# Chapter 1: Introduction

## 1.1. Problem Statement

The interconnection of the world and the smooth operation of communication and computing systems become vital as global networks expand. However, recurring events such as virus and worm attacks and the success of criminal attackers illustrate the weaknesses in current information technologies and the need for heightened security of these systems.

The immediate need for organizations to protect information assets continues to increase. To build your business, trust is absolutely essential—the trust of employees, customers, vendors, and investors. And to earn and maintain that trust, you must have the right information security measures in place.

Companies would like to believe that for every security problem they face, there is a technical product or suite of products that can solve it. Unfortunately, some problems are too subtle and entirely too complicated to be solved through a technical approach. [30]

Any computer system today is being used, maintained and supported by people. People never do what the designers of these system expect. Humans are inquisitive and inventive, yet lazy and ignorant. The can be malicious and nearly all of them are incompetent outside their particular area of skill. Humans also like to fiddle and play, leading to computer systems that seem bound to fail. [30]

> "Security is a chain; it's only as secure as the weakest link."[22]

All it takes is just ONE weak link in the chain for an attacker to gain a foothold into your network. [23] Because human beings are usually considered to be the weakest link in the security chain, implementing a security awareness-training program for your computer users is a must. A company's information system can not be secured properly unless the computer users have been properly trained in security awareness according to their job functions. "The statement that 'security is everyone's responsibility' is absolutely true." [23]

The documented increase in attacks on trade secrets, intellectual property, and customer data makes it imperative for corporations, government agencies, and the military to increase employee awareness of information security policies and procedures.

The problem statement therefore is that, according to the above discussion, it is becoming essential for organizations to have a general security awareness program in place, of which a web-based information security awareness program is one component.

## 1.2. The objectives of the project and dissertation

There are two primary objectives that this project will attempt to achieve:

- To develop an effective information security awareness program that can be implemented within an organization. This will include a web-based security awareness program that will form part of a bigger and more comprehensive security awareness program. Other mechanisms and their effectiveness in a security awareness program will also be discussed. One of the main objectives of an awareness program is to change the employees' attitude towards information security. A change in attitude will then lead to a change in behaviour that will make the employee more security aware or conscious.
- To study the area of social psychology and human performance systems with a view to identify the principles and techniques that was developed over many years of research into the modification of

people's behaviour, and to identify where these techniques and principles can potentially be incorporated into the awareness program so that it can become more effective. This knowledge should be incorporated into the total security awareness program, since the primary objective is to change the employees' attitude and behaviour to be more supportive of information security.

## 1.3. The approach and research

The project starts with a literature study. This focuses on the requirements for an information security awareness program, research that has already been done in this area and behavioural issues that need to be considered during the implementation of such a program. A secondary deliverable of this project is to develop a web-based security awareness program that can be used to make employees more security aware and that should compliment a total security awareness program within an organization.

The web-based security awareness program should be tested to ensure usability. This will only be a prototype and can be adapted to the organization's unique needs and look and feel. This testing could take place in the form of implementation in an organization and/or evaluation to ensure that all stated objectives have been achieved.

## 1.4. The overall structure of the dissertation

The project is documented through a set of chapters. A graphical representation or roadmap on how the chapters fit into the dissertation is depicted in figure 1.

The web-based security awareness program that was developed as part of this study can be found on the disk labelled "Information Security Awareness Program" at the RAU Standard Bank Academy for Information Technology.

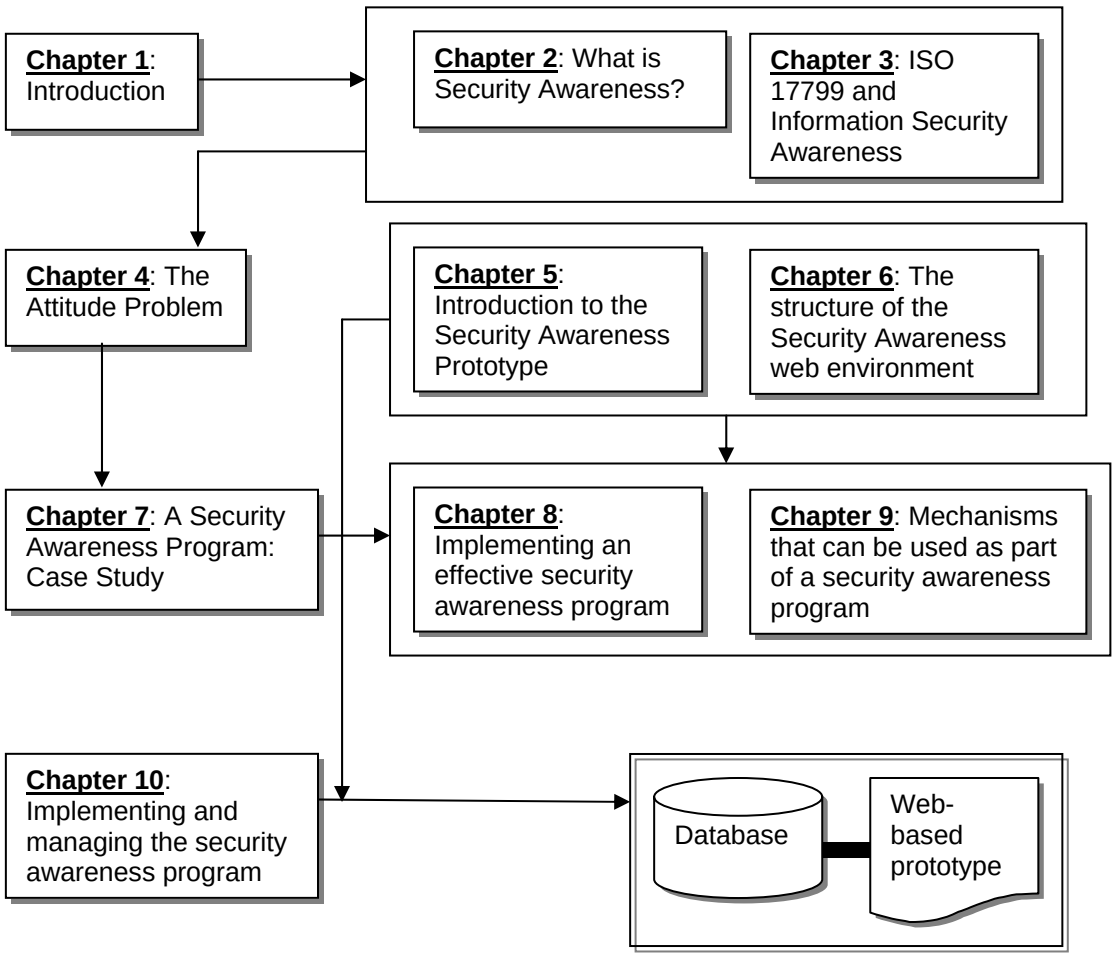



**Figure 1: A graphical representation or roadmap of the chapters**

It was a deliberate decision to write this dissertation in the first person.

# Chapter 2: What is Security Awareness?

## 2.1. Introduction

It is important to understand what security awareness is and to understand what the different components are that information security consists of.

Information security is the protection of information and the systems that use, store, and transmit that information. [29] But, to protect the information and its related systems from danger, such tools as policy, awareness, training and education, and technology are necessary.

What exactly does security awareness mean? Based on the definition from National Institute of Standards and Technology: "Awareness, Training and Education Controls include awareness programs which set the stage for training by changing organisational attitudes to realise the importance of security and the adverse consequences of its failure, training which teaches people the skills that will enable them to perform their jobs more effectively, and education which is targeted for IT security professionals and focuses on developing the ability and vision to perform complex, multi-disciplinary activities." [24]

To understand why security awareness is necessary, we need to start by having a look at the basic security problems. Basic problems with respect to security can occur in any of the following critical characteristics of information [2]:

- *Authenticity:* Establishment of the identity of the user and delivery of the right set of credentials to the user (e.g. logging into your internet home

banking set-up). Authenticity of information is the quality or state of being genuine or original, rather than a reproduction or fabrication. Information is authentic when it is the information that was originally created, placed, stored, or transferred.

- *Authorisation:* Activities the user or system can perform based on its credentials (e.g. some users can transfer up to different amounts)
- *Confidentiality:* Protection of the data exchange channel so that it becomes immune to eavesdropping (e.g. if you check your balance, this should be encrypted so that it is confidential). The confidentiality of information is the quality or state of preventing disclosure or exposure to unauthorized individuals or systems. Confidentiality of information is ensuring that only those with the rights and privileges to access a particular set of information are able to do so, and that those who are not authorized are prevented from obtaining access. When unauthorized individuals or systems can view information, confidentiality is breached.
- *Integrity:* Protection of the data channel so the exchanged messages cannot be modified (e.g. if you transfer money, the amount should be unchangeable in transit). The quality or state of being whole, complete, and uncorrupted is the integrity of information. The integrity of information is threatened when the information is exposed to corruption, damage, destruction, or other disruption of its authentic state.
- *Non-repudiation & Audit:* Establishment of proof of the performed activities (e.g. like signing a paper copy of an order)
- *Availability:* Offering business critical services warrants full-time availability. Availability enables users who need to access information to do so without interference of obstruction, and to receive it in the required format. A user in this case, means not only a person, but also another computer system.

These critical characteristics of information must be protected, and users must be made aware of the factors that can compromise the digital assets within their organization and how they can prevent it.

This is why It is also important to understand how security awareness fits into the bigger picture of the learning continuum. This is indicated in figure 2.

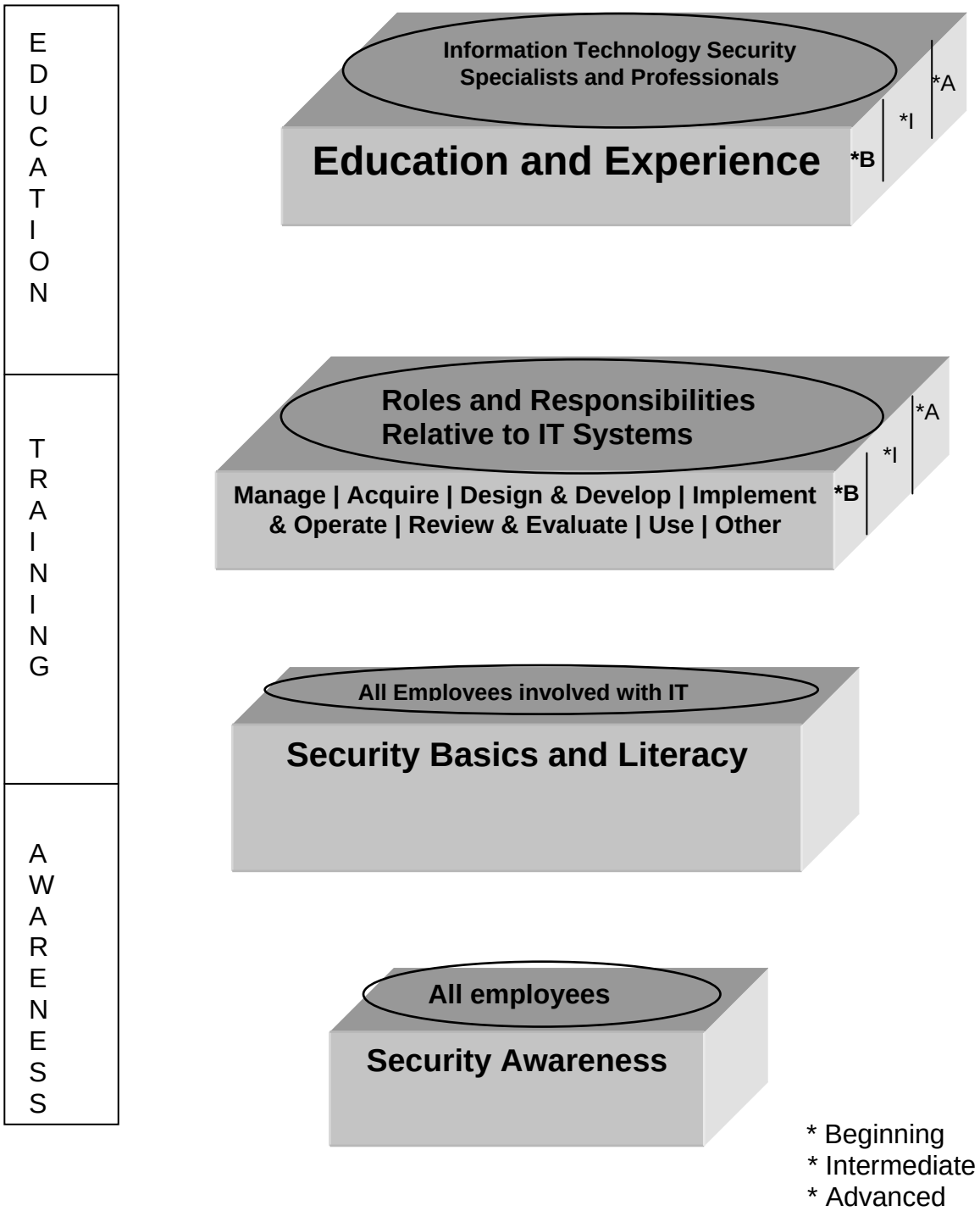



**Figure 2: Security Awareness in the learning continuum [26]**

There are three levels of learning in the learning continuum as depicted in figure 2: Awareness, Training and Education.

Awareness is targeted for all employees. Employees need to be made aware of the factors that can compromise the digital assets within their organization and how they can prevent it.

Training is targeted for all employees involved with IT. This takes awareness one step further and introduce security basics and literacy to these employees. This is important to all employees involved in IT as they are the people that work with the organizations digital assets on an ongoing basis. Training is also given to the persons responsible to manage, design and develop, implement and operate, and support the IT systems within your organizations to ensure that the systems are as safe as possible from possible attacks by cyber criminals. Training can be presented on a beginner, intermediate and advanced level.

Education takes training one step further and is targeted at Information Technology Security Specialists and Professionals. These people are the experts in Information Security and ultimately responsible for ensuring that the organization's digital assets are safe. They play an important role in helping to make sure that the proper awareness and training programs with regards to Information Security are in place in the organization. Education can be presented on a beginner, intermediate and advanced level.

The focus of this dissertation will be on awareness and the overlap into the training level in the learning continuum.

In this chapter the concept of security awareness will be explained. In paragraph 2.2, I will explain which components of an information system need to be secured. In paragraph 2.3, I will explain why it is important to implement a security awareness environment in your organisation. The difference between awareness and training will be highlighted in paragraph 2.4. Finally,

in paragraph 2.5, I will explain how the concept of threats, assets, countermeasures and responsibility fits into the security awareness picture.

## 2.2. Components of an Information System that need to be secured

As explained in paragraph 2.1, information security is protecting information and the systems that store, process, and transmit it. But, what are the components that an Information System consists of?

An Information System is much more than just computer hardware; it is the entire set of software, hardware, people, and procedures necessary to use information as a resource in the organization. [28: 15] Below are the five critical components that enable information to be input, processed, output, and stored. Each of these five components of the Information System has its own strengths and weaknesses, characteristics and uses, and security requirements:[28: 15]

*Software:* Software is the first major component of an Information System. This component comprises applications, operating systems, and assorted command utilities. Due to holes, bugs, weaknesses, or other fundamental problems in software, exploiting errors in software programming results in a substantial portion of the attacks on information.

*Hardware:* Hardware is the physical technology that houses and executes the software, stores and carries the data, and provides interfaces for the entry and removal of information from the system. Physical security policies deal with hardware as a physical asset and with the protection of these physical assets from harm or theft.

*Data:* Data that are stored, processed, and transmitted through a computer system must be protected. Data is usually the main object of intentional attacks.

*People:* People can be your weakest link when it comes to information security. They may not intend to be, but, unless policy, education and training, awareness, and technology are properly employed to prevent them from accidentally or intentionally allowing damage or loss of information, they are the weakest link. Social engineering can be used to manipulate the actions of people to obtain access information about a system.

*Procedures:* Procedures are written instructions for accomplishing a specific task. A threat to the integrity of information is posed if an unauthorized user obtains an organization's procedures.

As mentioned in paragraph 2.1, authenticity, authorization, confidentiality, integrity, non-repudiation and availability, are the critical characteristics of information. These characteristics need to be applied to all the components of an information system, i.e. software, hardware, data, people, and procedures in order to prevent any problems that might occur with respect to security.

Thus, security of information and its systems entails securing all components and protecting them from potential misuse and abuse by unauthorized users. The necessity for users to be security aware will be discussed in the next paragraph.

## 2.3. Why is security awareness necessary?

Security awareness is more than just a corporate buzzword. It is a philosophy and understanding that should be woven into the way your organization functions.

In today's environment with so much information being stored and shared electronically, keeping your organization's information secure is becoming a tremendous challenge.

Even with technology professionals dedicated to securing and monitoring your systems, your information is vulnerable if all your employees are not security-conscious. [6]

Making computer system users aware of their security responsibility and teaching them correct practices help users change their behaviour. Users cannot follow policies they do not know about or understand. Training also supports individual accountability, which is one of the most important ways to improve information security. Without knowing the necessary security measures and how to use them, users cannot be truly accountable for their actions. [7]

By providing your staff with knowledge of basic security practices, your organization [8]:

- Demonstrates its commitment to security.
- Illustrates the importance of its information.
- Provides a more secure environment.
- Encourages an even higher level of concern for security.
- Helps to maintain client trust and confidence.

There are numerous controls that IT professionals can implement to safeguard electronic information from unauthorised users. (See paragraph 2.5) These controls can only be efficient to a certain extent. It is the authorised end users that possess the Ids and passwords to access that data giving them the ability to print it, share it, alter it or delete it. If they are careless with or choose weak passwords, casually discard confidential printed reports in the trash, prop open doors to secured areas, fail to scan new files for viruses, or leave back-ups of data unsecured, then that information remains at risk. [5]

## 2.4. Security Awareness vs. Training vs. Education

Reading the previous paragraph it should be obvious that organizations need to have some sort of information security awareness program in place in order to ensure that the end users understand the importance of securing the information they work with on a daily basis.

Security Awareness programs set the stage for training by changing organisational attitudes to realise the importance of security and the adverse consequences of its failure and remind users of the procedures to be followed. [9]

Awareness is not training. [9] The purpose of awareness presentations is simply to focus attention on security. Awareness presentations are intended to allow individuals to recognise IT security concerns and respond accordingly. In awareness activities the learner is a recipient of information, whereas the learner in a training environment has a more active role. Awareness relies on reaching broad audiences with attractive packaging techniques. Training is more formal, having a goal of building knowledge skills to facilitate job performance. [9]

Awareness is used to reinforce the fact that security supports the mission of the organisation by protecting valuable resources. If employees view security as just bothersome rules and procedures, they are more likely to ignore them. In addition, they may not make needed suggestions about improving security nor recognise and report security threats and vulnerabilities.[9]

Awareness also is used to remind people of basic security practices, such as logging off a computer system or locking doors. [9]

## 2.5. The assets-, threats-, countermeasures-, responsibility concept

Weaknesses in the design or the implementation of systems software or an application program, that typically allow unauthorised access to the system, interruption of services, or unintended exposure of information, are commonly known as vulnerabilities. [3]

The assets, threats, countermeasures, responsibility concept can be used to explain to computer users what information security is. The users will need to understand this before they start with a security awareness program. Alternatively, these concepts can be incorporated in the early stages of a security awareness program.

These concepts can be explained with a simple example:

All of us have a number of things that has value to us, called assets. An example of an **asset** is a television. (See figure 3)

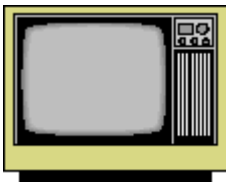


**Figure 3: A television: example of an asset**

As this asset has value to us, it is essential to protect it against **threats**. A threat is anything that can compromise the asset. Examples of threats may include:

- Theft
- Lightning
- Abuse, etc.

In order to protect the asset from the threats, you need to implement some **countermeasures**. Examples of such countermeasures are:

- Put locks on the doors of the house
- Install an alarm system
- Plug the television out when there is lightning
- Never hit the television or mess anything on it

It is the owner's responsibility to make sure that, where applicable, the relevant countermeasures are enforced.

Now, let us use a comparison to explain what information security awareness is.

Some of a company's most important **assets** are its information, the data from which this information is derived, and the computers, software systems and networks which are used to access, manipulate, process and transmit these information or electronic assets. (See figure 4)

**Figure 4: Company information or electronic assets**

**Threats** that may compromise the authenticity, authorization, confidentiality (privacy), integrity (correctness), non-repudiation (auditing) and availability of these assets include:

- Theft of information assets
- Unauthorised logons to computer systems
- Loading of malicious software on a computer, etc.

Examples of **countermeasures** include:

- User-ids and passwords to ensure that only authorised employees gain access to the system
- Regular backups to protect against lost information
- Virus control packages against virus infections

Every employee who is authorised to use these information assets has a **responsibility** to ensure that, where applicable, the relevant countermeasures are enforced.

**Information security awareness** is therefore all about executing your responsibility in ensuring that the relevant countermeasures are enforced when you use the company's information assets.

Examples of such awareness (responsibility) are:

- Never give your password to anybody, because then that person can get access to information assets to which he/she may not be authorised.
- Never load unauthorised software on your computer, either from the Internet or from a diskette. Such software may contain a virus and compromise the integrity of the company's information or electronic assets.

## 2.6. Summary

This chapter explained the fact that although there are numerous controls IT professionals can implement to safeguard electronic information from unauthorised users, these information can still be at risk because it is the authorised end users that possess the Ids and passwords to access that data giving them the ability to print it, share it, alter it or delete it. If they are careless with or choose weak passwords, casually discard confidential printed reports in the trash, prop open doors to secured areas, fail to scan new files

for viruses, or leave back-ups of data unsecured, then that information remains at risk. [5]

Having an ongoing security awareness program in place can greatly reduce these risks, many of which cannot be approached through technological or other automated methods. In these cases, it's the human element that must be addressed.

Information security can be aligned with the assets-, threats-, countermeasures- and responsibility concept to make it easier for users to understand and relate to.

Even if users can relate to security awareness because the assets-, threats-, countermeasures- and responsibility concept were explained to them, numerous problems can still exist. The biggest problem is people's attitude towards change. This important problem is addressed in the chapter 4.

Users must be aware of the company's policy with regards to security and the possible actions that can be taken if any digital assets are intentionally compromised by them. A security awareness and training program must also address all the necessary security-related factors and components that world best practices and standard bodies suggest. Chapter 3 will discuss security standards and best practises in more detail, specifically with regards to the ISO 17799 security standard.

# Chapter 3: ISO 17799 and Information Security Awareness

## 3.1. Introduction

Users must be aware of the company's policy with regards to security and the possible actions that can be taken if any digital assets are intentionally compromised by them. A security awareness and training program must also address all the necessary security-related factors and components that world best practices and standard bodies suggest.

This chapter will discuss what the ISO 17799 security standard says about security awareness in more detail. Paragraph 3.2 will explain the difference between a policy, standard and guideline. A brief description of the ISO 17799 document and its contents will be given in paragraph 3.3. Paragraphs 3.4 and 3.5 describe the importance of employee training and education with regards to security as described by the ISO 17799 and how the security awareness prototype that was developed as part of this study plays a role in achieving this.

## 3.2. Is it a Policy, a Standard or a Guideline?

We frequently hear people use the names "policy", "standard", and "guideline" to refer to documents that fall within the policy infrastructure. According to the SANS Institute:

- A Policy is typically a document that outlines specific requirements or rules that must be met. In the information security world, policies are usually point-specific, covering a single area. For example, an "Acceptable Use"

policy would cover the rules and regulations for appropriate use of the computing facilities within an organization.

- A standard is typically collections of system-specific or procedural-specific requirements that must be met by everyone. For example, you might have a standard that describes how to set up a Windows NT workstation for placement on an external (DMZ) network. People must follow this standard exactly if they wish to install a Windows NT workstation on an external network segment.
- A guideline is typically a collection of system specific or procedural specific "suggestions" for best practice. They are not requirements to be met, but are strongly recommended. Effective security policies make frequent references to standards and guidelines that exist within an organization. [31]

### 3.3. What is ISO 17799?

ISO 17799 is the most widely recognised security standard. It is comprehensive in its coverage of security issues and contains a substantial number of control requirements, some extremely complex. ISO 17799, is a detailed security standard and is organised into ten major sections, each covering a different topic or area. The ten sections are [32]:

- *Business Continuity Planning*: The objectives of this section are to counteract interruptions to business activities and to critical business processes from the effects of major failures or disasters.

- *System Access Control*: The objectives of this section are to control access to information, prevent unauthorized access to information systems, ensure the protection of networked services, prevent unauthorized computer access, detect unauthorized activities and to ensure information security when using mobile computing facilities.

- *System Development and Maintenance*: The objectives of this section are to ensure security is built into operational systems, prevent loss, modification or misuse of user data in application systems, protect the

confidentiality, authenticity and integrity of information, ensure IT projects and support activities are conducted in a secure manner and to maintain the security of application system software and data.

- *Physical and Environmental Security*: The objectives of this section are to prevent unauthorized access, damage and interference to business premises and information; to prevent loss, damage or compromise of assets and interruption to business activities and to prevent compromise or theft of information and information processing facilities.

- *Compliance*: The objectives of this section are to avoid breaches of any criminal or civil law, statutory, regulatory or contractual obligations and of any security requirements, ensure compliance of systems with organizational security policies and standards, maximize the effectiveness of and to minimize interference to and from the system audit process.

- *Personnel Security*: The objectives of this section are to reduce risks of human error, theft, fraud or misuse of facilities, ensure that users are aware of information security threats and concerns, and are equipped to support the corporate security policy in the course of their normal work, minimize the damage from security incidents and malfunctions and learn from such incidents.

- *Security Organization*: The objectives of this section are to manage information security within the Company, maintain the security of organizational information processing facilities and information assets accessed by third parties, maintain the security of information when the responsibility for information processing has been outsourced to another organization.

- *Computer & Network Management*: The objectives of this section are to ensure the correct and secure operation of information processing facilities, minimize the risk of systems failures, protect the integrity of software and information, maintain the integrity and availability of information processing and communication, ensure the safeguarding of information in networks and the protection of the supporting infrastructure, prevent damage to assets and interruptions to business activities and to

prevent loss, modification or misuse of information exchanged between organizations.

- *Asset Classification and Control*: The objectives of this section are to maintain appropriate protection of corporate assets and to ensure that information assets receive an appropriate level of protection.
- *Security Policy*: The objectives of this section are to provide management direction and support for information security.

### 3.4. ISO 17799 and Information Security Awareness

Research done by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) has shown that appropriate training and education are critical to the successful implementation of information security within an organization. [33: 11]

The objective of user training is to ensure that users are aware of information security threats and concerns, and are equipped to support the organizational security policy in the course of their normal work. Users should be trained in security procedures and the correct use of information processing facilities to minimize the possibility of security risks. [33:11]

According to the ISO 17799 all employees of the organization and third party users, should receive appropriate training and regular updates in organizational policies and procedures including security requirements, legal responsibilities and business controls. Before access is granted to information or services, training in the correct use of information processing facilities e.g. log-on procedure should be given. [33:11]

### 3.5. ISO 17799 controls and the Security Awareness Prototype

The objective of the security awareness prototype that was developed as part of this study is to serve as a mechanism that can be used to educate users on the basic security threats and to give them tips to prevent or deal with the threats in their normal working environment. A tool like this compliment the total security awareness program that should exist within an organization. The prototype is web-based and can also be used as an effective delivery mechanism to give the employees regular updates on the security policies, etc.

### 3.6. Summary

Good policies and procedures are not effective if they are not taught and reinforced to the employees. It is not enough to just publish the policies and expect employees to read and understand them. They need to be taught to emphasize their importance. Users must be aware of the company's policy with regards to security and the possible actions that can be taken if any digital assets are intentionally compromised by them. A security awareness and training program must also address all the necessary security-related factors and components that world best practices and standard bodies suggest.

This chapter focussed on what the ISO 17799 security standard says about security awareness. It also explained that the security awareness prototype that was developed as part of this study plays an important role in the overall security awareness program that should exist within an organization.

Having an ongoing security awareness program in place can greatly reduce the mentioned information security risks, many of which cannot be approached through technological or other automated methods. In these cases, it's the human element that must be addressed.

In order for a security awareness program to be effective, people's attitude or mindset towards change must be changed. Chapter 4 will focus on the attitude problem of people towards change and ways of overcoming this.

# Chapter 4: The Attitude problem

## 4.1. Introduction

As explained in chapter 2, having an ongoing security awareness program in place can greatly reduce the mentioned information security risks, many of which cannot be approached through technological or other automated methods. In these cases, it's the human element that must be addressed.

Even if users can relate to security awareness because the assets-, threats-, countermeasures- and responsibility concept were explained to them, numerous problems can still exist. The biggest problem is people's attitude towards change.

It is very usual to experience, especially during projects where new ideas and technology are introduced, that end users have tunnel vision when it comes to change. They are used to performing their duties a certain way and to be wary of certain problems that may occur. They do not want to change the way they are used to work and they do not want to worry about things they did not worry about before.

In order for a security awareness program to be effective, people's attitude or mindset towards change must be changed. An effective change management plan must be in place.

To develop a framework for awareness I adopted a model [26] to define behavioural and knowledge requirements. Figure 5 depicts this model.

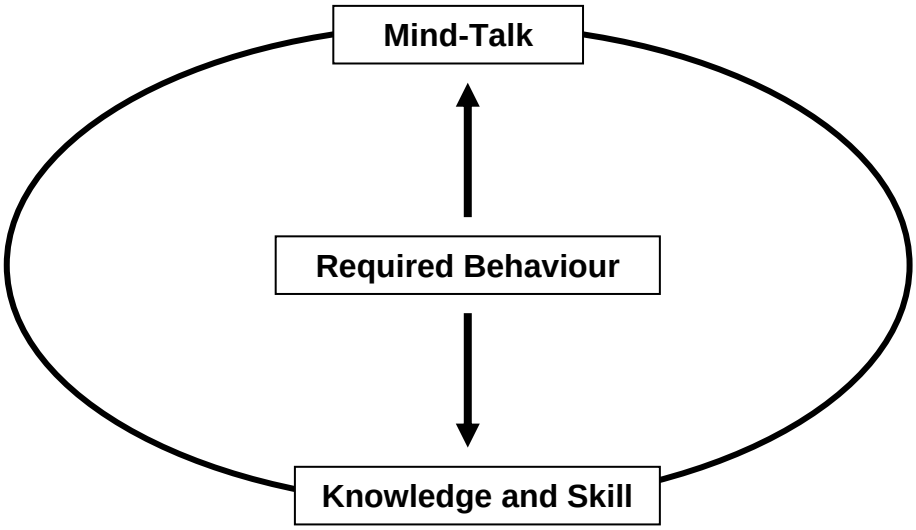



**Figure 5: Model that defines behavioural and knowledge requirements**

In order to ensure that a company achieves the desired behaviour and attitude towards information security, they need to focus on changing the mind-talk or attitude and establish the necessary skills. The bigger part of this document will focus on parts of this model and I will refer back to this model as needed.

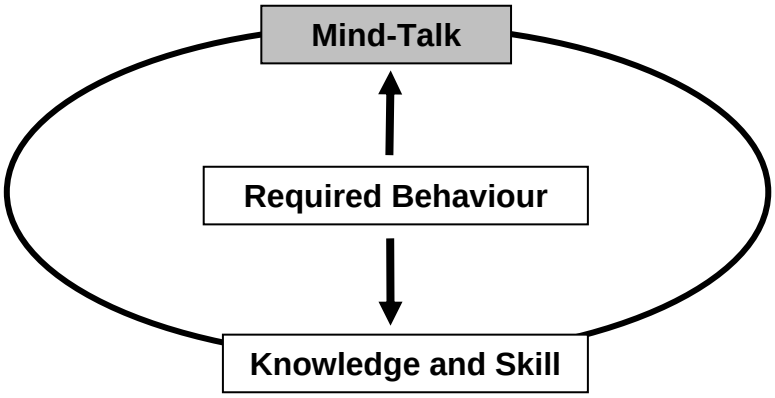
In this chapter I will discuss the attitude problem of people towards change and ways of overcoming this. In paragraph 4.2 and 4.3 I will give more detail on what I perceive as people's attitude towards security. This will be followed in paragraph 4.4 by an explanation on how these attitudes can be changed.

It is important to make sure that the people's attitude did change in order to make sure that the overall security awareness program in the organization is successful. Therefore, we need to measure the behavioural change. Some concepts regarding this will be mentioned in paragraph 4.5. In paragraph 4.6 I will explain how a security awareness program can be utilized to change the mind-talk or attitudes of users. For this I will introduce my security awareness program prototype. This prototype was built to demonstrate how a web-based program can assist an organization to achieve their security awareness goals

by complimenting all the other security awareness measures that might be implemented in an organization.

### 4.2. Mind-Talk or Attitude explained

This paragraph will focus on the Mind-Talk component of the model that was introduced in the previous paragraph:




The general mind-talk that is expected from an organisation's staff is crucial to establish the required level of security awareness. Some examples of expected and ideal mind-talk include: [26]

- "I will use business tools for business purposes and I understand that PC's, Internet and e-mail fall within such business tool definition."
- "I will ensure that information is only distributed to, or dealt with by the appropriate people within and outside the organisation."
- "I have a role to play in information security and will consciously act my entrusted information security role."
- "I will act on, and process information based on the required ability to differentiate and classify information."
- "I understand that information security is guided by policies and procedures, and I will be penalised for non-conformance."
- "I am aware of the serious risks and threats posed to information within my company."

- "I will ensure that access to information is disallowed from unauthorised individuals and institutions."

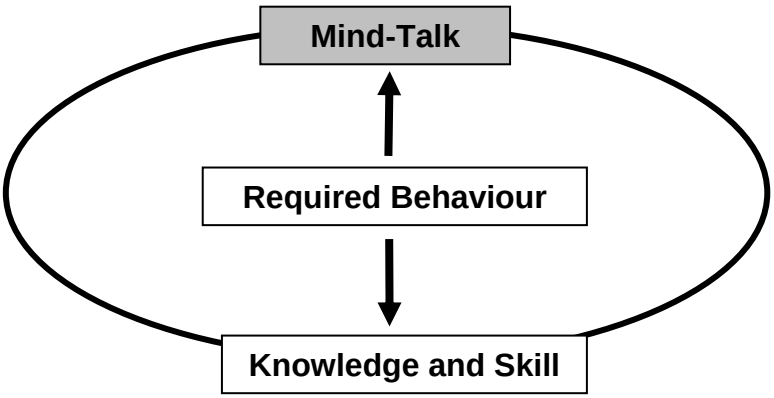
The organisation's staff must have a proper attitude or mind-talk towards security to ensure that they will behave accordingly. The required behaviour that is expected from every employee includes the following:

- A user will comply to the security awareness policy and the procedures it consists of
- A user will comply to the password policy and will practice safe Internet and e-mail usage
- A user will report an incident that he suspects can compromise computer security

Once a user's behaviour is adequate and in place then he/she has the necessary knowledge and skills to play an effective part in a security awareness program.

### 4.3. People's attitude towards security

Once again, this paragraph will explain concepts relating to the mind-talk concept introduced in the model in figure 5:

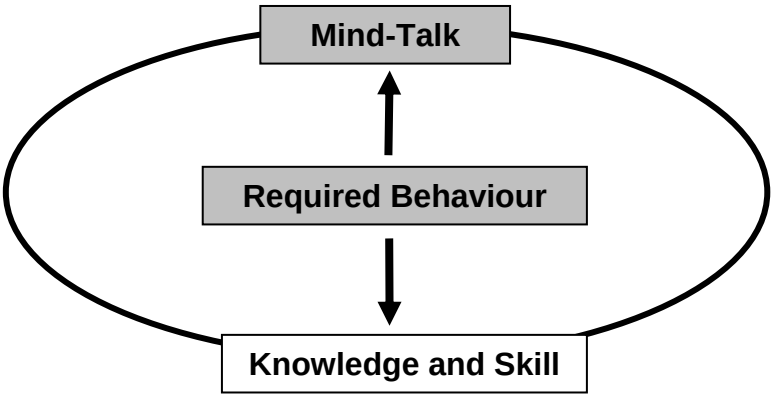


To establish the expected mind-talk as described in paragraph 4.2 a company should get rid of undesired norms and build the desired norms. Table 1 explains what the "mind-talk" and its associated desired and undesired norms are. [26]

| "Mind-talk" | Desired norm | Undesired norm |
|---|---|---|
| Ability to differentiate and classify information | Recognise sensitive information. Demonstrate an understanding of the different classes of information. | Information is information. |
| Use business tools for business purposes | Applying information to create business value. Using information tools to gain business information | Using business tool for private uses e.g. e-mail. Using business tools to gain access to undesired information (porn, etc.) |
| Information is distributed to, or dealt with by appropriate people | Demonstrate understanding of information "workflow". Information is distributed to authorised users only. | Information is distributed to the wrong people. Free access for all to all information. |
| Unauthorised access to information is disallowed | Sensitive information is appropriately stored and handled. | Give people access to log-in codes. "Selling" information for personal gains. |
| Penalised for not conforming to policies. | Aware of disciplinary actions. Equip myself to support organisational policy. Sound understanding of importance of policy. | No penalties, so I can do what I want. Policies are not applicable to me, and I really don't care. |
| Awareness of information risks and threats. | Understand threats and have ability to evaluate them. | No threat to my company. Our information is of little value and need not be guarded. |
| Act entrusted information security role. | Demonstrate understanding of roles. | Abdicate information security responsibility. It is somebody else's problem. |

**Table 1: The "mind-talk" and associated desired norms and undesired norms.**

### 4.4. How to change people's attitudes




In order to overcome the challenge of changing people's attitudes or mind-talk and behaviour from the undesired norm to the desired norm (refer to Table 1), the awareness program should first and foremost assist with a culture transition. This means that the organisation should move from the undesired norms to the desired norms.

Figure 6 shows some examples of these necessary transitions. [26]

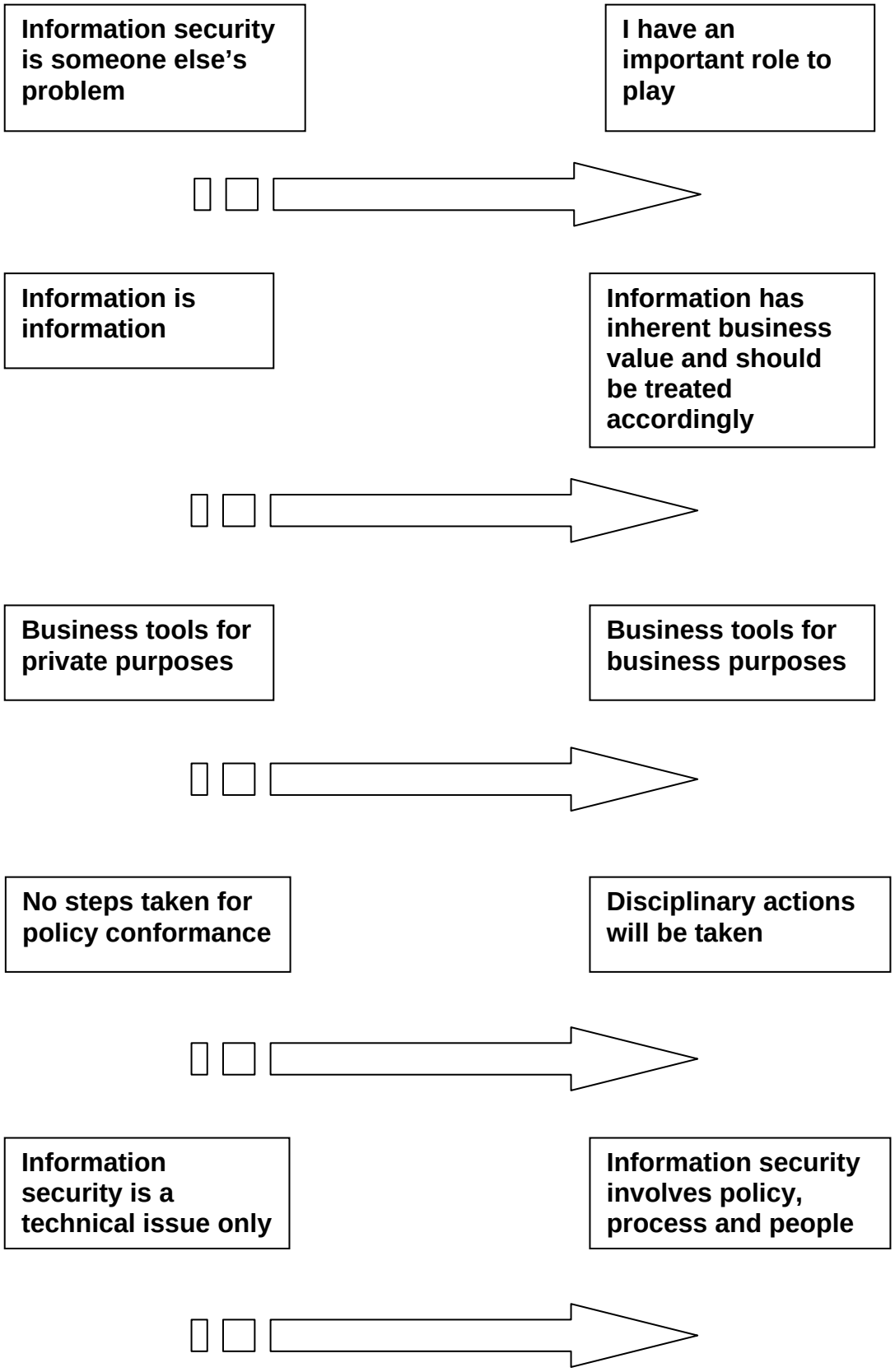



**Figure 6: The culture transition**

In order to establish these basics to achieve the transition, an integrated communication and awareness strategy is the best solution.

Such an integrated communication strategy should focus on three levels, with an immediate and future focus. (Figure 7) [26]

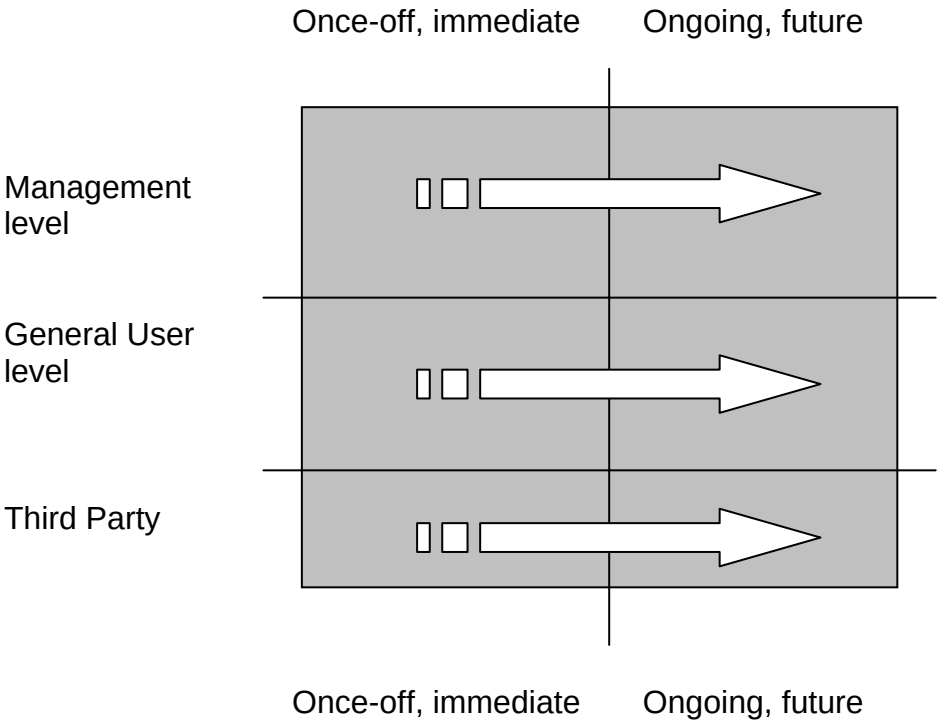



**Figure 7: Three levels of an integrated communication strategy.**

There are key content elements for each of the quadrants that should come across to the audience. [26] These key content elements are depicted in figure 8.

| | Once-off, immediate | Ongoing, future |
|---|---|---|
| **Management level** | ▪ Establish information security as an imperative<br>▪ Creating urgency and legal/governance implications<br>▪ Clarifying key roles and responsibilities<br>▪ Explaining key policies and procedures | ▪ Status/progress on initiatives<br>▪ Overall performance on measures and targets<br>▪ Keep all informed of security responsibilities<br>▪ Manage the risks<br>▪ Incident reports and management<br>▪ Status of security awareness<br>▪ New or changes in policies |
| **General User level** | ▪ Value of information<br>▪ Importance to the organisation<br>▪ Role of the individual and responsibilities<br>▪ Desired behaviours<br>▪ Demonstrate that management deals with security in a professional way | ▪ Specific themes<br>▪ Maintaining motivation<br>▪ Sharing general information of importance |
| **Third party** | ▪ Role of the third party<br>▪ Relevant controls<br>▪ Contractual arrangements<br>▪ Access management | ▪ Changes in mechanisms on contracts<br>▪ Relevant incident reports<br>▪ Access monitoring |
| | **Once-off, immediate** | **Ongoing, future** |

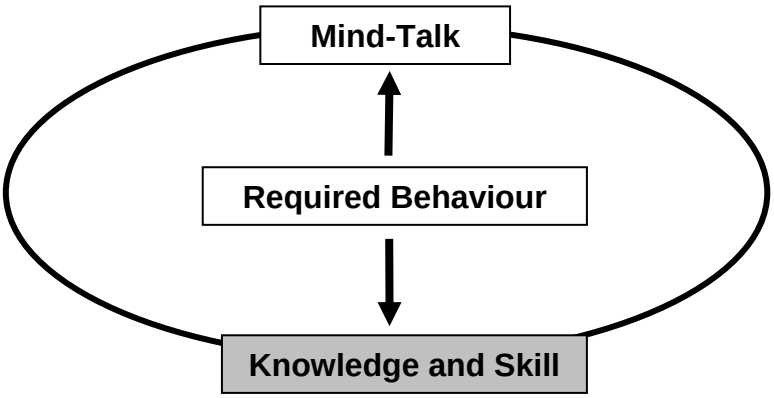
**Figure 8: Key content elements [26]**

There will be different communication channels for each of the quadrants to bring across the respective messages. (See figure 9)

| | Once-off, immediate | Ongoing, future |
|---|---|---|
| **Management level** | ▪ Face-to-face discussions and presentations<br>▪ Special executive Management sessions<br>▪ Mostly targeted through management committees and forums<br>▪ Content developed centrally to ensure consistent messages<br>▪ Executive decentralised by line groups | ▪ Quarterly newsletter<br>▪ Core of newsletter will be centrally developed<br>▪ Additions, customisation and distribution done decentralised<br>▪ Standing item on key meetings |
| **General User level** | ▪ Mostly automated communication as the medium<br>▪ Total user base as audience<br>▪ Targeted through e-mail, intranet, posters, screen savers, company television and company newsletters<br>▪ Content development done centrally<br>▪ Execution co-ordinated via Corporate communications | ▪ General user base as audience<br>▪ Intranet site regularly updated with specific themes (monthly)<br>▪ Retain presence in company newsletters (as and when)<br>▪ E-mail on general issues of interest and importance (as and when, not more than x2 a month)<br>▪ Centrally developed and maintained |
| **Third party** | ▪ Formal memorandum with discussion session<br>▪ Senior management level<br>▪ Third party to further communicate with their organisations | ▪ Formal memorandum with discussion session<br>▪ Senior management level<br>▪ Third party to further communicate with their organisations |
| | **Once-off, immediate** | **Ongoing, future** |

**Figure 9: Communication channels**

Apart from the correct mind-talk or attitude, it is as important to establish the right level of knowledge and skill:




Building knowledge and skill does not refer to establishing deep skills in information security, but rather an overall ability across the organisation. The only effective means to establish the required level of knowledge and skill is through well-structured training. [26]

Examples of generic training topics include: [26]

- Policies and procedures
- Information classification
- Risk identification and mitigation
- Processes, business rules and general workflow
- Roles and responsibilities
- Legal and regulatory requirements
- Baseline information security controls and measures

The training can be delivered differently to the specific audiences in order to provide a tailored training approach as shown in figure 10.

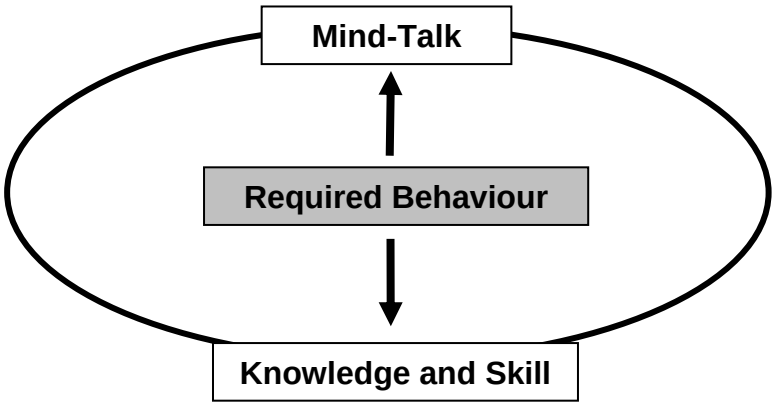
| Audience | Topics | Means |
|---|---|---|
| Management | ▪ Policies and procedures.<br>▪ Roles and responsibilities.<br>▪ Legal and regulatory requirements. | ▪ Computer based training (Intranet).<br>▪ Centrally developed. |
| General User | ▪ Policies and procedures.<br>▪ Processes, business rules and general workflow.<br>▪ Roles and responsibilities. | ▪ Computer based training (Intranet).<br>▪ Centrally developed. |
| Expert (IT services) | ▪ Policies and procedures.<br>▪ Information classification.<br>▪ Risk identification and mitigation.<br>▪ Processes, business rules and general workflow.<br>▪ Roles and responsibilities.<br>▪ Legal and regulatory requirements. | ▪ Classroom training.<br>▪ Centrally developed and delivered |

**Figure 10: Different means of delivering training**

A computer-based training tool, like the prototype that will be introduced in paragraph 4.6, or simply an intranet site containing this information, can be a tool available to management. Management can use this tool to ensure their staff develops the necessary level of skill required.

### 4.5. Measuring the behavioural change

In order to ensure that the required behaviour and attitude has been established, measurements will have to be in place:



Measurement will focus on the overall level of understanding and awareness of information security throughout the organisation. A yearly survey can be centrally conducted to establish the general awareness level within the wider user community. Another option might be to apply on-line monitoring mechanisms [26].

The organisation can leverage more benefits if behavioural change are managed and controlled. Figure 11 [27] explains this concept.

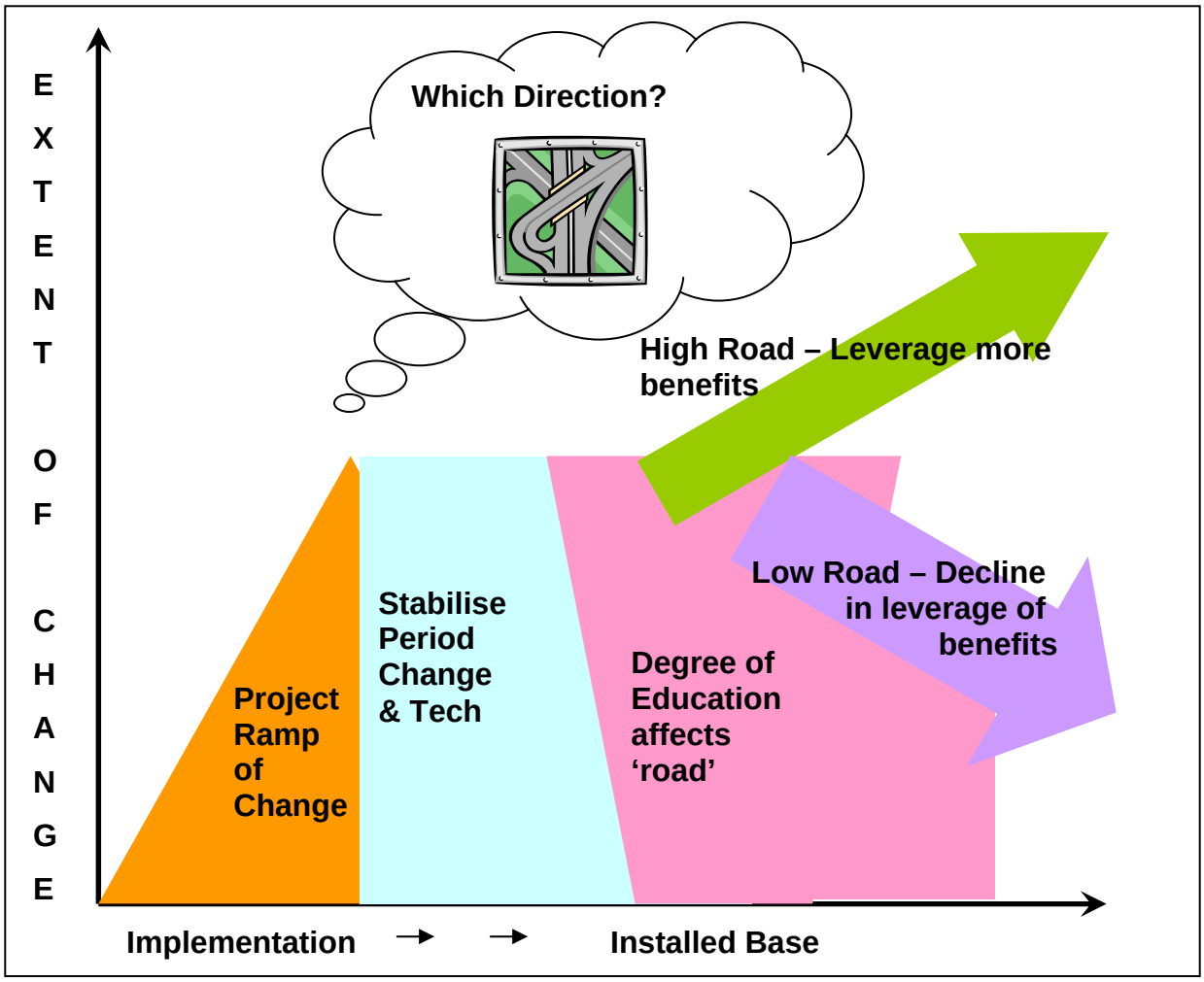



**Figure 11: The importance of managing behavioural change**

Figure 11 depicts very clearly that a lot of change takes place during the implementation of a project like a security policy or new technology being introduced to users. After some time has elapsed the changes and technology stabilises. It is at this point that education and awareness starts to

play a role. Users must be made aware of the new technology and must be educated in order to understand the impact of this in their day to day activities. The degree of education affects the 'road' forward. Two types of 'roads' are identified in figure 11:

- High Road – If the degree of education and awareness is sufficient for the end-user to apply it efficiently, the organization will leverage more benefits from the new technology or changes that was introduced.
- Low Road - If the degree of education and awareness is not sufficient for the end-user to apply it efficiently, the organization will suffer a decline in the leveraging of potential benefits from the new technology or changes that was introduced.

Measurement of what is trying to be achieved is very important, because if you cannot measure it, you cannot manage it.

### 4.6. Security Awareness Prototype: Changing users' mind-talk or attitudes

The security awareness prototype that was developed as part of this study explains the major security threats and means to prevent and deal with these threats in an easy-to-understand and user-friendly way. It enables the employees to revisit the different modules whenever they feel that they need to refresh their memories on what these threats entail.

The information is delivered through familiar means as it is web-based. This ensures that users feel comfortable and they will then be more likely to accept and adhere to the information contained in the program. A web-based user interface can be an effective means of pushing information to users, e.g. a "Tip of the Day" to reinforce certain policies.

## 4.7. Summary

In this chapter the user's attitude or mind-talk towards change was discussed. The situation where the user is typically very hesitant and negative towards change was explained in paragraph 4.2 and paragraph 4.3. This was then followed in paragraph 4.4 by the situation where the user is making the gap between old habits and new skills smaller by changing his attitude or mind-talk and adopting his behaviour accordingly. Here I showed what needs to be achieved in order to ensure that the required behaviour is in place. The user's attitude and changing mind-set needs to be measured in order to manage the whole process as explained in paragraph 4.5.

In the next chapter I will introduce the security awareness prototype that was developed as part of this study. This prototype will be referenced often in the rest of this document.

# Chapter 5: Introduction to the Security Awareness Prototype

## 5.1. Introduction

How can having security savvy employees help protect your organisation? Many hackers make ample use of "social engineering" skills in which they attempt to convince employees that they have a legitimate right to obtain and know information about your company. For example, a clever intruder may call your information services department claiming to be an outside vendor and simply ask for the name of your systems and what operating system they are running. He may follow up by asking for the names of key employees at your company. Armed with that basic information, this unwelcome visitor now knows how to identify your systems, what operating system holes they may be able to exploit and what potential user IDs they can try to use to access those systems.

Having employees who are mindful of such ruses and are prepared to respond appropriately moves any company miles closer to a secure information security infrastructure. [4]

One of the most important and often overlooked elements of a successful information security program is having employees trained to a higher degree of security awareness. [4]

Employees should be trained to appreciate the importance of data that they handle daily and not be lulled into a sense of ambivalence based on the routine of working with such information. Formal information security awareness training should be provided that reinforces the need to keep all

information on your company's information assets confidential - even data that appears the most innocuous. Workers should be further trained to not reveal this information until the requesting party is identified and their need to know authenticated.

An important follow-up measure is to have written an information security policy that explains the company's security philosophy and the business rationale behind it. This policy should be imparted to all new employees as a part of new-hire orientation.

This chapter will focus on the Security Awareness Program prototype that was developed as part of this study. This prototype is an example of a web environment that can be used to train users to a higher degree of security awareness. Paragraph 5.2 will describe the security awareness web environment and why a web-based approach was used. The technology that was used to develop the prototype will be explained in paragraph 5.3. The role players in such a security awareness program within an organization will be mentioned in paragraph 5.4.

## 5.2. The Security Awareness Web environment

Web Based Training software can drastically reduce training costs, effort, and complexity, while providing a cutting-edge, interactive, learning experience. [20]

The Security Awareness program was developed as a prototype to form part of this study. The program serves as a simplified example of a web-based security awareness program that can be implemented in an organization as part of their overall security awareness initiative. On its own, it is not sufficient to provide users with enough information on all security related aspects. It needs to be complimented with other mechanisms as will be explained in chapter 8.

This prototype needs to be improved, maybe even built on better technology, and it needs to be adopted to the organization's branding- and information (policies, procedures, etc) needs before it can be used as a productive security awareness program.

The next paragraph will briefly explain the technology that was used to develop this program.

## 5.3. The technologies that were used to develop the prototype

Due to the cost of programming languages and the timeframe allowed to experiment and learn different technologies, I decided to build this program in Visual Basic 6.0 using Active X documents. This allows me to demonstrate an easy to maintain web-enabled security awareness program. For the purpose of this prototype, the technology used was sufficient.

### 5.3.1. Database Technology

Visual Basic 6.0 was used as the chosen programming language for the development of this prototype. Due to the ease of which Visual Basic integrates with Microsoft Access 97, I decided to use this technology to develop the database in.

The database contains 3 tables with the following information:

- **UserInfo**
  - *UserID*: This is the ID the user will log in with
  - *FirstName*: The user's first name
  - *LastName*: The user's surname. The user's first name and surname will be displayed on all the screens after the user has logged in with his user ID.
  - *Initials*: The initials of the user

- *Password*: The password the user logs in with. The initial password is set to 'init'. The program can be enhanced to allow the user to be able to change his/her password. The security awareness prototype that was developed as part of this study does not cater for this for simplicity reasons.

- **Results**
  - *UserID*: This is the ID the user will log in with
  - *Result[A][B]*: e.g. Result11. This contains a '1' if the user answered the question of module [A], question [B] right and a '0' of the answer was wrong.
  - *Percentage*: This contains the percentage that the user got for the answers in this module. The user needs more than 50% to pass this module. There are 2 or 3 questions for each module.
  - *Pass*: '1' means the user passed this module and '0' means the user failed this module. This field is used for reporting purposes.
- **Answers**
  - *AnswerMod[A][B]*: e.g. AnswerMod11. This contains the answer of module [A], question [B]. The contents of this table is compared to the user's answers before a value is put into table **Results**.

All the tables are in third normal form.

### 5.3.2. Visual Basic Web Development

As mentioned in paragraph 5.3, Visual Basic 6.0 was used to develop this prototype. This software was available to me and I had the necessary skills to do the necessary programming and integration into Microsoft Access 97.

The program is based on Active X documents. Once the program is executed, the browse window will open with the main page displayed. The user will then be prompted for a username and password. This will enable the

program to “know” who is doing what modules and what results were obtained in what tests. All the user information and the test results are stored in an Microsoft Access 97 database from which basic reports can be drawn for referral and follow-up purposes. More detail on the structure of the security awareness prototype will be given in chapter 6.

### 5.3.3. Multimedia content

It is important to keep the user’s attention while he/she is working through the different modules. The modules need to be interesting to ensure that the user gives his/her full attention while reading the information contained in the modules and that the user wants to return to this program at a later stage to either refresh what he/she has learned previously or to do modules that was not completed earlier.

Multimedia content is usually the most effective way to do this. As this is only a prototype, the program does not contain a lot of multimedia content. There are modules that contain pictures to explain certain concepts. A corporate cartoon character can be added in all the modules to give the program a corporate identity. This character can give the user a short summary at the end of each module.

After a test is completed, the user will see a certificate with his/her name on it on the screen. The security awareness program that was developed as part of this study is just a prototype and multi-media content can be used much more broadly and effectively before this is rolled out in an organization.

## 5.4. The role players

Different people have different roles to play in order to ensure that an effective security awareness program is in place and that the desired behavioural change towards security is noticed in the organization.

Everyone, from the security professional to the user need to do his/her part for the overall security awareness program to be successful.

The roles and responsibilities of the IT Security specialist and administrator can include:

- Responsible for the security of all computing systems in your environment
- Provide ID's to access computing environments
- Provide Data access
- Provide security policies, procedures, standards and guidelines on information systems security
- Provide information and assistance to users and system developers

The user also plays and important role in such a program. The user's behaviour and attitude will be an indication of the effectiveness of such a program. The user's roles and responsibilities can include:

- Security Policy – know what it says
- Use strong passwords
- Keep their password confidential
- Use assigned computers, software, and Internet access for business purposes only
- Use e-mail for business purposes only – personal e-mails are not permitted
- Know that copying software is illegal

- Always lock their workstation when not using it
- Be aware of Social Engineering
- Protect the data that he/she "owns"
- Review access permissions regularly on data that he/she "owns"
- Store data on a server (not his/her C: drive)
- Read regular security awareness articles in newsletters, etc
- Scan diskettes and e-mail for viruses
- Contact the Information Security department for unexplained password resets, general advice and counseling purposes

If everyone, from the security professional to the end user understands his/her role to ensure that the organization's digital assets are not compromised, then the organization as a whole has taken a big step towards ensuring a comprehensive security awareness program is in place and working.

## 5.5. Summary

This chapter briefly introduced the security awareness program that was developed for this study. The technology that was used to develop this prototype with was also mentioned in paragraph 5.3.

Finally, the roles of the security specialists and administrators, as well as the roles and responsibilities of the user in such a security awareness program, were explained in paragraph 5.4.

The next chapter will discuss the structure and modules of the security awareness prototype in more detail.

# Chapter 6: The structure of the Security Awareness web environment

## 6.1. Introduction

The structure of the prototype that was developed will be discussed in detail in this chapter.

Figure 12 is a screen capture of the first screen that appears. The user needs to log in to the program:

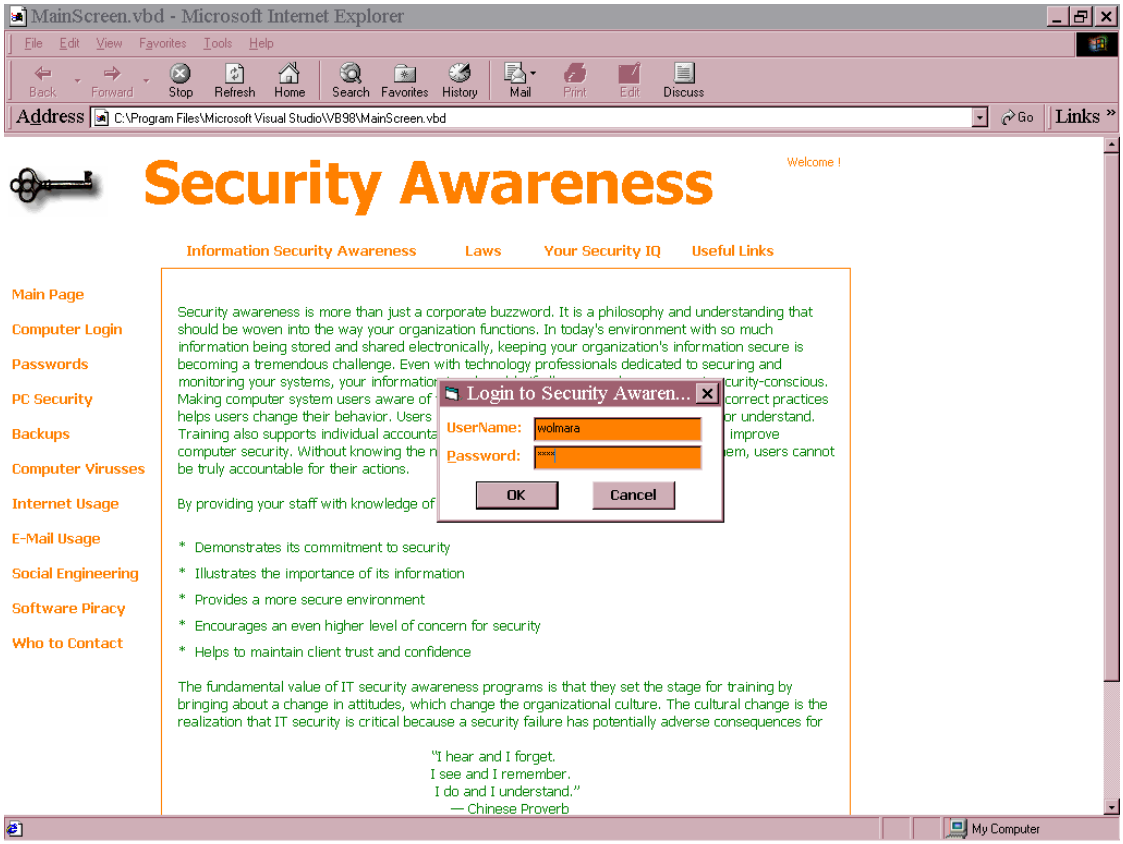



**Figure 12: The first screen of the Security Awareness Program prototype**

The security awareness prototype consists of the following components:

- Access Control – this is mainly used to identify the user. This way the program can "know" what user has worked through what modules and what results were obtained in each test.
- 10 modules, each explaining an important information security related concept. Modular programs are easier to read and there is a smaller chance of information overload on the user.
- Small tests containing 2-3 questions after each module. This is used to evaluate the user's knowledge on the subject that was covered in that module. The results are recorded for reporting purposes.
- Reports containing information and comparisons between the different modules' test results for the different users. More reports can be written to extract useful information from the database.
- Useful links including a Security IQ test, Information Security laws and security related definitions.

Paragraph 6.2 will mention some of the security awareness laws that the user can remember and be reminded of on a regular basis. These laws summarize some of the concepts explained in the different modules. The corporate cartoon character can be used to help the user to remember the laws in a fun way. Paragraph 6.3 will explain the reason for using access control and how this is implemented in the program. The different modules covered in the prototype will be discussed in paragraph 6.4. Finally, in paragraph 6.5, I will mention how the tests are analysed and what reports are generated from these results.

## 6.2. The Security Awareness Laws

This link brings the user to a page containing security awareness laws that the user can remember and be reminded of on a regular basis. These laws summarize some of the concepts explained in the different modules. The corporate cartoon character can be used to help the user to remember the laws in a fun way. An example of such a law might be to remind the user never to share his/her password with anyone. The user can at any time access this page to get a bulleted summary of the modules in the security awareness program.

## 6.3. Access control

This is mainly used to identify the user. This way the program can “know” what user has worked through what modules and what results were obtained in each test.

The prototype that was developed as part of this study incorporated access control by asking the user to log on with a user id and password when the web-based program is accessed. After the user has logged on his name and surname (from table UserInfo) is displayed on the top right-hand corner of the screen. As the user completes the questions at the end of each module, his name appears on the certificate he/she is awarded for completing the specific module successfully.

## 6.4. The modules

Paragraphs 6.4.1 to 6.4.10 will explain the 10 modules in more detail, focussing on the objectives for making this module part of the security awareness prototype.

### 6.4.1. Computer Login

The objective of this module is to explain to the user what it means to log on to a computer and what the result could be if his/her password is compromised and used by someone else.

The module starts by explaining the authentication process to the user using an easy example of an user offering his/her user id and password to a computer and the computer checking if the user id is registered and the password is identical to its records.

The next part of this module explains the concept of unauthorized access which can result in an unauthorized transaction being executed. It explains how the user can be blamed for executing this transaction if this was done using his/her user id and password.

Some tips are given at the end of this module on how the user can prevent unauthorized access e.g. by choosing easy to remember but difficult to guess passwords.

### 6.4.2. Passwords

Passwords are an integral part of overall security. Unfortunately, they are one of the vulnerabilities most frequently targeted by someone trying to break into a system.

This objective of this module is to teach the user how to create stronger passwords and how to properly protect them. This module should also contain a link to the company's passwords policy. This module explains the following in more detail:

- Tips on how to create stronger passwords, e.g. by not using words found in a dictionary.

- Methods for creating difficult to guess, but easy to remember passwords. Some of the methods and examples that are explained are:
    - Vanity passwords: By taking a combination of letters and numbers a phrase can be spelled out without using complete words, e.g. Too late again can be spelled out with ‘2L8again’.
    - Compound words passwords: These are words that are used everyday but that are spiced up with numbers and special characters, e.g. Tuna fish can be spiced up to ‘toona&Fish2’.
    - Phrase passwords: Using the first letter of each word in a phrase can also help to construct a good password, e.g. ‘I spent too much at the fair last night’ can be constructed into the password ‘Is2matfln’.
    - Keyboard pattern passwords: Patterns on the keyboard can sometime provide a password that is easy to visually remember, e.g. a triangle starting with the letter ‘x’ can result in ‘xdr5thnbvc’.
- Tips on how to manage these passwords, e.g. never write down your password.

### 6.4.3. PC Security

The objective of this module is to explain to the user that his/her computer contains valuable digital assets in the form of documents, etc. The computer itself is a company asset and needs to be protected too. Means to physically secure your computer or notebook and the other devices, e.g. printers that you use on a daily basis to do your job are explained in this module.

### 6.4.4. Backups

The objective of this module is to explain to the user what a computer is and why it is necessary to make regular backups of the data on the computer.

The module starts by explaining to the user what it means to make a backup. The importance of keeping the backup copy of the data separate from the computer and in a safe place is also mentioned. This module aims to change the user's behaviour to be more security conscious.

This module should contain a link to the company's backup and restore policy.

### 6.4.5. Computer Viruses

Whilst employees become suddenly aware during the ensuing media excitement that new computer viruses give, they soon forget about the virus threat as the stories disappear from the news headlines.

This is the danger. Complacency can set in when there is no perceived "action" on the virus front and no global crisis and the importance of being vigilant about viruses recedes in your users' minds. They forget what the big deal was in the first place, with a mindset that the anti-virus software deals with the viruses.

Employees see anti-virus software, firewalls and IT departments as guarantees that their computers will work and will be safe, but there aren't any guarantees. Anti-virus software plays one, albeit important, part in the defence of your company from malicious attack but the security of your computer system is only as strong as the weakest link. And that, more often than not, is the human factor.

It is vitally important that employees are educated about the virus threat but this cannot be a one-off event. The potential threat should always be in the

back of an employee's mind and precautionary measures should be taken as a matter of course.

You can have the best software in the world protecting your company's defences; you can even be the biggest IT company in the world; but without your users practising safe computing they will always be the weakest link. [21]

The objective of this module is to give the user the necessary knowledge about computer viruses. The following questions are answered in the module:

- What are computer viruses?
- How do you know if you are infected?
- What should you do if your machine does become infected?
- What can you do to prevent your machine from becoming infected?

This module should contain a link to the company's virus and protection policy.

### 6.4.6. Internet Usage

Web security is a complex topic, encompassing computer system security, network security, authentication services, message validation, personal privacy issues, and cryptography. [1]

The objective of this module is not to cover all of the above, but rather to explain to the user what the Internet and WWW are and what the consequences might be if you are not careful how you use the Internet. The module explains the following:

- What are the Internet and WWW?
- What type of information can be found on the Internet, e.g. Active X controls and the potential security risks it holds.
- Cookies and how this small file can be misused to get information from the computer without the user being aware of it.

This module should contain a link to the company's Internet Usage policy.

### 6.4.7. E-mail Usage

The objective of this module is similar to the Internet Usage module's objective. This module explains to the user what electronic mail is and what the consequences might be if safe usage is not practised.

This module should contain a link to the company's E-mail Usage policy.

### 6.4.8. Social Engineering

Social Engineering is the acquisition of sensitive information or inappropriate access privileges by an outsider, based upon the building of inappropriate trust relationships with insiders. It is the art of manipulating people into actions they would not normally take. The goal of a Social Engineer is to trick someone into providing valuable information or access to that information. It preys on qualities of human nature, such as the desire to be helpful, the tendency to trust people and the fear of getting in trouble. The sign of a truly successful Social Engineer is they receive the information without raising any suspicion as to what they are doing. [34]

People are usually the weakest link in the security chain, and Social Engineering is still the most effective method of circumventing obstacles. A skilled Social Engineer will often try to exploit this weakness before spending time and effort on other methods to crack passwords. Why try to hack through someone's security system when you can get a user to open the door for you? Social Engineering is the hardest form of attack to defend against because it cannot be defended with hardware or software alone. A successful defense depends on having good policies in place and educating employees to follow the policies. [34]

The objective of this module is to explain to the user what social engineering is, the different types of social engineering and how the user can prevent these attacks.

This module should contain a link to the company's policy that addresses social engineering.

### 6.4.9. Software Piracy

Software downloaded from the net is often unlicensed and unsupported, and may cause conflicts with existing software in use at your company. Unlicensed, pirated software is an ideal vector for a computer virus. Virus writers and hackers often use such software as the ideal "kick-start" for their virus distribution.

Employees need to be told that although downloading screensavers and computer games is not on the same scale as downloading pornographic or offensive material in many respects, it is when it comes to security. Ideally, employees should not be allowed to run any applications that are not strictly necessary for their job. The fewer opportunities there are for virus penetration, the better. All users should maintain a healthy paranoia if they want to protect the data on their computer.

The objective of this module is to explain to the user what software piracy is and what the consequences might be if unlicensed and unsupported software is loaded on their computers.

This module should contain a link to the company's Acceptable Use policy.

### 6.4.10. Who to contact

The objective of this module is to give the contact details of the IT security department within your company. The user should know that they must inform the IT security department in your company as soon as they suspect that they have a virus on their computer, that their password has been compromised or that a potential attack might be waiting to happen or has potentially already happened.

The IT security department must also be there to answer any security related questions that the user could have.

## 6.5. Testing the user

At the end of each module the user needs to answer 2 or 3 easy questions. The aim of these tests is to make sure that the user read and understood the contents of each module. The results are written to the database.

The administrator of this program can draw reports from this web-based program, e.g. which users have completed which modules and what results were obtained. This is only a prototype and more reports can be written as needed by the company.

## 6.6. Summary

This chapter explained the different components of the security awareness prototype that was developed as part of this study.

The security awareness laws that summarize the different modules in one single page were discussed in paragraph 6.2. Access Control was explained in paragraph 6.3. The 10 modules, each explaining an important information security related concept, was discussed in more details in paragraphs 6.4.1 to 6.4.10. Paragraph 6.5 mentioned how the tests are analysed and what reports are generated from these results. It is important to remember that this security awareness program is only a prototype and can be expanded and customized to the company's needs.

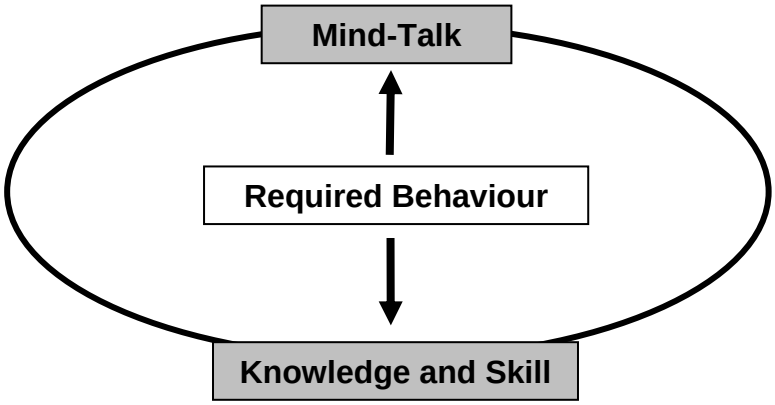
The reason for educating the users is because the human factor is the weakest link in the security chain and users need to be made aware of the different security risks and how to manage them. Changing user's mindset or attitude towards security or any new concept is not an easy task as explained in chapter 4.

The following two chapters will focus on a case study that I researched. I chose to discuss in detail some of the research done by Hi-Performance Learning [25] regarding the psychology involved with training humans and the training approach developed by them to improve human performance.

# Chapter 7: A Security Awareness Program: Case Study

## 7.1. Introduction

The following two chapters will focus on a case study that I researched. I chose to discuss in detail some of the research done by Hi-Performance Learning [25] regarding the psychology involved with training humans and the training approach developed by them to improve human performance. After I have done this research, I incorporated certain components of the Hi-Performance Learning training approach into the prototype as part of the study. These chapters will thus focus on the mind-talk and knowledge and skills components of the model in figure 5:




There is a lot of psychology involved in a training or awareness program. People's attitudes towards change must be changed and measured. In this chapter I will discuss how one company, Hi-Performance Learning [25], succeeded in addressing the human factor, i.e. people's attitudes and sensitivity towards change.

In paragraph 7.3 I will discuss what Hi-Performance Learning refers to as the Human Performance System. The non-training factors that impact human performance will be explained in paragraph 7.4. The environment in this developed approach to training, called the micro level environment, will be detailed in paragraph 7.5. Paragraph 7.6 will focus on streamlining the six micro factors in a practical, implementable manner. This can be applied in general cases where new ideas or technology are introduced in an organization, but it is also very applicable where a security awareness program is implemented in an organization. Paragraph 7.7 will explain how the security awareness prototype that was developed as part of this study addresses the six key factors.

## 7.2. The approach of the Security Awareness plan

The approach taken by a company in developing an effective security awareness plan is very important. Hi-Performance Learning [25] did a lot of research in on the psychology involved with training humans and formulated a training approach that translate to improved human performance. This approach can be modelled in the human performance system (See paragraph 7.3). This approach can be used as a framework to change the mindset of people and their attitudes towards change. [25]

## 7.3. The Human Performance System

The approach taken by Hi-Performance Learning [25] in designing solutions that empower people to perform and accept new technologies or rules given to them, depends on a number of factors relevant to the specific learning challenge. These include: [25]

- The organisational requirements
- The learner profiles and learning/performance needs
- The project/goal realities

In addition, the approach is based on theoretical research into effective learning techniques. These techniques go hand-in-hand with a broader change management view that focuses on the human performance system in which learning and performance is required to take place. [25]

The million-dollar question facing change management practitioners is “What factors impact on a person’s ability to perform effectively using a new process/system?” Much has been written, yet few can claim significant successes in this area. One problem is identifying the correct theoretical approach; the other is implementing that approach effectively. [25] In order to implement an effective and successful security awareness program, it is important to have the correct theoretical approach.

The approach I adopted for the security awareness program prototype and theoretical need-to-know for implementing such a program effectively, will use many of the concepts developed by Hi-Performance Learning. This will be explained in more detail in paragraph 7.7.

## 7.4. Non-Training factors that impact human performance

Many traditionalists view effective training delivery and post-training support, together with management buy-in and leadership to be the factors that need to be addressed when viewing human performance. [25]

However, to implement an effective training or awareness plan, a more systematic view of performance is needed. According to this view, one should not isolate a single part of the performance system to understand its properties and dynamics without understanding its relationship with all the other parts of the system as well. [25] This means that the properties of one part of a performance system will vary depending on the properties of the other parts of the system at that point in time.

Within this framework, improved performance cannot result from the analysis and adjustment of one factor (e.g. the skills and competence of people through extensive training) without understanding the impact on, and of, the other factors. [25] But what are these “other” non-training factors that impact human performance?

Hi-Performance Learning [25] have developed a model that addresses the key performance elements of any system/process rollout. [25] The model can be extracted into a macro, meso and micro level. The focus of this paragraph is on the micro factors, because these have impact on an individual’s performance. This model (see figure 11) explains why training by itself has not been able to provide the answer to improved performance. [25]

### 7.5. The Micro level environment

I will start by explaining how the Micro level environment and its components work. In paragraph 7.7 I will explain how this can be applied in order to implement an effective security awareness program.

The explanation that follows are summed up in figure 13:

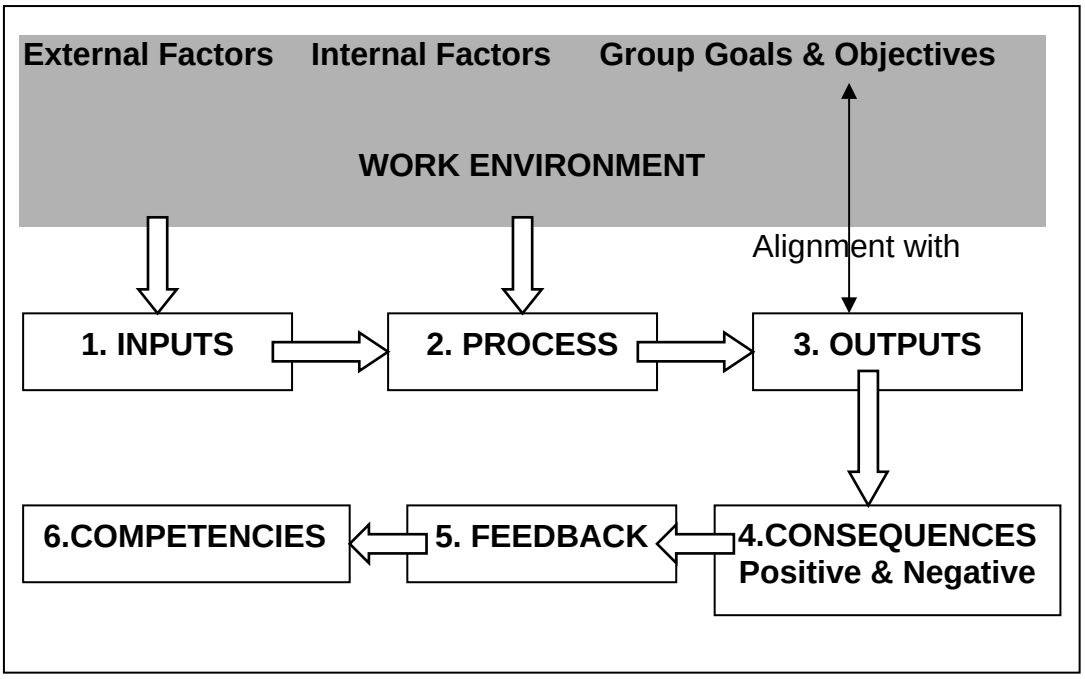



**Figure 13: The Micro Level Environment**

At the micro level, there are six key factors, as shown in figure 13 that need to be considered: [25]

1. Inputs
2. Process
3. Outputs
4. Consequences
5. Feedback
6. Competencies

Each factor has a different impact, and this impact depends on the state of each of the other variables. Unless all six factors are understood and addressed by the performance solution, the performance improvement will never be optimal. [25]

The single factor that is addressed by the traditional training approach is that of the individual's skills, understanding and building of competence to learn what is required from him to perform (Factor number 6 in the micro level environment). What needs to be understood is the learner's experience and

preferred learning styles in order to design courses that maximise their ability to learn new skills and knowledge. Using this model, however, one realises that there are five other factors that need to be analysed and addressed if performance is to improve. These are [25]: (Refer to figure 13)

- **The processes that the individual follows:** (This refers to number 2 in figure 13) Individuals need to be provided with a process that, if followed correctly, enables them to achieve the desired performance outputs. Organisations may be providing leading-edge software, yet are still supporting outdated and inefficient business processes. Alternatively, the process could be efficient but the system does not align with it. Often the software that is used does not align effectively with the process the individual has to follow, and therefore impacts on their performance. By understanding WHAT needs to be done to achieve performance (i.e. the process), and HOW it needs to be done (i.e. the system), human performance specialists can initiate critical adjustments that transform an individual's ability to perform a given process.
- **The inputs that individual's receive when performing the process:** (This refers to number 1 in figure 13) Each step of any process requires certain inputs to perform. Unless these are provided at the right time (and in the right way), individuals are unable to perform the process effectively. By analysing and correcting any bottlenecks (as well as any negative inputs e.g. noise and interruptions), one is often able to radically improve the individual's ability to perform.
- **The required quality and quantity of outputs:** (This refers to number 3 in figure 13) Individuals are often found to be under-performing simply because they lack a clear understanding of what effective performance really means in their jobs. This stems from the inability to place a measurement on required outputs, as well as the ability to communicate a clear performance benchmark. Without these in place, individuals often perceive themselves to be performing effectively, even though they know they are working well within their true potential.
- **Positive and negative consequences related to performance:** (This refers to number 4 in figure 13) A common reason for sub-optimal performance stems from the lack of positive (and negative) consequences

built into the process. People only change behaviour when the perceived gains (and negative consequences) stimulate them to do so. Often organisations demand greater outputs without addressing the important question: “What is in it for them?” These consequences vary within different organisational cultures, but remain critical in achieving optimal human performance.

- **Feedback on how each individual is performing and on ways for improvement:** (This refers to number 5 in figure 13) Nobody likes working without some form of feedback. This differs between people and tasks, but it remains a critical factor in the performance cycle. Many organisations forget this loop altogether, and hope that individuals who have learnt a new system or software programme will be able to gauge for themselves how effectively they are able to translate their learning into improved performance. This managerial/mentorship role is critical if learning within the “classroom” is to be continued on the job (where most learning should be taking place).

Given the systematic view of performance, it becomes clear why training can seldom (in isolation) improve to the levels required within our competitive industries. Human learning needs to be viewed within a broader performance system, and solutions need to become more holistic. Only once one start addressing all the variables in a systematic, structured fashion can we hope to glimpse the enormous human potential that exists within our organisations. [25]

### 7.6. The Practice

So, given this systematic theory, how do you ensure that people using a new solution perform effectively? The answer is to focus on streamlining the six micro factors, depicted in figure 13 and explained in paragraph 7.5, in a practical, implementable manner. This can be applied in general cases where new ideas or technology are introduced in an organization, but it is also very

applicable where a security awareness program is implemented in an organization.

From an input perspective (see number 1 on figure 13), employees need to be provided with the right information in the right format, at the right time. The processes need to be such that bottlenecks are minimised, and that processes support each other efficiently and effectively. Environmental inputs (e.g. noise, completing time and task demands) also need to be addressed to ensure employees are placed in a working environment conductive to performance.

From an output perspective (see number 3 in figure 13), every employee needs to be given clear, objective performance measures. These measures must benchmark tangible performance outcomes that need to be achieved by the employee, using the new processes and systems. Unless people are clear as to what effective performance looks and feels like, performance levels may remain below level.

In addition, employees need to be clear about the consequences linked to their performance. (This refers to number 4 on figure 13) The ownership of performance must reside with them, and they need to feel that the positive consequences of them improving their performance using these new processes and systems are sufficiently enticing to change their current behaviour. The negative consequences of them not changing must also be sufficiently unattractive (although negative reinforcement remains less effective than positive reinforcement). Without personal consequences attached to performance, the greatest process and system may prove ineffective.

Finally, the much spoken about and seldom implemented feedback loops need to be created and maintained. (This refers to number 5 in figure 13) What may appear to be a short-term performance improvement can often result in a long-term failure simply because of a lack of ongoing performance feedback. Employees must not have their competence (see number 6 in

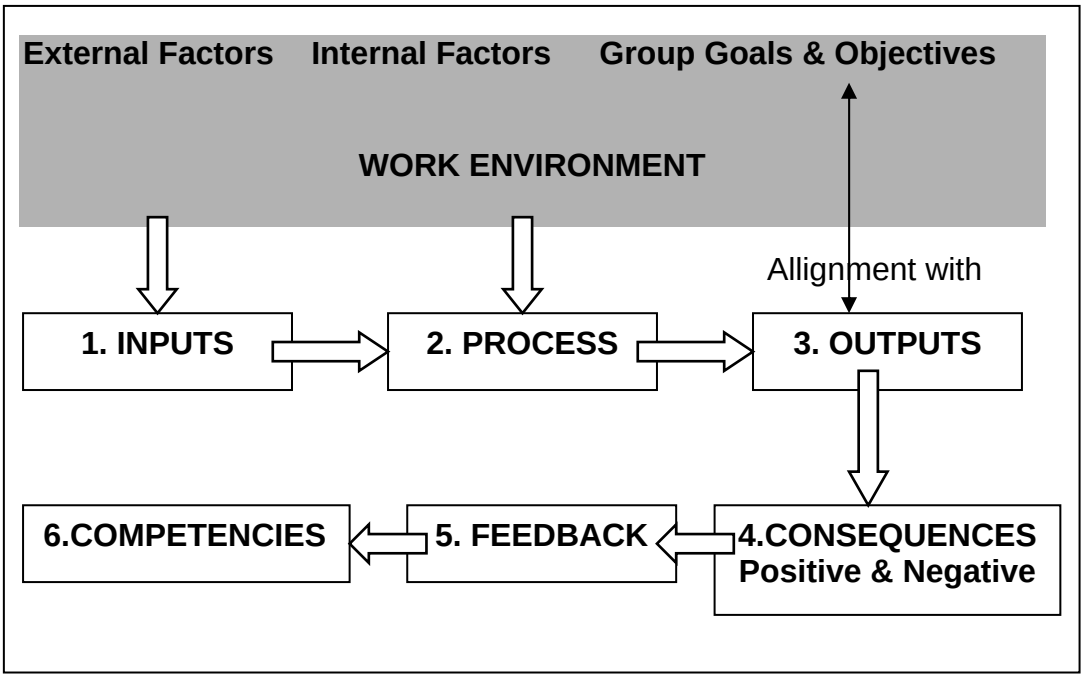
figure 13) assessed once, and then be left to get on with it without further input and feedback. Managers need to ensure ongoing feedback takes place. For this to happen, workable management processes and practices need to be defined.

The purpose of mentioning these factors is simply to highlight that few training solutions will succeed without adequate attention to these important and influential performance variables. The challenge is then to create a learning system that will adequately resolve the key skill and competence requirements. [25]

In the next paragraph I will explain how this practice forms part of an effective security awareness program with specific reference to the prototype developed for this study.

## 7.7. Bringing the concept of the Micro level environment and practice into the study

For reminder purposes, figure 13 will be repeated:



At the micro level, there are six key factors that need to be considered: [25]

1. Inputs
2. Process
3. Outputs
4. Consequences
5. Feedback
6. Competencies

All six key factors need to form part of the theoretical training approach that must then be implemented successfully to ensure that an effective security awareness program is the result. Let me explain how these key factors are be implemented in the security awareness prototype program that forms part of this study:

- **Inputs**: Each step of any process requires at the right time and in the right way, certain inputs to perform. The inputs in this case are the information that is provided in each module to help the user understand the concepts better.
- **Process**: Individuals need to be provided with a process that, if followed correctly, enables them to achieve the desired performance outputs. Each module discusses WHAT needs to be done when for example the user realizes that his/her password has been compromised as well as WHAT can be done to prevent this from happening.
- **Outputs**: Measurement must be placed on the required output and a clear performance benchmark needs to be communicated. The modules explain to the users what is required from them when security is breached. An example might be a user contacting the IT security department when he/she suspects that his/her password has been compromised. The user are also tested after each module to make sure that he understood the contents of the module and are aware of the security policies that exist in the company.
- **Consequences**: Positive and negative consequences need to be built into the process. People only change behaviour when the perceived gains

and negative consequences stimulate them to do so. The prototype make the users aware of the security policies that exist in the company and the steps that can be taken against them if they are responsible for a security breach that took place in the company. The users are also made aware of how they can benefit from practising safe usage of the company's digital assets.

- **Feedback**: Means for the users to give feedback should exist. The prototype allows for the users to give feedback in the form of completing the tests at the end of each module. This allows the IT department to know if the user understood the contents of each module and where they can help the user to understand and execute the desired behaviour better.
- **Competencies**: Users are trained to build their individual skills. The modules provide information to the users that build their competence and understanding of security. They can now perform by applying the security knowledge they have gained in the program in their day-to-day job.

## 7.8. Summary

This chapter focussed on a case study that I researched. Hi-Performance Learning did a lot of research regarding the psychology involved with training humans. I explained the training approach developed by them to improve human performance.

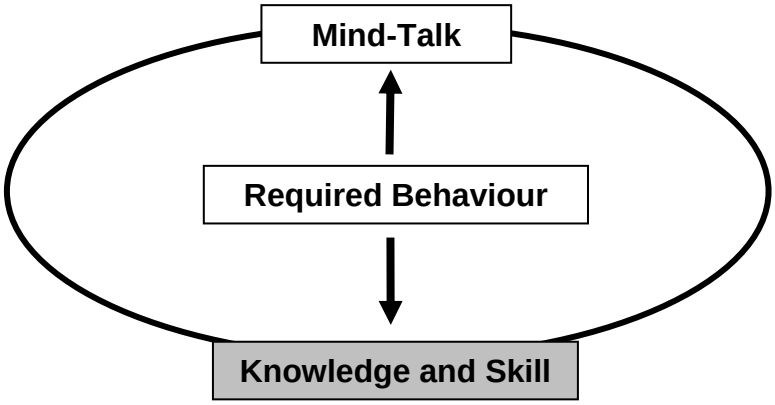
The Human Performance System, the Micro Level environment in this approach and the means of streamlining the six micro factors in a practical, implementable manner, was discussed in paragraphs 7.3, 7.5 and 7.6. The prototype that forms part of this study addresses most of these key factors. Paragraph 7.7 explained how this is done.

The effectiveness of any learning approach depends on a number of factors. Chapter 8 will discuss some of the issues related to existing means of training as researched by Hi-Performance Learning.

# Chapter 8: Implementing an effective Security Awareness program

## 8.1. Introduction

The Human Performance System, the Micro Level environment in this approach and the means of streamlining the six micro factors in a practical, implementable manner, was discussed in chapter 7. The effectiveness of any learning approach depends on a number of factors as also discussed in chapter 7. This chapter will discuss some of the issues related to existing means of training as researched by Hi-Performance Learning. Once again, this chapter will focus on the knowledge and skills of the model depicted in figure 5:




One could easily launch into a detailed review of learning theory when it comes to the learning of new technologies or processes. However, the effectiveness of any learning approach depends on a number of factors, importantly those of required learning outcomes, learner characteristics and the learning environment. Of these factors, the most critical remain those of required learning outcomes.

Paragraph 8.2 will explain the role of the skills and competence performance factor that form part of Hi-Performance Learning's model that was discussed in chapter 7. Paragraph 8.3 will detail some of the reasons why many training solutions struggle to deliver these learning outcomes and how an organization can overcome this by implementing appropriate performance need analysis and choosing the right course content, course structure and learning media. It will become clear how these issues are addressed in the study. The importance of choosing the right course content, course structure and learning media led me to implement a web-based security awareness prototype and this can be used as part of a more comprehensive overall security awareness program in an organization. Any learning or awareness program need to be managed and controlled. Some aspects surrounding this will be discussed in paragraph 8.4.

## 8.2. The skills and competence performance factor

In this paragraph I will explain the theory behind the skills and competence performance factor as defined by High Performance Learning [25].

When tackling a project rollout, with the complexities that go with it, the typical learning outcomes expected by an organisation are as follows: [25]

- The performance of employees must improve significantly as a result of the learning investment. How the learning is achieved is not important; that there is a significant improvement in performance is!
- Employees need to be provided with the knowledge and skills that will enable them to produce effective outputs. They do not need to be taught functionality that will not directly result in improved performance (i.e. "nice to know" functionality).
- After the learning experience, employees need to be provided with support that is readily available and very easy to access. If not, people will resort to disturbing their work colleagues or keeping quiet and compromising their outputs. Both results in increasing the time it takes to produce required outputs.

- Employees need to be able to learn when it is convenient for them. This means they may need to learn an hour a day, or everything in one go.
- The costs of providing employees with these skills should be as low as possible.
- The learning solution must be sustainable. This means that the organisation does not want to be left stranded when the consulting company leaves and ongoing learning remains a requirement. This includes not having to employ Security specialists on an ongoing basis.
- The learning solution must be designed within the project time line and cost realities.
- Assessments should be designed so that the organisation's employees can manage and assess competence on sight.

I will now discuss how these aspects were integrated into the security awareness prototype that was developed as part of this study. The prototype addresses the above required outcomes as follows:

- The performance of employees should improve significantly as a result of the learning investment. In the prototype, these can be measured by the test at the end of each module. Useful reports exist that can identify shortcomings in each module based on the results of the test. A significant improvement in the way that the user protects the information/electronic assets should be visible.
- Employees need to be provided with the knowledge and skills that will enable them to produce effective outputs. Each module in the security awareness prototype is short and contains the enough information to directly result in improved performance or awareness (i.e. "nice to know" functionality is optional).
- After the learning experience, employees need to be provided with support that is readily available and very easy to access. The user can at any stage return to any of the modules to refresh his memory on any information security related issue.
- Employees need to be able to learn when it is convenient for them. This means they may need to learn an hour a day, or everything in one go.

The program is web-enabled and available when it is convenient for the user.

- The costs of providing employees with these skills should be as low as possible. This is usually the case with most web-enabled applications. This prototype was easy to develop and did not require a lot of specialized skills.
- The learning solution is sustainable. It does not require very specialized skills to maintain the information or the technology it is based on.
- The learning solution was developed in a very short time frame and it is easy to maintain.

## 8.3. Why training solutions struggle to deliver these learning outcomes

There are a number of critical factors that are not being effectively addressed in the design and delivery of learning solutions. [25] The key problem areas faced by most training offerings and how the prototype developed as part of the study address this will be discussed in the following paragraphs.

### 8.3.1. Ineffective Learning and Performance Needs Analysis

Many learners throughout the world continue to find themselves scheduled on training courses that have little relevance to their immediate performance requirements, or training courses that last 5 days and only contain 1 day's worth of valuable learning.

This results in the learner resisting learning, or forgetting important information over time (due to a lack of skill and knowledge utilisation). The result is high training costs and low performance improvement. It is therefore critical to ensure that the learner has been given the opportunity to identify their own performance and learning needs, and that courses are designed to

focus on these, as this will affect the motivation and application of the learner. [25]

### 8.3.2. Inappropriate and Ineffective Course Content and Structure

There appears to be a number of key principles that need to be upheld when designing and structuring a learning process aimed at empowering people to use new technology. Many training solutions fail to address many of these principles, resulting in sub-optimal learning and performance improvement. These principles include: [25]

- **Explain the process; then explain how the system supports this process.** A common mistake made by many training designers is to focus on what the system can do, as opposed to the process of the tasks to be completed (and the outcomes to be achieved). People generally do not think in terms of system functionality in isolation of how this fits into the business process they must follow, and having software explained according to the various system functions, is often confusing and disempowering. It is therefore essential to first clearly define what the person must do without reference to the system. Once the process is clear (e.g. how to create a complex password), you then need to explain how the system supports this process. By linking the process step to the system, it ensures learners are able to transfer their learning to performance back at the workplace.
- **Prevent content overload.** Too often we overload the learner with system functionality that is not core to the required outputs (i.e. they don't need to know it to perform effectively). To optimise learning transfer, it is critical that only the system functionality required to perform clearly defined process steps and performance outcomes are covered. This requires first analysing and defining the process and required performance outcomes, and only then identifying the system functionality required to achieve these outcomes.
- **Ensure you use job-specific examples.** Generic training that does not focus on showing the learner how the new skills and knowledge apply to

their specific work context (i.e. where they will be used), limit the transfer and application of these skills and knowledge. It also relies on the learner making the connection between theory and practice, something few learners have time or patience to do.

- **Ensure that the information source is flexible and easily accessible.** Adult learners tend to learn more readily when they are given control over their learning objectives and content. Forcing and adult through a defined, inflexible learning process causes resistance and limits learning (e.g. if someone has to sit through a structured instructor-led course). In addition to defining his or her own learning objectives and structure, adult learners also resist having the source of information reside in another person (e.g. the trainer). This is because the access to this information is dependent on the presence of the trainer, and is therefore disempowering to an adult who wishes to take control of his/her own learning.

Apart from the course content and structure, it is also important to select the right combination of learning media to be used when introducing a user to a security awareness program. There are different options and these with its limitations and benefits will be discussed in paragraph 8.3.3.

### 8.3.3. Inappropriate Selection of Learning Media

The selection of the learning medium is critical to the success of the learning process, as this will be the way that the carefully planned and chosen course content and structure will be presented. Two dominant learning media continue to be extensively used in 'technology training', yet both have key limitations that have until now not been adequately addressed. These two media are Instructor-Led Training and Computer-Based Training.

An effective security awareness program as described in this study consists of both instructor-led training and computer-based training. I will first explain the limitations and benefits of both learning media and then explain how the right

combination of instructor-led training and computer-based training (paragraph 8.3.3.3) can be the key factor in an effective security awareness program.

#### 8.3.3.1. Instructor-Led Training.

Instructor-Led training continues to be the preferred medium used to skill people up in new technologies. This is primarily due to the fact that most people are familiar with this learning medium, and therefore assume that it will be as effective in the field of technology as it is in behavioural development.

- **Benefits of Instructor-Led Training:** The benefits of having a trainer 'facilitate' your learning are as follows [25]:
  - **(i) Peace of Mind.** You as the learner feel comfortable that if anything goes wrong, the trainer will be there to help you out. Technology scares many people, and just the knowledge that someone will be there in case something goes wrong is enough for them to opt for instructor-led learning.
  - **(ii) Familiarity.** Most traditional training programs are facilitated. Having technology explained in a medium familiar to most learners is therefore comforting to most people.
- **Limitations of Instructor-Led Training:** The key limitations to traditional instructor-led learning includes [25]:
  - **(i) Trainers are forced to set a specific learning pace.** This inevitably frustrates "quick" learners who are held back, and lose slower learners as they desperately try to keep up (and eventually give up and switch off). The result is that learning is stifled or prevented by the trainer's delivery pace.
  - **(ii) Learners are forced to listen to large content volumes for many hours at a time.** This demand on the auditory senses is extremely tiring, resulting in selective retention and frequent "headaches" (i.e. people struggle to concentrate for long periods on memorising detailed content using their auditory senses). Visual retention of detailed information, however, appears to be more effective for the majority of learners, who are able to read and concentrate for longer

periods than listening to someone else provide the information. Auditory senses are however effective for low detail information (e.g. remembering a musical tune, not the words sung in that tune). Learning how to use a computer system is all about details, hence the difficulty in listening to and remembering these details.

(iii) **The trainer's ability significantly influences the learning experience.** The lack of consistency in learning delivery limits a company's ability to guarantee learning outcomes (given the different skill levels of trainers).

(iv) **Having to learn with other people around, and having the trainer drive the learning process, intimidates learners who get confused.** This is because by asking a question to resolve a personal issue stops the trainer from continuing with the others. People therefore tend to keep quiet, rather than look for help when they need it.

(v) **Trainers can only teach one course at a time.** This prevents a group of people (e.g. a department) learning different skills and knowledge at the same time. It also prevents people covering different sections of the same course at the same time.

(vi) **Learned helplessness.** Many people believe that they are too 'stupid' or incapable of teaching themselves how to use a new software package. This assumption ensures that if something ever goes wrong, the user stops performing until an outside "guru" comes to help them. A key requirement for future technology learning is that learners control their own learning, and approach new technology with confidence as opposed to trepidation.

(vii) **Instructor-led training requires the provision of training facilities.** This is expensive, and also limits the flexibility of delivery times. With regards to outlying departments, the cost of transporting and accommodating trainers also proves very expensive.

#### 8.3.3.2. Computer-Based Training

Computer-based training continues to attract many IT and training managers who believe that their organisations need to embrace the new technology wave with learning media grounded in the technology itself. This 'solution' offer organisations many benefits. It also has many problems.

- **Benefits of computer-based training (CBT):** The key benefits offered by CBT include [25]:
  - **(i)** **Ease of delivery.** The CBT learning solution can be loaded onto the organisation's network and be accessed by learners from their desks.
  - **(ii)** **Reduction of training facilities.** The fact that learners are able to access the learning medium from their desks allows organisations to cut down on the provision of costly training facilities.
  - **(iii)** **Easy learning and performance assessments.** Most CBT products offer learners a multiple choice pre-assessment, followed by a similar post-assessment at the end of the training module. This provides training managers with instantaneous access to performance indicators, without having to arrange this independently.
  - **(iv)** **Flexible learning structure.** Most CBT solutions offer learners the ability to pick and choose the system functionality they wish to cover. This flexibility empowers the learner to decide what they want to learn, and when.
  - **(v)** **Ongoing access to information.** The fact that the CBT solution is normally accessible over the network allows learners to access different modules again and again. This empowers them to review previous learning, and to brush up on areas that they have forgotten.

- **Limitations of computer-based training (CBT) [25]:** Computer-based training is certainly showing some wonderful results in adult learning. There are, however, a number of reasons why people struggle learning new software using this medium. These include:
  - **(i) Unfamiliar learning medium.** Many learners find the technical aspects of operating a CBT program difficult (and daunting), and they frequently spend more time trying to work out the system than actually learning. People learning to use software are often techno-phobic, and the last thing we want to do is to scare them off with the technical aspects of the learning process.
  - **(ii) Inability to provide a non-simulated learning experience.** People tend to find it very frustrating having to switch between the CBT screen and the actual software program they are learning.
  - **(iii) Inability to customise.** Most CBT solutions are generic, and offer the client limited flexibility. The learning of internal software (i.e. software that is company-specific) is also seldom done via CBT, due to the exorbitant costs of designing a customised CBT solution. This means that learners are expected to learn generic software using a CBT medium, and the organisation-specific software using another medium.
  - **(iv) Poor help or summary information.** Once the learner has completed the CBT course, they often find accessing the support material difficult and time consuming. This is because few CBT solutions provide user-friendly learning support. Most solutions require the learner to repeat the section, as opposed to having quick look-up facility that provides summarised information regarding the specific query at hand. This limits the learner's overall ability to learn and improve their performance.
  - **(v) Not all organisations are able to support CBT requirements.** It is often difficult to provide learners in isolated places with a CBT solution (and the learning support they tend to require). This is because the learners need to either have machines that have a CD-ROM drive, or have access to a network that has the CBT loaded

and available. For a CBT solution to be successful, all learners need to have access to computers that meet these requirements.

#### 8.3.3.3. Combining instructor-led training and computer-based training

The limitations and benefits of Instructor-led training and computer-based training was discussed in paragraph 8.3.3.2. To get the optimal benefits from both scenarios it is possible to combine the instructor-led training and computer-based training to ensure that an effective security awareness program exist in an organization.

Instructor-led training can be very informal. Information security awareness days or workshops can be held on a regular basis to communicate and explain critical factors that need to be in place to protect an organization's information or electronic assets.

This can be complimented with a computer-based training tool, like the prototype that was developed as part of this study. The user can at his own convenience visit a website that resides on the organization's intranet to get modular summaries of the categories that was discussed in detail on the security awareness day or in the workshops. They can then complete a small test to measure their awareness of each security topic. They can return to a specific module or look at the other modules at any time.

Learning does not end after the training or awareness session. Support mechanisms need to be in place in order to assist the user with ongoing learning and application of the gained knowledge and skills. This will briefly be discussed in paragraph 8.3.4.

### 8.3.4. Ineffective Learning Support

Learning does not end after the training session. In fact, the best form of learning takes place back at the person's workstation, when they are required to apply the learned skills and knowledge in their work environment. Thick "never-to-be-looked-at-again" manuals do not help learners continue the learning process at their desks. Learners find these reference support tools very unfriendly and intimidating, and tend to store them in the 13th drawer. What often happens is that people ask a colleague or limit their use of the system functionality to what they can recall. It is therefore critical to provide learners with learning support that is both user-friendly and informative.

In light of the security awareness plan, this can be achieved in the following ways:

- The users need to be able to go back to the security modules on the computer-based training tool at any time to recap on some issues that need clarification.
- A mechanism need to exist on the computer-based training tool that will allow the user to ask for more information on a specific topic or to pose a question. These queries can be answered by e-mail.
- Regular information security awareness days or workshops need to be held to update the users on new developments and to share tips and experiences. This will allow the user to ask questions.

Additional mechanisms that can be incorporated in a security awareness program will be discussed in chapter 9.

It is very ineffective to have security awareness days and workshops and to give the users access to computer-based training tools, but have no means to know if the users gained the necessary knowledge and skills to apply what they have learned. Ineffective learning assessment will be the focus in paragraph 8.3.5.

### 8.3.5. Ineffective Learning Assessment

It is no use testing a person's knowledge of system steps in isolation of the required performance outcome [25]. Most training solutions certificate on attendance or on the person's ability to regurgitate system steps. This, however, is no indication on whether learning has taken place (and that performance has improved). It is therefore critical to assess the person's competence, based on their ability to produce a clearly defined performance output.

A user's competence and performance regarding security awareness and application can be assessed by letting the user complete a small test at the end of every module that is completed. The user can be awarded with an electronic certificate. Means to draw reports on modules completed and the test results need to exist.

Given the new National Qualifications Framework (NQF) requirements, outcomes-based assessments will need to become a basic learning requirement. It is therefore critical that the organisation becomes familiar with the NQF, and the requirements going forward. [25]

## 8.4. Learning management requirements

In addition to the learning outcome requirements, organisations implementing a security awareness program typically look for the following from a learning management perspective: [25]

- A learning solution that can be managed from a central point
- A solution that can be maintained on an ongoing basis by the learning manager, or by the consulting firm (depending on the business requirements)
- A learning solution that empowers the individual companies to manage their own performance learning, without being constantly dependent on the central office.

The information security awareness program prototype can be managed from a central point. It can be loaded on the network and made accessible via the organization's intranet. The solution is easy to maintain on an ongoing basis. This can be done within the organization's own security department to empower the organization to manage their own performance learning.

## 8.5. Summary

The effectiveness of any learning approach depends on a number of factors, importantly those of required learning outcomes, learner characteristics and the learning environment. Of these factors, the most critical remain those of required learning outcomes.

This chapter discussed some of the issues related to existing means of training as researched by Hi-Performance Learning.

The role of the skills and competence performance factor that form part of Hi-Performance Learning's model that was discussed in chapter 7. The limitations and benefits of instructor-led training and computer-based training was mentioned. Combining these two training methods provides a balanced means of introducing security awareness to users.

Reference was made to the security awareness prototype that was developed as part of this study and how the explained concepts were applied or incorporated into the program.

To ensure that the organization continues to benefit from the investment made to implement a security awareness program, they need to ensure that the users are reminded about the importance of information security awareness on a continuous basis. Effective mechanisms exist that can be incorporated on the organization's overall security awareness plan. This will be the focus of chapter 9.

# Chapter 9: Mechanisms that can be used as part of a Security Awareness Program

## 9.1. Introduction

To ensure that the organization continues to benefit from the investment made to implement a security awareness program, they need to ensure that the users are reminded about the importance of information security awareness on a continuous basis. This way you will ensure that the user's attitude towards security is right and the user will behave accordingly. Effective mechanisms exist that can be incorporated on the organization's overall security awareness plan. This will be the focus of this chapter.

The mechanisms and the benefits of using these mechanisms as part of a security awareness program will be the discussed in this chapter. These mechanisms include: Posters, Screensavers, the Intranet, Brochures, Multi-media computer-based training, Custom awareness programs, talks and trinkets. Different ways to participate in a security awareness day or workshop will be mentioned in paragraph 9.10.

A Corporate cartoon character can be introduced to the users. The users will then be able to remember information security related issues in fun way. The important role of this character will be highlighted in paragraph 9.11. The primary goal of some security companies is to raise awareness of all computer systems users about security awareness. The benefits of obtaining professional help for this purpose will be explained in paragraph 9.12.

The prototype that was developed for this study is only one component of an effective and comprehensive security awareness plan.

## 9.2. Posters

Posters are a great tool for promoting awareness of any topic. Posters must be designed to capture the reader's attention with an alluring graphic and lead-in, then, educate them on a security topic in an interesting and informative manner. By placing them in areas such as break rooms, or above water fountains and coffee machines (or behind every bathroom door), you can efficiently and effectively educate numerous staff on security topics.

Topics that can be covered include: password construction and management, viruses, Internet and e-mail usage, software piracy, telephone fraud, personal computer security and more.

The benefits of using posters as a security awareness tool, include: [10]

- Year-round awareness
- Eye-catching
- Each poster reaches many
- Openly demonstrates your commitment to security

Figure 14 contains and example of a poster that can be used as part of a security awareness program.

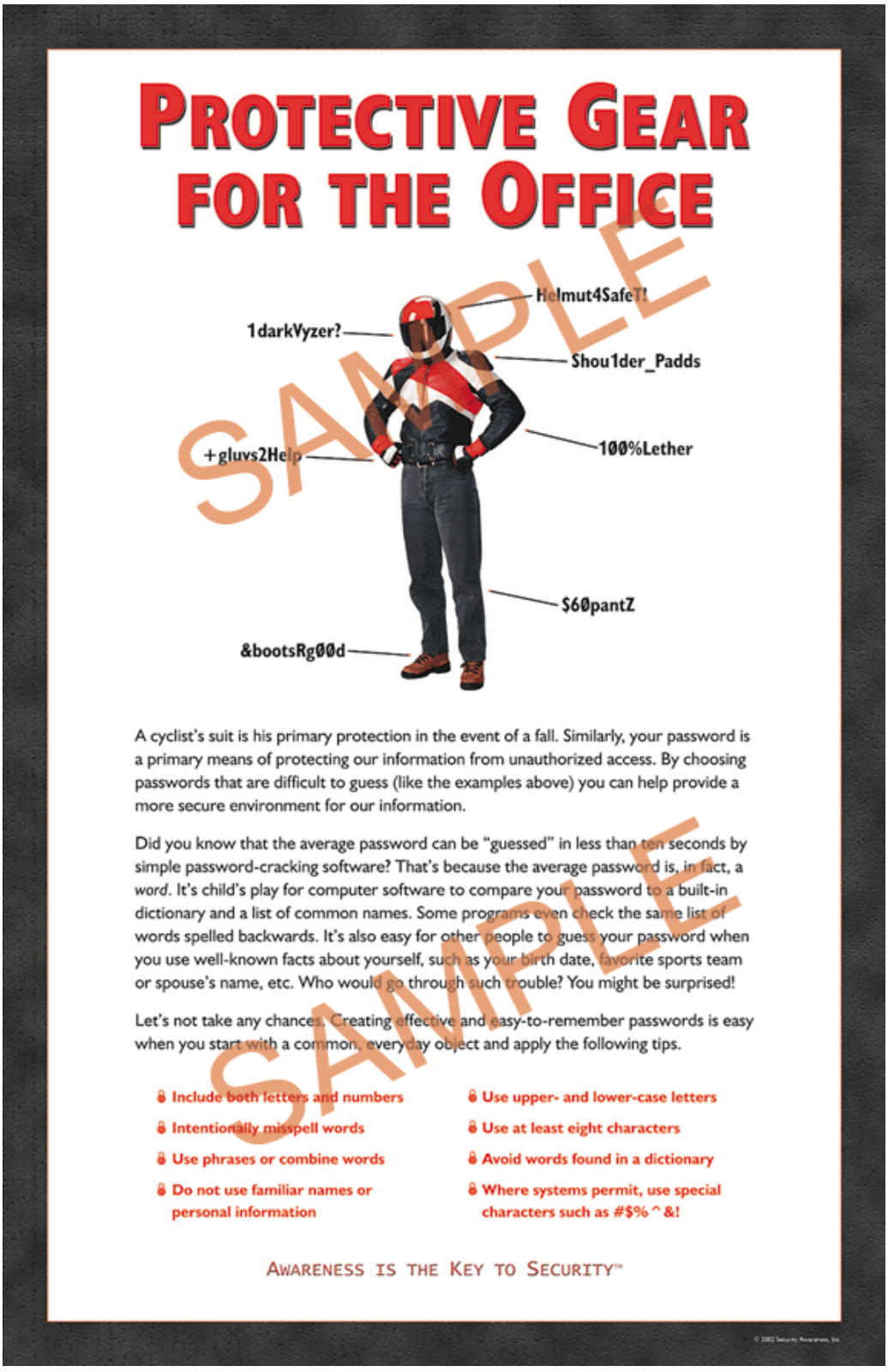



**Figure 14: An example of a poster that can be used as part of a Security Awareness Program.**

### 9.3. Screen Savers

People seem to be intrigued with screen savers. That is why screen savers are an effective way to bring security awareness messages right to the individual end users.

Security facts, awareness tips, and quiz questions followed by answers will provide repetitive learning. Short security-related animations can be included to help elevate interest and encourage attentiveness.

Some of the screen saver's features can include: [11]

- Password protection
- Set as the default screen saver with every reboot (setting in registry)
- Easily customisable with your logo file
- Security facts, tips, quizzes, graphics and animations

The screen savers should cover a wide variety of topics such as password construction, software piracy, backups, password management, viruses, Internet usage and PC security.

The benefits of using screen savers as a security awareness tool, include: [11]

- Learning through repetition
- Intriguing
- Secures the PC
- Direct presentation

An example of a screensaver that can be used as part of a security awareness program can be found on the disk labelled "Information Security Awareness Program" at the RAU Standard Bank Academy for Information Technology. This demo screensaver was developed by Security Awareness Inc. [11] This screensaver can be customized to the organization's need and branding requirements can be incorporated.

## 9.4. The Intranet

An effective way to provide information for an organisation's staff is through a company Intranet. This allows each user to browse through the information and learn at their own pace.

Intranets provide a vehicle to present large amounts of information in an organised manner. Users will have an easy time finding the topics they need to learn.

The Intranet site can be developed to compliment the posters, screen savers, and brochures.

The benefits of using Intranets as a security awareness tool, include: [12]

- Always accessible
- Self-paced learning
- Comprehensive
- Organised presentation
- Customisable

The prototype that forms part of the study is web-based and can be easily deployed on the organization's intranet.

## 9.5. Brochures

Brochures can be distributed as a complete packet or individually by topic at regular intervals.

The benefits of using brochures as a security awareness tool, include: [13]

- Modular
- Portable for road warriors
- Great orientation material for new staff
- Various combinations can be utilised for different learning objectives

## 9.6. Multimedia computer-based training

Interactive computer based training is user navigable and includes sound, video, and illustrations to create an enjoyable learning experience.

The benefits of using multimedia training as a security awareness tool, include: [14]

- Individualised training
- Self-paced
- Multimedia CBT provides comprehensive learning

The prototype that is developed as part of this study does contain basic multimedia content, like the personalized certificate that the user receives after completing each module successfully, certain diagrams and pictures used to describe concepts better, etc. This program is self-paced.

## 9.7. Custom Awareness Programs

Custom ideas can help bring the right “fit” to an organisation’s awareness program and include: [15]

- Special events like a security awareness day
- Customised items like videos
- Printed materials like newsletters and booklets
- Fun activities like an award for fostering security or for implementing innovative security techniques.

Some ideas for a security awareness day or workshop will be discussed in paragraph 9.10.

### 9.8. Talks

Nothing will ever take the place of face-to-face talks with employees. They present opportunities to make suggestions that are specific to the group or department, handle questions as soon as they arise, and gauge the attitudes and familiarity with protecting corporate assets and information systems. [16:209]

### 9.9. Trinkets

Everyone loves a freebie. Post-it notes, pens, mouse pads, coffee mugs, stickers, and the like also spread the security message. If carefully chosen, the trinket will be both handy and readily in sight. [16:210]

### 9.10. Security Awareness day

Management may decide to have a security awareness day once or twice a year according to their needs. A few different ways to participate in the security awareness day, include: [17]

- Display computer security posters
- Present computer security briefings
- Show computer security videos, films or slides
- Modify the logon message on your computer system to notify users that Computer Security Day is 30 November, for example
- Initiate a computer security poster design contest for next year
- Demonstrate computer security software
- Publicise existing computer security policy
- Declare an amnesty day for computer security violators who wish to reform
- Announce “INFORMATION SECURITY DAY” in you internal newsletter
- Post “No Drinking” and “No Smoking” signs in computer areas
- Have a mini training session to provide all computer users with a basic understanding of computer security

- Install all security-related updates to your computer's operating system
- Plan to attend a computer security meeting or seminar

## 9.11. Professional Help

Some companies are designed to collect and disseminate computer security information and to supply resources to help users, systems administrators, managers, and security professionals to protect their data and systems better. A primary goal of these companies is to raise awareness of all computer systems users – from novice to expert – about computer security. This is perhaps the most important way of improving information systems security. [6]

Examples of such companies include Security Awareness Inc. (http://www.securityawareness.com) and the Computer Security Resource Clearinghouse (CSRC) (http://csrc.nist.gov/).

## 9.12. Summary

The fundamental value of IT security awareness programs is that they set the stage for training by bringing about a change in attitudes, which change the organisational culture. The cultural change is the realisation that IT security is critical because a security failure has potentially adverse consequences for everyone. Therefore, IT security is everyone's job. The tools that are used must be carefully selected:

"I hear and I forget.
I see and I remember.
I do and I understand." — Chinese Proverb

Awareness is the key to security!

Chapter 10 will discuss how an overall security awareness program can be implemented and managed within an organization.

# Chapter 10: Implementing and Managing the Security Awareness Program

## 10.1. Introduction

The implementation of information security in an organization must begin somewhere, as security of all systems does not magically appear overnight. It should be an incremental process that requires coordination, time and patience. [28:19]

This chapter explains how an overall security awareness program can be implemented and managed within an organization. Paragraphs 10.2.1 and 10.2.2 will describe 2 approaches, the bottom-up and top-down approach that can be used for implementing an effective information security awareness program. Paragraph 10.2.3 will explain how the development strategy can be used to support the implementation of a security awareness project.

## 10.2. Approaches for implementing an effective Information Security Awareness Program

The implementation of information security in an organization must begin somewhere, as security of all systems does not magically appear overnight. It should be an incremental process that requires coordination, time and patience. [28:19]

A methodology is a formal approach to solving a problem based on a structured sequence of procedures. Using a methodology ensures a rigorous process and avoids missing those steps that can lead to compromising the

end goal. The goal in this case is creating a comprehensive security posture. A methodology also increases the probability of success. Once a methodology has been adopted, the key milestones are established and a team of individuals is selected and made accountable to accomplish the project goals. [28:21]

A bottom-up or top-down approach can be used. Figure 15 explains the difference. [28:20]

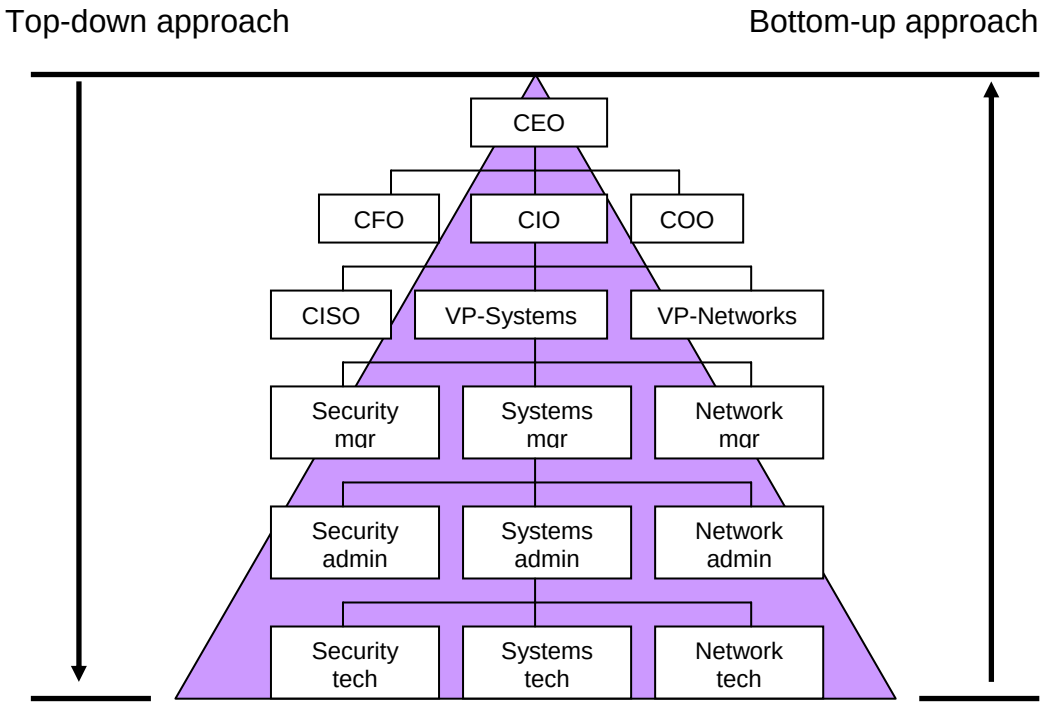



**Figure 15: Approaches to Security Implementation**

This figure will be described in detail in the following two paragraphs.

### 10.2.1. The Bottom-Up Approach

The bottom-up approach [28:19] is when security begins as a grassroots effort in which systems administrators attempt to improve the security of their systems. The technical expertise of the individual administrators is the key advantage of the bottom-up approach. These administrators possess in-

depth knowledge that can greatly enhance the development of an information security system as they are working with information systems on a day-to-day basis. They know and understand the threats to their systems and the mechanisms needed to successfully protect them.

Unfortunately, this approach seldom works, as it lacks a number of critical features, such as participant support and organizational staying power. Figure 15 depicts the levels of organization hierarchy involved with the bottom-up approach.

For any organization-wide effort to succeed, management must buy into and totally support an information security system or program. Such a system or program must have a champion that moves the project forward and ensures that it is properly managed. This executive must push for acceptance throughout the organization.

Typically, the champion is the chief information officer (CIO) or another senior executive as the vice president of information technology (VP-IT). Many of the midlevel administrators fail to make time for the project or dismiss it as a low priority without this high-level support.

Also, very critical to the success of this type of project is the involvement and support of the end users. These individuals are most directly impacted by the process and outcome of the project or program and must be included in the information security process. Key end-users should be assigned to a development team that have staying power. The processes and procedures must be documented and integrated into the organizational culture and must be adopted and promoted by the organization’s management.

### 10.2.2. Top-Down Approach

The top-down approach has a bigger probability of success. [28:20] The most significant difference between this approach and the bottom-up approach is the fact that with the top-down approach, the project or program is initiated by upper management who issue policy, procedures and processes, dictate the goals and expected outcomes or the program, and determine who is accountable for each of the required actions.

This approach has strong upper-management support, a dedicated champion, dedicated funding, a clear planning and implementation process, and the opportunity to influence the organizational culture.

The best approach for implementing an information security program in an organization with little or no formal security in place is to use a formal development strategy. [28:21] This development strategy consists of the following 6 components or phases [28:22], where each phase begins with the results and information gained from the previous phase (see figure 16): [28:21]

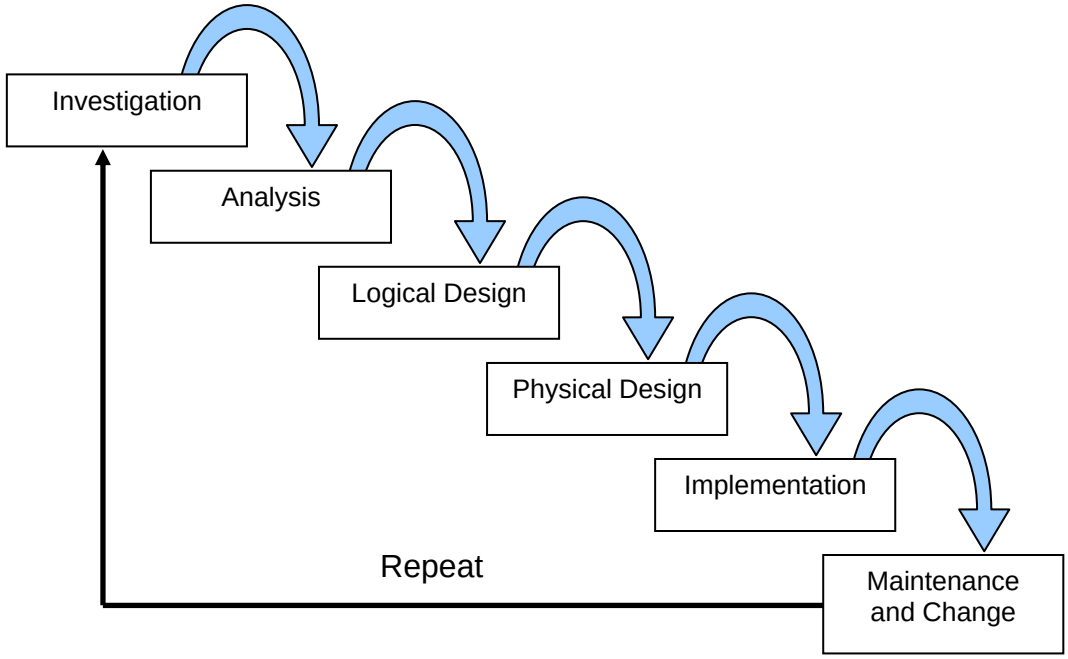



**Figure 16: The Development Strategy with the 6 phases**

***Investigation**:* This is the first and most important phase. What is the problem the system is being developed to solve? The investigation phase begins with the examination of the event or plan that initiates the process. The objectives, constraints, and scope of the project are specified during this phase. The perceived benefits and the appropriate levels of cost for those benefits are evaluated when the preliminary cost benefit analysis is developed. At the conclusion of this stage, and at every stage following, a feasibility analysis is performed. This is done to assess the economic, technical, and behavioural feasibilities of the process and ensures that implementation is worth the organization's time and effort. [28:22]

***Analysis***: This phase begins with the information gained during the investigation phase. During the analysis phase assessments of the organization are done, the status of current systems is determined, and the capability to support the proposed systems is assessed. What the new system is expected to do and how it interacts with existing systems is analysed. This phase ends with documentation of the findings and an update of the feasibility analysis. [28:22]

***Logical Design***: The information gained from the analysis phase is used to begin creating a solution system for a business problem. The first and driving factor must be the business need. Based on this business need, applications are selected that are capable of providing needed services. Then, based on the applications needed, data support and structures capable of providing the needed inputs are chosen. Finally, based on all the above, specific technologies to implement the physical solution are delineated. The logical design is, therefore, the blueprint for the desired solution. Another feasibility analysis is performed. [28:23]

***Physical Design***: Specific technologies are selected to support the alternatives identified and evaluated in the logical design during this phase. The selected components are evaluated and final designs that integrate various components and technologies are designed. After another feasibility

analysis, the entire solution is presented to the organizational management for approval. [28:23]

***Implementation***: Any needed software is created during the implementation phase. Components are ordered, received, and tested after which users are trained and supporting documentation created. After all components have been tested individually, they are installed and tested as systems. The sponsors are presented as with the system for a performance review and acceptance test after a feasibility analysis has been prepared. [28:23]

***Maintenance and Change***: This is the longest and most expensive phase of the process. It consists of the tasks necessary to support and modify the system for the remainder of its useful life cycle. Formal development may conclude during this phase, but the life cycle of the project continues until it is determined that the process should being again from the investigation phase. The system is periodically tested for compliance and upgrades, updates and patches are managed. The system that supports the organizations must change as the needs of the organization change. When the current system can no longer support the evolving mission of the organization, the project is terminated and a new project is implemented. [28:23]

### 10.2.3. Using the development strategy to support the implementation of a Security Awareness project

The same phases as described in paragraph 10.2.2 can be adapted to support the specialized implementation of a security awareness project. The process might differ in intent and specific activities, but the overall methodology is the same. The fundamental process is the identification of specific threats and the creation of specific controls to counter those threats. Using this development strategy will help to unify the process and to make it a coherent program rather than a series of random seemingly unconnected actions. The phases of the development strategy for this type of project can be as follows: [28:24]

***Investigation**:* This phase begins with a directive from upper management that dictates the process, outcomes, and goals of the project, as well as its budget and other constraints. The investigation phase can begin with a statement of the company security policy that outlines the implementation of a security program within the organization. Teams of responsible managers, employees and contractors are organized, problems analysed and the scope defined. Finally, an organizational feasibility analysis is performed to determine whether the organization has the resources and commitment necessary to conduct a successful security analysis and design.

***Analysis**:* The documents from the investigation phase are studied during the analysis phase. A preliminary analysis is conducted of the existing security policies or programs, along with documented current threats and associated controls. The relevant legal issues that could impact the design of the security solution is also analysed. Risk management also begins in this phase. Risk management is the process of identifying, assessing, and evaluating the levels of risk facing the organization, specifically the threats to the organization's security an to the information stored and processed by the organization.

***Logical Design**:* This phase, as explained before, develops the blueprints for security, and examines and implements key policies that influence later decisions. Critical planning is also developed for incident response actions to be taken in the event of partial or catastrophic loss. Planning with regards to Continuity planning, Incident response and disaster recovery is done. Solutions are documented and a feasibility study is done to determine whether or not the project should continue or should be outsourced.

***Physical Design**:* The security technology to support the blueprint outlined in the logical design is evaluated, alternative solutions generated, and a final design agreed upon. Included at this time are the designs for physical security measures to support the proposed technological solutions. At the end of the physical design phase, a feasibility analysis is done to determine

the readiness of the organization for the proposed project. All parties involved have a chance to approve the project before implementation begins.

***Implementation**:* The security solutions are acquired, tested, and implemented, and tested again. Personnel issues are evaluated and specific training and education programs conducted. Finally, the entire tested package is presented to upper management for final approval.

***Maintenance and Change**:* This is perhaps the most important phase during the implementation of a security awareness project, given the high level of ingenuity in today's threats. Constant monitoring, testing, modification, updating, and repairing are needed. Threats from outside as well as from within must be constantly monitored and checked with continuously new and more innovative technologies.

## 10.3. Summary

Computer Security depends on all of us, not just the technical employees who set up and monitor the organisations network, the traditional area people tend to focus regarding security. Every organisation should have some sort of computer security awareness training for their employees. The security of your computer networks depends on it.

This chapter explained how an overall security awareness program can be implemented and managed within an organization. Paragraphs 10.2.1 and 10.2.2 described the bottom-up and top-down approach that can be used for implementing an effective information security awareness program. Paragraph 10.2.3 explained how the development strategy can be used to support the implementation of a security awareness project.

There were two primary objectives that this project attempted to achieve:

- To develop an effective information security awareness program that can be implemented within an organization. A web-based security

awareness program were developed that should form part of a bigger and more comprehensive security awareness program. This is only a prototype and can be adapted to the organization's unique needs and look and feel.

- A study was done in the area of social psychology and human performance systems with a view to identify the principles and techniques that was developed over many years of research into the modification of people's behaviour, and to identify where these techniques and principles can potentially be incorporated into the awareness program so that it can become more effective.

In my view, the objectives of the project and dissertation were successfully met. This project and dissertation can be used by organizations to assist them in implementing an effective Information Security Awareness Program.

# References


[1] W3C Security Resources; http://www.w3.org/Security; Lincoln D. Stein; 6 April 1999

[2] Education/FAQ; http://www.securitywatch.com/EDU/fr_education.html; 3 May 2001

[3] Vulnerability Knowledge; http://www.securitywatch.com/; 3 May 2001

[4] Back to Information Security Basics; Robert Geiger; http://www.info-defense.com ; 2000

[5] Your End Users May Be Undermining Your Security Efforts!; www.securityawareness.com; 2000

[6] Security Awareness inc.; "Awareness is the key to security"; http://www.securityawareness.com/index2.htm; Copyright 2000

[7] Barbara Guttman, Robert Bagwill; "Sample policy areas"; http:///csrc.nist.gov/isptg/html/ISPTG-5.html; 31July 1997

[8] Security Awareness inc.; "Security awareness inc. introduction"; http://www.securityawareness.com/page1.htm; Copyright 2000

[9] Wilson, M; "Information Technology Security Training Requirements: A Role- and Performance-Based Model"; http://csrc.nist.gov/nistpubs/800-12/; April 1998.

[10] Security Awareness inc.; "Monthly Poster Subscription Program"; http://www.securityawareness.com/postersub.htm; Copyright 2000

[11] Security Awareness inc.; "Security awareness screen saver"; http://www.securityawareness.com/scrnsaver.htm; Copyright 2000

[12] Security Awareness inc.; "Intranet site"; http://www.securityawareness.com/intranet.htm; Copyright 2000

[13] Security Awareness inc.; "Brochures"; http://www.securityawareness.com/brochure.htm; Copyright 2000

[14] Security Awareness inc.; “Interactive multimedia Computer based Training”; http://www.securityawareness.com/multimed.htm; Copyright 2000

[15] Security Awareness inc.; “Custom awareness programs”; http://www.securityawareness.com/custom.htm; Copyright 2000

[16] Alexander, M; “The Underground Guide to Computer Security”; Addison-Wesley, United States; 1996

[17] Ohringer, L; “50+ Ways to Participate in Computer Security Day”; http://www.cio.ufl.edu/tips.htm; 26October 1999.

[18] Futuremedia Learning; “Solstra 2000 E-learning – planned, delivered and managed”; 2000

[19] Syberworks Inc.; “Syberworks Learning Centre”; 2000

[20] FlextrainingInc.; “Flextraining – Courseware made simple”; 2000

[21] Cluley, Graham; “You Are The Weakest Link, Goodbye”; http://www.itsecurity.com/papers/sophos.htm; 2000

[22] Bruce Schneier; “Secrets & Lies Digital Security in a Networked World”; Copyright 2000

[23] Helsing, Cheryl. Swanson, Marianne. Todd, Mary Anne; “Computer User’s Guide to the Protection of Information Resources”; http://nsi.org/Library/Compsec/usergide.txt

[24] Federal Computer Security Program Managers Forum and the Federal Information Systems Security Educators' Association (FISSEA); "NIST Special Publication 800-16, Information Technology Security Training Requirements: A Role- and Performance-Based Model."; April 1998; http://patapsco.nist.gov/itl/div893/gits/glossary.htm

[25] Felkenberg, Ryan; “Empowered learning for new technologies”; Hi-Performance Learning; 2001

[26] Deist, Leon; Internal Eskom document; 2001

[27] Benade, C; Internal Iscor document; 2001

[28] Michael E. Whitman & Herbert J. Mattord; “Principles of Information Security”; Thomson Course technology; 2003

[29] National security telecommunications and information systems security; “National training standard for information systems security (infosec) professionals”; 20 June 1994; File 4011; cited 1 February 2002; http://www.nstissc.gov/Assets/pdf/4011.pdf

[30] Tuesday, Vince; “Human factor details best-laid security plans”; Computing SA; Vol 21 No 16: 7 May 2001; p20

[31] The SANS Institute; “The SANS Security Policy Project”; 2002-2003; http://www.sans.org/resources/policies

[32] ISO17799 World; “What is ISO17799?”; 2002; http://www.iso-17799-security-world.co.uk/what.htm

[33] Information technology – Code of practice for information security management; ISO/IEC 2000; Reference number: ISO/IEC 17799:2000(E) first edition

[34] Tims, Rick; “Social Engineering: Policies and Education a Must”; 16 February 2001; URL: http://www.sans.org/rr/social/policies.php