INFORMATION SECURITY AWARENESS:
Baseline Education and Certification

LINDIE DU PLESSIS AND ROSSOUW VON SOLMS
Port Elizabeth Technikon, s9944977@student.petech.ac.za rossouw@petech.ac.za

Key words: Information Security, Awareness, Baseline, Education, Certification

Abstract: People have become an important factor in securing the information technology environment. They need to be made aware of its importance, as well as what their role is in securing information assets. Despite the widespread acceptance of this fact many organisations still lack an information security awareness program to instil this knowledge. This paper will explore the possibility of improving current information security levels through a baseline approach to information security awareness.

1. INTRODUCTION

Information and information technologies have become a vital component of successful businesses and organisations. Information is being used to support every part of business, from operations to managerial decision-making and strategic competitive advantage (O'Brien, 1999, p.19). Information has therefore become an asset that, like other important business assets, has value and should be well protected (British Standards Institute, 1999, p.1).

The protection of these information assets seeks to be fulfilled by the discipline of information security. Information security is introduced into the information technology environment by implementing controls to protect against possible threats to information assets (Barnard & von Solms, 2000, p.185). The controls necessary to effectively protect information assets have been influenced by technological advancement in the information technology environment. These technological advancements have brought computer processing to a wider group of employees than ever before (Thomson, 1998, p.8). It is important in today's information technology environment that the employees are guided as to their information security responsibilities (von Solms, 1998, p.174). For employees to play an effective role in information security in the organisation, they need to be educated on the importance of their role in protecting information assets and they need to know how to behave in order to fulfill this role. These are just some of the aspects of what is known as the need for information security awareness (Thomson, 1998, p.12). To ensure that an adequate level of security awareness exists within an organisation it is important to establish an information security awareness program (ISO/IEC TR 13335-1, 1996, p.13). Current standards clearly underline this need and give guidelines on the implementation of awareness programs. However, the small number of organisations implementing awareness programs and the low level of awareness within organisations suggests that these approaches are ineffective.

According to a survey done by multinational advisor group KPMG, in conjunction with research group BMI-TechKnowledge, only 34% of all end-users view information security as important in the organization (Khan, 1999, online). Current efforts to address this problem take the form of awareness programs that stem directly from the policies and procedures already in place in an organization (British Standards Institute, 1999, p.1). Policies are management instructions on the security objectives of the organisation, while procedures are the specific operational steps that users must take to achieve the goals of this policy (Wood, 1994, p.2). The development of such policies and procedures is a lengthy process that requires time, money and specialized knowledge. These constraints could prove prohibitive for small to medium sized companies and is a possible cause for low level awareness in organisations.

The alternative to such a company-specific approach would be a generic awareness program suitable for most employees from most organisations. The objective of this study is twofold. Firstly, to identify which aspects of a complete awareness program could be catered for in a non company-specific, non user-specific way. Secondly, to determine the educational material that needs to be included in such a generic program.

These findings will be used in developing a model containing the components of a complete awareness program and showing where the generic component exists.

The paper will highlight the increasing importance of people in securing information assets, and will briefly discuss the operational controls that seek to guide these employees. The need for an information security awareness program will be pointed out and a company-specific approach to such a program investigated. Following problems identified by such an approach, a generic approach to information security awareness will be proposed. The possibility of such an approach being used for baseline education and certification will then be highlighted. The conclusion will highlight aspects that will require further investigation.

2. THE INCREASING IMPORTANCE OF PEOPLE IN PROTECTING INFORMATION

The task of protecting information assets is accomplished by introducing controls into the information technology environment. As IT advanced, so did the controls necessary to successfully protect the environment. These advancements will be discussed to highlight how controls need to be increasingly focused on the people in the environment.

When computers were first introduced into organisations, they took the form of standalone mainframe computers with single processors (Von Solms, 1998, p.174). These mainframe systems did not support the use of databases and only supported one user working on them at a time. These users were limited to dedicated computer personnel trained in the secure use of such systems (Thomson, 1998, p.7). To make sure that only these users were allowed access, physical controls such as locking doors were implemented and proved to be adequate protection.

The multi-user era was brought on by the introduction of computers that could perform multi processing and allow multiple users to log on at the same time. Workstations for users were now provided in their working environment and became part of their daily functions. Resources, like memory and databases were now shared and could be accessed remotely in a distributed fashion (Thomson, 1998, p.7). This brought the problem of ensuring that only authorized users gained access to these resources. To ensure this, technical controls such as authentication and access control were needed.

Despite the distributed nature of the multi-user environment, the central computer still held the intelligence. Workstations held no intelligence and were simply able to communicate with the mainframe to share its resources (Thomson, 1998, p.7).

With the increased capability and reliability of personal computers and the availability of end-user packages, the power and therefore responsibility has shifted to the end-user. The users that now have all these capabilities are generally not trained in the information technology field and therefore do not possess the skills to use them in a secure manner (Thomson, 1998, p.8). Using passwords to control access to data would be useless if the computer housing the data could be carried out the door because a user left the door unlocked, or if the user posted the password next to the screen. Operational controls are now needed to dictate and ensure that users operate in a manner that would not undermine these physical and technical controls in place.

The evolution of the information technology environment has put this environment in a position where it is increasingly dependant on people to successfully secure its assets. The move beyond purely physical and technical controls is also evident in current laws and standards. The revised version of BS7799 amended its common best practices to include consideration beyond electronically processed data (Pounder, 1999, p.308) For example, the section on information exchange identifies controls that are relevant to the databases via the Internet as well as simple information exchanges in a telephone conversation. The UK data protection Act of 1984 displays a similar change in its 1998 amendment. The act now makes no distinction between automated and non-automated files in the information it requires protected (Pounder, 1999, p.308). A move away form technology can only serve to highlight the people aspect in computing.

3. GUIDING EMPLOYEES THROUGH POLICIES AND PROCEDURES

It has become increasingly important for people to actively assist in successfully protecting information of organisations, and this has enhanced the importance of implementing operational controls as guidance to them.

3.1 Policies

Policies are management instructions on how an organisation should be run (Wood, 1994, p.2). These instructions reside at the top of the organisational structure and are high-level statements that set the direction of the organisation. The important role that policies play in the organisation is listed in ISO/IEC TR 13335. This report suggests that the first step towards effective IT management is the development of an information security policy to be included in the corporate policy of the organisation (ISO/IEC TR 13335-2,1996, p.2).

Policies are used as a reference for a wide variety of information security activities. One of these activities is the development of procedures.

3.2 Procedures

Procedures are specific operational steps that workers must take to achieve a certain goal. They are based on the broad guidance provided by policies, but are much more specific. Procedures should be tailored to the specific environment into which they will be implemented, and should be geared towards providing understandable help to the people who will be using them (Wood, 1994, p.2).

Operational controls such as policies and procedures rely on human behaviour to be implemented. Unlike physical and technical controls, simply having policies and procedures in place is not enough. Employees must be aware of these policies and procedures and be motivated to follow them before the company can experience the benefits of these controls.

4. INFORMATION SECURITY AWARENESS

Making users aware of their responsibilities in securing the information technology environment and motivating them to do so, form part of what is known as information security awareness. An information security awareness program is a vital control in securing the information technology environment (ISO/IEC TR 13335-1, 1996, p.13)

The importance of such awareness programs is illustrated by their inclusion in current information security standards such as BS7799 and ISO/IEC TR 13335 (British Standards Institute, 1999, p.10; ISO/IEC TR 13335-1, 1996, p.13)

Despite the widespread acceptance of the need for information security awareness and the guidance provided on how to implement such programs, very few organisations use them. According to the Information Security Breaches Survey 2002 (ISBS2002) released by Price Waterhouse Coopers in April this year: “UK businesses are spending considerable time, effort and money on implementing sophisticated technology, without developing a security awareness culture within their organisation to support it." (PricewaterhouseCoopers, 2002, online)

A possible reason for such a lack of awareness programs in organisations could be the approach used to implement such programs. Both BS7799 and ISO/IEC TR 13335 stress the need for implementing information security awareness programs based on the policies and procedures already in place in the organisation. This approach seems sound when looking at the statistics provided by the ISBS 2002. According to this survey only 4% of organisations that had information security policies failed to make an effort towards awareness programs. The problem is that only 27% of the organisations interviewed had developed an information security policy. If these policies were the only basis for awareness programs it would follow that only 27% of organisations would have something on which to base their information security awareness programs

The alternative approach to such a company-specific awareness program would be to develop an awareness program that would not be dependent on an organisation's policy. This could be seen as a generic approach to establishing information security awareness in an organisation.

5. COMPANY-SPECIFIC VS. GENERIC APPROACH TO SECURITY AWARENESS

A company-specific approach is when an awareness program is based on the information security policies of a specific organisation. The current lack of policies in organisations proves problematic to this approach. This might be a temporary situation, but other points against a company-specific approach still stand. Consider the following: since the goals of organisations are different it would follow that policies, and therefore awareness programs that stem from these policies, will also be different for different organisations. This means that awareness programs need to be developed from scratch for every organisation.

The development of an awareness program that is not based on the policies of an organisation would solve this problem. The question is then what such an awareness program would be based on.

The focus in today's information technology environment is not only on educating employees on the policies of the organisation, but also on changing behaviour and cultivating an information security culture right through the organisation (Von Solms, 2000, p.618) To achieve this an information security program would include aspects other than just the policies of an organisation. Such aspects include basic information technology concepts, threats to and vulnerabilities of computer systems and the importance of protecting information in today's business environment. These aspects will be discussed in more detail later, but it is important to note that they could be catered for in a generic awareness program.

Merely including these issues might not prove beneficial enough in guiding employees on appropriate behaviour in their everyday tasks. Procedures are still needed to guide employees on specific steps to promote security. Among other things, the next section will highlight how these procedures could be provided in a generic awareness program

6. A GENERIC APPROACH TO INFORMATION SECURITY AWARENESS

It is likely that aspects provided by a company-specific approach to information security awareness will be lost when trying to cater for as many employees of as many organisations as possible. To ensure that the aspects lost will not deprive an awareness program of its function, two issues need to be looked at. Firstly, the subset of employees that could be reached by a generic awareness program will be identified. Secondly, the contents of an awareness program will be investigated to show which aspects could be catered for in a non company-specific, non user-specific way.

6.1 Employees to be addressed by an awareness program

According to ISO/IEC TR 13335, a security awareness program should be implemented at all levels of the organisation, from top management down to every employee. The report also suggests that users will require different awareness training depending on these different levels (ISO/IEC TR 13335-1,1996, p.13). Despite the different roles and responsibilities that come with different levels in the organisation, all these users use information systems or the information it produces. This means that, at some level, these users are all end-users and need to be made aware of the security issues required at this level (O'Brien, 1999, p.10). A generic awareness program will focus on promoting awareness at this end-user level.

6.2 Contents of a company-specific vs. generic awareness program

This section will point out the content of a company-specific approach to information security awareness that could be catered for in a non-company specific way. Motivations will be included where needed as well as examples of specific material to be included. The aspects identified will be illustrated in a model showing which part of a company-specific program makes up the generic component.

6.2.1 Importance of information and information security

The importance of information and the information technology infrastructure that supports it has to be impressed on employees. Understanding the importance of information will serve as motivation to do their part in securing this asset (Hansche, 2001). Material would include examples of how information supports today's business environment and the consequences of that information being compromised.

6.2.2 Threats to and vulnerabilities of computer systems

To understand why they need to protect information, employees need to be aware of the threats to, and vulnerabilities of, computer systems (Hansche, 2001). Material would include topics such as viruses, hacking and the concept of social engineering.

6.2.3 Information security policy

Since the security policy of the organisation sets the security direction for the organisation, knowledge of this policy will help the employee understand what the organisation is striving for in information security. Such company specific information would be impossible to cater for in a generic program, although this point may be debateable. The ideas behind many information security policies are similar from organisation to organisation (Wood, 1994, p.1). Manuals, books and packages have been written in an attempt to provide a comprehensive set of policies that could be chosen from to suit most organisations. If policies move towards being more standardised, they could well be catered for by a generic awareness program in the future.

6.2.4 Specific procedures and how to implement them

Employees must be made aware of specific procedures to follow to promote information security. Procedures are generally derived from the specific policies of the organisation. There are, however, certain procedures that are generic to most organisations. For instance, all computer users need to be aware of the proper way to use passwords, the importance of logging off and backing up system information. This is where a generic awareness program could be beneficial by providing a general set of procedures that could be followed to promote information security. Certain procedures would, however, remain specific to the organisation. Procedures such as where to report security incidents could not be catered for in a generic way.

6.2.5 Basic information security concepts

Basic information security concepts need to be taught to the user. This knowledge will stand them in good stead when trying to understand the threats to and vulnerabilities of computer systems. It will also aid understanding of the procedures learned. Material would include basic information security concepts such as availability, risks, impact etc. (United States of America. Dept. of Commerce, 1998, pp.25-32).

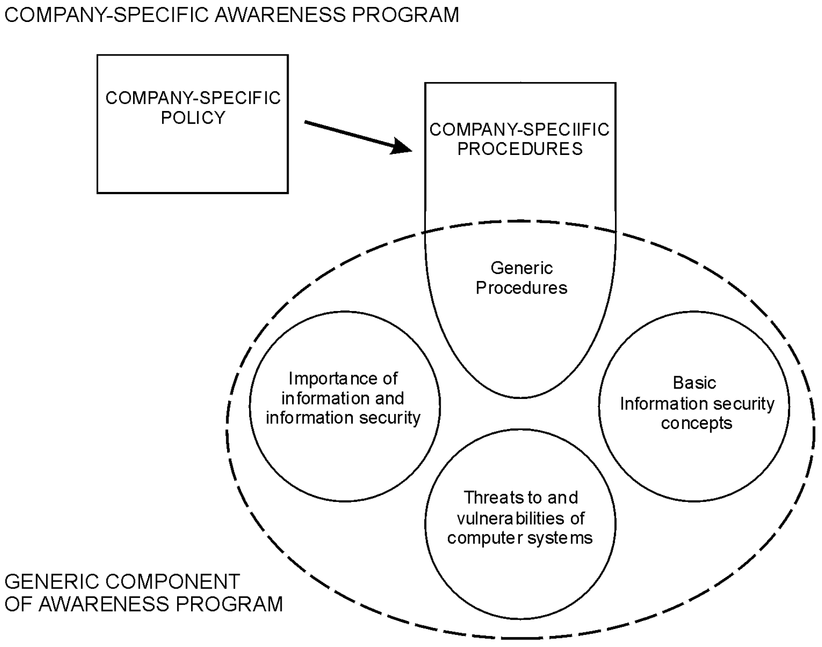
COMPANY-SPECIFIC AWARENESS PROGRAM
COMPANY-SPECIFIC POLICY
COMPANY-SPECIIFIC PROCEDURES
Generic Procedures
Importance of information and information security
Basic Information security concepts
Threats to and vulnerabilities of computer systems
GENERIC COMPONENT OF AWARENESS PROGRAM

Figure 1. The generic component of a company-specific awareness program

7. BASELINE EDUCATION AND CERTIFICATION

The generic component identified shows that a large part of a company-specific awareness program can be catered for by a generic approach to information security awareness. This generic component can be useful in establishing a baseline of awareness by educating employees and other individuals on the essentials of information security awareness.

Such a baseline effort could be compared to the BS7799 best practices for information security management. This standard suggests choosing controls from a set that was identified to work for most organisations through experience, instead of going through a company-specific approach to identifying what exactly that company requires (Von Solms, 2000, p.616) A baseline approach cannot exactly fulfil a company's specific needs, but can provide the assurance that some basic standard is adhered to.

Certification based on this baseline would reinforce this assurance and could be used as a basis for establishing trust between organisations, customers and suppliers. Certification of the employees of an organisation can also provide proof, in legal cases, that an organisation has made an effort towards securing their information assets.

8. CONCLUSION

Information security awareness levels are still low among the employees of organisations, but despite this fact organisations are still not making an effort to implement awareness programs to improve the situation. A possible cause is that current efforts towards awareness programs focus on promoting the policies and procedures already in place in the organisation. A problem exists with this company-specific approach in the fact that these policies and procedures are often lacking in organisations. A generic approach would solve this problem by effectively making the awareness effort independent of the policies and procedures specific to one organisation. A generic awareness program cannot exactly fulfil a company's specific needs, but could provide a baseline of awareness for most employees of most organisations. Simplifying the process of developing an awareness program could go a long way towards improving the current levels of awareness in organisations.

A general idea of the material to include for each part of a generic awareness program has been identified but it is felt that the identified material should be corroborated by a survey. Such a survey, along with an investigation on how a generic awareness program will be presented, will form part of further research.

REFERENCES

Barnard, L. & von Solms, R. (2000). A formalized approach to the effective selection and evaluation of information security controls. Computers & Security.19 (2), pp.185-194. Elsevier Science Ltd.

British Standards Institute. (1999). Code of practice for information security management. DISC PD 0007. London.

Hansche, S. (2001, July 17). Making security awareness happen. TechRepublic [online]. [Cited March 18, 2002] Available from Internet URL: http://www.techrepublic.com/article.jhtml?id=r00520010717aue01.htm&rcode=&rcode=&page=1

ISO/IEC TR 13335-1 (1996). Information technology - guidelines for the management of IT security – part 1: Concepts and models for IT security (First Edition), Switzerland.

ISO/IEC TR 13335-1 (1997). Information technology - guidelines for the management of IT security – Part 2: Managing and planning IT security (First Edition), Switzerland.

Khan, B (1999, November10). SA information security awareness at a low [online]. [Cited March 15, 2001] Available from Internet URL: http://196.36.119/sections/news/default.asp

O'Brien, J.A. (1999). Managing information systems: Managing information technology in the internetworked enterprise (4th ed.). United States of America: Irwin/McGraw-Hill.

Pounder, C. (1999). The revised version of BS7799 – So what's new? Computers & Security.18 (4), pp.307-311. Elsevier Science Ltd.

PricewaterhouseCoopers (2002). Information security breaches survey 2002 [online]. [Cited May 14, 2002] Available from Internet URL: https://www.security-survey.gov.uk/

Thomson, M. (1998). The development of an effective information security awareness program for use in an organisation. Unpublished master's thesis. Port Elizabeth Technikon, Port Elizabeth, South Africa.

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.

Von Solms, B. (2000). Information security – The third wave? Computers & Security.19 (7), pp.615-620. Elsevier Science Ltd.

Von Solms, R. (1998). Information security management (1): Why information security is so important. Information Management and Computer Security 6 (4), pp. 174 – 177. MCB University Press.

United States of America. Dept. of Commerce. (1998). Information security training requirements: A role- and performance-based model. Washington: U.S Government Printing Office.

Wood, C.C. (1994). Information security policies made easy. Ohio: Bookmasters