given that expenditure for direct care activities is likely to receive higher priority than security. In addition, organisational constraints will play a role in so far as recommendations will need to integrate with existing practice (or at least not conflict

too greatly) in order to gain acceptance. If such constraints are present, establishments should bear in mind that every guideline implemented will improve the security of their systems.

Conversely, some environments and / or applications may demand a level of security significantly higher than the proposed baseline. In these cases a risk analysis review is recommended in order to determine the level of additional protection that is necessary. A specifically designed healthcare protection methodology, that has also been developed by this group, could be utilised for this purpose [8].

8 Conclusions

In conclusion, it is believed that the guidelines have fulfilled the objectives of this phase of the SEISMED project and will provide a solid foundation for the improvement of security within existing HCE systems.

Whilst the principles will remain relatively static, it is expected that the underlying guidelines will require periodic updates to account for changes within the healthcare field or in the types of information system technology available (e.g. the increasing use of multimedia systems may introduce new considerations). Changes within the local HCE (e.g. organisational structure, medical applications and practices) may also necessitate re-evaluation of some recommendations.

The guidelines will now form the basis of a further SEISMED workpackage dedicated to the validation of the projects recommendations. This will include full trials of the guidelines at the Reference Centres and will provide an extensive test of their applicability in practice. It is anticipated that the Reference Centres themselves will then be able to document their findings in due course.

Acknowledgements

We would like to acknowledge the various partners and collaborators within the SEISMED project for their valuable contributions during the development of these guidelines. In particular, we would like to thank the following individuals for their help and assistance throughout the project :

References

1. AIM SEISMED Project. 1991. *Technical Annex*. Secure Environment for Information Systems in MEDicine. SEISMED (A2033).

2. AIM SEISMED Project. 1995. *Enhanced Survey Report*. Deliverable 34. Secure Environment for Information Systems in MEDicine. SEISMED (A2033).

3. CCTA. 1993. *Baseline Security for IT Systems*. (June.).

4. Department of Trade & Industry. 1993. *A Code of Practice for Information Security Management*. (Sept.).

5. NHS Management Executive Information Management Group. 1992. *Basic Information Systems Security*.

6. AIM SEISMED Project. 1994. *Security Guidelines for Existing Healthcare Systems*. Deliverable 26. Secure Environment for Information Systems in MEDicine. SEISMED (A2033).

7. Warren, M.J. and P.N.Gaunt. 1993. "Impact of security on a healthcare environment and how to overcome it", In *Proceedings of IMIA Working Conference on Caring for Health Information* (Heemskerk, The Netherlands, Nov. 13-16).

8. Furnell, S.M; P.N.Gaunt; G.Pangalos; P.W.Sanders; and M.J.Warren. 1994. "A Generic Methodology for Health Care Data Security", *Medical Informatics* 19, no.3; 229-246.

A generic methodology for health care data security

S. M. FURNELL†, P. N. GAUNT‡, G. PANGALOS§,
P. W. SANDERS† and M. J. WARREN†

† Security Research Group, Faculty of Technology,
University of Plymouth, UK
‡ Department of Health Care Informatics,
University of Plymouth/Derriford Hospital, UK
§ Informatics Laboratory, Faculty of Technology,
Aristotelian University of Thessaloniki, Greece

Abstract. The aim is to outline the framework of a generic methodology for specifying countermeasures in health care environments. The method is specifically aimed at the enhancement of security in existing health care systems, and a key element is the use of predetermined 'profiles' by which these may be classified. Example scenarios are presented to illustrate how the concept could be applied in practice. The paper is based upon work that was initially carried out as part of the Commission of European Communities SEISMED (Secure Environment for Information Systems in MEDicine) project, the aim of which is to provide security recommendations for European health care establishments (HCEs).

1. Introduction

During the past few decades the use of information technology (IT) has become more widespread in all areas of society, and the types of activities that it performs or supports have become increasingly more important. As a result, information systems are now heavily utilized by all levels of staff, and relied upon to the extent that it would be difficult to manage without them.

The health care field has been no exception to the trend, as witnessed by the wide variety of applications that now handle many types of health data [1]. These systems contain vast amounts of information, much of it relating to individuals and of a sensitive nature. In addition to direct care applications, some parts of the European Community are now making the transition to a purchaser–provider funding system, meaning that an increasing volume of traditional business type data must also be maintained.

The combination of these points serves to make the protection of health information systems a vital concern, and necessitates that security is now considered as an essential aspect of the information technology field.

At a high level, information security is defined as being the combination of the following key factors [2]:

(1) *Confidentiality.* This refers to the prevention of unauthorized disclosure of information. All access to data must be restricted to authorized users who have a legitimate 'need to know'. Confidentiality is fundamental in health care since certain categories of data may be of a particularly sensitive nature,

and disclosure could result in significant embarrassment or prejudice to the individual concerned.

(2) *Integrity.* The prevention of unauthorized modification of information. There is a requirement to be able to trust the system and be confident that the same information can be retrieved as was originally entered. For example, the accidental or deliberate alteration of patient-related data could have serious implications for care delivery.

(3) *Availability.* Data and systems should be accessible and usable (by authorized users) when and where they are required. This requirement necessitates both prevention of the unauthorized withholding of information or resources, and adequate safeguards against system failure. In some medical environments, for example, critical systems may be required to be in operation 24 h a day, 7 days a week.

Security breaches may result from a variety of accidental or deliberate acts, with potential threats being posed by outsiders and from staff within the organization. Deliberate acts may include activities such as fraud, theft, hacking and virus infection. The health care field has certainly not been immune to these threats, with the most recent UK survey [3] showing that 10% of *reported* security incidents were related to health care systems (with roughly an even split between the above categories).

The introduction of information security seeks to eliminate or, more realistically, reduce the vulnerability to any risks that may be present. Protection must encompass the computer system and everything associated with it (e.g. from the computer unit itself to the building in which it is housed). Most important, however, is the protection of the information stored in the systems. These goals may be realized via a variety of measures [4], of both a technical and non-technical nature (e.g. physical, personnel and administrative controls).

In a health care establishment (HCE), any part of the computing system could provide the basis for a security breach, and this multiplicity of targets makes medical security a difficult issue. Large-scale introduction is complicated by the myriad of different system configurations (in terms of hardware, networking and actual applications) that may be identified within a single country, let alone within the full European scenario [5]. The issue is further complicated by the variety of information that may be held, and the fact that several different levels of data sensitivity may exist. The desired protection will depend upon several factors including the computer configuration, the operational environment and the information itself. As such it is impossible to assert a single level of security that will be appropriate for all cases without it being excessive in some applications.

Introducing security is a balancing process between providing the desirable level of protection against the maintenance of an adequate level of availability and performance (so that legitimate users have easy access to the data). Specifying the level of security that should be included involves some judgement about the dangers associated with the system, the required level of availability and the resource implications of various means of avoiding or minimizing those dangers.

Guidelines are therefore required on the selection of appropriate security measures, as well as on where and how to put them into HCE systems in general. The commonly accepted means of achieving this is to conduct a risk analysis investigation. However, this can be a time-consuming and costly proposition, and

may consequently be prohibitive in many cases. It would obviously be undesirable for security to be overlooked when this occurs. Given that many of the threats and vulnerabilities of individual HCEs are not unique, a full risk analysis in each case may also be largely unnecessary.

This paper proposes the framework of a methodology that is able to simplify the identification of security requirements for individual systems. This provides a straightforward means by which system administrators/security officers can select solutions appropriate for their own particular arrangements.

2. A conceptual overview of the generic methodology

Security should be examined from the perspective of the whole system, with all factors that influence protection requirements being considered. In general terms the security-relevant elements of existing systems are characterized as follows:

Information system = Computer configuration + Operational environment
+ Data sensitivity

These elements have been incorporated into the framework of a system protection methodology as shown in figure 1. This illustrates (at a high level) the steps involved in profiling existing systems to determine their requirements and select appropriate countermeasures.

The rationale of the methodology is that similar organizations/systems will have similar security requirements and a key factor in the approach was to devise a number of predetermined security 'profiles' for each element of existing systems. What the methodology proposes is a 'mix-and-match' approach to countermeasure selection, based upon a comparison of existing systems against general profiles. Using appropriate combinations it is possible, at a high level, to generate existing system profiles/categorizations that could then account for the majority of health care IT scenarios. From these it should be feasible to specify appropriate protection measures to meet the security requirements in each case.

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

2.1. *Computer configuration*

This refers to the IT assets (both hardware and software) of the organization. At a high level it is possible to identify a relatively small number of elements which may be included in any given computer configuration, as shown in figure 2. Individual systems would be considered to determine which elements are applicable, and countermeasures selected accordingly. Examples of associated baseline countermeasures have been identified for each configuration, and are grouped as shown in table 1.

2.2. *Operational environment*

This considers the nature of the environment in which the IT assets are actually located and used, which may also affect the type and level of protection that is required. Table 2 indicates the main environmental considerations that may have security bearing. Appropriate combinations of these factors can be used to describe the majority of health care establishments (i.e. from GPs to general hospitals). Again, appropriate baseline countermeasures can be specified for each type of environment, and the key issues are indicated in table 3.
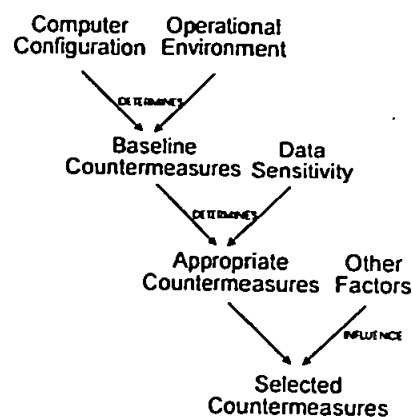
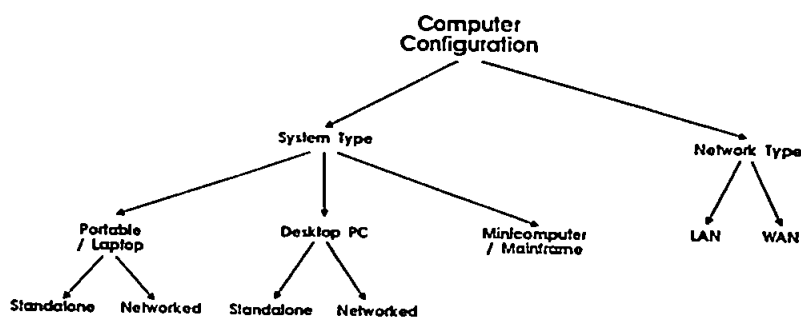Figure 1.   Existing system protection methodology overview.

Figure 2.   Computer configuration groups.

Table 1.   Computer configuration countermeasure categories.

Category	Example issues
Physical	Physical access, theft prevention
Disaster planning	Maintenance contracts, alternative systems, backup arrangements
System	Authentication, logical access controls
Procedural	Backup/recovery policy, software usage, hardcopy control
Personnel	Operational training, computer-related awareness

2.3. *Data sensitivity*

The sensitivity of data is determined by two major factors, as shown in figure 3. These factors, and the means of rating sensitivity, will now be considered in more detail.

2.3.1. *Data type.*
In consultation with a number of HCEs within Europe, the general care activities carried out by hospitals, general practitioners, community health care centres, and various other support services were examined. This enabled a generic model of medical data to be developed as the basis for further investigation [6]. The model is composed of 12 main data groups, as described in table 4. The purpose is to allow a simple means of specifying what data are available within

Table 2. Operational environment categories.

Factor	Options	Comments
Location	Fixed/mobile	Variable environment (e.g. portable computer system) limits environmental measures
	Rural/urban/city	Local environment is an indicator of local population density, crime potential and likelihood of natural disasters
Buildings	Single/multiple	Number of buildings will determine access control, site security requirements
	Old/modern	Age of building may indicate risk of fire, natural damage, etc.
People	Number (low, medium, high)	Number and mixture of people influences access controls and personnel-related measures
	Staff/contract/public	

Table 3. Operational environment countermeasure categories.

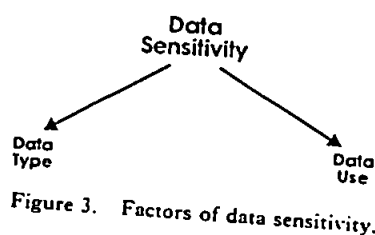| Category	Example issues
Site security	Building/site access, theft prevention
Disaster planning	Fire, flood, natural disasters
Procedural	Control of visitors, controls on smoking, eating/drinking
Personnel	Job recruitment/termination, awareness

Figure 3. Factors of data sensitivity.

a system and help in the allocation of appropriate sensitivities, thus simplifying the process of identifying how and where data are located in different computer systems and networks. The information used by the HCE may be of varying levels of sensitivity, and this will again be highly dependent upon the cases involved.

The models groups are of a (necessarily) broad nature, but they may be broken down into further levels of detail as required. For example:

Patient care: Episode information, Dates of admissions/discharges, Staff involved, Diagnosis including clinical codings(s), Care plan, Specific needs, Health care delivered, Drug therapy, Outcome of the treatment, Consultants' and anaesthetists' reports.

The model provides a generic framework that should encompass all data required by a HCE. Specific medical applications may store and communicate information from all of the data groups, or a particular subset of them. It is consequently possible to map such applications on to the model, indicating the data groups that are

Table 4.   Generic data group descriptions.

Data group	Description
Patient identification	General information held regarding individual patients referred to the health care service. Often utilized by a number of different systems/applications
Patient administration	Information used in the day-to-day scheduling of various non-clinical care activities related to patients (i.e. concerned with the delivery of resources that in turn facilitate clinical care)
Patient care	Contains medical history, diagnosis, care decisions and treatment information relating to individual patients
Clinical services	Information related to the functioning of service departments of the HCE. Data are for the department's internal use (not patient-related)
Finance	Information covering all aspects of finance that are involved in the operation of HCEs
Hotel services	Information stored on all the basic 'housekeeping' functions of health care systems
Staff	Personnel information relating to all grades of HCE staff
Resource management and planning	Information used in the management, monitoring and planning of health care organizations
Library and information services	Encompasses the existing medical knowledge that is referenced by clinical staff, and national/local protocols for clinical management
Expert systems	Information utilized by decision support tools and/or neural networks within the HCE
Communication services	Identifies the process of communication within the HCE. Could contain a variety of additional data generated during organizational communication (e.g. activity requests, transaction information
External systems	Recognizes potential data relationships (interfaces) that may exist with other HCE applications/systems

Table 5.   General categories of medical data usage.

Data use	Description
Operational clinical	Planning, delivery and monitoring of health care
Emergency care	Provision of care in a clinical emergency, where optimal conditions/information cannot be guaranteed
Critical clinical	Control of instrumentation/systems in direct feedback loops
Expert systems	Use in decision support tools or neural networks
Operational non-clinical	Supporting HCE infrastructure, but not directly influencing care of individuals
Financial	Contract management, purchasing and billing
Planning and resource managment	Aggregation of data for planning and review purposes
Quality management	Clinical audit, assessment of care efficiency and outcome
Clinical research	Identifiable or anonymized data used for research purposes; usually utilizes aggregated data

involved, and from this derive the basic sensitivity of the information. Examples of such mappings are given later in the text.

2.3.2. *Data use.* Incorporating this factor of data sensitivity into the methodology demands that an appropriate range of general uses can be identified. Related work within the SEISMED project [7] has determined a high-level set of data uses that are appropriate for our purposes. A total of nine categories is considered, as described in table 5.

2.3.3. *Sensitivity ratings.* Sensitivity is quantified in terms of several different types of impact that may relate to the data in the system. Four main types of impact can be identified, with appropriate countermeasures being given in each case.

(1) *Disclosure.* Unauthorized disclosure of information to HCE staff or outsiders.
(2) *Denial.* Denial of access to the information for varying periods.
(3) *Modification.* Accidental or deliberate alteration of the information.
(4) *Destruction.* Destruction of the system or information. An extreme form of unavailability.

The type and use of the data will have different influences over the protection requirements in each of these cases.

> *Disclosure.* Data type is the most significant factor in determining the confidentiality requirement, as data will generally portray the same information in all contexts. The protection afforded should therefore remain constant regardless of which application uses it. However, data usage may still have some effect as it can influence problems arising through data aggregation. It is conceivable that, if certain data elements are combined, then the impact of disclosure may be greater than that of any one element in isolation.

> *Denial, modification and destruction.* The requirements for these are primarily determined by the data usage, as the context will determine the seriousness of the impact.

Impacts are rated low, medium or high (where low indicates that the baseline countermeasure level is satisfactory, and high is the maximum protection that can be provided). The level is determined by considering a number of potential influencing factors: (*a*) confidentality (both personal and commercial), (*b*) disruption, (*c*) embarrassment, (*d*) financial loss, (*e*) legal, (*f*) personal safety. For example, the disclosure of sensitive patient care information to HCE outsiders could be seen as a serious risk in terms of legal action, patient personal privacy and embarrassment to both the patient and the HCE. The level of impact will in turn determine the level of countermeasure.

Medical opinion from within various European HCEs was sought in obtaining the impact valuations (using a small survey distributed to appropriate personnel). Nevertheless, it is recognized that, because of the inherent subjectivity in any judgements (based largely on individual roles and/or perceptions of the problems), the resulting figures represent 'reasonable' rather than 'correct' values (i.e. values which the majority of health care professionals would be prepared to accept as an adequate representation of the situation).

2.4. *Other factors*

This element of the methodology highlights the fact that whilst the 'appropriate countermeasures' suggested may be suitable when considering the existing system in isolation, a number of real-world factors are also likely to influence the final selection process. Such factors are principally considered to include the following:

(1) *Cost constraints.* The cost of adopting particular countermeasures may be considered from several angles (e.g. financial, performance, practicality, etc.). The acceptable levels will obviously be highly dependent upon individual environments and their priorities. Financial cost is perceived as being a particularly key factor in security-related decision-making for the majority of health care establishments.

(2) *Operational constraints.* The selection of countermeasures will also be influenced by the nature of the organization itself. Any proposals must fit in with what is likely to be tolerated/accepted within the particular health care environment, and should not conflict too greatly with established practice. This relates to the 'business culture' of the organization.

(3) *Existing countermeasures.* Any security countermeasures that are already in place in relation to the existing system will obviously influence whether some of the suggested countermeasures need to be considered/adopted.

These would obviously be very subjective elements in the application of the methodology, and it is not possible to formalize them further.

2.5. *Countermeasures*

Actual security countermeasures are identified and refined at various stages within the methodology, and it can be seen from figure 1 that they are categorized under three headings. These are distinguished as shown below:

(1) *Baseline countermeasures.* Represents the minimal security considerations for a given computer configuration in a particular environment, and should be considered irrespective of the data held or the purpose(s) the system is used for.

(2) *Appropriate countermeasures.* Represents the overall set of countermeasures that may be appropriate for a given system, considering what data are used and how, but not taking into account any practical constraints that may apply in respect to implementation.

(3) *Selected countermeasures.* Represents the final output of the methodology, namely a set of countermeasures that may be added to the existing system to address the security requirements (having considered any imitations of the individual HCE).

The countermeasures used with the methodology are derived from a representative set that are being developed for use within the SEISMED project [8].

3. Methodology implementation

This section describes the specific steps by which the methodology would be implemented when considering individual existing systems.

In order to apply the method the following factors would need to be identified for the specific system/application being considered: (*a*) computer configuration involved, (*b*) type of operational environment(s), (*c*) data groups involved,
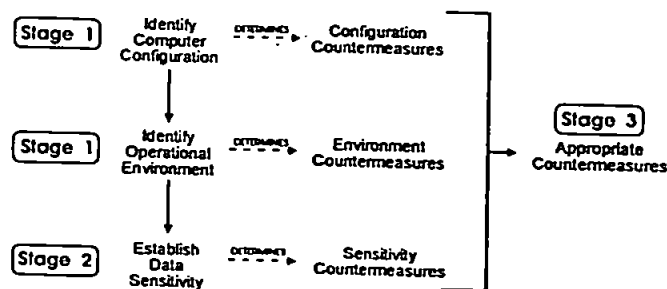
Figure 4. Methodology implementation steps.

(*d*) purpose of application (data use(s)). Countermeasures would then be derived as shown in figure 4. At each stage appropriate countermeasures would be selected from corresponding categories (NB: It is likely that some duplication may occur in terms of the countermeasures suggested within different categories).

The stages of the methodology may be more formally described as follows:

Stage 1: Determine basic system profile

Input: none.

Output: baseline countermeasures.

Description: categorize computer configuration and operational environment of the existing system according to predetermined profile categories. For computer configuration choose appropriate elements from: (*a*) laptop/portable, (*b*) desktop PC, (*c*) mini/mainframe, (*d*) network. For operational environment categorize elements of: (*a*) location, (*b*) buildings, (*c*) people.

Stage 2: Determine data sensitivity

Input: none.

Output: data-related countermeasures.

Description: establish data types and uses. Select countermeasures based upon sensitivities encompassed. Choose appropriate levels from *each* of: (*a*) disclosure countermeasures, (*b*) denial countermeasures, (*c*) modification countermeasures, (*d*) destruction countermeasures. This stage is described in more detail below.

Stage 3: Determine appropriate system countermeasures

Input: baseline countermeasures, data-related countermeasures.

Output: appropriate system countermeasures.

Description: generate countermeasure set that would satisfy the requirements of the existing system.

Stage 4: Select system countermeasures

Input: appropriate countermeasures.

Output: selected (final) system countermeasures.

Description: refine countermeasure set by considering any HCE specific factors/constraints that may apply.
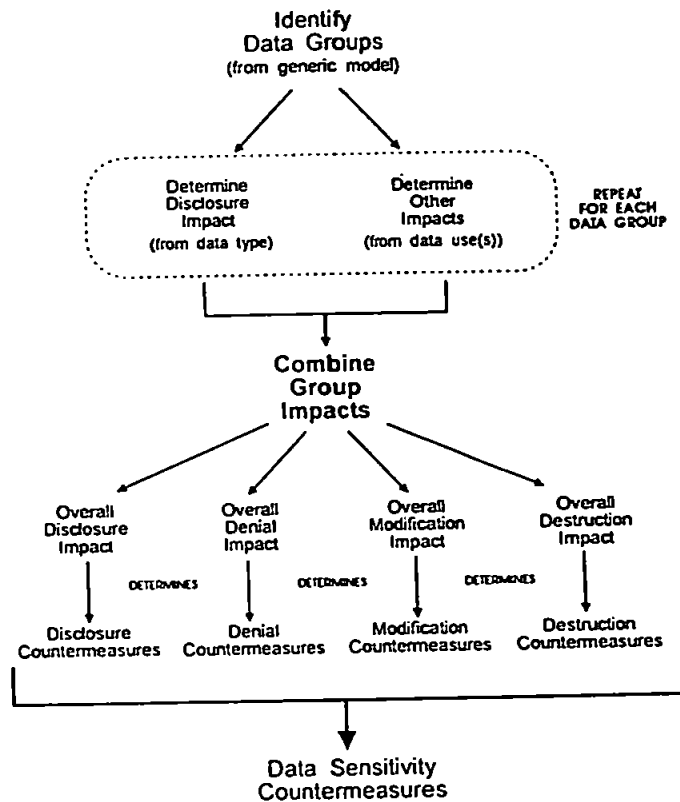
Figure 5.   Determining data sensitivity.

3.1. *Determining data sensitivity*

Determining the data sensitivity countermeasures for an existing system is the most complex stage of the methodology, as they will be based upon a variety of impact values derived from the data involved. *All* data groups in the system must be considered to establish: (*a*) impact valuations for disclosure (based on data type only); (*b*) impact valuations for denial, modification, destruction (based on data type and use). The specific procedure involved is illustrated in figure 5. These stages and descriptions are listed below:

2.1. Identify the data groups involved using generic data model.

2.2. Determine disclosure impacts from model group valuations.

2.3. Identify general data usage category(s) that applies to the system.

2.4. Determine denial, modification and destruction impacts from usage valuations for each data group involved.

2.5. Derive overall sensitivity values for application by selecting 'worst-case' values from component groups (four values in total).

2.6. Determine appropriate data sensitivity countermeasures using values from 2.5.

4.   Illustrative examples

The following section presents two basic examples to illustrate how the

methodology may be applied in practice. These are based on typical information system scenarios that may be found within the UK health service.

Note that the countermeasures and impact levels given in the examples are selected from predetermined lists. However, listing a full set of countermeasures is outside the scope of this paper, and the examples therefore provide only a small representative selection. It should also be noted that the examples only proceed to stage 3 of the methodology. The reason for this is that stage 4 is very much related to the subjective factors of real-world environments, and imposing artificial constraints would add little to the examples.

4.1. *Example 1*

4.1.1. Scenario. A patient records system maintained by a small GP practice. The system is primarily based upon a standalone PC, although selected data may be transferred to and from this using a portable computer that the GP takes on general visits and emergency call-outs. The practice is based in a single, modern building located in an inner city.

4.1.2. *Methodology implementation*

Stage 1: Determine basic system profile
Computer configuration: Laptop/portable—standalone; Desktop PC—standalone.

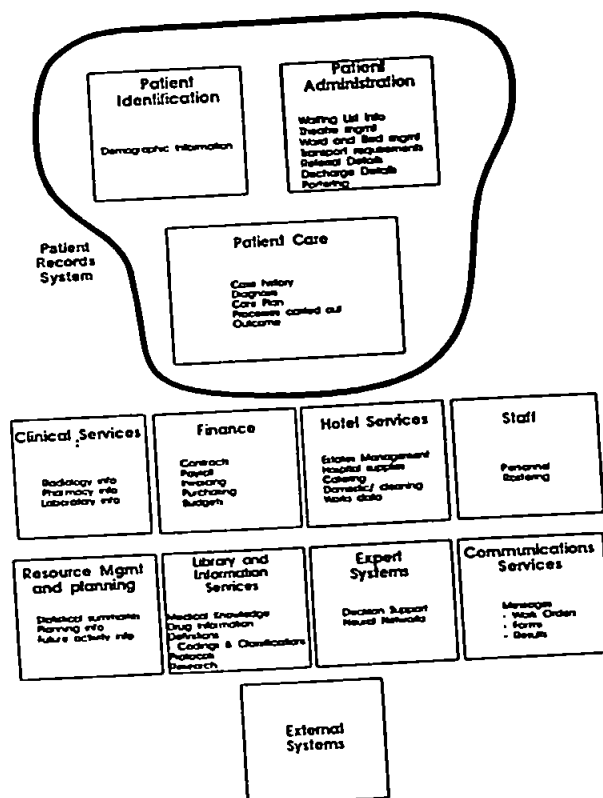Figure 6.   GP records system mapping.

Operational environment: Location—fixed and mobile, city; building—single, modern; People—staff, public, low.

Stage 2: Determine data sensitivity

Stage 2.1: Identify data groups. Three data groups are encompassed, and can be identified from the existing model as shown in figure 6.

Stage 2.2: Determine disclosure impacts

Data group	Impact level
Patient identification	Low
Patient administration	Medium
Patient care	High

Stage 2.3: Identify data uses. Potential data uses are identified as follows: (a) operational clinical, (b) emergency care.

Stage 2.4: Determine denial, modification and destruction impacts

Data group	Use	Impact levels		
		Denial	Modification	Destruction
Patient identification	Operational clinical	Medium	Medium	Low
	Emergency care	Low	Medium	Low
Patient administration	Operational clinical	Low	Low	Low
	Emergency care	Low	Low	Low
Patient care	Operational clinical	Medium	High	High
	Emergency care	Low	High	Medium

Stage 2.5: Derive overall sensitivity ratings. The 'worst-case' impacts from the previous tables are extracted to determine the overall sensitivity: disclosure, high; denial, medium; modification, high; destruction, high.

Stage 3: Determine appropriate system countermeasures

Computer configuration

Countermeasure category	Example countermeasures	
	Laptop/portable (standalone)	Desktop PC (standalone)
Physical	Casing locks Property markings (visible and UV) Protective carry case	Locks and/or alarms Property markings (visible and UV) Site to deny casual access
Disaster planning	Service warranty Maintain/store data backups Carry spare batteries, etc.	On-site service contract Maintain/store data backups Documented/tested recovery strategy
System	Use of any standard features Password protection Virus checking	Use of any standard security features Password protection Virus checking

Procedural	Hard disk encryption	Menu-only access (no DOS) Integrity checksums
	Store sensitive data on separate media Care of floppy disks Lock away when not in use Regular backup to desktop machine	Ban unauthorized software Control software updates Regular (automatic?) backups Care of floppy disks
Personnel	Stress individual accountability for machine/data when off-site	Provide software training Disciplinary procedures for misuse

Operational environment

Countermeasure category	Example countermeasures	
	Single-building/modern/city	Mobile
Site	Use of staff ID badges Receptionist/guard at main entrance Room access control (locks) Alarm systems	The nature of this environment is, by definition, variable, making it difficult to cite environment-specific countermeasures.
Disaster planning	Smoke and moisture detectors Fire alarm (linked to fire station)	Additional attention should therefore be devoted to the physical countermeasures
Procedural	Visitors escorted (non-public areas) Strangers challenged (non-public areas) Prohibit smoking	relating to the computer configuration, with the level of protection being appropriate to account for the 'worst-case' scenario.
Personnel	Controlled access hours Defined responsibilities Monitor maintenance work	

Data sensitivity

Countermeasure level	Example countermeasures		
	Disclosure	Denial/destruction	Modification
Medium	File-level passwords SMART cards Hard-copy controls	Regular recovery checks Alternative processing arrangements Disk shadowing Resource control	File-level passwords Integrity checksums Auditing
High	Encrypted transmission Encrypted storage Removable storage media Secure disposal of media/paper TEMPEST protection	Backup generators Separation of key assets	Digital signature Data encryption

4.2. *Example 2*

4.1.1. *Scenario.*
A pharmacy department serving a large general hospital uses a minicomputer-based system for drug administration. The system may be accessed from a number of locations within the HCE over a local area network.
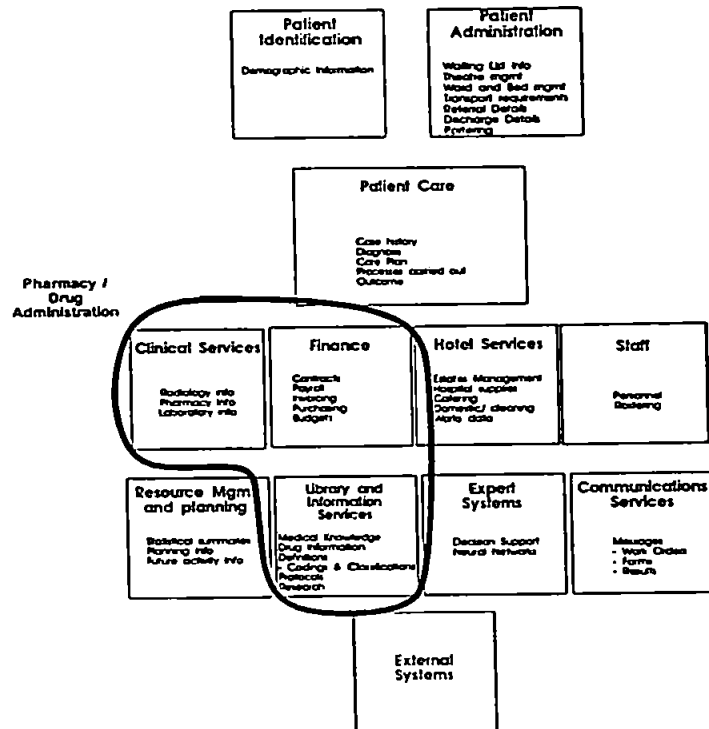
Figure 7.   Drug administration system mapping.

4.1.2. Methodology implementation

Stage 1: Determine basic system profile
Computer configuration: mini/mainframe; Network—LAN.
Operational environment: location—fixed, urban; building—multiple, modern; people—staff, public, contract, high.

Stage 2: Determine data sensitivity

Stage 2.1. Identify data groups.   Three data groups are encompassed, and can be identified from the existing model as shown in figure 7.

Stage 2.2: Determine disclosure impacts

Data group	Impact level
Clinical services	Low
Finance	Medium
Library and information services	High

Stage 2.3: Identify data uses. Potential data uses are identified as follows: (a) operational non-clinical, (b) financial, (c) planning and resource management.

Stage 2.4: Determine denial, modification and destruction impacts

Data group	Use	Impact levels		
		Denial	Modification	Destruction
Clinical Services	Operational non-clinical	Low	Medium	Medium
	Financial	Low	Medium	Medium
	Planning and resource management	Low	Low	Low
Finance	Operational non-clinical	Low	Medium	Medium
	Financial	Medium	Medium	Medium
	Planning and resource management	Low	Medium	Low
Library and information services	Operational non-clinical	Medium	Medium	Medium
	Financial	Low	Low	Low
	Planning and resource management	Low	Medium	Low

Stage 2.5: Derive overall sensitivity ratings. The 'worst case' impacts from the previous tables are extracted to determine the overall sensitivity: disclosure, medium; denial, medium; modification, medium; destruction, medium.

Stage 3: Determine appropriate system countermeasures
Computer configuration

Mini/mainframe		Network (LAN)	
Countermeasure category	Example countermeasures	Countermeasure category	Example countermeasures
Physical	Control access to computer suite Identifiable marking on terminals Site to deny casual access/viewing	Physical	Protect cabling from interference/tampering (data and power) Provide alternate routeing
Disaster planning	24-hour maintenance contract Duplicate/alternative system Maintain/store data backups Prioritize recovery options Documented/tested recovery plans	System	Monitor for overuse/failure Automatic re-routeing Integrity checking on transmission Secure WAN gateways
System	Use OS security features Access time/location controls Enforced password criteria Automatic terminal logout Auditing of activity	Procedural	Maintain list of network assets/access points
Procedural	Log/investigate reported variances Control software development/updates Formal testing of new programs		
Personnel	Provide software training Disciplinary procedures for misuse Avoid reliance on individuals		

Operational environment

Multi-building/modern/urban	
Countermeasure category	Example countermeasures
Site	Security patrols Closed-circuit TV monitoring Use of staff ID badges Receptionists/guards for sensitive areas Room access control (locks) Alarm systems
Disaster planning	Smoke and moisture detectors Fire alarm (linked to fire station) Backup generator
Procedural	Visitors escorted (non-public areas) Strangers challenged (non-public areas) Prohibit smoking
Personnel	Defined responsibilities Controlled access hours Monitor maintenance work

Data sensitivity

Countermeasure level	Example countermeasures		
	Disclosure	Denial/destruction	Modification
Medium	File-level passwords SMART cards	Regular recovery checks Alternative processing arrangements	File-level passwords Integrity checksums
	Hardcopy controls	Resource control Disk shadowing	Auditing

5. Future enhancement

The most significant extension that is planned is to develop an expert system to be used in conjunction with the methodology. This would contain the expert knowledge necessary to apply the methodology, as well as a knowledge base of appropriate countermeasures.

An expert system would contribute further to the user-friendliness and general accessibility of the method, as it would allow the techniques to be used by health care staff who were not necessarily security-trained (e.g. a hospital general manager). A major advantage of this would be cost, as expensive consultancy would not be required to carry out security reviews. If the system was developed for PC environments it could be made available in nearly all HCE environments.

6. Conclusions

The paper should have served to illustrate how high-level categorizations of health care systems may be used to simplify considerably the process of security selection. Such an approach would be valuable in cases where a full security review has been denied on the grounds of budget or inconvenience.

It is envisaged that the overall methodology should be compatible with the majority of systems, catering for a range of general existing system categorizations. Despite this, however, it is still conceivable that systems will be encountered that do not fit comfortably within the profiles suggested. In these cases it will be necessary to perform a more detailed risk analysis to determine the specific requirements of the system/environment. Additionally, in systems where extremely high levels of risk are identified, more detailed study is also advisable.

The methodology itself is at an early stage of development, and requires further refinement before it can be considered practically viable. The next stage of development will be to encompass it within an expert system so that it can be used within various HCE environments. This will serve to test the methodology and allow adjustments to be made accordingly.

Acknowledgements

References

1. ABBOT, W. (1992) *Information Technology in Health Care—A Handbook* (London: Longman, in association with the Institute of Health Services Management).
2. ITSEC (1991) *Information Technology Security Evaluation Criteria, Provisional Harmonised Criteria* (Commission of European Communities).
3. AUDIT COMMISSION (1990) *Survey of Computer Fraud and Abuse.*
4. MUFTIC, S., PATEL, A., SANDERS, P., COLON, S., HEIJNSDIJK, J., and PULKKINEN, V. (1993) *Security Architecture for Open Distributed Systems* (Chichester: Wiley).
5. TRITECH (1992) *Report of Questionnaire Study 1992—Statistical Tables and Verbal Responses.* SEISMED Internal Report SP03-01.
6. SANDERS, P. W., and FURNELL, S. M. (1993) Data security in medical information systems using a generic model. *Proceedings of MIE 93 Congress,* Jerusalem, 18–22 April.
7. GAUNT, P. N., and FRANCE, R. F. (1993) The need for security in health care information systems—a clinical view. SEISMED Internal Report SP11-02.A08.02.
8. FURNELL, S. M., and SANDERS, P. W. (1993) First draft guidelines for existing systems. SEISMED Internal Report SP07-0.7.

ODESSA - A new risk analysis method

by [1]M.J.Warren, [1]P.W.Sanders and [2]P.N.Gaunt

[1]Network Research Group,   [2]Health Care Informatics,
Faculty of Technology,   Faculty of Medicine,

University of Plymouth,
Plymouth, UK

Email: matw@soc.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 by 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 most of these problems. The paper also presents example security scenarios. It is based upon work carried out as part of the European Union AIM (Advanced Informatics in Medicine) SEISMED (Secure Environment for Information Systems in MEDicine) project, the aim of which was to provide security recommendations for European health care establishments.

Keywords: Security Risk Analysis, Baseline 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.

Risk analysis is used to:

    - Identify the risks associated with computer systems;

- Assess the seriousness of risks in relation to the objectives of the organisation;

- Identify parts of the system which are lacking in security.

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 the computers and is communicated between computers. Medical computer security is primarily concerned with:

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

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

Availability
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:

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

Risk to the patient
The failure of a healthcare computer system could affect the treatment given to patients with perhaps dire results.

Confidentiality

Medical data contains information that may be extremely sensitive to an individual, i.e. the person may be mentally ill or have HIV. 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.

Data retention

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.

As part of the EU SEISMED (Secure Environment for Information Systems in MEDicine) project a new medical risk analysis method was developed [2]. 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; that 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), 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.

The ODESSA system working prototype, has been designed :

- to be 'user friendly', so that general management and technical staff can use the system;

- to be able to produce easy to understand reports;

- to have extensive on-line help facilities;

- to be inexpensive to buy;

- to use a standard PC machine.

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.
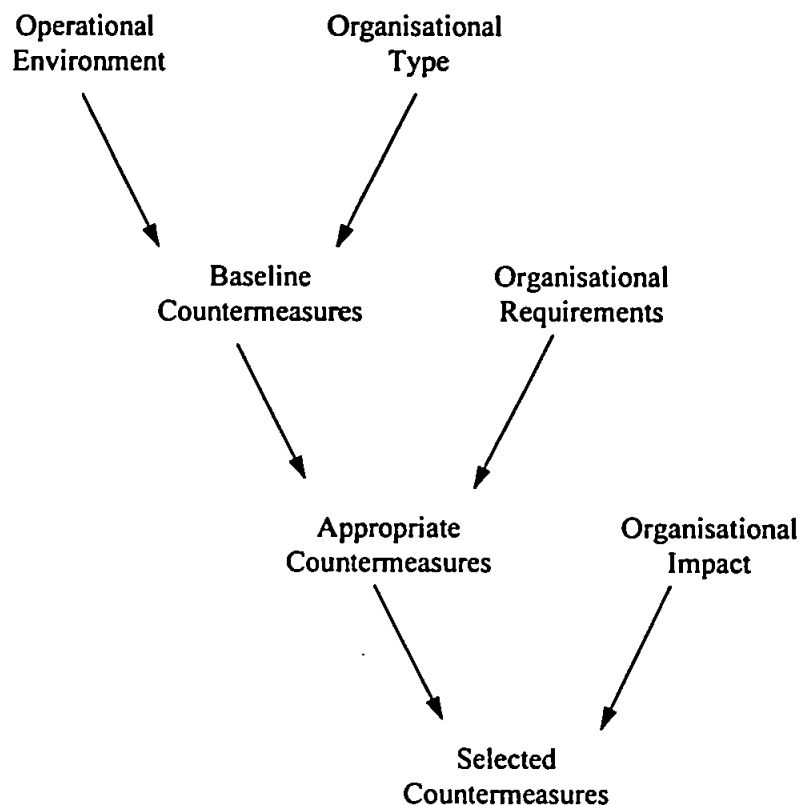

Figure 1. ODESSA methodology overview

The ODESSA system suggests three sets of security countermeasures.

1) Baseline Countermeasures.
These represent the minimally acceptable security countermeasures for any organisational type.

2) Appropriate Countermeasures

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

3) 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. - may result in a need for increased physical security.
	Urban	Location may indicate risk of theft. - may result in a need for a CCTV system.
	Rural	Location may be many miles from emergency services, i.e. fire station. - may result in increased fire drills, fire awareness schemes, automated fire fighting system, etc.
Building	Old / Modern	Age of building may indicate risk of fire, disasters, etc. - may result in a review of buildings, looking at electricity wires, water pipes, 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. Within the SEISMED project a comparison was made 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 amongst 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. special home nursing, 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 within a variety of different sites.

3.3 Organisational Baseline Security

Work on the SEISMED project has shown that within a healthcare environment that certain HCE's have 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 [4], [5].

The baseline security countermeasures are broken down into particular groups, as shown in table 3.

Table 3. Security Groups

Security Type	Sub groups	Description
Disaster	7	Relates to disaster prevention, contingency planning.
Physical	5	Relates to physical protection of sites and assets.
Hardware /Software	10	Relates to protection of computer systems and the data contained on those systems.
Human	8	Relates to training, procedural issues, etc.

The countermeasures are defined as being physical, procedural, programmable or communicational countermeasures.

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[6], as described in table 4.

Table 4. 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 and planning	Information used in the management, monitoring and planning of HCE.
Library and information systems	Details of existing medical knowledge that is used by clinical staff.
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.
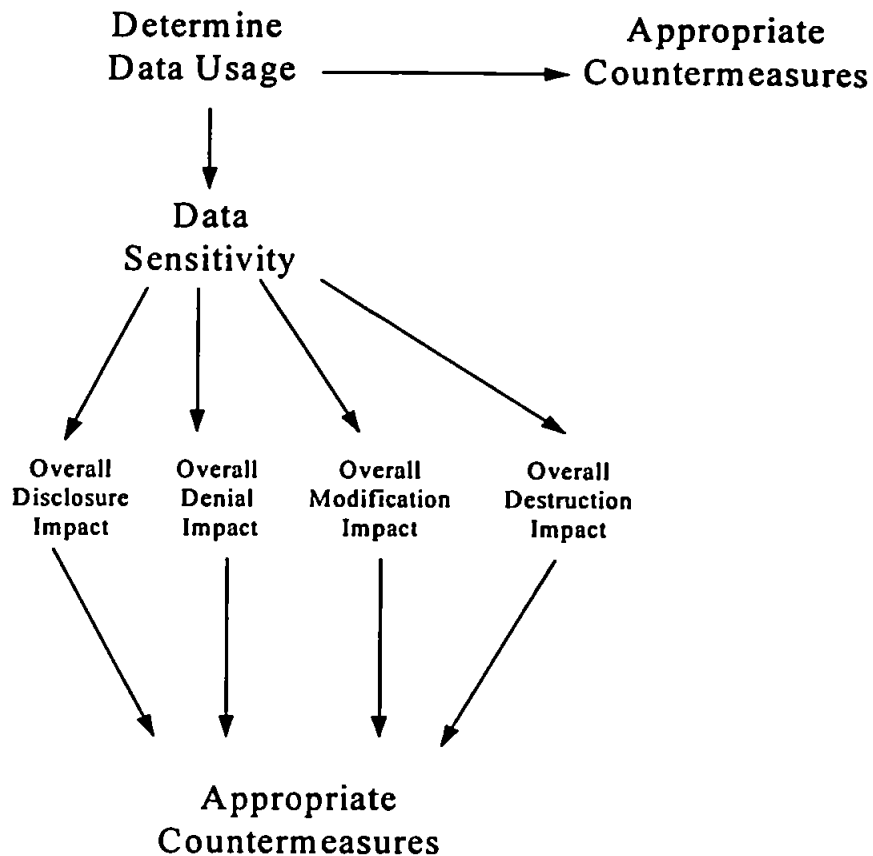
Figure 2. Organisational Requirement

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 [7] (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. Example Scenario

The scenario is that of a single GP (General Practitioner - primary community care provider) - , based in an old building located in an inner city.

Stage 1: Determine Baseline Countermeasures

Stage 1.1 Determine Organisational Criteria

Determine baseline security criteria from the above information.

Stage 1.2 Determine Baseline Countermeasures

Summary of some of the baseline countermeasures given are:

Disaster & Damage Protection

Physical
Adequate site fire protection.
Fitting of smoke detectors.

Hardware/Software

Programmable Features
Use of passwords to protect systems.

Software Training/Use

Procedural
Offence to use unauthorised software.
All users should be trained in the packages they use.

Special Consideration

Inner City

Physical Access Control

Physical

To counter an increased risk of theft and vandalism improved physical security should be introduced, i.e. window locks, secure locks.

Stage 2: Determine Organisational Requirement

Stage 2.1 Determine Data usage

The data types are selected from a list from nine data types (see table 4). In this example the GP uses the following data types :

Patient Identification

Patient Administration

Patient Care

Stage 2.2 Determine Data Sensitivity

The data sensitivity impacts are determined by answering a series of questions related to the sensitivity impacts.

i.e. If there were problems with your system, would the delay cause any of the following:

a) Patients may be kept waiting for treatment.
b) Patients may receive inappropriate treatment.

c) Patients may receive inappropriate treatment resulting in additional time spent in hospital.

d) Patients may suffer immediate harmful problems due to lack of treatment.

The hypothetical sensitivity impacts for the scenario are:

- Denial   Medium

- Destruction   Medium

- Disclosure   High

- Modification   Medium

.

Stage 2.3 Determine Appropriate Countermeasures

Certain countermeasures are specific to the type of data used and it's function, i.e.

Data Usage	Example Countermeasures
Patient Identification	Encryption of data
Patient Administration	Use of levels of access to ensure only authorised staff have access.
Patient Care	" "

The next step is to determine the countermeasures for data sensitivity. The type of countermeasures for a particular sensitivity would be dependant upon the impact level.

The following are examples of some countermeasures:

Data Sensitivity	Level	Example Countermeasures
Denial	Medium	Disk shadowing. Resource control.

.

Destruction	Medium	Alternative process arrangements. Contingency plan development.
Disclosure	High	Encrypted storage. Secure disposal of media/paper.
Modification	Medium	Checksums of data. Audit of modifications.

Stage 2.4 Determine Security Profile

The next stages is to determine countermeasures which are unique to the organisation. This is determined by the user answering a series of questions, i.e. :

Question

Hardware/Software Related Questions
Are special provisions made for the use of portable PC's.

Countermeasures

Hardware and Software Related

PC Protection

    Physical
    Ensure portable PC is secured when in transit.

    Procedural
    Removed important information when portable PC is in transit.

    Programmable
    Encrypt the contents of the hard disc.
    Implement password protection system.

Stage 3: Determine Organisational Impact

The countermeasures are reviewed and the appropriate SIM-ETHICS criteria (see 3.5) selected. The impacts are dependant upon the type of organisation and each countermeasure would have a unique impact description.

Example use of SIM-ETHICS criteria:

Sample Countermeasure:

    Introducing security awareness program.

Criteria:

Ease of Implementation
Once the basic program framework has been determined it can be repeatedly used.

Training Issues
Awareness program may be included as part of initial computer training for new staff.

Training seminars should be held on a regular basis, i.e. once every two months.

User Impact
Users will be more aware about security, therefore security problems should be reduced, i.e. virus outbreaks, passwords naming conventions.

Organisational Impact
The program will help raise security awareness amongst all staff and help establish a security culture within the organisation.

Human Issues
Expertise for such a training scheme might not exist with the GP's staff, therefore outside help would be needed in setting up the awareness program.

5. 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. The ODESSA system has been evaluated by members of the HCE profession as well as members of the SEISMED project.

The next stage is to develop a complete working system from the prototype, this system will be initially developed for use within healthcare. ODESSA will be developed so that it can be used by other business sectors, government, etc. for security reviews.

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.

The computer implementation of the methodology is complete, but by the use of independent evaluation of the prototype it will allow for any adjustments to be made.

7. Acknowledgements

We would like to acknowledge the various partners within the SEISMED project for their contributions to the content of this paper.

References

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

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

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

[4] P.Sanders and S.M.Furnell,
Guidelines for Information Systems Security in Existing Systems,
AIM SEISMED Deliverable 26, UK, 1994.

[5] S.Katsikas,
High Level Security Policy for Healthcare Establishments,
AIM SEISMED Deliverable 23, Greece, 1993.

[6] P.W. Sanders and S.M. Furnell,
Data Security in Medical Information Systems using a Generic Model,
Proceedings of MIE 93 Congress, Jerusalem, Israel, April 1993.

[7] M.J.Warren, P.W.Sanders and P.N.Gaunt,
Particaptional Management and the Implementation of Multimedia Systems,
MEDIACOMM 95 - International Conference on Multimedia Communications,
Pages 131 - 135, Southampton, UK, April 1995.

Provision of healthcare security information services using the World-Wide Web

S.M.Furnell, P.W.Sanders and M.J.Warren
Network Research Group, School of Electronic, Communication and Electrical
Engineering, University of Plymouth, Plymouth, United Kingdom.
e-mail : stevef@soc.plym.ac.uk

Abstract

The paper considers the continuing need for information security and associated awareness methods within modern European Healthcare Establishments (HCEs). It presents details of a novel security information dissemination service that will soon be offered as part of the new European Union ISHTAR (Implementing Secure Health Telematics Applications in Europe) project. The objective of the project is to increase the awareness of both the public and healthcare personnel on issues related to health data protection, by way of seminars and world-wide dissemination. The selected means of achieving the latter is to promote healthcare security issues over the Internet, utilising a dedicated server on the World-Wide Web.

The paper examines the way in which the service will be implemented, the features that it will offer and the advantages that the approach provides. The principal point here is considered to be the easier availability of consistent security advice to a wide audience.

Introduction

Information Technology (IT) is now widely used in all aspects of modern healthcare, from administration to direct patient care activities. In all areas, the potential exists to find sensitive information and systems which require protection to preserve their confidentiality, integrity and availability. As such, the issue of IT security is at least as applicable in healthcare as it is in other domains such as business and government.

Although the need for information security is gaining increasing recognition within the medical informatics community (with a wealth of relevant material having been produced), a problem remains in terms of promoting security issues to the widest possible audience and thereby developing a "security culture" within healthcare establishments (Fowler 1996). However, thanks to advances in IT itself it is now possible to offer appropriate information services on demand. At the present time, the most suitable and easily accessible means of doing this is considered to be via the World-Wide Web (Berners-Lee et al. 1994), the popularity of which has increased dramatically in recent years.

The WWW is considered to be an appropriate medium for information delivery within HCEs for a number of reasons. Firstly, HCEs have a significant existing investment in IT facilities and can increasingly be found to have connections into wide area networks (WANs). As such, they already have an inherent ability to receive information from sources such as the Web. In addition, the Web has the general advantage of being more instantly accessible than more traditional documentation or outside expertise. Security

issues and enquiries could, therefore, be addressed more quickly - even if the establishment in question does not possess its own local documentation or experts.

The need to promote security is recognised as one of the principal aims of the ISHTAR (Implementing Secure Health Telematics Applications in Europe) project, part of the European Union's Health Telematics initiative. To this end, a dedicated WWW server is being established to help in fulfilling the project's overall objective.

Service Objectives

In order to be able to properly observe security requirements, healthcare professionals (HCPs) need to have access to appropriate documentation and / or be able to obtain answers to ad hoc queries. However, documentation is often expensive (especially if many copies are required) and can be difficult to share if many people wish to make use of it. With regard to the second point, many establishments will not have trained personnel who can answer security questions. In this situation, the normal options would be either the use of costly external consultancy or the development of bespoke solutions without the benefit of proper advice (which could, therefore, still result in security weaknesses). As such, there is scope for a service which can overcome these problems in an effective manner.

The principal objectives of the planned ISHTAR service are as follows :

- to provide on-line access to guidelines for healthcare security;
- to provide and maintain an on-line help-desk and discussion forum for healthcare security issues;
- to provide a centre for the dissemination and retrieval of other information.

All of these objectives can be realised within a WWW framework.

Implementation Approach

Work on ISHTAR commenced in November 1995 and an operational version of the Web service is expected to come on-line by mid-1997, having firstly been validated by a quality assurance programme and a closed-trial within the project. It is planned that a number of useful security information services will be offered to the healthcare community at this time. These can be categorised into those that are purely of an information *dissemination* nature and those that can be viewed as being more *interactive*, as described below.

Dissemination services

- Provision of on-line access to healthcare security guidelines and related published papers (cross-referenced with hypertext links), with searching facilities and options for user feedback.

- Descriptions of example protection scenarios, highlighting recommended approaches to security for different environments and types of system. These would act in support

of the guidelines as an illustration of "good practice", highlighting ideas on security measures, policy and awareness initiatives based upon real-life scenarios.

- Provision of automated presentations and demonstrations promoting security.

- Maintenance of an on-line directory of interested parties, including profiles and contact information, provision of links to any other related projects also accessible on the WWW and to other sites with relevant security content.

- Provision of a number of other occasional and supporting services as considered appropriate. Examples that could be included here are notification of training courses and workshops; information gathering exercises (e.g. surveys) and the facility for users to download information (e.g. guidelines, papers, other deliverables).

Interactive services

It can be seen that all of the above are essentially "one-way" services (i.e. from the server to the user). However, in many scenarios the user will need more than just access to pre-prepared material and may require further explanation or the ability to ask questions. With this in mind, the ISHTAR server will also support a number of more interactive services, as outlined below.

- Facilities for an on-line expert panel / help desk to which queries and problems may be submitted. This would work by accepting basic details of user's problems from a WWW form and then automatically (and securely) forwarding them to an appropriate "expert" (from within the ISHTAR consortium) who could then contact the user with advice. This idea is illustrated in figure 1 below.
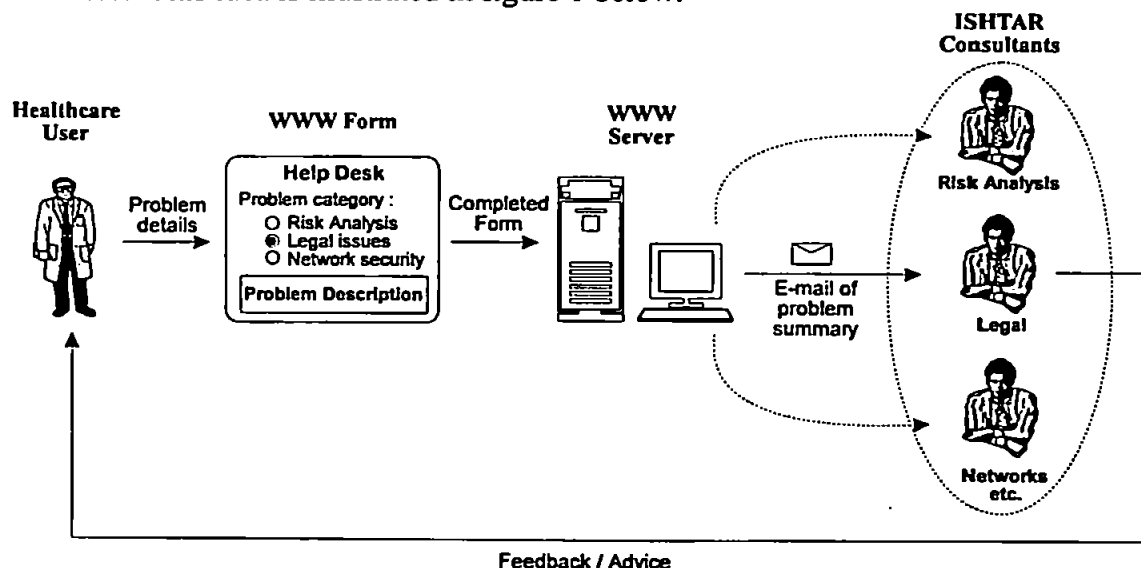

Figure 1 : Potential implementation of security "help-desk"

The potential will exist for a Frequently Asked Questions page to be spawned from this facility over time, if it proves popular.

- Facilities to allow the establishment of an on-line healthcare security discussion forum (based on an e-mail type facility).

With regard to the content of the information offered by the service, a number of avenues are being pursued. For example, appropriate guidelines for European healthcare security have already been produced as part of the EU SEISMED (Secure Environment for Information Systems in MEDicine) project, the forerunner of ISHTAR, covering areas such as high level security policy, risk analysis, security in system development and the protection of existing healthcare systems and networks. The distillation of these guidelines will enable useful summary recommendations to be provided as a first stage. In addition, further output from the ISHTAR project itself (covering areas such as enhancement of the guidelines, training and legal issues) will also be included as the service develops.

The quality of the dissemination service will be measured to ensure satisfaction of the following criteria :

- integrity of the information content (e.g. to ensure correct and accurate advice);
- understandibility and ease of use for healthcare professionals;
- conformance to general Web "standards" for the presentation of information;
- visually pleasing displays with adequate hypertext links;
- adequate response time for operations with human involvement (e.g. help-desk);
- compliance with other standards internal to ISHTAR (e.g. terminology).

The "ease of use" issue will be partially ensured by the user-friendly interfaces that are a standard feature of most current WWW browsers (e.g. Netscape). However, whilst the majority of use may be expected to come from IT professionals, it is recognised that the potential will always exist for access by other, less IT literate, audiences. As such, it will still be important to ensure that the services offered are as friendly as possible and avoid unnecessary levels of complexity. This requirement will be addressed (and assessed) by means of a "closed trial" of pilot services, conducted within HCEs acting as ISHTAR Validation Centres. A wider quality assurance of the services will then be possible later, based upon any feedback received from end-users via the operational on-line system.

Discussion

The concept offers a number of important advantages, the core of which being the promotion of security awareness to a wider audience. As an indication of the popularity of the Web, the advent of graphical browsers in 1993 caused a 300,000% increase in the level of Web-related Internet traffic. Thousands of Web sites now exist world-wide, with exponential growth predicted over the next few years (Manger 1995). As previously mentioned, it is conceivable that any HCE with WAN access could make use of the service.

The service can be provided free of charge and, whilst it will not be appropriate to address all situations, it will be able to provide solutions (or at least a good starting point) for basic scenarios and common problems. This will consequently enable savings to be made on external consultancy charges in many such cases.

The help-desk concept is particularly useful in that it provides a means of ensuring that some level of *consistency* can be maintained in terms of the advice given to different establishments in relation to similar security issues. It can, therefore, indirectly provide another means of promoting the *baseline* security recommendations that have already been advocated by SEISMED (AIM SEISMED 1994).

However, it should be noted that a WWW service will not totally remove the responsibilities for promoting security awareness within local HCE domains. Staff will still require training in aspects of security as applied in their particular establishment (e.g. password procedures) and will need to be made aware of specific issues as they arise (e.g. virus outbreaks).

In addition, whilst the Web can be seen to offer some demonstrable benefits in terms of promoting security, there may still be something of a "catch 22" situation to be faced in that the existence of the ISHTAR web server will need to be publicised in order to, in turn, promote the security issues. It is considered that sufficient publicity within the on-line community should be largely achievable by including references to the server in the many WWW catalogue services. However, there is still a potential problem to be overcome in that many HCPs may not view the Web as a viable source of information on such matters and will need to be encouraged to use the service. One solution in the short term will probably lie in sufficient publicity of the ISHTAR project as a whole, which will in turn serve to alert HCPs of the potential opportunities offered on-line. In the longer term, the fact that the Web is now maturing to offer a range of professional and commercial services (Kelly 1994) in a variety of domains (with sites run by research establishments, libraries, commercial organisations and even government agencies) will increase public awareness and alter the way in which it is generally perceived.

Conclusions

Once appropriate security guidelines have been developed, their dissemination to the affected audience is the obvious next requirement. The use of an IT based medium to achieve this objective would appear to be a logical choice, and the WWW offers an easy and widely accessible option.

At a project level, it is envisaged that ISHTAR will build upon the success of SEISMED, extending the level and types of security guidance available to healthcare professionals, and providing various means to promote the information (including the Web service). At the HCE level, use of the service will be beneficial where security (and associated knowledge) is lacking. Alternatively, the service will both compliment and ease the burden on any local security expertise that is present. In either case, the provision of consistent advice, free of charge and on a wide scale, will be a significant step in promoting healthcare security.

References

AIM SEISMED. 1994. *Security Guidelines for Existing Healthcare Systems*. Deliverable 26. S.M.Furnell and P.W.Sanders, University of Plymouth, United Kingdom.

Berners-Lee, T; Cailliau, R; Luotonen, A; Frystyk, H; Secret, A. 1994. "The World-Wide Web", *Communications of the ACM* 37, no.8: 76-82.

Fowler, J. 1996. "Developing The Security Culture At The SEISMED Reference Centres", In *Towards Security in Medical Telematics: Legal and Technical Aspects*, B.Barber et al. (Eds.), IOS Press. 156-161.

Kelly, B. 1994. *Running a World Wide Web Service.* Advisory Group on Computer Graphics. SIMA Report Series, Number 6. ISSN 1356-5370.

Manger, J.J. 1995. *The World-Wide Web, Mosaic and more.* McGraw-Hill Book Company, London, UK. ISBN 0-07-709132-9.

Assessing staff attitudes towards information security in a European healthcare establishment

S.M.Furnell[*], P.N.Gaunt[†], R.F.Holben[*], P.W.Sanders[*], C.T.Stockel[*] and M.J.Warren[‡]

[*] Network Research Group, Faculty of Technology, University of Plymouth, Plymouth, United Kingdom.	[†] Department of Healthcare Informatics, Derriford Hospital, Plymouth, United Kingdom.	[‡] Plymouth Business School, University of Plymouth Plymouth, United Kingdom.

E-mail : matw@soc.plym.ac.uk, stevef@soc.plym.ac.uk

Abstract

Information security is now recognised as an important consideration in modern healthcare establishments (HCEs), with a variety of guidelines and standards currently available to enable the environments to be properly protected. However, financial and operational constraints often exist which influence the practicality of these recommendations.

This paper establishes that the *staff culture* of the organisation is of particular importance in determining the level and types of security that will be accepted. This culture will be based upon staff awareness of and attitudes towards security and it is, therefore, important to have a clear idea of what these attitudes are. To this end, two surveys have been conducted within a reference environment to establish the attitudes of general users and technical staff, allowing the results to be fed back to HCE management to enable security policy to be appropriately defined. These results indicated that, although the establishment had participated in a European healthcare security initiative, staff attitudes and awareness were still weak in some areas.

Introduction

The issue of information security is of increasing importance in modern healthcare establishments. The traditional concerns of maintaining the confidentiality, integrity and availability of systems and data are now compounded by the new requirements that are emerging within the environment. Examples here include the interconnection of computer systems and institutions, the increasing storage of highly sensitive data, the computerisation of primary care practices and the development of telemedicine and mobile computing.

In terms of the specific security requirements in healthcare, it has been suggested (Commission of European Communities 1991) that it is "probably not possible to draw a distinction between medical requirements and needs and those from other sectors or the general domain". However, whilst this may be true from the perspective that many protection methods appropriate to other domains will also be applicable in healthcare, the establishments are generally subject to a number of practical constraints that limit the types of security that can be tolerated. These principally include :

- the generally open and public nature of the environment (which restricts the potential for physical access controls);
- financial constraints (which limit the amount of money that can be directed at non-care activities);
- staff culture (relating to the typical attitudes and behaviour of members or groups within the organisation).

This last point is closely linked to the need for convenience within the environment, which influences the types of security that are appropriate to, and will be tolerated within, a HCE. Young (1991) cites

that there are often problems enough entailed in trying to get healthcare professionals (HCPs) to use information systems in the first place (as a result of system designers ignoring the clinical environment and the ways in which HCPs are motivated) and, as such, the addition of cumbersome or restrictive protection measures would only be likely to worsen the situation. For example, effects on staff might include demotivation and reduced efficiency, whilst at an organisational level operational costs could increase as a result of tasks taking longer to perform. In some contexts this significantly limits the types of security that are appropriate and it is consequently important to determine what can be tolerated in order to avoid wasted effort and unnecessary disruption.

The staff culture often highlights discrepancies in the need for security as perceived by technologists and as seen by HCPs. Healthcare users are generally no different to those in other sectors in terms of a tendency to regard security as "someone else's problem" and, hence, often have little appreciation of the main issues. However, all healthcare staff involved in the development, operation, maintenance and use of information systems should be responsible to some degree. It has been observed that security is a human issue (Warren and Gaunt 1993) and there is consequently a definite need to move towards a more security conscious culture in HCEs (where security ideally becomes an ever-present background consideration for all system users).

Background and reference environment

The types of security that are appropriate within a healthcare environment have been most recently assessed as part of the Commission of the European Communities SEISMED (Secure Environment for Information Systems in MEDicine) project. This work has led to the formulation of a series of guidelines covering all major aspects of security, including high-level policy, security in existing system, systems development and healthcare networks (AIM SEISMED 1991). These recommendations are envisaged to be broadly applicable to all European HCEs.

However, in terms of the actual implementation of security, it is necessary to assess the extent of potential obstacles prior to attempting large-scale introduction. Staff attitudes and beliefs regarding security are important and will be valuable in ensuring correct implementation strategies. However, these attitudes are not necessarily easy to ascertain as they are not routinely documented. As such, it was considered useful to assess the attitudes of staff within an operational healthcare environment in order to determine the practical realities and provide a basis for future reference.

The chosen method of assessment was to conduct a survey of healthcare personnel, having the advantages of facilitating reasonably detailed data collection whilst also allowing broad staff coverage. The investigation was mounted within a local reference environment (namely Derriford Hospital, Plymouth, which is the largest HCE in south west England and significantly advanced in terms of Information Technology (IT) usage) and supported by the Trust Information Doctor to encourage staff co-operation and ensure a healthy level of response.

Previous work conducted by the SEISMED project has identified three principal divisions of HCE staff that should be considered when introducing security (AIM SEISMED 1994) :

- general HCE staff (e.g. clinicians, nurses, administrators);
- HCE management;
- IT and Security personnel.

It was considered most important for the survey to assess the attitudes of the general users and IT staff, so that management would then be able to determine which security concepts needed to be promoted to their staff and where resistance or problems would be likely to occur.

It was initially anticipated that the staff within Derriford hospital would possibly be more security aware than those within many other European HCEs, given that the establishment participated as a reference centre in the SEISMED project, involving many of them in the implementation and validation of the recommended guidelines.

Survey of general HCE staff

The first investigation attempted to determine the attitudes of the general staff within the reference environment. The survey document ran to four pages and contained a total of 37 questions. These were divided into four sections, which obtained general background information followed by responses to questions in three key areas of security awareness, as summarised below.

1. *General*
   Obtained information on general computer usage (in terms of system, application and data access) and opinions on basic aspects of security.

2. *Physical*
   A small section which collected basic information concerning attitudes towards the physical protection measures employed within the HCE.

3. *Logical / computer system security*
   This section concentrated upon respondents awareness of security breaches and their use of passwords (the latter being the prime method of authentication and access control used in operational systems at the time and, therefore, expected to be well understood by the staff).

4. *Personnel*
   Assessed staff security awareness in respect of their own role within the HCE, including specific security and data protection responsibilities and their attitudes towards the level of security training provided.

Although it would have been desirable to explore some areas in more detail, it was considered that the inclusion of too many questions would serve to make the questionnaire appear daunting and consequently reduce the potential response rate. Amongst the staff targeted were consultants, doctors, nurses, administrators and secretaries, with respondents being asked to identify their discipline to allow potential for subdivision of the final results.

A total of 200 questionnaires were distributed and responses were gathered over a period of about two weeks. At the end of this time, a total of 75 usable responses had been received (i.e. a successful return of 37.5%). Whilst this represented a good overall figure, the distribution of responses from within the individual staff categories was rather uneven and, in some cases, the number of responses was too low to allow any confident analysis (for example only 4 responses were received from doctors, whilst a more healthy 18 responses were obtained from nurses). For this reason we did not attempt to assess attitude differences between the staff groups and restricted the analysis to the general domain. The principal findings of the study will now be discussed in the paragraphs that follow.

From the basic introductory questions there was a general consensus amongst the respondents that information security was of most importance to help preserve patient safety and confidentiality. Only 10% of staff felt that the current levels of security restricted them in their work. Respondents were generally more confident in the effectiveness of the HCEs logical security controls than the physical and personnel measures, but even in these cases the consensus appeared to be that the measures were at least adequate.

From the responses to the *physical* security questions, it was established that almost a third of staff do not wear their identity badges. However, some 83% claimed that they would challenge someone not wearing a badge - indicating that many staff do not follow the practice that they expect others to observe. Some 16% of respondents were unaware that areas of the HCE were monitored / under surveillance - which provided a first indication that security awareness was not all that it could be.

In terms of *logical* security the results firstly established that only 5% of staff were aware of security breaches within the HCE. However, this figure is still worrying in that it represents violations

perpetrated by HCE staff. The results relating to the use of passwords and general observance of system security were of even more concern. Some 59% of respondents admitted to leaving their terminals logged in and unsupervised, whilst an even greater proportion (65%) claimed to have used *someone else's* system when left in such a condition. These factors indicate lax attitudes towards the protection and privacy of individual accounts.

Proceeding from the basis that a password is supposed to represent secret knowledge known only to the legitimate user (Jobusch and Oldehoeft 1989), the survey proceeded assess how carefully the HCE users attempted to abide by this concept. The responses established that some 21% of respondents legitimately shared a *group* password with other users. However, a further 18% admitted that their password had been shared with other users without authorisation and 15% claimed to know other peoples passwords illegitimately, again indicating scant regard for the purpose of the controls.

Other worrying statistics were that 18% of staff felt that their password could potentially be guessed (on the basis that it was related to their name, hobbies or a dictionary word) and almost a third of respondents admitted to keeping a written record of their password (which further defeats the point of having one - especially if the information is left around for others to read).

Finally, respondents were asked what they considered would be a reasonable length of time between password changes. Opinions here varied dramatically, as indicated in figure 1 below, and it should be noted that only 26% of users concurred with the view of 30 days that would be advocated by the authors.
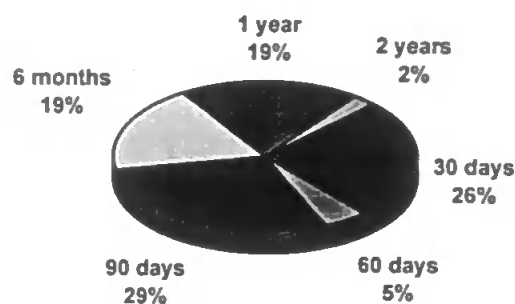

Fig. 1 : Respondents opinion on optimal frequency of password changes

The responses to the final section, *personnel* security, were also rather mixed. Some 64% of staff were aware of security-related clauses in their contracts of employment (this would appear to be quite encouraging in the sense that, at the time of the study, the reference centre was still in the process of revising contracts to incorporate such clauses and, therefore, a fair proportion would genuinely not have incorporated them). Also encouraging was that almost all staff (92%) claimed to be aware of the Data Protection Act (1984) and how it applied to their information.

However, problems were still apparent in that approximately two thirds of staff were unaware of the existence of local or general HCE security documentation. This represents a problem irrespective of whether the staffs views were actually correct or not, as it means that the HCE is either failing to provide the documentation or promote sufficient awareness of its existence.

The final questions in the survey actually concerned the issues of security training and on-going awareness initiatives. Unfortunately, the indications in both cases were disappointing, with only 25% of staff having received security training and 15% claiming to receive adequate security awareness. These figures would tend to explain some of the significant weaknesses observed elsewhere (e.g. the poor use of passwords).

The conduct of the survey and results obtained are described in more detail in Holben (1995).

Survey of IT personnel

The second investigation concentrated on the HCE's technical personnel, obtaining information regarding the security awareness and attitudes of the local system administrators. The potential response base in this case was obviously somewhat smaller than that of the general user population, and 14 usable questionnaires were returned from a total of 20 distributed (with the document in this case containing 13 questions spread over five pages).

The content of this survey was considerably different in that it was intended to elicit information from those who responsible for selecting and implementing security as opposed to those who were ultimately affected by it. As such, the prime issues covered were the respondents confidence in their own knowledge of security and the factors that they considered important when trying to incorporate it into their systems. As a result, few opportunities existed for direct comparison with the general staff responses.

The first group of questions related to system administrator's knowledge of security. Some 64% felt confident in their knowledge, with 71% indicating that they would like specific training relating to security. Although this seems strange, it implies that respondents require on-going training in order to improve their security knowledge and that of their users.

The next section was concerned with costs and revealed that 50% of respondents felt that consultancy costs were very important when implementing security and 30% thought that subsequent training costs were irrelevant. This attitude is important since it indicates that more emphasis is placed on the cost of introducing security features than the issue of training several hundred staff in how to use them.

The most important issues in implementing security was considered to be ease of implementation (85%). The *level* of training required by staff was also considered very important by 77% of respondents.

Considering the priorities relating to the training itself, 75% of administrators felt that the level and cost of training was important, whilst only 50% gave priority to the number of staff to be trained. This implies that the administrators are more concerned with training costs (i.e. the expense of in-depth training and the associated time lost) than the number of people who require it.

When the impact of security was considered, it was found that 92% of respondents were concerned if it would affect the way people would use the system, 61.5% were concerned that security would change the users job and 30% would be concerned if new security features in turn created new responsibilities. This shows that administrators wish to ensure that the level of disruption can be minimised.

The next section was concerned with departmental security set-ups. The survey found that 77% of departments had a person concerned with security, 46% had a general computer security policy and 20% had a policy relating to portable PCs. These results indicate that even though most departments have some form of security personnel, these individuals have not taken steps, and indeed may not have the appropriate knowledge, to develop departmental or specific security policies. This in turn implies that further training may be necessary.

The final section of this questionnaire was concerned with the security training received by users and found that 71% were given initial training, whilst only 23% undertook regular awareness programmes. The contrast here is clearly shown in figure 2 and it may also be inferred from the results that there is a sizeable group of staff for whom no training is provided at all.
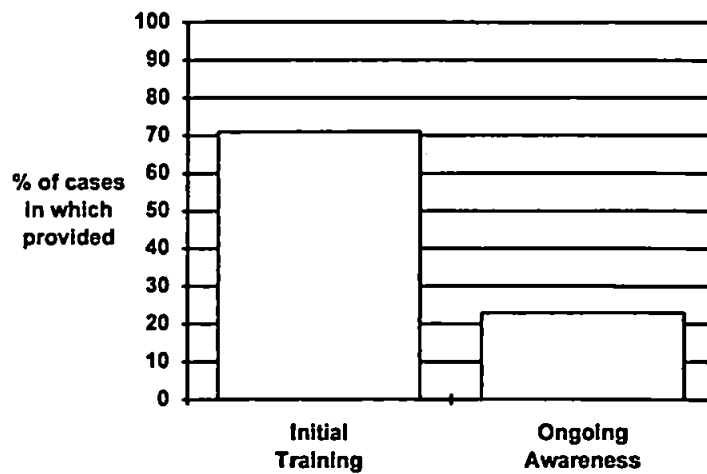
Fig. 2 : Security training provided for system users

These results imply that staff may become less security conscious as time goes on, as ideas are not introduced and / or adequately re-enforced. It is interesting to note that the figure of 71% does not tally with the earlier perceptions of the general users, where only 25% claimed to have received initial training. An explaination for the discrepancy is not obvious, but may be related to recent changes in which security training has now been introduced, but has not affected the majority of existing staff. The views of users and administrators in relation to the provision of ongoing awareness can, however, be considered to be broadly comparable.

The work described in this section is covered in more detail in Warren (1995).

Summary of problems identified

The two surveys were considerably useful in highlighting a variety of potential security weaknesses. The results observed, in conjunction with a series of supplementary interviews, identified that the following problems existed within the reference environment and *some* of its systems :

- no formal policy relating to IT security;
- a lack of procedures relating to security matters;
- poor use of passwords;
- poor use of access controls (e.g. once set, they are seldom changed or checked);
- poor use of system security features;
- inadequate security training and awareness;
- historical problems with physical security (e.g. equipment theft);
- historical incidents of attempted "hacking" by staff and outsiders;
- historical incidents of unauthorised data modification by staff;
- problems with information control (e.g. staff able to download information onto floppy disks).

The findings, therefore, provided a clear indication of several problem areas and a represented a good starting point from which management could then attempt to address the issue. A number of steps have consequently been taken to improve the situation. An IT security committee has been established, which has since produced a security policy for the whole organisation. It will also develop specialised policies for more specific areas (e.g. PC security). Members of the committee will also be involved in the running of security awareness seminars for both system managers and users. In addition, the transition of the local health authority to NHS Trust status has meant that the staff have had to sign new contracts. This has been used as an opportunity to incorporate clauses relating to security, providing another means of promoting awareness.

Conclusions

Given the relatively small respondent groups, it is obvious that the results of the investigations should not be used to make blanket assumptions of the attitudes of all healthcare staff (even within the reference environment). However, they do provide a useful illustration of the areas in which weaknesses and misconceptions can occur, and the consequent need for comprehensive training and awareness initiatives. They also indicate that there are often notable weaknesses, even in an environment where information security has been given a relatively high profile.

The system administrators perceptions and awareness of security varied from good to bad, depending upon the different individuals and the issues under consideration. The lack of knowledge in some cases can be related to the administrators originally coming from a non-IT background. Given that the users of the different systems will generally seek security advice from the associated system manager, it can be seen that the quality of the advice that they receive will vary. As a consequence, this can be cited as one of the principal reasons for awareness problems amongst end-users.

Once the problems have been acknowledged, they can be addressed (and overcome) using a security methodology which considers and involves the affected staff (Warren and Gaunt 1993).

In conclusion, the overall security attitudes observed in the surveys may be considered somewhat disappointing, given the reference environment's participation in a European healthcare security initiative, and consequently do not bode well for the likely results from other establishments that have not had this advantage. That said, however, the situation within the reference environment has improved in the months since the survey was conducted, given the points previously mentioned and the fact that further implementation and validation of the guidelines from the SEISMED project has subsequently taken place.

References

AIM SEISMED. 1991. *Technical Annex*. Secure Environment for Information Systems in Medicine (SEISMED), Project A2033.

AIM SEISMED. 1994. *Security Guidelines for Existing Healthcare Systems*. Deliverable 26. S.M.Furnell and P.W.Sanders, University of Plymouth, United Kingdom.

Commission of European Communities. 1991b. "Executive Summary", In *Data Protection and Confidentiality in Health Informatics (Handling Health Data in Europe in the Future)*; Proceedings of the AIM Working Conference, Brussels, 19-21 March 1990, edited by CEC DG XIII/F AIM; IOS Press, Amsterdam 1991: 1-61.

Holben, R.F. 1995. *Attitudes to information security in Healthcare Establishments*, Final Year Project, BSc (Hons) Business Information Management Systems, The Business School, University of Plymouth.

Jobusch, D.L. and Oldehoeft, A.E. 1989. "A Survey of Password Mechanisms : Part 1", *Computers & Security* 8, no. 7: 587-604.

UK Data Protection Act. 1984. Office of the Data Protection Registrar, Wycliffe House, Water Lane, Wilmslow, Cheshire, UK.

Warren, M.J. 1995. *A Security Advisory System for Healthcare Environments*. PhD Thesis. School of Electronic, Communication and Electrical Engineering, University of Plymouth, UK.

Warren, M.J. and Gaunt, P.N. 1993. "Impact of security on a healthcare establishment and how to overcome it", In *Proceedings of IMIA Working Conference "Caring for Health Information"* (Heemskerk, The Netherlands, Nov. 13-16).

Young, D. 1991. "Can we get Doctors to use computers ?", *Health Services Management* (June): 116-118.