Information Security Awareness: Towards a Generic Programme

H. Mauwa and R. Von Solms

Nelson Mandela Metropolitan University, Port Elizabeth, South Africa
Email: hope.mauwa@nmmu.ac.za; rossouw@nmmu.ac.za

Abstract

Basing information security awareness programmes on existing information security policies in organizations is a sound approach, since these policies are seen as the basis for effective information security. But this approach does not satisfy the needs of organizations that do not have such policies in place. Therefore, another approach, which does not entirely depend on existing policies, is needed so that organizations, even those without the policies, can implement such a programme.

Keywords

Information Security Awareness Programmes, ISO/IEC 17799, ISO/IEC 13335-3.

1. Introduction

In today's computing environment, awareness programmes now play a much more important role in organizations' information security programmes because the maintenance of effective security is more dependent than ever on the vigilance of users. Even though awareness programmes have become increasing important, the level of awareness in most organizations is still low. The current approach of developing these programmes recommends that they should stem directly from information security policies already existing in organizations (Du Plessis & Von Solms, 2002).

It is the objective of this paper to argue that the most effective type of information security awareness programme is a generic type, which is suitable for most organizations and does not depend entirely on existing policies in organizations.

In order to accomplish this, this paper will look at several issues, including the role that information security awareness programmes play, in order to gain an understanding of the impact they have on information security. The current approach to the development of these programmes will be discussed to highlight its limitations. Once this has been established, an alternative approach will be proposed by examining the topics discussed in information security awareness programmes.

Then, sources used to identify the contents for the proposed approach will be discussed. Finally, topics that can form part of the contents for the proposed approach will be identified based on the above studied sources.

2. Why Information Security Awareness?

Information security awareness efforts are designed to change behaviour or reinforce good security practices, and they provide a baseline of security knowledge for all users, regardless of job duties or positions (Du Plessis & Von Solms, 2002). Security awareness allows individuals to recognize information security concerns and respond accordingly. Courtney Gilbert (2003) described security awareness as a learning process, which changes individual and organizational attitudes and perceptions so that the importance of security and the adverse consequences of its failure are realized. Thomson and Von Solms (1998) motivate that information security awareness gives employees the necessary knowledge to maintain security by ensuring the confidentiality, integrity and availability of information.

Information security awareness focuses on developing an organizational culture that is both aware and capable of responding to security-related risks. It aims at changing the way employees behave towards an organization's vital information and cultivating an information security culture throughout an organization. The way in which people work with information assets in their daily job functions eventually becomes the way things are done in an organization, and this eventually becomes part of the culture of an organization (Du Plessis & Von Solms, 2002).

Achieving this level of understanding represents a major challenge because no amount of technology can reduce the overriding impact of human complexities, inconsistencies, and peculiarities (Ernst &Young, 2004). Ernst and Young (2004) claim that any strategy that overlooks this realization is inherently flawed. With proper awareness, employees become the most effective layer in an organization's security defence.

With the important role that these awareness programmes play in organizations' complete information security programmes, experts have developed guidelines to assist organizations in developing them.

3. The Current Approach to Security Awareness

The current approaches to the development of information security awareness programmes need to be examined. Studying these current approaches will assist in understanding the effect such programmes have on various organizations.

3.1 Guidelines and Standards

The current guidelines recommend that awareness programmes should be developed, based on the security policies and procedures currently in place in organizations.

This is advocated prominently in current information security guidelines and standards. Two such standards are ISO/IEC 17799:2005 and ISO/IEC 13335-3:2005. This is because management instructions, i.e., policies, are mainly seen as the basis for effective information security within an organization (ISO/IEC 13335-1, 2004).

It has to be said that every organization is unique, and as such, different organizations have different management instructions about how they should be run. Therefore, the awareness programmes that stem from these management instructions also differ from one organization to another. This could be called a company-specific approach to information security awareness, since it is based on elements that are very specific to a particular organization (Du Plessis & Von Solms, 2002).

Despite the illustrated importance of information security awareness and the widespread acceptance of this fact in current guidelines and standards, the level in most organizations is still low, according to some of the recently conducted surveys (Ernst & Young, 2004; Deloitte Touche Tohmatsu, 2005).

3.2 Limitations of Current Approaches

According to the *Global Information Security Survey* by Ernst & Young (2004), respondents named the ***"lack of security awareness by users"*** as the top obstacle to effective information security; however, only 28% listed ***"raising employee information security training or awareness"*** as being a top initiative in 2004. In the *Global Security Survey*, conducted by Deloitte Touche Tohmatsu – Australia (2005), respondents pointed to a host of continuing challenges to their businesses. One of the most prominent among them was the "***lack of employee awareness and training***" - (48%). According to the same survey, overall, security awareness and training implemented, or maintained, decreased from 77% in 2004 to 65% in 2005.

A possible reason for such a lack of awareness programmes in organizations could be the approach used to implement such programmes (Du Plessis & Von Solms, 2002). As pointed out in the last section, both ISO/IEC 17799:2005 and ISO/IEC 13335-3:2005 stress the need for implementing them, based on the information security policies and procedures already in place. But not all organizations have these policies in place. A recent survey conducted by PricewaterhouseCoopers LLP (2004), *Information Security Breaches Survey 2004*, reveals that a third of all companies and two-thirds of large businesses in the United Kingdom now have information security policies. This means that only those organizations would have a basis on which to formulate their information security awareness programmes.

The current lack of awareness programmes in most organizations suggests that a problem exists with the traditional method of basing awareness programmes on the policies and procedures already in places (Du Plessis & Von Solms, 2002). Therefore, an *alternative* approach to the development of information security awareness programmes has to be developed that will not depend entirely on existing policies.

4. A Generic Information Security Awareness Programme

An examination into the different areas of security knowledge covered in awareness programmes reveals that some aspects are company-specific while others are generic components that are non-company-specific.

Company-specific information includes an organization's information security policy's contents and specific procedures. Policy documents are different for different organizations, since the goals and directions are also different. As such, employees of different organizations are, therefore, educated by different awareness material concerning their organization's policies. Procedures are based on the broad guidance provided by policies, and as such, they are much more specific to every organization. It is through policies and these procedures that employees within a specific organization are guided in their role of securing the organization's information technology environment (Du Plessis & Von Solms, 2002).

Du Plessis and Von Solms (2002) argue that the focus is not only on educating employees on the policies of their organization, but also on changing their behaviour and cultivating an information security culture throughout the organization. To achieve this, an information security programme would include aspects other than only the organization's policies. Such aspects include general procedures, basic information technology concepts, threats to and vulnerabilities of computer systems and the importance of protecting information in today's business environment, which tend to be the general and common aspects that affect most organizations. Generally, these aspects are part of a company-specific content but could be catered for in a non-company-specific way. Such an approach to implementing an awareness programme can be called a generic approach to information security awareness (Du Plessis & Von Solms, 2002).

In most organizations an information worker needs to be aware of the general information threats and vulnerabilities that exist today, specifically when using electronic means to transact business processes, and it is these aspects that should form part of a generic information security awareness programme.

Having examined what would constitute a generic programme, several sources were studied in order to formulate its actual contents.

5. Towards a Generic Information Security Awareness Programme

Several internationally recognised sources, information security awareness programmes located on the Internet and a survey conducted by the authors were used to identify the contents of a generic information security awareness programme and to ensure that the foundation on which it is based is as broad as possible.

5.1 The Standards

The ISO/IEC 17799:2005 and the ISO/IEC 13335-3:2005 were used because they comprehensively cover awareness programmes. Both standards recommend that these programmes should reflect on the contents of a corporate information security policy, and should cover all objectives of an information security plan. The ISO/IEC 13335-3 goes on to say that the programme should ensure that the IT staff and the end-users have enough knowledge of the hardware and software systems to understand why safeguards are necessary, and to know how to use them correctly.

5.2 The Internet

Some awareness programmes offered on the Internet were studied thoroughly to gain more insight into the topics covered in them. A well-known one is the SANS Security Awareness Programme.

This covers general security areas affecting most organizations, such as passwords, computer viruses, malicious codes, personal use and gain, data backup and storage, incident response, environmental security, inventory control, physical security and social engineering. It also reports on true-life stories that have happened to people and organizations to demonstrate and reinforce the importance of the concepts covered. Each example demonstrates the consequences of simple mistakes or lapses in information and computer security.

5.3 The Authors' Survey

Having studied what is covered in the international information security standards and the Internet, a questionnaire was drafted and sent out to some well-known South African organizations known to follow sound information security principles. The main aim of the survey was to solicit ideas on what their managements recommend for inclusion in a generic programme.

It is important to point out that the organizations that were selected and participated in the survey operate in diverse industrial sectors: mining, manufacturing, food and beverages, education, communications and IT. This was done in order make sure that the identified content is suitable for interdisciplinary organizations.

The guidance and recommendations provided by the above sources and the survey are sufficiently broad to identify and base the contents of a generic programme on them.

6. Generic Contents of an Information Security Awareness Programme

It is important to bear in mind that general and common aspects affecting most organizations' employees would need to be included when identifying the topics for

a generic programme. Any company-specific information, such as information security policies, guidelines and procedures, would only be introduced to the employees to make them aware of their existence and encourage them to find out more from their respective organizations. Based on the guidance and recommendations from the sources studied and the survey, the following broad topics were identified as part of the contents of a generic information security awareness programme:

- Data backup and storage
- Social engineering
- Remote/mobile worker security
- Malicious code security
- Password security
- E-mail security
- Physical and environmental security
- Computer ethics
- Privacy and confidentiality
- Paper-copy document security
- Accountability and responsibility
- Anti-virus software and firewalls
- Information security policies, standards and procedures.
- Information risk management
- Contingency planning
- Incident management
- IT laws, regulations and standards
- Computer auditing
- Change management.

It is important to point out that a generic awareness programme has to compromise the scope of the material that it presents in order to satisfy the primary goals of keeping the programme generic. All that the generic approach tries to achieve is to provide a baseline of awareness by educating the employees on the essentials of information security. Having such a baseline in place can provide organizations with the assurance that some basic level of awareness exists among employees.

7. Conclusion

It has been established that the general approach of basing awareness programmes on security policies and procedures already in place in organizations is a limiting factor: if organizations do not have them, they do not have a basis on which to support awareness programmes. This has contributed to the current low level of information security awareness in most organizations.

The contents of awareness programmes identified on the Internet were examined, and it was realized that these programmes contain a generic component that is

company-independent. Therefore, a generic approach, which does not depend entirely on existing company policies and procedures and caters only for this non-company-specific component, was further investigated and proposed. The actual contents of the generic programme were also formulated using guidance from the ISO/IEC 17799:2005 and ISO/IEC 13335-3:2005, the Internet and the survey that was conducted with some South African organizations. These sources were used to make sure that the foundation on which the contents of the generic programme are based is as broad as possible.

The generic approach allows for the creation of an awareness programme that would be suitable for most organizations, even those without security policies and procedures. As such, it is expected to improve the level of awareness programmes in organizations. It must be noted though, that such a generic information security awareness programme, as suggested in this paper, should be augmented eventually by some contents to cater for the company-specific information that cannot be included in such a programme.

References

Deloitte Touche Tohmatsu - Australia. (2005). *2005 Global Security Survey.* Retrieved August 21, 2005, from http://www.deloitte.com/.

Du Plessis, L. & Von Solms, R. (2002). *Information Security Awareness: Baseline Education and Certification.* Baccalaureus Technologiae. Port Elizabeth: Information Technology Department, Nelson Mandela Metropolitan University.

Ernst & Young. (2004). *Global Information Security Survey 2004*. Retrieved August 21, 2005, from http://www.ey.com/global/.

Gilbert, C. (June 2003). *Developing an Integrated Security Training, Awareness, and Education Program.* GSEC Practical Assignment version 1.4b Retrieved August 8, 2005, from http://sans.org/rr/whitepapers/awareness/.

ISO/IEC 13335-1 (2004). *Information Technology - Security Techniques - Management of Information and Communications Technology Security.*

PricewaterhouseCoopers. (2004). *Information Security Breaches Survey 2004.* Retrieved August 21, 2005, from http://www.infosec.co.uk/.

Thomson, M. & Von Solms, R. (1998). *The Development of an Effective Information Security Awareness Programme for Use in an Organization.* Magister Technologiae. Port Elizabeth: Information Technology Department, Nelson Mandela Metropolitan University.

Von Solms, B. (2000). Information Security - The Third Wave? *Computers and Security* 19(7): pp.615-620.