INFORMATION SECURITY AWARENESS AND TRAINING -

THE LEGAL COST OF UNTRAINED PERSONNEL

Verine Etsebeth

Faculty of Law, University of Johannesburg

Faculty of Law
University of Johannesburg
PO Box 524 Auckland Park 2006
Fax +27 11 489 2049
space_law@yahoo.com

ABSTRACT

The essence of an information security awareness and training program is best captured by the following quotation: "…if the road to hell is indeed paved with good intentions, then the sidewalks are built of grand ideas that never saw the light of day or languished as the best kept secret within the corporate walls".[1]

Although the development and implementation of information security policies, standards, procedures and guidelines are imperative to the success of the overall information security discipline, it will be a futile exercise if these policies, guidelines and procedures are not brought under the attention of those people who are expected to adhere to them, therefore the employees of the company. The importance of awareness and training can not be overemphasised as awareness and training may be the most cost-effective action a company may take against information security breaches and incidents. The employees of a company may be viewed as the first line of defense when it comes to the early detection of problems. Consequently, employees on all levels of the company must be made aware of the pivotal role security, and specifically information security plays within a company. They need to be educated on, and kept informed of potential threats, vulnerabilities and risks, and shown how their actions could increase or decrease the likelihood of a threat materialising. Furthermore, it should be kept in mind that although traditionally information security was viewed by the board of directors and top management as a necessary evil, at present companies are being placed under increased pressure by means of new laws and regulations to ensure that information security is effectively implemented within the company. Consequently, if an information security breach or incident occurs because of the actions of an untrained or uninformed employee of the company, the board of directors and top management may be held personally liable for the acts of the company's employees. It is therefore imperative that the awareness and training program should start with top management and work its way down to lower levels of the company.

The account contained in this contribution is meant to give a broad overview of information security awareness and training having specific regard to the salient legal issues embedded in the development and implementation of the awareness and training program. More specifically the aim of this paper is to provide companies with a framework against which they may develop their own

awareness and training program which they can adapt to provide for the specific needs of their individual company.

KEY WORDS

Information Security, Awareness and Training and Legal Liability.

INFORMATION SECURITY AWARENESS AND TRAINING -

THE LEGAL COST OF UNTRAINED PERSONNEL

1 INTRODUCTION

Companies may feel bewildered by the plethora of seemingly disjointed information security components that they must consider when wanting to implement information security within their company. Implementation of information security within a company is embodied in a multitude of layers/phases with each phase acting as a continuation of the previous phase and a predecessor of the next. The implementation process will address numerous issues, including (i) determining the radius of risk to information security within the company by making use of an effective risk management process; (ii) the development and implementation of information security policies, standards, procedures and guidelines, to ensure information security is deployed and enforced in a consistent manner throughout the company (this phase is said to be the foundation of any information security initiative); (iii) raising the awareness of information security issues amongst employees by educating them on why the need for information security exist, what is expected of them, and what consequences will ensue if they do not adhere to the proposed policies, standards and procedures is crucial. Event the best formulated information security policy will sit dormant on a shelf if those people who are expected to comply with it are not made aware thereof; and (iv) maintaining and monitoring information security is just as important as implementing it in the first place. It might even be harder to achieve, as maintenance and monitoring requires renewed commitment to information security efforts on a daily basis.

This article focuses attention on the third phase of the implementation process, namely information security awareness and training. Information security awareness and training is presented to include definitions and benefits of the program. This is done before moving on to provide directors and top management with a methodology in the form of a usable framework for the implementation of information security awareness and training program within the company in order to make employees on all levels of the company aware of information security practices, procedures and documentation. Moreover, the impediments to the development and implementation of an effective awareness and training is highlighted. Finally, emphasis is placed on the legal consequences which may ensue if the company does not have an effective information security awareness and training program in place.

2 INFORMATION SECURITY AWARENESS AND TRAINING DEFINED

Although the terms awareness and training are often used concurrently, they are not synonymous with one another. Awareness is "a passive mechanism that occurs through less formal methods such as posters, themes and objects such as key rings and cups."[2] It is contended by Russel[3] that the goal of awareness is "to raise the collective awareness of the importance of security and security controls."[4] Training or instructional design, may be viewed as being "more formalised, typically in a classroom, or conference setting where the objective is to gain knowledge about a particular subject."[5] Russel[6] argues that the goal of training is "to facilitate a more in-depth level of user understanding."

For the purpose of this article information security awareness and training may be defined as the process by which all role players in the company are made aware of what the information security policies, standards, procedures and guidelines entail, what is expected of them, why this is expected of them, and what consequences may ensue if they do not adhere to or comply with these policies, standards, procedures and guidelines.[7]

3 AWARENESS AND TRAINING PROGRAM OBJECTIVES

The first and foremost objective of any information security awareness and training program is to give prominence to the importance of information security within the company, and raise the consciousness of all employees regarding this subject-matter.[8]

Other objectives include:

(i) Enabling employees to recognise their responsibility for protecting the company's information assets.[9] Employees must realise that information security forms part of their job.[10] By tying information security responsibilities to their job description employees can understand the importance of information security and the concept of ownership for it.[11] It must be made clear to employees that information security is everybody's responsibility,[12] it forms part of the corporate culture.[13]

(ii) Ensuring that employees realise the value of information security.[14] The program must be developed in such a way that it "defines exactly how corporate information assets are defined, who uses them, and what steps must be taken to protect them."[15] Employees must be made aware of the value of the company's information assets by emphasising the legal and financial consequences that will ensue if the confidentiality, integrity and/or availability (CIA) of information assets are not adequately protected.[16]

(iii) Enabling employees to recognise potential violations and know who to contact.[17] Apart from making employees vigilant by highlighting what risk and threats must be guarded against, they should also be informed of the correct procedure to be followed from the moment a security incident or potential security incident has occurred.[18] Warning signs and indicators must furthermore be implemented and pointed out to employees on when a potential threat arises.[19]

(iv) "Ensuring that the level of security awareness and training among existing employees remains high."[20] Training should be offered to new recruits, as well as to existing employees. All employees need to be kept up-to-date on the latest development on new and existing threats, vulnerabilities and risks facing the company.

4 IMPLEMENTING THE INFORMATION SECURITY AWARENESS AND TRAINING PROGAM

The following framework (7-step plan) will assist companies in developing and implementing the information security awareness and training program.

(i) STEP 1: Launch an in-depth investigation into policies and procedures that already exist within the company, proceed to analyse these documents to find out if any information security aspects are embedded in them.[21] This step will necessitate interviews and discussions with internal auditors, personnel from the human resources department (HR) and people responsible for the drafting of the documents of the company. Only after this process has been completed work can start on the development of new policies, standards, procedures and guidelines.[22]

(ii) STEP 2: Obtain top management support and commitment for the awareness and training program.[23] One of the biggest and arguably most important challenges is to obtain management support and commitment for the awareness and training program.[24] Executives must support and be committed to the information security program otherwise it will be abandoned, and widely ignored by all.[25] This step would involve the development and scheduling of a training session targeted at executive-level management.[26] The purpose of this training session is not only to

educate executives on the subject-matter of information security, but also to gain their support for it.[27] In order to obtain management's support the internal hierarchy existing within the organisation must first be determined. When attempting to "sell" information security to management a presentation should be developed that is centred around the following information: (a) the nature and size of project; (b) identify business needs it will meet; (c) point out impact of not going forward with project state probable cost; (d) cite estimated losses if not implemented; (e) show how you would reach ultimate goal; and (f) allow for questions and answers. It should furthermore be kept in mind that managers are only concerned with costs. Therefore the message to managers must be articulated in business terms that managers understand and are interested in. Top management will only support the program if they are convinced it will succeed. In stark contrast to the education of employees executives need full disclosure on all potential vulnerabilities that may be exploited and/or threats that may materialise. They must furthermore be educated on the costs associated with information security, as well as the benefits and detriments attached to this discipline. The following motivational "tools" will impel managers to support the program: (a) money - anything that reflects positively on the bottom line will be supported by management; (b) FUD (fear, uncertainty and doubt) functions as a major motivational tool. Specifically the fear of damage to the organisation's reputation, in the form of deleterious publicity; (c) knowledge on the part of management that they are obliged in terms of a statute, regulation and/or contract to perform a certain act will proof to be a powerful motivational tool for managers; (d) sustaining the existing level, and/or increasing the levels of productivity in the organisation; and (e) compliance with their duty of due care. After initial buy-in from management the second challenge is maintaining management's commitment. Apart from the commitment and support of senior management, the effectiveness of any information security awareness and training program will furthermore dependent on the long-term appropriation of resources and funding.[28] However, it should be kept in mind that most benefits delivered by information security are of an intangible nature, and therefore inherently hard to place a monetary value on. The general formula used to calculate the value of such a benefit would be to deduct the cost of an investment in awareness and training from the estimated cost of losses or damages that would have been incurred if the aforementioned investment was not made.[29]

(iii) STEP 3: Evaluate and develop security policies, standards, procedures and guidelines.[30]

(iv) STEP 4: Determine who the target audience is that will be addressed on the subject matter. "To be successful, the awareness program should take into account the needs and current level of training and understanding of the employees and management."[31] When focussing on your target audience apply the AUDIENCE – principle:[32]

Analysis: Who are they, how many will there be?

Understanding: What is their knowledge of the subject?

Demographics: What is their age, gender, educational background?

Interest: Why are they there? Who asked them to be there?

Environment: Where will I stand? Can they all see and hear me?

Needs: What are their needs? What are your needs as speaker?

Customise: What specific needs do you need to address?

Expectations: What do they expect to learn or hear from you?

Even before the training of employees commences the very first step should be to focus on the selection and appointment of suitable candidates. An investigation should therefore be launched into the background and history of the prospective employee, while simultaneously taking into consideration factors that might influence his/her attitude towards the company. Keep in mind that previous employers seldom provide an honest account of how they experienced the candidate. Only after the company has identified and appointed competent and suitable personnel can the issue of training be addressed. When the new employee is employed it is recommended that he or she undergo preliminary training. Furthermore employees who were employed by the company before the implementation of the information security awareness and training program must also undergo refresher training.

There are three major constituencies that influence security effectiveness,[33] namely end-users, line managers (IT managers) and top management. The training of employees and that of top management differs (see Table 1). When training and educating employees guard against making security breaches and incidents seem inviting and challenging. Furthermore, adopt a need-to-know philosophy, also referred to as the principal of least privilege. Thereby only telling them what they need to know in order to perform their duties effectively and efficiently. Do not educate employees on how to hack or break into systems, because they may view this as an invitation. It is recommended that reference to websites that supply hacking tools and tips should be omitted. Deter them by explaining the dire consequences that will ensue if they violate any of the security policies or procedures.

To gain a better understanding of what influences each of these constituencies it is recommended that a (SWOT) strength, weaknesses, opportunities and threats analysis is performed:[34]

(a) Strengths: In what way do they think well of information security?

(b) Weaknesses: In what way do they think poorly of information security?

(c) Opportunities: What are the best opportunities for information security? and

(d) Threats: What issues could undermine information security?

(v) STEP 5: Message creation - obtain certainty regarding the message the company wants to convey to their target audience. This step will entail obtaining clarity regarding the objectives of the information security awareness and training program.

The content of the awareness and training program will differ depending on the target audience. “Not everyone needs the same degree or type of information security awareness to their jobs.”[35] An awareness program that distinguishes between groups of people, and presents only information that is relevant to that audience and their job description will have the best results. Consequently segmentation must take place.[36] This would imply segmenting the audience by, for instance (a) level of awareness; (b) job category; (c) specific job function; (d) information processing knowledge; and (e) technology, systems, or applications used.[37]

Course curriculum of the information security awareness and training program will address the following issues: (i) identify and explain the threats facing the company; (ii) security monitoring program; (iii) security policy; (iv) information classification and handling;[38] (v) user ID and password requirements; (vi) virus

scanning and reporting; (vii) social engineering; (viii) software license; (ix) Internet and e-mail use; (x) use of encryption[39] ect.

(vi) STEP 6: Evaluate and consider communication tools available to get the security message across. Launch an investigation into current training trends. The style and method of training will depend on the nature of the company. The following tools may be used to get the information security message across:[40]outside speakers; videos[41] and multimedia presentations; company and departmental newsletters with information such as, who the security team is, what their mission is, references to developments or amendments in security policy and/or programs; contests and drawings; create an online information security awareness and training test/quiz;[42] screensavers; information security web site; security brochures and magnets; banner page showing the information security tip of the day; posters, cups, calendars, key chains (reminders); distribution of security alerts; ect.

(vii) STEP 7: Follow-through with program. An information security awareness programs is often developed and implemented with a certain degree of enthusiasm, unfortunately once the implementation process is complete, the enthusiasm fades away.[43] It must however be realised that information security awareness and training is a continuous process with no end destination in sight. It is therefore essential to develop ways in which to keep the program "alive and growing." In order for the awareness campaign to be successful its message must be communicated repeatedly.[44] Therefore, three critical success factors of the program are: (a) "tell them what you are going to say; (b) say it; and (c) remind them of what you have said."[45]

Analogous to other programs operating within the company the awareness and training program must be monitored and evaluated[46] on a regular basis. When performing an evaluation of the program consideration must be given to whether or not the original objectives and goals of the security awareness program have been achieved. By evaluating effectiveness of the awareness and training program the following will be measured:

(a) "The extend that conditions were right for learning and the learner's subjective satisfaction;

(b) what a given student has learned from a specific course;

(c) a pattern of student outcomes following a specific course; and

(d) the value of the class compared to other options in the context of an organisation's overall [information] security training program."[47]

Table 1[48]

CONSTITUENCIES	*TOP MANAGEMENT*	*LINE MANAGEMENT*	*END-USERS*
Focus Group	*"Expect a sound rational approach to information security. Interested in the overall cost implementation the policies and procedures and how this program stacks up against others in the industry."*	*Focused on getting their job done. Will not be interested in anything that will slow them down. To win them over show how controls will improve their job performance.*	*Will encounter some reluctance. "Identify what is expected of them and how it will assist them in gaining access to information and systems they need to complete their tasks. Point out that by protecting access to information they can have reasonable level of assurance that their information assets will be protected from unauthorised access, modification, disclosure or destruction.*
Style	*Professional and intellectual, but never threatening.*	*Informative, collegial and receptive*	*Can include elements of seriousness and fear, but also fun and concern*
Schedule	*At least on a quarterly basis.*	*Monthly, no less*	*Annual updates*
Best technique	*Cost justification;* *Industry comparison;* *Audit report; and* *Risk analysis*	*Demonstrate job performance benefits, and* *Perform security reviews*	*Sign responsibility statements; and* *Policies and procedure*
Best approach	*Presentation;* *One-on-one session;* *Video; and* *Violation reports*	*Presentation;* *Circulate news articles;* *Videos; and* *Rely on existing; and communication vehicles*	*Presentation;* *Newsletters;* *Video or live presentations; and* *Policy booklets and posters*
Expected result	*Funding and support*	*Support*	*Adherence and support*

5 IMPEDEMENTS TO THE AWARENESS AND TRAINING PROGRAM

The responsibility for information security resides in two entities, namely the board of directors and top management. The board is accountable to the owners of the company. The board will furthermore be held accountable for information security, regardless of their knowledge or lack thereof on the subject-matter. Consequently within the board the ultimate responsibility for information security reside. Therefore they need to be involved in and committed to information security if they wish to escape liability. Top management is in turn answerable to the board on this subject-matter. However, information security practitioners are generally astounded at director's and top management's perception of, and attitude towards, information security awareness and training programs.[49] Moreover, they find it difficult to understand why these entities are grappling with the question why the need for such a program exist in the first place. For information security practitioners the answer to this question is self-evident, unfortunately this answer still often evades top management.

The reluctance and apprehension with which this subject-matter is approached manifests itself in various ways, ranging from inadequate resources allocation to a general lack of follow-through and commitment to information security efforts. Other inhibitors that will be encountered when wanting to develop and implement an awareness and training program include:

(i) In most companies "security is implemented as an afterthought". This results in: (a) employees having to overcome the bad habits they have already learnt, and (b) employees having to be educated on how and why information security is of such crucial importance;[50]

(ii) Information security is still viewed as an IT problem. Therefore the need exist to tie information security to every employee's job;[51]

(iii) Awareness and training programs imitate the programs of competitors, or companies in a similar fields. The program must however be tailor-made for the company it is going to be used in;[52]

(iv) Care should be taken not to over educate the audience;[53]

(v) After development and implementation of the awareness and training program it must be maintained;[54]

(vi) Most employees still view information security as an inhibitor of performance and productivity. Therefore security and productivity must have equal force within the company resulting in a sustainable, workable equilibrium. "Where information security programmes overextend themselves they become burdensome and impede the productivity of the user community."[55]

6 THE LEGAL COST OF UNTRAINED AND UNEDUCTAED PERSONNEL

As should be evident from the above the development and implementation of an information security awareness and training program is a complicated, time-consuming endeavor which is neither straightforward, nor inexpensive. However, at present it is expected of all companies to have an effective information security awareness and training program in place. From a legal perspective the importance of this program is two-fold:

(i) Firstly, it is expected of all companies to take reasonable steps to secure their information assets, resources and systems prior to an attack. If the company fails to do this and an information security incident or breach occurs resulting in damages or losses for the company or a third party, the company as well as those people

responsible for the governance of the company (directors and top management) may be held liable in civil law for failed or inadequate information security. Liability may arise form the following sources:

a. Common law - The common law places the primary role players, and specifically the board of directors, under a fiduciary duty of care and skill. This duty is the most prevalent within the information security domain, as this would be the ground on which a stakeholder will be able to hold a director personally liable should information security fail. Within the information security domain this duty would require of the board to take reasonable steps to secure the information assets of the organisation.

b. Statutory and regulatory obligations - The newly-enacted Electronic Communications and Transaction Act 25 of 2002 contains specific provisions pertaining to technical information security. The King II report places the ultimate responsibility for information security firmly in the hands of the board of directors. Although the board is allowed to delegate certain activities associated with the development and implementation of information security within the organisation to designated employees, they are not allowed to abdicate their responsibility therefore. Furthermore, the JSE New Listing Requirements require of all listed companies to disclose the extend to which they comply with King II, and for the first time ever makes provision for directors to be held jointly and severally liable for failure to comply with the listing requirements, therefore with King II. A director that contravenes this provision may face a penalty of R1 000 000.

c. Contractual obligations;

d. Self-imposed obligations; and

e. International legislation will also impact on information security - Because of the fact that cyberspace is a borderless, faceless environment, organisations who wish to do business in this realm will have to give due consideration to internationally accepted standards, regulations and best practices concerning information security. If they fail to do so organisations might find themselves in a situation where a country refuses to do business with them because they have inadequate information security practices and/or procedures in place. Organisations will therefore have to investigate, consider, and in certain instances comply with the following: Organisation for Economic Co-operation and Development (OECD) security guidelines; European Union (EU) security directives; information security standards and best practices (ISO 17799 and COBIT); and enacted information security legislation and regulations of the specific country with which they want to do business.

(ii) Secondly, if an employee of the company uses the corporate information assets, resources or systems in an inappropriate manner that contravenes an information security policy, procedure, standard or guideline, the first question that a court will ask is whether or not the employee was aware of the specific policy, procedure, standard or guideline. Therefore, what efforts were made to bring this information security document under the attention of the employee, and furthermore, were attempts made to educate him/her on the contents thereof. It is not enough that the employee knows about the existence of the information security document, he/she must be educated on the contents thereof as well. The absence of an effective awareness and training program could therefore be highly problematic for a company who wishes to take disciplinary steps against an employee who has

transgressed an information security document. The employee would be able to raise as a defense the fact that he was unaware of the existence or contents of such documentation.

A popular method used in practice to exploit untrained and uneducated personnel is social engineering.

Social engineering may be defined[56] as "successful or unsuccessful attempts to influence a person(s) into either revealing information or acting in a manner that would result in unauthorized access, unauthorized use, or unauthorized disclosure, to an information system, network or data."[57] The success rate of social engineering is alarmingly.[58] Even more disturbing is the fact that social engineering bypass cryptography, computer security, network security and all other technological defenses. Security is therefore defeated without ever making use of technical means. Often companies forget that computers and technology are merely tools used by human beings. The problem with these tools are that humans must use, configure, install and implementing them.[59] Social engineering therefore exploits the weakest link in any company - its own employees.[60] If a successful social engineering attack takes place a company or third party who suffers damages and/or losses as a result of the attack may approach the court for relief. A key conceptual question which the court will ask is whether the company (including those entities responsible for the governance of the company) took reasonable steps to secure the information assets, resources and systems of the company.

7 CONCLUSION

It should be evident from the above that it is expected of a diligent company director to ensure that the company takes reasonable steps to protect its information assets, resources and systems prior to an incident or breach occurring. Included in the concept of "reasonable steps" would be the development and implementation of an effective information security awareness and training program. If a company does not have an effective information security awareness and training program in place the board of directors will have breached their fiduciary duty of care and skill and the company will be liable in civil law on the basis of negligent information security.

Traditionally information security was viewed by top management as a necessary evil. With the advent of the information age management is beginning to realise that information security is a business enabler, rather than a business inhibitor. It is therefore important that any information security program should first review the business objectives of the company and ensure that these goals are being met.

8 REFERENCES

[1] Desmand Building an Information Security Awareness Program (2002) 101.
[2] Tudor Information Security Architecture (2001) 147.
[3] Russell "Security awareness – implementing an effective strategy" (last visited 31 March 2003) http:// www.sans. org/rr/aware.php 3.
[4] Tudor Information Security Architecture (2001) 147.
[5] Tudor Information Security Architecture (2001) 147.
[6] Russell "Security awareness – implementing an effective strategy" (last visited 31 March 2003) http:// www.sans. org/rr/aware.php 3.
[7] Memory "Security awareness – everybody's business" (last visited 31 March 2003) http://www.sans. org/rr/start/ everyone.php 1.
[8] Desmand Building an Information Security Awareness Program (2002) 319.
[9] Tudor Information Security Architecture (2001) 139.
[10] Tudor Information Security Architecture (2001) 139.
[11] Tudor Information Security Architecture (2001) 140.
[12] Tudor Information Security Architecture (2001) 140.
[13] Corporate culture may be defined as the beliefs and values shared by people in an organization, and is akin to the personality of the organization. It comprises of an omnipresent set of assumptions that is often difficult to fathom and that directs activities within the organization.
[14] Tudor Information Security Architecture (2001) 140.
[15] Desmand Building an Information Security Awareness Program (2002) xvi.
[16] Tudor Information Security Architecture (2001) 140.
[17] Tudor Information Security Architecture (2001) 142.
[18] Tudor Information Security Architecture (2001) 142.
[19] Tudor Information Security Architecture (2001) 142.
[20] Tudor Information Security Architecture (2001) 146.
[21] Desman Building an Information Security Awareness Program (2002) 10.
[22] Desman Building an Information Security Awareness Program (2002) 10.
[23] Tipton and Krause Information Security Management Handbook Vol 3 (2003) 318.
[24] Tipton and Krause Information Security Management Handbook Vol 3 (2003) 326.
[25] Voss "The ultimate defense of depth: security awareness in your company" (last visited 31 March 2003) http:// www.sans.org/rr/aware/utlimate.php 2.
[26] Russel "Security awareness – implementing an effective strategy" (last visited 31 March 2003) http://www.sans.org/rr/aware.php 6.
[27] Russel "Security awareness – implementing an effective strategy" (last visited 31 March 2003) http://www.sans.org/rr/aware.php 6.
[28] Tudor Information Security Architecture (2001) 147.
[29] Tudor Information Security Architecture (2001) 149.
[30] Russel "Security awareness – implementing an effective strategy" (last visited 31 March 2003) http://www.sans.org/rr/aware.php 5.
[31] Tipton and Kraus Information Security Management Handbook Vol 1 (2000) 201.
[32] Hall "Selling security to management" (last visited 31 March 2003) http://www.sans.org /rr/aware/selling_ sec.php 3.
[33] Tudor is of the opinion that the awareness and training program focuses on five different groups, namely system administrators ("participate in security technical training for the operating system, network, database, or application that he or she manages"); security liaisons; security officers ("need to focus on the information security architecture and its components and how these components are integrated into the security awareness and training program"); department management ("additional responsibility of ensuring all employees within its span of control understand and adhere to security policies and receive security awareness training" also responsible for information classification in their business unit.); and executive management ("must make decisions relating to information security awareness and training and will be responsible for the long-term financial commitment to the program") Tudor (n 3) 146-147; 153.
[34] Meta Group "Do not forget the marketing principles in your security program" (last visited 24 July 2002) http://www.cio.com 4.
[35] Russel "Security awareness – implementing an effective strategy" (last visited 31 March 2003) http://www.sans.org/rr/aware.php 9.
[36] Russel "Security awareness – implementing an effective strategy" (last visited 31 March 2003) http://www.sans.org/rr/aware.php 9.
[37] Russel "Security awareness – implementing an effective strategy" (last visited 31 March 2003) http://www.sans.org/rr/aware.php 9.

[38] Kaur "Introducing and education of information security policies to employees in my organisation" (last visited 31 Mach 2003) http://www.sans.org 2.

[39] Tudor Information Security Architecture (2001) 145.

[40] For more ideas on tools to get the information security message across visit http://awarenessmaterials.homestead.com/. Included in their suggestions are:

(i) First aid kids with the slogan: "It's healthy to protect your patience's information; it's healthy to protect your information."
(ii) Mirror with slogan "Look who is responsible for protecting your information."
(iii) Toothbrush with slogan: "Your password is like this toothbrush; use it regularly, change it often, and do not share it with anyone else.
(iv) "Badge holder retractable with slogan: "Think Security."
(v) Key-shaped magnet with slogan: "You are the key to good security."
Flashlight with slogan: "Keep the spotlight on information protection."

[41] Commonwealth films (www.commonwealthfilms.com) have a variety of information security videos available under the information and computer security section Kaur (n 760) 3.

[42] For more information on how to develop and implement such a test/quiz within your organisation visit http://www.sans.org/rr/aware/quiz.php.

[43] Tipton and Kraus Information Security Management Handbook Vol 1 (2000) 200.

[44] Tipton and Kraus Information Security Management Handbook Vol 1 (2000) 200.

[45] Tipton and Kraus Information Security Management Handbook Vol 1 (2000) 206.

[46] For examples of practical ways in which to evaluate the information security awareness and training program, consult Tipton and Krause 322 – 323.

[47] Tipton and Kraus Information Security Management Handbook Vol 3 (2002) 323.

[48] Tipton and Krause Information Security Management Handbook Vol 1 (2000) 208.

[49] Tipton and Krause Information Security Management Handbook Vol 2 (2001) 241.

[50] Russel "Security awareness – implementing an effective strategy" (last visited 31 March 2003) http://www.sans.org/rr/aware.php 3-4.

[51] Russel "Security awareness – implementing an effective strategy" (last visited 31 March 2003) http://www.sans.org/rr/aware.php 3-4.

[52] Russel "Security awareness – implementing an effective strategy" (last visited 31 March 2003) http://www.sans.org/rr/aware.php 3-4.

[53] Russel "Security awareness – implementing an effective strategy" (last visited 31 March 2003) http://www.sans.org/rr/aware.php 3-4.

[54] Russel "Security awareness – implementing an effective strategy" (last visited 31 March 2003) http://www.sans.org/rr/aware.php 3-4.

[55] Ludwig "Security awareness: preventing a lack of security consciousness" (last visited 31 March 2003) http://www. sans.org 2.

[56] The SANS Institute "SANS glossary of terms used in security and intrusion detection" (last visited 26 March 2004) http://www.sans.org/resources/glossary.php 23 defines social engineering as: "a euphemism for non-technical or low technology means – such as lies, impersonation, tricks, bribes, blackmail, and threats – used to attack information systems."

[57] Tipton and Krause (ed) Information Security Management Handbook Vol 3 (2003) 52.

[58] Social engineering is found extensively in all manner of viruses and Trojan horses. Harley, Slade and Gattiker Viruses Revealed (2001) 132.

[59] Tipton and Krause (ed) Information Security Management Handbook Vol 3 (2003) 51.

[60] Tipton and Krause (ed) Information Security Management Handbook Vol 3 (2003) 51.