A WEB-BASED PORTAL FOR INFORMATION SECURITY EDUCATION

JOHAN VAN NIEKERK and ROSSOUW VON SOLMS
Port Elizabeth Technikon, johanvn@petech.ac.za rossouw@petech.ac.za

Key words: Information Security, Security Awareness, Security Standards, BS7799

Abstract: Today's organizations have become so dependant on information resources that even the effects of a single information security incident could be devastating. Increasing Information Security awareness is the most cost-effective control that an organization can implement. However, most organizations do not have the necessary financial or knowledge resources needed for a comprehensive awareness education program. A web-based portal acting as a knowledge repository and providing training material might alleviate this problem.

1. INTRODUCTION

In today's business world information is a valuable commodity and as such needs to be protected. It affects all aspects of today's businesses from top management right down to operational level. In order to stay competitive in this information age, organizations typically make large investments in terms of time, money and energy to streamline the processes of capturing, generating and distributing vital information resources throughout the organization. Unfortunately, this distribution of mission-critical information throughout the company also increases the likelihood of misuse or damage to information resources (Haag, Cummings & Dawkins, 2000). Such misuse or damage could have devastating effects on an organization's overall well being.

Organizations have become so dependant on information resources that even the effects of a single information security incident could severely damage an organizations overall financial fitness. In order to avoid loss or damage to this valuable resource, companies need to be serious about protecting their information.

This paper forms part of an ongoing research project at the Port Elizabeth Technikon. The overall goal of the research project is to develop a web-based portal for information security education. This portal should serve as a comprehensive information and knowledge repository for information security related materials.

The need for affordable and effective information security education has in recent years become well established. According to Dhillon (1999) the widespread use of IT by businesses today has given rise to "security blindness" on the part of the users. However, when addressing this lack of knowledge and need for information security awareness, the term "users" no longer mean your traditional end-users, but includes staff at all levels of responsibility inside the organisation. Nosworthy (2000) states that each person in the organization from the CEO to House Keeping staff must be aware of and trained to exercise their responsibilities towards information security.

Taking into consideration the number of different information security standards that are available today, as well as the complexity and comprehensiveness of these standards, the task of educating "each person in the organization" with regards to their responsibilities towards information security is enormous. Very few organizations, especially in South Africa, have the kind of economic resources or the necessary knowledge available that such an educational program would require. It is envisaged that a web-based portal might fill this gap by supplying both the required knowledge and a set of comprehensive training programmes in a single place. It is further envisaged that such a portal could serve as a contact point and discussion forum for information security specialists.

The rest of this paper will focus mainly on the set of information security training programmes that will form part of the web-portal. Information security is typically implemented in the form of various security controls. One such security control is the introduction of a corporate information security awareness program. The training programmes that form part of the web-portal is aimed at addressing this control. The following sections will examine some of the issues regarding what such a program should be

teaching, to whom it should be teaching it and will lastly discuss the usage of web-technology as a delivery mechanism for such teaching. The reason the user education program is singled out is because increasing awareness of security issues is the most cost-effective control that an organization can implement (Dhillon, 1999).

2. WHAT SHOULD BE TAUGHT?

As mentioned previously information security is typically implemented in the form of various controls. However, it is very difficult to know exactly which controls would be required in order to guarantee a certain acceptable minimum level of security. This also makes it very difficult to decide on the content of a user education program.

There exist several standards and codes of practice to assist organizations in the creation and management of an effective information security management system. Some of the better-known examples would include the BS7799 (now also ISO/IEC 17799), the Trusted Computer Security Evaluation Criteria (TCSEC) of the U.S. Department of Defence and the Guidelines for the Management of Information Technology Security (GMITS).

These standards and codes of practice provide organizations with guidelines specifying how the problem of managing information security should be approached. Since these standards already comprehensively address all issues relating to information security, and are widely accepted it is sensible that these standards should be used as guidelines when deciding what to teach in a corporate information security educational program.

This paper will focus mainly on one of these standards, the BS7799. BS7799 gained a lot of support since it was introduced as a Code of Practice in 1993. Today, many businesses in many countries have accepted ISO/IEC 17799 as the preferred approach in introducing information security to the organisation. This code of practice defines a baseline security standard and covers the full scope of any business quite extensively. BS7799 is divided into two parts:

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

Part 1 is furthermore divided into twelve sections. The first two sections explain the scope as well as terms and definitions used. The third and the fourth section discuss the security policies that should be implemented in organisations. The remaining eight sections provide a very comprehensive list of controls to be implemented to attain information security.

An Information security policy as discussed in section three and four of BS7799 is a document containing high-level statements that describe the organisation's security requirements. These high-level statements or policy statements refer to the appropriate security counter measures that actually implement information security.

Security controls can be broadly classified into three categories: Physical controls, Technical controls and Operational controls. A physical control typically deals with one or more physical aspects of Information Security. An example of such a control would be to physically lock the office when the user leaves the office. A technical control is a control that can be implemented through the use of technology, for example a network server might require the user to log in allowing that user access to network resources.

The third category, operational controls deals with controls that are dependent upon the user's behaviour in order for it to be effective. An example of such a control would be password use. This control deals with several issues relating to good security practices users should follow in the selection and use of passwords (BSI, 1999). Should the user write their username and password down and tape it to their desk the technical controls dealing with identification and authentication would be rendered useless.

Having physical and technical controls is very important, however, these controls are ineffective if not used in conjunction with operational controls. In other words the user has to log off in the evening and lock his or her office in order for the first two controls to be effective. This demonstrates how dependant secure systems have become on the user's behaviour (Thompson & von Solms, 1998, p168) in order for the physical and technical controls to remain efficient.

Because operational controls deal with the behaviour of users, and the physical and technical controls are dependant on this behaviour, these operational controls should form the focus of any effective user education program. All users inside an organisation should be educated as to their

individual roles in the effective implementation of information security. Thus individual users should be made aware of the specific operational controls that are dependant on their behaviour in order to be effective.

The BS7799 states that all employees of the organisation and, where relevant, third party users, should receive appropriate training. This training should include security requirements, legal responsibilities and business controls, as well as training in the correct use of information processing facilities before access to information or services is granted (BSI, 1999 p.9) This statement, even though it greatly clarifies the issues relating to what should be taught in an information security educational program, raises another question namely, what is appropriate training.

It would make sense for an organisation's awareness program to cover all the controls specified by the specific information security standard used by the organization. However, it is clearly an overkill to expect each and every end-user to be educated about all the controls specified by a standard such as the BS7799. According to GMITS, another popular information security standard, each employee should know his or her role and responsibility, his or her contribution to IT security, and share the IT security vision. (GMITS, 1996, p.14) It is therefore necessary to tailor the awareness educational material used to the needs of the individual user.

3. WHO SHOULD BE TAUGHT?

Creating a user awareness program that is tailor-made to the training needs of each and every individual user, although theoretically possible, is in practice very difficult if not impossible to implement. Furthermore such an awareness program would be extremely costly to create and thus not feasible for the average organization. It is however possible to have some distinction between the different levels or profiles of users in an information security awareness program.

Since the training needs of individuals is heavily dependant on the actual role that individual plays inside the organization, and forms of role-based schema's are already widely used for the implementation of access control, it would be logical to create a form of role-based awareness education. Such a system would solve the dilemma of creating a customized educational

program for every individual by reducing the number of customizations to a manageable, and affordable, level.

According to Thompson & von Solms (1998) there are essentially three categories of users that need to be educated in information security awareness namely:

– The End User
– IT Personnel
– Top Management

A further distinction can be made between different categories of end-users based on their actual role in the organisation. For example the role played in terms of information security by human resources (HR) end-users would differ from the role played by users from the manufacturing department.

The educational needs in terms of information security awareness for these different profiles of users would be very different. Not all users would need to be educated about all the controls specified by the information security standard used by the organization. For example:

· A typical end-user would at the very least need training in password management and would probably need to be educated about computer viruses and the safe usage of email.

· A top management user's training needs would include those of an end-user but would probably also include extensive coverage of corporate information security policies.

· An IT personnel member would probably need information security education about some of the more technical controls that neither of the other categories would need.

· An HR end-user would in addition to "normal" end-user awareness training also need training specific to the role of the HR department in information security. For example, the need to notify the IT department when a personnel member resigns so that that person's access to sensitive information resources can be revoked.

It can thus be summarised that what should be taught to a specific individual user will depend on both the user's category and the specific departmental role that user plays within the organization. For the average organization it should be possible to create a generic set of information security awareness needs profiles. Any awareness education program should be based on such a profile in order for it to be effective.

When constructing such an education program special care should be taken that the awareness program is presented in such a form that it does not go beyond the comprehension of the average user. The emphasis should be to build an organizational sub-culture of security awareness.

Unfortunately very few organisations today can afford to implement and maintain such an awareness program on a company-wide basis using a traditional classroom approach. This means that organisations wanting to implement an effective information security program where each and every user knows their role and responsibilities towards information security and is information security literate, has to look at alternative delivery mechanism for such a program.

4. WEB-BASED INFORMATION SECURITY EDUCATION

Probably the most cost-effective substitute for traditional classroom training is to provide employees with intranet-based instruction. Web-based training material has been used to great effect in many other areas and has proven to be an extremely cost-effect delivery mechanism for such programs. For example, AT&T was able to cut classroom time in half for 4500 customer service reps because they were provided with intranet-based instruction (O'Brien, 1999, p.361).

Web-based training solutions as an alternative to classroom training also have several benefits over other media such as paper. These benefits include:

- The web is a very rich media. This means that educational material developed in this media is not restricted to simple text and static graphics, but can consist of a mixture of text, graphics, animations and even sound or video clips.
- Web-based training solutions are cheap to distribute organisation wide and can easily be administrated from a centralised point.
- It is very easy to maintain, manage and update web-based training materials.
- Web-based training materials can include programmatic components. This makes it feasible to add automated assessment modules to such training materials, which means that learners can receive continuous feedback on their progress.

- It is also possible and feasible to create web-based material that will automatically adapt to the needs of the specific user being trained based on the predefined information security profile of the user.
- Most computer literate users will already be familiar with a web-based interface, which reduces additional training overheads that might be experienced should another form of computer based teaching solution be implemented.

Apart from the cost effectiveness and the richness of the web as a medium, the ability to provide automated assessment and feedback facilities as part of an educational program, is probably the single most important benefit a web-based educational portal provide over any other alternative to classroom training.

Being able to assess progress and provide feedback to the learner is a prerequisite for any educational program to be successful. Fingar (1996) states that feedback, specifically in the form of knowledge regarding the outcomes of the learners' actions, is required for learning to take place. This feedback should be continuous and constructive (DOE, 2001).

When using a web-based training solution to replace traditional classroom type training the web plays the role of the educator. In a classroom situation educators are responsible for helping the learners achieve the instructional objectives designated for their classes. These instructional objectives are that each learner should attain the learning outcomes by being able to demonstrate their mastery of the assessment standards. The purpose of assessment is to determine whether the learners have achieved these objectives (Cunningham, 1998). The capability of web-based training material to automate this assessment process and provide continuous feedback on progress is therefore vital if such training is supposed to replace classroom training.

Assessment, in this case, should not be confused with evaluation. According to Siebörger (1998) assessment is similar to evaluation, but assessment is the measurement of the extent of learning in individuals, whereas evaluation is a process by which the effects and effectiveness of teaching are determined. Evaluation would need to take place only if an organization wish to introduce a form of information security awareness certification scheme as a part of the corporate information security awareness program.

In summary it can thus be seen that a web-based information security education portal is an ideal substitute for traditional classroom types of awareness training. Not only is a web-based solution cost-effective and therefore economically viable, it is also easy to administrate, it don't require additional training and it provides facilities which, from an educational viewpoint, is essential if learning is supposed to take place.

5. CONCLUSION

This paper has introduced the concept of a web-based portal for information security education. It has shown that there exist a widespread need for information security education and has suggested that web-based technologies are ideally suited as a delivery mechanism for information security educational programmes. The contend and target audience of such programmes were also discussed showing that information security education should ideally be based on information security standards and that the contents of such educational programmes can be modelled to the needs of individual users through the definition of a finite set of information security educational profiles.

As has been mentioned, this paper forms part of an ongoing research project at the Port Elizabeth Technikon. Future plans for this research includes the definition of a set of such information security educational profiles, the creation of information security related educational material aimed at specific user profiles, as well as the creation of a web-based portal for information security education to test and implement these ideas.

6. REFERENCES

British Standards Institute (1999), BS 7799 Part 1: Code of Practice for Information Security Management (CoP), BSI, UK.

British Standards Institute (1999), BS 7799 Part 2:Specification for information security management systems, BSI, UK.

Cunningham, G. K. (1998) Assessment in the classroom: Constructing and interpreting tests. London, UK : Falmer Press.

Department of Defence (1985), Department of Defence Trusted Computer Security Evaluation Criteria (TCSEC), DoD, Washington DC.

Dhillon, G. (1999) Managing and controlling computer misuse, Information Management & Computer Security, 7 (4), pp. 171-175.

DOE. (2001) Draft Revised National Curriculum Statement: Technology Learning Area. Department of Education. Available at:
http://education.pwv.gov.za/DoE_Sites/Curriculum/New_2005/draft_revised_national_curriculu.htm

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

Haag, S., Cummings, M. & Dawkins, J. (2000). Management Information Systems for the Information Age (2nd ed.). United States of America : Irwin/McGraw-Hill.

Nosworthy, J. D. (2000) Implementing Information Security In the 21st Century – Do You Have the Balancing Factors? Computer & Security 19, pp. 337- 347. Elsevier Science Ltd.

O'Brien, J. A. (1999) Management Information Systems: Managing Information Technology in the Internetworked Enterprise (4th ed.). United States of America : Irwin/McGraw-Hill.

Siebörger, R. (1998) Transforming Assessment: A guide for South African teachers. Cape Town, RSA : JUTA.

Thompson, M. & von Solms, R. (1998) An Effective Information Security Awareness and Training Program. Mtech thesis. Port Elizabeth: Port Elizabeth Technikon.

Von Solms, R. (1998) Information Security Management (1): why information security is so important, Information Management & Computer Security, 6 (4), pp. 174-177.

Von Solms, R. (1998) Information Security Management (2): guidelines to the management of information technology security (GMITS), Information Management & Computer Security, 6 (5), pp. 221-223.

Von Solms, R. (1998) Information Security Management (3): the Code of Practice for Information Security Management (BS 7799), Information Management & Computer Security, 6 (5), pp. 224-225.

Wood, C. C. (1994) Information Security policies made easy: A comprehensive set of information security policies. Ohio: Bookmasters.