2

A PRACTICAL APPROACH TO INFORMATION SECURITY AWARENESS IN THE ORGANIZATION

Cheryl Vroom [a] and Rossouw von Solms [b]

[a] *Port Elizabeth Technikon, South Africa,* s9815862@student.petech.ac.za

[b] Port Elizabeth Technikon, South Africa, *rossouw@petech.ac.za*

Abstract: The competitiveness of the global marketplace means that organizations are relying increasingly on information to stay ahead. This information needs to be protected at all costs and the users play a huge role in the protection of this vital asset. All employees need to be educated in the procedures and controls that will secure the organization's information and the most direct way to do this is by implementing a formal information security awareness program that addresses all aspects of information security awareness and caters for all types of users in the organization.

Key words: Information Security, Security Awareness, Security Standards, BS 7799

1. INTRODUCTION

Information is the key factor in decision-making for organizations nowadays and so has become arguably the most important asset that a company owns. As the global market comes into play, information is the vital ingredient that leads to a competitive edge. By recognizing the value of information, it is realised that this information and the associated information resources need to be well protected from malicious or unintentional damage. (Barnard & von Solms, 1998, p. 72)

Natural and unnatural elements are threats to this asset and can be either internal or external to the organization. A fire or a hacker can cause an equal amount of damage to the information and, in consequence, to the well being

---

The original version of this chapter was revised: The copyright line was incorrect. This has been corrected. The Erratum to this chapter is available at DOI: 10.1007/978-0-387-35586-3_46

M. A. Ghonaimy et al. (eds.), *Security in the Information Society*

of the organization. By establishing these threats, the vulnerabilities (weak points) can be determined and the risks can be assessed. Once the risks have been assessed, safeguards can be put in place to minimize these risks. This is the essence of information security – using controls to reduce the risk to the organization's information from all kinds of threats.

There are three objectives of information security that determine if information is being protected (Pfleeger, 1997, p. 5). They are as follows:

- *Confidentiality*

Ensuring that the information of the organization remains secret and is not disclosed to unauthorised parties.

- *Integrity*

Ensuring that the information stored is correct and has not been tampered with and can only be modified by authorised persons.

- *Availability*

Protecting information in the format that it was stored and that the information is accessible only to authorised persons.

All three of these qualities need to be in place to ensure that the information of the business is being safeguarded effectively. Thus, some form of defence needs to be exercised to protect this valuable resource. The task of protecting this information has changed over the past thirty years due to the technological advances that have been made, as well as the profile of the user whose responsibility it is to protect this information. (Thomson & von Solms, 1998, p.167)

2. HISTORY OF INFORMATION SECURITY

The protection of information and other valuable assets has adapted over the years to meet the changes of technology and methods of business trading within the organization.

The introduction of computers into the organization began with the stand-alone mainframes. These were extremely huge computers that were kept in a separate computer centre in a strictly controlled environment. (Schweitzer, 1987, p. 169) Protection of these mainframes was restricted to locked and guarded rooms with only the computer personnel being granted access to them. (Von Solms, 1996, p. 282) These forms of security, using locks and access control, are known as physical controls. However, once multi-user computing was introduced, a different approach to security was required.

The multi-user computing environment allowed multiple users to access various computers or workstations simultaneously from different locations. These locations were not always within the computer centre, and so suddenly the computers of the organization were spread across a geographically dispersed area. (Schweitzer, 1987, p. 167)

With these advances, more stringent controls to secure the physical assets and the information were needed. Technical controls were introduced, making use of the operation system of the computer itself to impose control over the users that accessed the information. (Thomson & von Solms, 1998, p.168) Included in these technical controls were authentication and authorization of users, all managed by the computer itself. An example of a technical control would be an authorized username and password to log on to the company network. Nevertheless, computers have continued to evolve with the popularity of personal computers and distributed networking.

Presently, with the advent of personal computers and distributed networking, especially the Internet, controls beyond the purely physical and technical are required. It makes no difference if a computer has password authorization, if the user has taped the password to the monitor. Influencing the human behaviour to ensure the proper and effective use of the physical and technical controls is vitally important to the security of the information of the organization. For this reason, operational controls were introduced.

Operational controls are information security measures or procedures within the organization that rely on the user's behaviour to be properly and efficiently implemented. For example, although a technical control can be used to protect sensitive information on a computer by means of a password, the user must log off when not at their computer. Likewise, a computer can be protected by being in a locked office, but this physical control is ineffective if the user does not lock his office when not there.

Logging off the computer and locking the office are examples of operational controls. It supports the technical and physical controls implemented by the organization, rendering them ineffective if not used in conjunction with operational controls. This demonstrates how dependent secure systems have become on the user's behaviour (Thomson & von Solms, 1998, p.168) along with the aforementioned technical and physical controls.

Unfortunately, the users are not aware of the role that operational controls play in the security of information and that they themselves, are a vital ingredient in protecting the assets of the organization.

3. MAKING USERS AWARE

According to the results of the InformationWeek's 2000 Global Information Survey, 65 percent of the more than the five thousand companies across 42 countries that were surveyed experienced lost productivity due to security breaches. This amounted to over $1.5 trillion in financial losses in the past year alone. (TSEC, 2000)

To illustrate the importance of the user of the organization, in the same survey it was discovered that of all the security breaches reported, 20 percent of these breaches were due to viruses. These attacks on information could have been prevented with relative ease if users had been made sufficiently aware of the need to virus check incoming e-mail and files before opening them.

This simple procedure could have prevented over $200 million worth of losses. This demonstrates that users are not aware of the role that they play in information security. In fact, 66 percent of users do no even regard information security as important (Khan, 1999) and most think of the security issues in the organization as an IT issue only.

These users need to be educated about the importance of securing information. They need to perform the operational controls of the business, such as virus checking, as if it were second nature. Users in the organization need to make information security awareness a part of the everyday routine.

Information security awareness in an organization is such an integral component of protection of information that leading international standards regarding information security specifically include this topic in their codes of practice.

4. INTERNATIONAL SECURITY STANDARDS

Information security standards, such as GMITS and BS 7799, relate to guidelines and regulations regarding information security in the organization

that should be implemented in order to make the business as secure as possible.

4.1 GMITS

GMITS, the guidelines for the management of IT systems, is a series of technical reports that provides guidance in the identification and management aspects of IT security. (Munyiri and von Solms, 1998, p. 12) It is divided into five parts, of which the first three parts have been published, with the aim of providing the business with a basis to assist with the development and enhancement of its own internal security architecture.

Information security awareness is a continuing theme throughout the first three parts of GMITS. In Part 1, GMITS states that "security awareness is an essential element for effective security and that the lack of security awareness can render safeguards, namely physical and technical controls, ineffective." (GMITS, 1996, p. 9)

In Parts 2 and 3, GMITS again expresses the need for information security awareness and the realism that it is applicable to all users of the organization, and a modification in behaviour is imperative to increase the responsibility in everybody. (GMITS, 1996, p. 20)

While GMITS is a high level document that provides a framework for thinking about managing IT security, BS 7799 specifies a set of comprehensive controls to implement some of the ideas given in GMITS. These two documents complement each other to provide a very good information security solution for the organization.

4.2 BS7799

BS 7799 is a standard using a business initiated approach to best practice on information security management (Sy, 2001) and specifies a comprehensive range of controls for the development of an information security management system, including information security awareness. Originally developed in Britain, BS 7799 has been adopted as a standard on best practice by many organizations around the world. In addition, several countries have made it a national standard.

BS 7799 is divided into 2 parts:

- *Part 1*
Code of Practice for information security management
- *Part 2*
Specification for information security management systems

In 2000, BS 7799 Part 1 was adapted as an international information security standard, the ISO/IEC 17799. This first part of BS 7799 is divided into twelve sections, with the first two sections explaining the scope along with the terms and definitions used in BS 7799. The third and fourth sections discuss the organization and the information security policies to be implemented in the business. The remaining eight sections address controls to be implemented. Section 6.2 stresses the importance of user education and training with regard to information security procedures and the proper use of information processing facilities. (BSI, 1999, p. 9)

BS 7799 also lists one of the critical success factors towards the successful implementation of information security within the organization as providing appropriate training and education of employees. (BSI, 1999, p. 2)

These two standards outline information security awareness as a crucial factor in the security of an organization and that the users in the company need to be made aware of the relevance of protecting information. The most direct way of doing this is to include the guidelines and controls with regard to information security awareness from GMITS and BS 7799 in the information security policies and procedures of the organization.

5. INFORMATION SECURITY POLICIES

The information security standards should be used as a guideline when creating the information security policies of the organization. They underpin the security as well as the well being of information resources and are the foundation of information security within an organization. (Information Security Policy World, 2001) These information security policies need to be developed and supported by top management to be effective and to ensure that information security awareness is recognized as a priority. This will be discussed in more detail later in this paper.

The specification of information security awareness in the information security policies that includes the operational controls recommended by BS

7799 ensures that the protection of information is integrated into the user's everyday behaviour and work routine. This can be done by including an information security awareness program in the policies of the organization.

The need for a formal information security awareness program should be specified in the information security policies in order to ensure that all users in the organization receive the proper education and training to make them aware of the security threats and risks, what procedures and operational controls need to be abided by according to the rules and regulations of the company and the consequences if these operational controls and procedures are not followed.

Currently there are no direct information security awareness programs that integrate BS 7799 controls with regard to information security awareness with the procedures and measures of the organization. These programs need to be tailor-made to the organization according to their line of business.

A formal awareness program needs to be created that encompasses all aspects of information security in the organization and caters for all employees in order to educate users on the critical role that information security plays in the organization and the part they play in the securing of that information.

6. LEVEL OF USERS IN THE ORGANIZATION

For an information security awareness program to be successfully implemented, all users within the organization need to be involved and support it. There are essentially three categories of users, all of whom play a part in information security that need to be educated in information security awareness. (Thomson and Von Solms, 1998, p 29) These are:

- The end-user
- IT Personnel
- Top Management

For the purposes of this paper, only the end-user and top management categories will be discussed.

6.1 The End-User

The end-user category comprises of all employees that have access to information. Users can be almost any type of employee, contractor or consultant, and may be at any level of the organization. (Wood, 1996, p. 34) The profile of the user has changed over the years. While once thought to be only those people that entered data into the computer system for managers to access, now all levels of employees, from the CEO downwards, at some stage need access to information. (Thomson, 1998, p. 168)

This accessibility to information highlights the fact that educating and training of all end-users in the importance of securing information is vitally important to the well being of the organization.

6.2 Top Management

Top management is regarded as those employees that establish the policies and guidelines that will be beneficial to the organization.

In Ernst & Young's 2nd Annual Global Information Security Survey, which highlights and assesses information security trends, concerns and practices, one of the major barriers to achieving adequate levels of security was identified as lack of employee awareness. The survey found that only 45% of organisations have formal information security policies and procedures, and just 19% run information security awareness and training programmes. (C-cubed communications, 1998)

In an information security context, the top management need to implement information security policies in order to legalize the stance that the company has on information security and the commitment of the company in protecting this information. Top management is a key player in a successful information security awareness program, as will be demonstrated in the next section.

7. ELEMENTS FOR A SUCCESSFUL SECURITY AWARENESS PROGRAM

The establishment of an information security awareness program requires proper planning and preparation in order to be productive in the long-term. To implement such a campaign, a number of questions need to be answered satisfactorily, namely –

- Who establishes the need for information security awareness in general in the organization?
- What sources should be applied in the execution of the program?
- Who develops the program?
- How should the program be structured?

This section is divided into further sub-sections, each answering one of the questions above. Once the solutions have been found, a model for the establishment of a formal information security awareness program can be created.

7.1 Establishing the Need for Information Security Awareness

The most important aspect of awareness training and education is to accentuate the need for information security. If the users do not understand the necessity of information security from the outset, then any information security awareness drive is destined to failure.

For users to realize this importance, top management need to be involved in and support the program. They themselves need to understand how critical the significance of information security is for the organization. To do this, those that make the corporate decisions need to be educated in the indispensability of information security awareness training for all users.

Once top management recognise the essentialness of an information security program, measures can be taken to integrate information security awareness into the organization. This is done by means of information security policies, stipulating a formal information security awareness program for all users.

By committing themselves, it shows that the senior employees of the company regard information security as crucial and that all users should make a conscientious effort at protecting the valuable assets of the organization.

According to GMITS, the commitment that management needs to show for effective information security include the following (GMITS, 1996, p. 14) –

- An understanding of the organization's global needs,
- An understanding of the need for information security within an organization,
- A demonstration of the commitment to information security,
- The propagation of an IT security vision. Each employee should know his or her role and responsibility, his or her contribution to IT security, and share the IT security vision.

The commitment of top management to information security is critical and should take the form of a formally agreed upon and documented information security policy. (GMITS, 1996, p14)

7.2 Sources Used for the Information Security Awareness Program

To compose the information security policies of the organization, top management needs a basis from which to work. These should include the international information security standards, such as BS 7799, as discussed in section 4.2, which consists of controls that should be implemented in an organization for the proper securing of information.

With regard to information security awareness, the security policy should feature topics such as (BSI, 1999, p 8-10) –

- Security in job definition and resourcing
- User training
- Responding to security incidents and malfunctions

Once the information security policies have been written and top management has pledged their support and commitment to the project, a formal training program can be constructed.

7.3 Responsibility of Developing the Information Security Awareness Program

Creating and implementing a formal information security awareness program should be the responsibility of the Information Security Officer (ISO) or a person/persons in a similar capacity. As proposed in GMITS in Part 2 – Managing and Planning IT Security, the chief responsibilities of the ISO are (GMITS, 1996, p 13) –

- Oversight of the implementation of the IT security program
- Co-ordinating incident investigations
- Managing corporate-wide awareness programs

Every organization that intends to embark on an information security awareness campaign needs to employ a person dedicated in undertaking the above-mentioned tasks. The ISO should be responsible for the establishment and management of the formal information security awareness program, responsible for determining the structure and the methods to be used in the effective training and education of the users in the organization.

7.4 Construction of the Information Security Awareness Program

The structure of an information security awareness program should essentially cater for two different categories of end-users, namely –

- *General*
  Security information about general information security practices
- *Specialized*
  Security information specific to certain roles in the organization

Each category is discussed below to give a better understanding to the classification of the actual awareness program.

7.4.1 General Training

The general section of the information security awareness program applies to all users within the organization. Regardless of what department or level the user is, if there is the ability to access the information of the company, this education on general information security awareness is applicable.

The general section itself is divided into a number of topics, each addressing an important aspect of information security and the measures that should be taken in guarding this information. Areas to be covered include –

- Information Security Policies of the Organization
- Virus and Password Protection
- Data Backup and Recovery
- Office Discipline

- Physical Security
- Internet and Email

Each topic should be informative, educating the user in the dangers of breaching security and the preventative measures that can be taken to protect the information of the organization, as well as the steps to be followed in the case of an information security violation.

This section of the program affects all the users of the company, from the CEO downwards to data entry clerks. All users should be educated and trained on the general principles of information security awareness. In addition to these general guidelines, extra education and training should be given to those users who perform specialized tasks.

7.4.2 Specialized Training

While all users should be educated in information security awareness, a number of users that perform specific roles in an organization necessitate specialized training above the general guidelines. An example of this would be the personnel that work in the Human Resources (HR) department of a company.

Although these users should be educated in general principles of information security awareness, there are further surety measures that need to be taken into consideration when performing the duties specific to Human Resources. Information security education for HR would be, for example –

- Notifying the IT personnel when a member has left the employment of the organization in order to revoke all user rights,
- Notifying the IT personnel when an employee is on vacation in order to suspend their user rights.

There are a number of departments that a typical company is divided into, depending on the nature of the organization. The Information Security Officer should take this into consideration when designing the information security awareness program in order to tailor it to the requirements of the organization.

By answering these questions, a framework for a model for a formal information security awareness program has been established. The following section will formulate this model.

8. MODEL FOR AN INFORMATION SECURITY AWARENESS PROGRAM

Taking everything mentioned above into account, a generic model for implementing an information security awareness program can be developed. This model can be tailored to suit the needs of most organizations.

Following is a step-by-step approach that demonstrates the structure that should be adopted in launching a formal information security awareness program. The information security awareness model is displayed as follows –

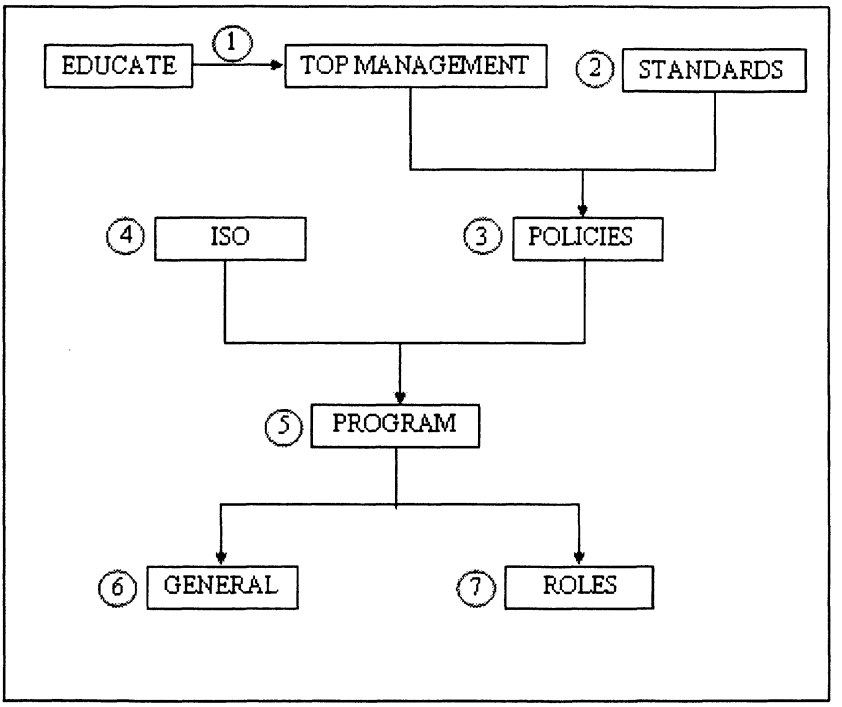

Figure1. Information Security Awareness Model

The steps for the Information Security Awareness Model are –

1. Educate top management in the necessity of information security awareness within the organization.

2. Make use of the international information security standards as a guideline for the information security policies of the organization.
3. Top management utilises the standards to create the information security policies of the company. This includes pledging commitment to information security awareness.
4. The ISO reviews and maintains the information security of the organization.
5. A formal program for information security awareness is implemented by the ISO practising the information security policies and procedures of the organization.
6. The main section of the program addresses general security measures applicable to all users in the organization.
7. The program should also cater for specialized roles within the organization and provide guidelines on the protective measures within specific departments.

Using this model, a practical information security awareness program can be implemented that caters for all users with the goal of utilising information is a secure way in the organization.

9. PRACTICAL IMPLEMENTATION

The most effective practical approach to implementing an information security awareness program would be to make use of the existing infrastructure of the company's Local Access Network (LAN) by creating an intranet-based information security awareness website. In this way all users with access to computers and the organizational network, will have access to the intranet website. This is a simple and efficient way to distribute information to all personnel.

The information security awareness program is divided into two basic segments. The first and main section is the information security awareness website itself. This displays all the information about security awareness with regard to both general and specialized training. The second part is the administration side. This is utilized by the Information Security Officer (ISO) who creates and maintains the content that will be displayed on the website.

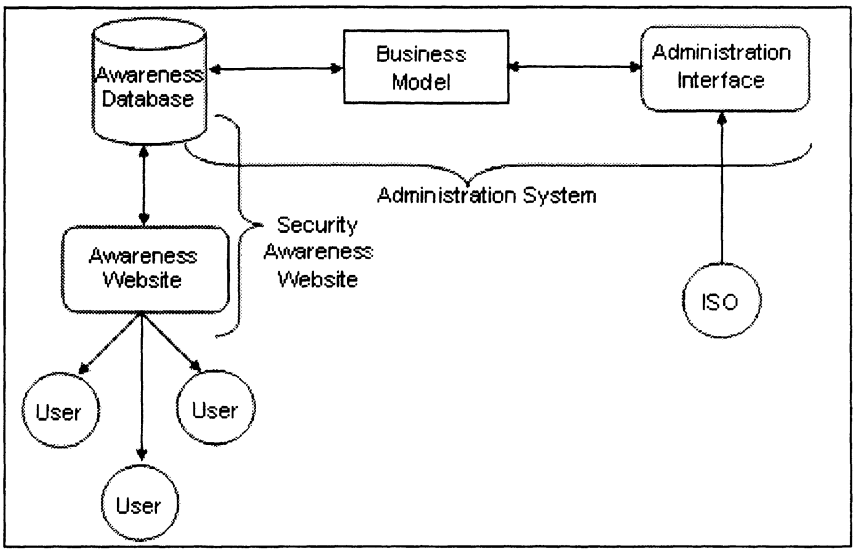

Figure2. Technical Architecture

As can be seen in Fig. 2, the ISO enters information into the database via the interface of the administration system and this database is then used to display the information security awareness content. The users of the organization then access the web pages on the intranet security awareness website and any information that is entered by the users is then relayed back to the database. The ISO can then access this new information through reports.

The Information Security Awareness Website should be divided into a number of categories –

- Introduction
- Logon
- Security Policies
- Questionnaires
- Tutorials
- Knowledge Base

Each of these categories is explained in the following sub-sections.

9.1 Introduction to Awareness Website

This introduces general information security to the user and explains the reason for its importance. It also explains the rest of the website, and how to use it.

9.2 User Logon

Each user in the organization needs to register with the information security awareness website. This is to keep track of all the users that have completed the security awareness program. It is also to monitor the performance of the users with regard to the awareness tests that are taken, as explained below. The ISO can use this logon information to create reports to gauge the effectiveness of the information security awareness website.

9.3 Security Policies

All users should have access to the information security policies of the organization to familiarize themselves with the rules and procedures of the company. Employees can read the information security policies online or download and print a copy. Easy accessibility to policies assist in familiarization and compliance to the guidelines and regulations of the organization.

9.4 Questionnaires

The concept of the online tests is to examine the user's knowledge on information security procedures and see how security aware they are. Each aspect of general information security awareness e.g. virus protection, consists of a number of questions related to the topic. Questionnaires relating to specialized information security awareness are also provided for those users that require specialized training. The test results are recorded and once the user has passed a test on a particular topic, he/she needs not repeat it.

The goal is to pass all these tests. By doing so, the user is declaring himself information security aware. This entitles the user to Information Security Awareness Certificate signed by the ISO commending his information security awareness. All users will be required to obtain the certificate within three months of starting the program. Tutorials are

available to assist the users with information security awareness education in order to pass all the online tests.

9.5 Tutorials

To help users gain the Information Security Awareness Certificate and a better understanding of information security, a number of tutorials are provided, each covering a topic of information security awareness. Users can go through these at their leisure or refresh their memory before doing a test. Extra tutorials are provided for users that require training in the specialized areas of information security awareness.

9.6 Knowledge Base

The knowledge base consists of a repository of visual aids that are available for download in order to assist in information security awareness training. These would be used in the more formal sector of classroom training or as reminders to people about information security. Examples of these aids include –

- Presentations
- Posters
- Videos
- Quizzes
- Games
- Role-playing exercises

The knowledge base provides access to these awareness aids for all users in the company to use for training purposes.

10. CONCLUSION

By monitoring the evolution of computing and information security over the last few decades, it can be seen that the users of the organization play a much more important role in the protection of information than ever before. All employees, from the top management to the end-users need to be educated and trained in the methods and procedures of information security awareness and this is best done through the implementation of a formal information security awareness campaign.

Charles Cresson Wood argues that an information security awareness program is vitally important to the organization and that "all users must be provided with sufficient training and supporting reference material to allow them to protect the organization's information resources". (1994, p 166)

Using a practical implementation such as an intranet website allows all users to access information about information security awareness as set out by the organizational policies and procedures and thus helping to secure the information of the business.

11. REFERENCES

Barnard, L. & von Solms, R. (1998). Evaluation and Certification of Information Security against BS 7799. Information Management and Computer Security 6(2), pp.72-77. MCB University Press.

British Standards Institution. (1999). Code of Practice for Information Security Management. DISC PD 0007. London.

C-cubed communications. (1998, November 10). Information Security Risk Continue to Escalate [online]. [Cited March 17, 2001] Available from Internet URL http://196.36.119.109/sections/computing/news/default.asp.

Guidelines to the Management of Information Technology Security (GMITS). (1996). Part 1 & 2, ISO/IEC, JTC 1, SC27, WG1.

Information Security Policy World (2001). The Information Security Policies / Computer Security Policies Directory [online] [cited August 28, 2001] Available for Internet URL http://www.information-security-policies-and-standards.com/

Khan, B. (1999, November 10). SA Information Security Awareness at a low [online]. [Cited March 15, 2001] Available from Internet URL http://196.36.119.109/sections/news/default.asp.

Munyiri, E. & von Solms, R. (1998). The Development of an Information Security Policy Satisfying the BS 7799 Standard. In von Solms, R.(Ed.). Information Technology on the Move. pp.10-25. Port Elizabeth : Port Elizabeth Technikon.

Sy, P. (2001). Information Security Management System (ISMS) and BS7799 Standards [online]. [Cited March 22, 2001] Available from Internet URL http://www.psbcert.dir.com.sg/new/isms.html.

Thomson M. & Von Solms, R (1998). An Effective Information Security Awareness and Training Program. MTech thesis. Port Elizabeth : Port Elizabeth Technikon.

Thomson, M. & von Solms, R. (1998). Information Security Awareness: educating your users effectively. Information Management and Computer Security 6(4), pp.167-173. MCB University Press.

Schweitzer, J.A. (1987). How Changes in Computing Practices Affect Security. Computer Security – Readings from 'Security Management' Magazine, pp.167-180. Stoneham : Butterworth Publishers.

TSEC. (2000). InformationWeek Research Study [online] [cited August 24, 2001] Available from Internet URL
http://www.itsecurity.com/tecnews/jul2000/jul102.htm

Von Solms, R. (1996). Information Security Management: The Second Generation. Computers & Security 15(4), pp.281-288. Elsevier Science Ltd.

Wood C.C. (1994). Information Security Policies Made Easy. Ohio:Bookmasters.

Wood C.C. (1996). Information owners, custodians and users. Information Management and Computer Security 4(4), pp. 34-35. MCB University Press.