ESTABLISHING AN INFORMATION SECURITY CULTURE IN ORGANIZATIONS: AN OUTCOMES BASED EDUCATION APPROACH

by

Johannes Frederick van Niekerk

Dissertation

submitted in fulfillment
of the requirements
for the degree

Magister Technologiae

in

Information Technology

in the

Faculty of Engineering

of the

Nelson Mandela Metropolitan University

Promoter: Prof. Rossouw Von Solms

2005

Abstract

Information security is crucial to the continuous well-being of modern organizations. Humans play a significant role in the processes needed to secure an organization's information resources. Without an adequate level of user **co-operation** and **knowledge**, many security techniques are liable to be misused or misinterpreted by users. This may result in an adequate security measure becoming inadequate. It is therefor necessary to educate the organization's employees regarding information security and also to establish a corporate sub-culture of information security in the organization, which will ensure that the employees have the correct attitude towards their security responsibilities. Current information security education programs fails to pay sufficient attention to the behavioral sciences. There also exist a lack of knowledge regarding the principles, and processes, that would be needed for the establishment of an corporate sub-culture, *specific* to information security. Without both the necessary knowledge, **and** the desired attitude amongst the employee, it will be impossible to guarantee that the organization's information resources are secure. It would therefor make sense to address both these dimensions to the human factor in information security, using a single integrated, holistic approach. This dissertation presents such an approach, which is based on an integration of sound behavioral theories.

Acknowledgements

My grateful thanks goes to the following people:

My promoter, Professor Rossouw von Solms. His knowledge, guidance, support and patience have played a major role in the completion of this dissertation.

My wife, Ezanne, for her support, especially when things were not going according plan.

Contents

List of Figures

Chapter 1

INTRODUCTION

1.1 Background

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

In order to avoid loss or damage to this valuable resource, companies need to be serious about protecting their information. This protection is typically implemented in the form of various security controls. However, it is very difficult to know exactly which controls would be required in order to guarantee a certain acceptable minimum level of security (Barnard & Von Solms, 2000). Furthermore, managing these controls to see that they are always up to date and implemented uniformly throughout the organization is a constant headache to organizations. This problem is compounded even further by the enormous growth-rate of the Internet and the demand for business-to-business e-commerce, which forces an organization to worry not only about their own security but about the security of their business partners

as well. Managing information security is a serious challenge and can only be achieved successfully on a large scale with the help of a holistic approach based on internationally acceptable standards (Eloff & Von Solms, 2000; Von Solms, 1999).

Several standards and codes of practice exist to assist organizations in the management of their information security efforts. Some of the better known examples would include the ISO/IEC 17799 (2000), and the Guidelines for the Management of Information Technology Security (GMITS) (ISO/IEC, 1995). These standards and codes of practice provide organizations with guidelines specifying how the problem of managing information security should be approached. One of the key controls identified by all the major IT Security standards published to date is the introduction of a corporate information security awareness program. The purpose of such a program is to educate the users about information security or, more specifically, to educate users about the individual roles they play in the effectiveness of one type of control, namely, operational controls.

Information Security controls can generally be sub-divided into three categories: physical controls, technical controls and operational controls. Physical controls deal with the physical aspects of security, for example; a physical control might state that an office containing sensitive documents should have a lock on the door. Technical controls are controls of a technical nature; for example, forcing a user to authenticate with a unique username and password before allowing the user to access the operating system would be a technical control. The third category, operational controls, consists of all controls that deal with human behavior (Thomson, 1998).

Employees, whether intentionally or through lack of knowledge, are the greatest threat to information security (Thomson, 1998) and because these operational controls rely on human behavior, hence employee behavior, they are the weakest link in information security. Unfortunately both physical and technical controls rely heavily on these operational controls for effectiveness. As an example, an operational control might state that users leaving their offices must logoff from the operating system and lock their office doors. If a user were to ignore this control, both the technical control forcing authentication and the physical control of having a lock on the door would be rendered useless. Thus anyone who thinks that security products, i.e. tech-

nical and physical controls, alone offer true security is settling for the illusion of security (Mitnick & Simon, 2002).

According to Dhillon (1999), the user education program is singled out because increasing awareness of security issues is the most cost-effective control that an organization can implement. This control is so cost-effective because it ensures that all users are aware of the operational controls without which most other controls cannot operate efficiently. Special care should be taken that the awareness program is presented in such a form that it does not go beyond the comprehension of the average user. The emphasis should be to build an organizational sub-culture of security awareness.

Many recent studies have shown that the establishment of an information security sub-culture in the organization is in fact necessary for effective information security (Eloff & Von Solms, 2000; Von Solms, 2000). Some of these studies have presented definitions of what an information security culture is, but currently there exists very little knowledge on how such a culture can be established. A lot of knowledge exits in the management sciences regarding corporate culture in general (Schein, 1999a; Alpander & Lee, 1995; Woodall, 1996), but very little knowledge exists regarding the applicability of this knowledge to information security specifically. It is, however, clear that an user education program will have to play a major role in the establishment of such a culture.

The currently available standards and codes of practice do give some guidelines as to the contents of such an educational program. Unfortunately these guidelines are not complete enough to be used as a framework for such an educational program. For example, the ISO/IEC 17799 (2000) states that all employees of the organization and, where relevant, third party users, should receive appropriate training. This training should include security requirements, legal responsibilities and business controls, as well as training in the correct use of information processing facilities before access to information or services is granted (ISO/IEC 17799, 2000, p. 9). This statement, even though it greatly clarifies the issues relating to what should be taught in an information security educational program, raises another question namely, what is appropriate training.

It would make sense for an organization's awareness program to cover all the controls specified by the specific information security standard used by

the organization. However, it is clearly not appropriate to expect each and every end-user to be educated about all the controls specified by a standard such as the ISO/IEC 17799 (2000). According to ISO/IEC TR 13335-1 (2004), another popular information security standard, each employee should know his or her role and responsibility, his or her contribution to IT security, and share the IT security vision (ISO/IEC TR 13335-1, 2004, p. 15). From this one can deduce that it is necessary to tailor the awareness educational material used to the needs of the individual user.

Neither the ISO/IEC 17799 (2000) nor ISO/IEC TR 13335-1 (2004) provides any guidelines as to which controls should be included or excluded for a specific type of user in such an educational program. These standards also neglect to mention the appropriate educational principles to which such a program would have to adhere. This lack of adherence to proper educational principles is further compounded by the fact that the user education programs used in organizations are often designed by IT professionals and not by educationalists. There are also several other factors that render current awareness programs ineffective, for example:

- The actual contents of the program are not difficult to understand or to present, so there is a distinct possibility of the course attendees becoming bored (Thomson, 1998, p. 13).
- Less than 25% of CEO's see information security as important (Thomson, 1998, p. 17).
- Current programs are inadequate, not comprehensive enough and mostly target only end-users (Thomson, 1998, p. 26)
- Current programs fail to pay attention to behavioral theories. (Siponen, 2001)

If one takes into account the importance of the user education program in establishing information security in an organization, it would make sense that these programs should be designed according to sound educational principles. Furthermore, the aim of the user education program is not to prepare the users for further levels of formal education, but rather to help them achieve information security know-how for use in their everyday jobs. The educational methodology used should thus be chosen accordingly.

One educational methodology that could play a role in these programs is outcomes based education (OBE). OBE is an approach to teaching and learning which stresses the need to be clear about what learners are expected to achieve. The educator states beforehand what "outcome" is expected of the learners. The role of the educator is then to help the learners achieve that outcome (Siebörger, 1998). OBE might in fact be ideally suited for use in such programs since the aim of OBE is not to prepare a learner for exams or further levels of formal education, but rather to help learners achieve a specific goal, in this case information security awareness. However there is little or no information available about the suitability of OBE for information security education.

1.2 Problem Statement

Information security is dependent on the behavior of the users in order to be effective. The establishment of a corporate culture of information security is one way to positively influence user behavior. An information security education program is one of the components that can contribute towards fostering such a culture.

Currently, information security education programs do exist, but, even though the aim of such programs should be to change user behavior, current programs fail to pay attention to behavioral theories (Siponen, 2001).

Several educational models exist that might be appropriate for information security education. One such model is outcomes based education (OBE). However, little or no knowledge exists regarding the suitability of OBE as a methodology for creating corporate information security education programs.

The problem facing organizations is therefore twofold:

- Information security depends on the humans involved in the process of securing information resources. These humans must have both the necessary knowledge, and the correct attitude towards information security. An information security user education program could be used to teach organizational employees the requisite knowledge. However, current user education programs fail to pay sufficient attention to behavioral theories. Outcomes based education is a pedagogical methodology that *could* be suitable for the creation of information security

user education programs. Little, or no, knowledge exists regarding the suitability of outcomes based education for the creation of information security education programs.

- Secondly, the fostering of an organizational sub-culture of information security is necessary, in order to ensure that the organization's employees have the required attitude towards information security. The problem of establishing, or changing, corporate culture in general has been well studied. However, little, or no, knowledge exists on **how** such a sub-culture, *specific* to information security, could be fostered.

Both the above problems are closely related, due to the large degree of co-dependency an organization's overall information security strategy will have on both employee knowledge, and employee attitude. It would therefor make sense to attempt to address both these problems using an integrated holistic approach.

1.3 Objective

The primary objective of this dissertation is to develop a holistic framework for the establishment of a corporate sub-culture of information security compliance. This framework should use educational principles that directly contribute towards the establishment of such an information security sub-culture, and that will also produce a high level of user awareness and behavioral discipline.

This framework will be based on a combination of various behavioral sciences as well as outcomes based educational principles. The framework should also provide guidelines for the creation and management of information security education programs.

Secondary objectives include:

- Identifying the educational needs specific to information security in a corporate environment.

- Identifying behavioral theories that could play a role in such educational programs.

- Evaluating outcomes based education to determine its suitability for the creation of such programs.
- Identifying the major elements that should play a role in the active changing of a corporate culture.
- Integrating the elements from various disciplines into a single holistic approach.

1.4 Methodology

The methodology used in this dissertation comprises of several research methods. Initially a literature study was conducted to establish the current state of information security awareness education in modern businesses. This literature study was followed by literature studies to establish the educational principles that should be adhered to in such programs in order for them to be successful. The information gathered during the literature studies was analyzed and evaluated. The initial literature studies were then expanded into the area of outcomes based education (OBE). The information gathered during this literature study into OBE was explored. A critical evaluation was conducted to determine whether OBE can match the needs of information security, as established in earlier studies.

A third literature study was then conducted into corporate culture. The aim of this literature study was to identify the behavioral principles and processes needed to actively change, or introduce, such a culture. The information gathered during this literature study was analyzed. A critical evaluation was conducted in order to determine which principles and processes should be applied to the fostering of an information security sub-culture. The suitability of these principles and processes, to information security, was then extensively argued.

Finally all previously gathered information was integrated, using a combination of modelling techniques and analytical argumentation. This integrated model was then used to construct a single holistic framework for the fostering of an organizational sub-culture of information security. The elements of this framework were introduced and argued, with the help of an example, in order to demonstrate its suitability to information security.

1.5 Layout Of The Dissertation

Chapter 1 serves as an introduction to the disciplines involved in this project. It outlines the problem itself, the objectives of this dissertation and the methodology used. The second chapter discusses information security in general. It defines information security and discusses the different elements and services needed for information security. It then examines the process of information security with specific emphasis on the role humans play in this process. Two dimensions to the human factor in information security, namely knowledge, and attitude, are identified in this chapter. Chapter 3 examines information security education, which can be used to address the knowledge dimension of the human factor in information security. It briefly examines issues surrounding the scope of security education programs. It then proposes and argues a set of criteria that should be met by an educational methodology, in order for such a methodology to be suitable for information security education. The fourth chapter discusses outcomes based education (OBE). It explains what outcomes are, discusses the basic premises of OBE, and explores curriculum design using OBE. Lastly, this chapter attempts to show that OBE matches the requirements for information security education, by linking OBE to the criteria defined in the previous chapter. In chapter 5 this dissertation focuses on the second dimension to the human factor in information security, namely attitude. This chapter examines corporate culture, which can be used to address issues regarding employee attitude towards information security. The chapter defines corporate culture and then expands this definition towards an information security culture. This chapter then examines organizational learning theory in general. Lastly a process for changing corporate culture is presented, and a list of psychological factors that should be considered in a cultural change process is give. Chapter 6 combines the concepts introduced in previous chapters into a single, holistic, outcomes based, framework for the introduction of an information security sub-culture in organizations. The proposed framework is presented and argued extensively. The example of introducing a sub-culture of proper password security is used throughout this chapter to assist with the necessary explanations. Finally, this dissertation is concluded in chapter 7, which briefly summarizes the finding in this dissertation and present areas

for further study leading from this dissertation.

1.6 Summary

This chapter briefly introduces information security and its importance in modern organizations. The role humans play in an organization's overall information security effort was identified as a *weak link*. Both human knowledge about information security, and human co-operation are needed in order for an organization's information security efforts to be successful. In order to address this *weak link*, organizations need to educate their employees regarding information security. The aim of such a user education program should be to establish an organizational sub-culture of information security. Two problems regarding such a user education program, and the fostering of an organizational sub-culture of information security, were identified. The methodology used in this dissertation, to address the identified problems, is outlined. Finally a brief outline of the chapters in this dissertation is given.

Chapter 2

INFORMATION SECURITY

This chapter discusses information security in general. It defines information security and discusses the different elements and services needed for information security. It will then examine the process of information security with specific emphasis on the role humans play in this process.

2.1 Introduction

Humans today live in an emerging global information society, with a global economy that is increasingly dependent on the creation, management, and distribution of information resources (O'Brien, 1999, p. 11). Information and its use permeate all aspects of modern society. Today, most organizations need information systems to survive and prosper (Laudon & Laudon, 2002, p. 4). Information has become such a valuable commodity in modern society that a large part of the workforce in many nations consists of knowledge workers (O'Brien, 1999, p. 11). These knowledge workers spend most of their time communicating and collaborating in teams and workgroups creating, using, and distributing information (O'Brien, 1999, p. 11).

This information is typically stored on computers in systems known as Information Systems. An Information System (IS) is an organized combination of people, hardware, software, communications networks, processes and data resources that collects, transforms, and disseminates information in an organization (O'Brien, 1999, p. 9),(Whitman & Mattord, 2003, p. 15). Even though it is possible to have non-computerized information systems, this dissertation will focus on electronic-based information systems, systems

that use hardware, software, networks and computer based data management techniques or other forms of Information Technology.

The advent of Information Technology (IT) has had a profound impact on modern society. It affects all aspects of today's businesses from top management right down to operational level. In order to stay competitive in this information age, organizations typically make large investments in terms of time, money and energy to streamline the processes of capturing, generating and distributing vital information resources throughout the organization. Unfortunately, this distribution of mission-critical information throughout the company also increases the likelihood of misuse or damage to information resources (Haag et al., 2000). Such misuse or damage could have devastating effects on an organization's overall wellbeing. In order to avoid loss or damage to this valuable resource, companies need to be serious about protecting their information. The technologies and processes used to provide this protection of information resources is collectively known as Information Security.

2.2 Information Security Defined

The aim of Information Security is to ensure business continuity and minimize business damage by preventing and minimizing the impact of security incidents (Von Solms, 1998). Information Security can be defined in many ways. The international standard ISO/IEC 17799 defines information security as the preservation of the **confidentiality**, **integrity** and **availability** of information (ISO/IEC 17799, 2000, p. 1). Information, in the context of the ISO/IEC 17799 standard, can take on many forms. It can be printed or written on paper, stored electronically, transmitted by post or electronic means, shown on films, spoken in conversation, etc. (ISO/IEC 17799, 2000, p. 1). Since the primary focus of this dissertation is on information as it exists in the context of computer based information systems, a more focused definition used for information security in this context is also required.

The international standard ISO/IEC TR 13335-1 defines information technology security, or IT security, as all aspects relating to defining, achieving and maintaining **confidentiality**, **integrity**, **availability**, **non-repudiation**, **accountability**, **authenticity**, and **reliability** of information resources

(ISO/IEC TR 13335-1, 2004, p. 5). A few concepts in these two definitions need closer examination. Firstly, it should be clear that information security is not a product or a technology. Information security is a process (Mitnick & Simon, 2002, p. 4). This process might require the use of certain products, but it is not something that can be bought off the shelf.

The second important factor to note about the above definitions is that ISO/IEC 17799 defines information security in terms of the properties, or characteristics that secure **information** should have, namely, confidentiality, integrity and availability. Conversely ISO/IEC TR 13335-1 adds additional characteristics, which in this context could also be better described as services that should be provided by secure **information resources**, namely; non-repudiation, accountability, authenticity, and reliability. The difference between secure information and secure information resources is important to note. A secure information resource could include any entity from which information was received or to which information was sent. Thus, in terms of computer-based systems, the information alone cannot be deemed secure unless all resources, and processes, dealing with that information is secure as well. The above-mentioned characteristics will now be examined in more detail.

The first three characteristics, confidentiality, integrity and availability, are commonly known as the **CIA** triangle and has been considered the industry standard for computer security since the development of the mainframe (Whitman & Mattord, 2003, p. 10). These three characteristics are as important today as they were at the inception of information security, but no longer encompass the constantly changing environment of the computer industry (Whitman & Mattord, 2003, p. 10). The additional characteristics were added to the definition to address the additional security needs of organizations in today's inter-networked business environment, hence their inclusion in the definition for information *technology* security. A clear understanding of the meaning of these characteristics and services is essential to an understanding of information-, and information technology security, therefore the following sub-sections will briefly discuss each of the characteristics individually.

2.2.1 Confidentiality

Confidentiality is defined by both ISO/IEC TR 13335-1 and ISO/IEC 17799 as the property that information is not made available or disclosed to unauthorized individuals, entities, or processes (ISO/IEC 17799, 2000, p. 1), (SABS, 2002, p. 10). Confidentiality is about ensuring that only those who have 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 accessing the information (Whitman & Mattord, 2003, p. 11). Confidentiality deals with the "for your eyes only" property of information. If a person, entity, or process, gains access to information that he/she/it are not authorized to access, the confidentiality of that information has been compromised. It is important to realize that, due to modern encryption techniques, gaining unauthorized possession of information does not necessarily breach the confidentiality of the information (Whitman & Mattord, 2003, p. 14).

2.2.2 Integrity

Both ISO/TEC TR 13335-1 and ISO/IEC 17799 define integrity as the property of safeguarding the accuracy and completeness of assets (ISO/IEC 17799, 2000, p. 1), (SABS, 2002, p. 21). Another definition would be that the integrity of information is the quality or state of being whole, complete, and uncorrupted (Whitman & Mattord, 2003, p. 13). If information has integrity, it means that the user(s) can ascertain that this information is in its original state and has not been altered (Laudon & Laudon, 2002, p. 447). The integrity of information is threatened when the information is exposed to corruption, damage, destruction, or other disruption of its authentic state. Many computer viruses and worms have been created with the specific purpose of corrupting data. Loss of integrity could also result from internal sources, such as data transmission errors (Whitman & Mattord, 2003, p. 13).

2.2.3 Availability

Availability, the third of the "traditional" characteristics of secure information, is defined in ISO/IEC TR 13335-1, and in ISO/IEC 17799, as the property of being accessible and usable upon demand by an authorized entity

(ISO/IEC 17799, 2000, p. 3, Section 2.1),(SABS, 2002, p. 7). Availability enables users who need to access information to do so without interference or obstruction, and to receive it in the required format (Whitman & Mattord, 2003, p. 10). However, availability, as defined above by the two international standards, does not imply that the information should be accessible to any user (Whitman & Mattord, 2003, p. 10). It requires that the user be verified as an *authorized* entity. Thus, provided the user is allowed to access the information, availability implies that the information should be available when and where needed, and that it should be in the correct format (Whitman & Mattord, 2003, p. 10). Loss of availability could result from several factors. For example, a power failure could cause network downtime, which in return would cause information to be unavailable. Denial of Services attacks, a type of malicious attack usually aimed at an organization's Internet services, are directly aimed at compromising the availability of information.

2.2.4 Non-repudiation

With the advent of e-commerce, and the increasing use of information technology as a tool for business communications, it became necessary to add non-repudiation to the definition of secure information. Non-repudiation is the ability to prove that an action or event has taken place, so that this event or action cannot be repudiated later (SABS, 2002, p. 28). Thus, non-repudiation should be seen as a *service* provided by an information source, rather than a property of the information itself. Non-repudiation is vital if the information in question is to be used as evidence in a court of law. The international standard ISO/IEC WD 13888-1 defines the following subcategories of non-repudiation services (SABS, 2002, p. 28):

- Non-repudiation of delivery token (NRD token): A data item, which allows the originator of a piece of information to establish non-repudiation of delivery for a message. Thus, a token issued to the sender of information, which proves that the information was received by the intended recipient.

- Non-repudiation of origin token (NRO token): A data item, which allows recipients to establish non-repudiation of the origin for a message.

Thus, a token issued to the receiver of information, which proves that the sender of the information is who he/she/it claims to be.

- Non-repudiation of submission token (NRS token): A data item, which allows either the originator or the delivery authority to establish non-repudiation for a message (information) having been submitted for transmission. Thus, a token issued to both the sender of information and the entity responsible for delivering the information, which proves this information was "handed over" to the entity responsible for delivery, by the sender.

- Non-repudiation of transport token (NRT token): A data item, which allows either originator, or the delivery authority, to establish non-repudiation of the transport for a message. Thus, a token issued to both the sender of information and the entity responsible for delivering the information, which proves this information was transported by the entity responsible for its delivery to its intended destination.

Non-repudiation services are especially important in an electronic-commerce context. For example; If an email is to be used to negotiate a legally binding contract, the following tokens would be needed during the process of sending and receiving such an email. Firstly the sender of the message would receive an NRS token, which proves that the message has been submitted for delivery. The delivery authority would receive a similar token, which proves the identity of the sender for this message. Once the message arrives at its destination the sender would receive an NRT token. This proves to both the sender and the delivery authority that the message has arrived at its destination. When the recipient now receives this message from the delivery authority, the recipient is issued with an NRO token, which proves the identity of the sender of this message. At the same time, the sender is issued with an NRD token, which proves that the recipient has indeed received the message. Clearly, in e-commerce, these non-repudiation services plays an integral role in establishing trust between parties who have never met in person.

2.2.5 Accountability

Accountability as a property of a secure information resource goes hand in hand with the property of non-repudiation. The ISO/IEC TR 13335-1 defines accountability as a property that ensures that the actions of an entity may be traced uniquely to the entity (SABS, 2002, p. 3). Without the ability, for example, to trace the actions of a person uniquely to that person, it would not be possible to hold such a person accountable for their actions. Accountability in this sense should not be confused with accountability **for** information security. Accountability **for** information security will be discussed in more detail in a later section.

2.2.6 Authenticity

The authenticity of an information resource is a property that is closely linked to the integrity of the information itself. The ISO/IEC TR 13335-1 defines authenticity as a property that ensures that the identity of a subject or resource is the one claimed. Authenticity applies to **entities**, such as, users, processes, systems and information (SABS, 2002, p. 7). The authenticity of information depends on the ability to authenticate the information. Authentication is the ability of each party in a transaction to ascertain the identity of the other party (Laudon & Laudon, 2002, p. 447). If a user or entity is fooled into believing the wrong information is the right information, for example mistaking a spoof-site on the Internet for the real site it is mimicking, the authenticity of the information resource has been compromised and the integrity of the information itself would thus be lost. Clearly, non-repudiation services would also depend on the ability to authenticate all entities involved in a transaction.

2.2.7 Reliability

The last property of secure information listed in the definition is defined in the ISO/IEC TR 13335-1 standard as the property of consistent intended behavior and results (SABS, 2002, p. 36). This property basically means that an information resource should be consistent, in terms of both its integrity and availability. It also means that the results to a particular query against the information should be consistent. In other words, if the same question is

asked, with the same parameters given, the answer returned should be the same, otherwise the reliability of the information is questionable.

Without the **confidentiality, integrity, availability, non-repudiation, accountability, authenticity,** and **reliability** of information resources, information cannot be deemed secure. All of the above play an integral role in information security, and should be deemed equally important. It is, however, possible for one or more of these characteristics or services to **seem to be more applicable** in specific scenarios than the other characteristics. This applicability would depend on the nature of the information itself. For example, the integrity of inflationary statistics is of obvious importance for economists, whilst the confidentiality of the same data appears to be unimportant. Everyone would probably be allowed to have access to such information, thus the confidentiality *seems to be* unimportant. However, by definition, a breach of confidentiality would only occur if an *unauthorized entity* obtained the information. Since everyone would be an authorized user of inflationary statistics, in this case, the confidentiality of the information would actually be maintained. In an organizational context, ensuring the security of the organization's information is thus not a case of deciding which characteristics or services are applicable, but rather a case of *defining the authorized entities, and other parameters* for any given piece of information correctly. In order to define these parameters, a structured process is required. Without such a structured process, important parameters might easily be overlooked.

2.3 Information Security - The Process

The ultimate aim of the information security process is the protection of all information assets. These assets could have vulnerabilities to both internal- and external threats. The information security process attempts to reduce the risk posed by such vulnerabilities through the selection, implementation and maintenance of security controls. These controls serve to reduce the risk to an acceptable level. When selecting the security controls to implement in an organization, it is important to refer to accepted international standards (Von Solms, 1999). Basing the organizational information security policy on internationally accepted standards is especially important for organizations

wanting to prove to their trading partners that their information resources are safe (Von Solms, 1999). Several internationally accepted standards and codes of practice exists to assist organizations in the implementation and management of an organizational information security strategy. Some of the better known examples would include the ISO/IEC 17799 (ISO/IEC 17799, 2000) and the Guidelines for the Management of Information Technology Security, ISO/IEC 13335 also known as GMITS (ISO/IEC TR 13335-1, 2004). These standards and codes of practice provide organizations with guidelines specifying how the problem of managing information security should be approached (Von Solms, 1999).

The controls listed in these information security standards can generally be sub-divided into three categories: Physical controls, Technical controls and Operational controls, the last of which collectively includes business controls, administrative controls, managerial controls, and procedural controls (Thomson, 1998). Each of these will be briefly described.

2.3.1 Physical Controls

Physical controls deal with the physical aspects of security, for example; a physical control would be the lock on the door of an office containing sensitive documents. Physical controls constitute the oldest form of information security. It began in the early days of computing, almost immediately after the first mainframes were developed and put to use. In those days the primary threats to security were physical theft of equipment, espionage against the products of the systems, and sabotage (Whitman & Mattord, 2003, p. 5).

2.3.2 Technical Controls

With the introduction of computer networks, databases, shared memory, etc, physical controls alone were no longer deemed sufficient protection (Whitman & Mattord, 2003, p. 5). Security was needed to protect not only the physical location of the computer or information resource, but also the integrity of the data (Whitman & Mattord, 2003, p. 7). This protection was implemented in the form of technical controls. Technical controls are controls of a technical nature, usually software based, for example; forcing a user to authenticate

with a unique username and password before allowing the user to access the operating system would be a technical control. According to Von Solms (2000) these controls constituted the "first wave" of information security.

This first wave, primarily mainframe based, approached information security as something which can be addressed by using the "built-in" facilities of the mainframe operating systems - facilities like access control lists, user-ids and passwords (Von Solms, 2000). At this stage, aspects like information security policies, information security awareness of users etc., were not deemed important (Von Solms, 2000). However, even at this early stage, the technical professionals responsible for implementing information security, started to realize that management would have to get involved at some time (Von Solms, 2000). This management involvement eventually came, with the advent of distributed computing, in the form of information security policies (Von Solms, 2000). Information security policies were introduced because technical controls alone could not provide sufficient security. It became necessary for people to take responsibility for security. Those responsibilities were outlined in policies, which form part of the third category of controls, viz operational controls.

2.3.3 Operational Controls

Operational controls (also referred to as; business-, administrative-, managerial-, or procedural controls) consist of all controls that deal with human behavior. These controls would include those that deal with the creation of information security policies and procedures, and administration of other controls. Both physical and technical controls, even though they do not deal directly with operational issues, usually require some form of human involvement. In an organizational context, these controls would thus have to be supported by procedures outlining the employee's involvement in the use of these controls. The introduction of operational controls, in the form of security policies and procedures, hence operational controls, heralded the start of the second wave in information security (Von Solms, 2000).

This wave is characterized by management involvement in Information Security, and generally improved Information Security (Von Solms, 2000). The above-mentioned three categories of controls, together with the information security policy forms the basis upon which the process of information

security is built. In this process the security policy, and possible sub-policies, outline a set of controls that should be implemented in order to secure the organization's information. These controls are in turn supported by operational procedures, which ensure the effective deployment of the controls, as outlined in the policy. Conceptually, these procedures can be seen as further operational controls. The interaction between these different types of controls, as well as the dependence on human involvement during this process, is of vital importance for the purposes of this dissertation and will thus be examined in more detail.

2.4 Information Security - The "Human Factor"

As mentioned above, both physical and technical controls, even though they do not deal directly with operational issues, usually require some form of human involvement. This means that these controls have to be supported by procedures outlining the employee's involvement in the use of these controls. Employees, whether intentionally or through negligence, often due to a lack of knowledge, are the greatest threat to information security (Thomson, 1998, p. 12), (Mitnick & Simon, 2002, p. 3). Operational controls rely on human behavior. This means that operational controls are arguably some of the weakest links in information security. Unfortunately, both physical and technical controls rely to some extent on these operational controls for effectiveness.

As an example, an operational control might state that a user leaving his/her office must logoff from the operating system and lock his/her office door. If a user was to ignore this procedure, both the technical control forcing authentication and the physical control of having a lock on the door would be rendered useless. Thus, anyone who thinks that security products, i.e. technical and physical controls, alone, offer true security is settling for the illusion of security (Mitnick & Simon, 2002, p. 4).

Siponen (2001) describes this tendency of organizations to settle for the illusion of security as a general human tendency to often blindly ignore complications in IT related issues. Without an adequate level of user **co-operation**

and **knowledge**, many security techniques are liable to be misused or misinterpreted by users. This may result in even an adequate security measure becoming inadequate (Siponen, 2001). It is important to note that there are two dimensions to this "human factor" in information security, namely cooperation, or behavior, and knowledge.

The first dimension to this human factor in information security is the requirement for human **co-operation**. This means that information security depends, to a degree, on the attitude(s) of humans involved in the security process. Without a proper attitude towards information security on the parts of the humans involved, there cannot be sufficient cooperation. It is thus necessary to ensure that the attitude of the humans is such that it leads to the desired behavior. However, even if the humans involved have a positive attitude towards security, an organization's information will not be secure if the same humans do not also possess the necessary knowledge.

The second dimension to the "human factor" is a requirement for the humans involved to have adequate knowledge. Each and every human involved in the security process not only needs knowledge relating to **what** they should do, but also knowledge as to **how** to perform their security related functions. These two dimensions to the human factor are, to a large degree, closely related to each other but will be discussed separately in order to clarify the different emphasis of each.

2.4.1 Knowledge

Organizations cannot protect the integrity, confidentiality, and availability of information in today's highly networked systems environment without ensuring that each person involved understands his/her roles and responsibilities and is adequately trained to perform them (NIST 800-16, 1998, p. 3). Thus individual users should be made aware of the specific operational controls that are dependant on his/her behavior in order to be effective. In order to ensure this required level of knowledge, extensive awareness, training and educational programs will be needed. The obvious question at this point would be to ask exactly what should users be taught?

ISO/IEC 17799 states that all employees of the organization and, where relevant, third party users, should receive appropriate training. This training should include security requirements, legal responsibilities and business con-

trols, as well as training in the correct use of information processing facilities before access to information or services is granted (ISO/IEC 17799, 2000, p. 9, section 6.2.1) This statement, even though it greatly clarifies some issues relating to what should be taught in an information security educational program, raises another question namely, what is appropriate training? Determining exactly how much knowledge a user requires can be a daunting task.

It would make sense for an organization's security educational program to cover all the controls specified by the specific information security standard used by the organization. However, it is clearly unreasonable to expect each and every end-user to be educated about all the controls specified by a standard such as the ISO/IEC 17799. According to ISO/IEC TR 13335-1 each employee should know his or her **role** and **responsibility**, his or her **contribution to IT security**, and should **share the IT security vision** (ISO/IEC TR 13335-1, 2004, p. 14). It is therefore necessary to tailor the educational material used to the needs of the individual user.

Creating a user education program that is tailor-made to the training needs of each and every individual user, although theoretically possible, is in practice very difficult, if not impossible, to implement. Furthermore such an awareness program would be extremely costly to create and thus not feasible for the average organization. It is, however, possible to have some distinction between the different levels or profiles of users in an information security awareness program. Since the training needs of individuals are heavily dependant on the actual role that an individual plays inside the organization, and forms of role-based schema's are already widely used for the implementation of access control, it would be logical to create a form of role-based awareness education. Such a system would solve the dilemma of creating a customized educational program for every individual by reducing the number of customizations to a manageable, and affordable, level. According to Thomson (1998) there are essentially three categories of users that need to be educated in information security awareness, namely:

- The End User: including anyone using information resources.
- IT Personnel: including anyone responsible for the technical side of information technology resources and in this case, the technical imple-

mentation of security controls.

- Top Management: including anyone responsible for providing high-level direction and leadership in an organization. In a security context, top management provides the leadership via security policies and by committing the organization to the security process. Top management users are also end-users.

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

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

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

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

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

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

It can thus be summarized that the knowledge needed by, and thus, **what** should be taught to, a specific individual user would depend on both the user's category and the specific departmental role which that user plays

within the organization. For the average organization it should be possible to create a generic set of information security educational needs profiles. Many of these profiles would contain elements that apply to end-users, in one form or another. In fact, only the IT personnel whose security education needs include highly technical knowledge about controls, cannot be classified as end-users in the strict sense of the word. This dissertation will focus exclusively on the knowledge needed, and thus educational requirements, relating to end-users. This includes typical end-users, top-management, as well as other organizational roles end-users could fulfill.

Once these users have sufficient knowledge about their roles in the security process, there is still no guarantee that they will adhere to their required security roles. It is possible that users understand their roles correctly but still don't adhere to a security policy because it conflicts with their beliefs and values (Schlienger & Teufel, 2003). It is therefore imperative to also ensure that the users have the correct attitude, and thus desired *behavior*, towards information security.

2.4.2 Behavior

Most current user education programs fail to pay adequate attention to behavioral theories (Siponen, 2001). The emphasis of user education programs should be to build an organizational sub-culture of security awareness, by instilling the aspects of information security in every employee as a natural way of performing his or her daily job (Von Solms, 2000). Recent studies have indicated that the establishment of an information security "culture" in the organization is desirable for effective information security (Von Solms, 2000). Such a culture should support all business activities in such a way that information security becomes a natural aspect in the daily activities of every employee (Schlienger & Teufel, 2003). According to The American Heritage Dictionary of the English Language (2000) a culture is:

- The totality of socially transmitted behavior patterns, arts, beliefs, institutions, and all other products of human work and thought.
- The predominating attitudes and behavior that characterize the functioning of a group or organization.

In terms of information security, a corporate culture of information security can thus be seen as the predominating attitudes towards information security and security related behavior that characterize the functioning of the employees within the organization. Thus, in an organization that has a culture of information security, the employees would adhere to proper security practices during execution of their day-to-day functions because that is simply the way things are done. In other words, employees would have the correct attitude towards information security. It is obvious that in order for employees to be able to adhere to proper security practices the employees would have to know what proper security practices are. Therefore, information security education would have to play a key role in the establishment of such a culture.

Even though user education is essential for the establishment of a successful corporate culture of information security, education on its own cannot change a corporate culture. To ensure the successful protection of information assets, a formalized approach towards establishing and maintaining a corporate culture needs to be taken. Since the aim of such a process would be to change employee behavior, it would be sensible to "borrow" the necessary methodologies from the behavioral sciences. Corporate culture, and approaches towards changing such a culture, will be examined in depth in a later chapter.

2.5 Conclusion

In this chapter information security was introduced. A definition for information security was given and discussed. From the definition several characteristics that information has to have in order to be called secure, were identified. It was also stated that security is a process, not a product. Information security serves to protect an organization's information assets from both internal- and external threats. This protection is typically implemented in the form of various security controls. These controls serve to reduce the risks posed by vulnerabilities to threats against information assets. Three main categories of controls exist, namely, physical-, technical-, and operation controls. The first two of these categories of controls depends to a large degree on the third category, operational controls, in order to be effective. Operational controls, in turn, depend on human cooperation, hence behavior, as

well as knowledge in order to be effective. These two "dimensions", behavior and knowledge, constitutes the human factor in information security. Humans involved in the security process need to possess the required knowledge about their security related roles, and thus need to be educated. They also need to have the desired attitude towards security. Organizations thus need to establish a corporate sub-culture of information security compliance. The education of users, and the establishment of an information security sub-culture in the organization will be examined in depth in the next chapters.

Chapter 3

INFORMATION SECURITY EDUCATION

This chapter examines information security education. It briefly examines issues surrounding the scope of security education programs. It then proposes and argues a set of criteria that should be met by an educational methodology, in order for such a methodology to be suitable for information security education.

3.1 Introduction

The previous chapter highlighted that the "human factor" in information security consists of two inter-related dimensions, namely user **co-operation** and **knowledge**. In order for an organization to have adequate information security, the users in that organization needs to have both knowledge and the desired "secure" attitude. This chapter will examine the knowledge dimension in more depth. The other dimension, co-operation (or attitude), will be discussed in depth in chapter 5.

In order to convey the necessary knowledge to an organization's users, it is necessary to educate the users. The need for affordable and effective information security education has in recent years become well established. According to Dhillon (1999) the widespread use of IT by businesses today has given rise to "security blindness" on the part of the users. However, when addressing this lack of knowledge, the term "users" no longer mean your traditional end-users, but includes staff at all levels of responsibility

inside the organization. Nosworthy (2000) states that each person in the organization from the CEO to house keeping staff must be aware of and trained to exercise their responsibilities towards information security.

Taking into consideration the number of different information security standards that are available today, as well as the complexity and comprehensiveness of these standards, the task of educating "each person in the organization" with regards to their responsibilities towards information security is enormous. Very few organizations, especially in South Africa, would have the kind of economic resources, or enough "teachers" with the necessary knowledge, available that such an educational program would require. It is therefor vital to ensure that the educational methodology used for such an user education program match the requirements for information security *exactly*. The first step towards determining such a match is to delimitate the boundaries of such programs clearly.

3.2 The Scope of Information Security Education Programs

In order to determine the required scope of an information security education program the following two fundamental questions need to be answered regarding such user education, namely:

- **Who** (exactly) should be educated?
- **What** should be taught to the "learners"?

The answers to these questions are to a large degree interdependent and will now be examined in more depth. The related question: "**How** should the users be taught?" will be explored in depth later in this chapter.

According to the international standard ISO/IEC 17799, "**All employees** of the organization and, where relevant, **third party users**, should receive appropriate training ... before access to information or services is granted" (ISO/IEC 17799, 2000, p. 9, section 6.2.1). As mentioned earlier, "all employees" include staff at all levels of responsibility inside the organization from the CEO to House Keeping staff (Nosworthy, 2000).

It would make sense for an organization's information security education program to cover all the controls specified by the specific information security

standard used by the organization. However, it is clearly an overkill to expect each and every end-user to be educated about all the controls specified by a standard such as the ISO/IEC 17799. According to ISO/IEC TR 13335-1 (2004, p. 14) each employee should know *his or her* role and responsibility, *his or her* contribution to IT security, and share the IT security vision. It is therefore necessary to tailor the information security educational material used to the needs of the individual user.

As mentioned in 2.4.1, the training needs of individuals are heavily dependant on the actual role that individual plays inside the organization. Since forms of role-based schemas are already widely used for the implementation of access control, it would be logical to create a form of role-based information security education. Such a system would solve the dilemma of creating a customized educational program for every individual by reducing the number of customizations to a manageable, and affordable, level.

Section 2.4.1 also stated that information security roles can be broadly categorized into three groups: End users, IT Personnel and Top Management, and that a further distinction between different types of users can be made based on their actual departmental role inside the organization. Thus, an end-user in the finance department might have different information security education needs to an end-user in a manufacturing department. This need to distinguish between users based on their actual **role** in the organization is also supported by the American information security training standard NIST 800-16 (1998), which states that an individual's need for security training will change as their organizational **role** changes (NIST 800-16, 1998, p. 43). The need to *customize* what is taught to an individual is explored in more depth in a later section. Because the American standard (NIST 800-16, 1998) is the only major security standard dealing specifically with **role-based** security education this model will first be briefly explored.

3.2.1 NIST Special publication 800-16: Information Technology Security Training Requirements: A Role- and Performance-Based Model

The American National Institute of Standards and Technology (NIST) provides an information security specific training model (NIST 800-16, 1998).

This model provides a framework that serves as the American standard for information security training. The NIST model, entitled: "Information Technology Security Training Requirements: A Role- and Performance-Based Model", is currently the only standard that focuses exclusively on the learning needs related to information security.

The NIST model is based on the premise that learning is a continuum. Specifically, learning in this context starts with **awareness**, builds to **training**, and evolves into **education** (NIST 800-16, 1998, p. 14). Furthermore the model is *role-based*, meaning that it defines the IT security learning needed as a person assumes different roles within an organization and different responsibilities in relation to IT systems (NIST 800-16, 1998, p. 14).

The premise that information security learning is a continuum consisting of awareness, training and education is fairly widely accepted (Horrocks, 2001; Schlienger & Teufel, 2003). The three levels of learning in this continuum can be described as follows:

- Awareness: The purpose of awareness programs is simply to focus attention on security issues. In awareness activities, the learner is simply the recipient of information and does not actively participate (NIST 800-16, 1998, p. 15). Awareness campaigns often make use of tools such as posters, videos and promotional slogans.

- Training: The learner has to know how he/she can behave securely. This level strives to produce relevant and needed security skills and competency by practitioners of functional specialties other than IT security (e.g., management, auditing). Training of special security tools or features within applications must be offered (NIST 800-16, 1998, p. 16),(Schlienger & Teufel, 2003).

- Education: The "Education" level integrates all of the security skills and competencies of the various functional specialties into a common body of knowledge. It also adds a multi-disciplinary study of concepts, issues, and principles (technological and social). This level strives to produce IT security specialists and professionals capable of vision and pro-active response (NIST 800-16, 1998, p. 16). An important characteristic of education is that the employee must understand **why**

information security is important for the organization (Schlienger & Teufel, 2003).

The model in NIST special publication 800-16 deals primarily with the *training* part of this learning continuum. The NIST document uses this continuum to identify the knowledge, skills, and abilities an individual needs to perform the IT security responsibilities specific to each of his or her roles in the organization. According to this model all employees would need awareness. Training would only be required by individuals whose roles in the company indicate a need for specific knowledge of security threats and risks, as well as the safeguards against these threats and risks. Lastly, according to this model, education would only be needed by information security specialists. Thus, the type of learning that individuals need, starts simplistically and then becomes more comprehensive and detailed towards the top of the continuum (NIST 800-16, 1998, pp. 13-14).

In addition to the three levels of the learning continuum, NIST 800-16 (1998) defines six generic categories into which most organizational roles can be categorized, namely: Manage, Acquire, Design and Develop, Implement and Operate, Review and Evaluate, and Use. The NIST model also has a seventh category, Other, that acts as a place holder, to accommodate any additional functional roles identified in the future (NIST 800-16, 1998, p. 43).

Once the specific information security related roles of an employee have been determined, the NIST document can be used to identify the specific learning requirements of that employee. These are sub-divided into a further three levels, beginner, intermediate and advanced. Finally, the document provides a framework for the planning of information security training curricula and the evaluation of training effectiveness. This framework consist of a "training matrix" that is used to determine the specific training needs of individuals based on their organizational roles, the level of training they require (beginner, intermediate or advanced), and the applicable training areas, which could vary depending on the organization's information security policy and supporting procedures. Figure 3.1 illustrates such a training matrix.

The entries in the first column of each row in Fig. 3.1 correspond to specific training areas. The column headings specify the organizational roles of the users. The entries in the actual cells specify the specific training

Training Areas	**A** Manage	**B** Acquire	**C** Design and Develop	**D** Implement and Operate	**E** Review and Evaluate	**F** Use	**G** Other
1 Laws and Regulations	1A	1B	1C	1D	1E	1F	n/a
2 Security Program							
2.1 Planning	2.1A	2.1B	2.1C	2.1D	2.1E	2.1F	n/a
2.2 Management	2.2A	2.2B	2.2C	2.2D	2.2E	2.2F	n/a
3 System Lifecycle Security							
3.1 Initiation	3.1A	3.1B	3.1C	3.1D	3.1E	n/a	n/a
etc ...							

Figure 3.1: Training Matrix adapted from NIST 800-16, p. 14

programs applicable to the denoted **training area**, for a user fulfilling the corresponding **role**. Each of these training programs would have beginner, intermediate and advanced levels. As mentioned earlier, this model deals specifically with security *training* needs, as opposed to awareness or eduction needs. It would, however, be possible to devise a similar training matrix to identify the specific information security education needs for individuals within an organization.

3.2.2 An organizational information security education matrix

For the purposes of this dissertation the term "education" will be used in an *encompassing* sense. In other words, the term information security **education** will be used in a sense that includes both training and awareness activities, where these are required. Standards such as ISO/IEC 13335-3 (1998), use the term awareness in a similar encompassing sense that includes all three aspects of the learning continuum as outlined in NIST 800-16 (1998). See also section 3.3.2.

In order to adapt the NIST training matrix to the educational needs of a specific organization, the following tasks would have to be completed:

- The specific training/education areas applicable to the organization

would have to be determined. These will depend on several factors, including the legal obligations of the organization regarding information security, the organization's information security policy and the specific information security standard used by the organization.

- The organizational roles applicable would have to be defined. These roles could be "borrowed" from a framework such as NIST 800-16 (1998), or it could be defined in a more "customized" manner, in order to suit the specific organization's needs better.

- Educational goals or *outcomes* for each cell would have to be defined. These outcomes would essentially be a clear definition of exactly what knowledge and/or skills a person should attain at the end of a specific course. As in NIST 800-16 (1998), these could be subdivided into several staged levels, i.e. beginner, intermediate and advanced levels.

Figure 3.2 illustrates an example of how such an educational needs matrix might look.

Training Areas	Top Management		Finance				IT		
	Manage	Info Sec Officer	Manage	Account-ing	Audit	Admin	Manage	Develop	etc
1. Strategic Security Issues									
1.1 Laws	1.1 A	1.1 A	1.1 A	1.1 A	1.1 A	n/a	1.1 A	n/a	...
1.2 IT Governance	1.2 A	1.2 A&B	n/a	n/a	n/a	n/a	1.2A&B	n/a	...
2. End User Security									
2.1 Email & Web Security	2.1 A	2.1 A	2.1 A	2.1 A	2.1 A	2.1 A	2.1 A	2.1 A&B	...
2.2 Virus Prevention	2.2 A	2.2 A	2.2 A	2.2 A	2.2 A	2.2 A	2.2 A	2.2 A&C	...
Etc..	...	...	...	...	...	...	...	...	...

Figure 3.2: Information Security "Educational Needs Matrix"

In figure 3.2, the rows correspond to the broad educational areas for the organization. These areas should be defined to fit the specific needs of the organization. The columns in figure 3.2 represent the organizational structure and the specific roles which individuals within that structure would fulfil.

The cells contain references to the specific educational outcomes that a person in a specific role would have to attain for a defined educational area. As an example: All managers, regardless of the department they head in the organization, might need familiarity with the legal and statutory obligations of the organization towards information security. On the other hand, only the top management, the information security officer, and the CIO might require education regarding IT security governance issues. These needs would probably vary from organization to organization, although similarities between the needs of organizations within the same sector would exist.

Once the educational needs for an organization's personnel have been clearly defined, it is necessary to decide on an appropriate educational methodology in order to design the necessary curricula and to educate the users. In other words, once an organization has determined **who** needs to be educated, and **what** they should be taught, it is necessary to decide **how** to do the teaching.

3.2.3 How should the users be taught?

Humans play a vital role in an organization's information security efforts. Without adequate knowledge, the humans involved will not be able to perform their respective roles, which in turn could negate the effectiveness of both physical and technical controls. It is therefor necessary to take special care to ensure the success of the user education programs used. For educational programs this would mean ensuring adherence to *proper pedagogical principles* when these educational programs are compiled. Most current user education programs fail to pay adequate attention to behavioral theories (Siponen, 2001). In order to answer the question: "How should the users be taught?", it is necessary to determine a set of criteria an educational methodology would have to meet in order to be effective for security education. A pedagogical model or methodology can then be selected based on how well it fits the criteria for information security education.

3.3 Criteria for Information Security Education

The user education programs needed for information security purposes differ from traditional educational programs. Unlike traditional educational programs, these programs will primarily be aimed at teaching adults. Adults have well established, not formative, values, beliefs, and opinions (NIST 800-16, 1998, p. 20). The educational methodology used should thus be suitable for adult education. Furthermore, there are several other requirements specific to the role that such a program will play in the overall organization's information security efforts. In the rest of this section, this dissertation will suggest and attempt to motivate some of the criteria that should typically be considered when selecting an educational methodology for the creation of an information security education program.

3.3.1 Everyone should be able to "pass" the course

Nosworthy (2000) states that each person in the organization from the CEO to house keeping staff must be aware of, and trained to exercise their responsibilities towards information security. However, in traditional educational models there are usually a percentage of the learners who do not pass the course, or in other words, successfully meet the assessment criteria. In order for an organization's information resources to be secure, everyone needs to not only be trained, but to "pass" the training. Unlike traditional education, failing an information security educational program cannot be accepted. Workers at every level, even those who do not use a computer, are liable to be targeted (Mitnick & Simon, 2002, p. 39). This means that having even a single person who does not know his/her information security responsibilities should be unacceptable.

3.3.2 Employees must know *Why*

Employees must know why information security is important and why a specific policy or control is in place. Recent studies have suggested that current information security awareness programs are failing (Siponen, 2001). This failure is due to many reasons. Schlienger and Teufel (2003) have shown that

even employees who know their responsibilities with regards to information security will still disobey security policy if they disagree with the policy. They suggest that the mere awareness of the policies and procedures is in fact not sufficient, the users also need to know why a specific policy or control is in place (Schlienger & Teufel, 2003). In information security, being taught why a specific policy or control is in place is generally considered to be a feature of education, and not of awareness (Schlienger & Teufel, 2003; NIST 800-16, 1998, pp. 16-17). A feature of the educational level is that the user must understand why information security is important (Schlienger & Teufel, 2003; NIST 800-16, 1998, pp. 16-17). However, it is important to realize that this clear distinction between awareness, training and education is **not** universal between the different standards. Standards such as ISO/IEC 17799 and ISO/IEC TR 13335 use the term awareness when discussing any of the three levels in the user education continuum. As an example: according to ISO/IEC 13335-3 (1998, p. 24) the "awareness" program should ensure that IT staff and the end users have enough knowledge of the IT systems (hardware and software), and that they understand **why** safeguards are necessary and how to use them correctly. It also states that only safeguards accepted by the IT staff and end users can work effectively (ISO/IEC 13335-3, 1998, p. 24). Clearly in terms of the NIST learning continuum this refers to education as opposed to awareness. It should also be obvious that end-users do not require the same level of understanding as information security professionals (NIST 800-16, 1998, p. 14). One does not need to understand why procedures are in place or how the technologies work to use them effectively (Tripathi, 2000), (NIST 800-16, 1998, p. 14). However, in information security, if a user asks why, it should always be explained (Tripathi, 2000).

3.3.3 Learning materials should be customized

Learning materials should be customized to the needs of individual learners. In an organizational context, users of information exist at several levels. There are essentially three categories of users that need to be educated in information security awareness namely: the end-user, IT personnel and top management (Thomson, 1998). The National Institute for Science and Technology (NIST) expands on this classification by stating that training and education are to be provided selectively, based on individual responsibilities

and needs. Specifically, training is to be provided to individuals based on their particular job functions (NIST 800-16, 1998, p. 43). The ISO/IEC 17799 states that the information security policy should be communicated throughout the organization to users in a form that is relevant, accessible and understandable to the intended reader (ISO/IEC 17799, 2000, p. 3, section 3.1.1). According to NIST, individuals learn in several ways, but each person, as part of his/her personality, has a preferred or primary learning style. Instruction can positively, or negatively, affect a student's performance, depending on whether it is matched, or mismatched, with a student's preferred learning style (NIST 800-16, 1998, p. 19). Thus, what should be taught to a specific individual user and how it should be taught, will depend on both the user's preferred learning style, and the specific role which that user plays within the organization.

3.3.4 Users should be responsible for their own learning

In today's organizations it is crucial to maximize return on investment. Through its very nature classroom training requires the availability of highly trained specialists to present the courses. It also requires that the learners take time off from their regular duties to attend classes. These factors make classroom training very expensive. One of the most cost-effective substitutes for traditional classroom training is to provide employees with intranet-based instruction (O'Brien, 1999, p. 361). Such web-based instructional programs require individual learners to be responsible for their own acquisition of knowledge instead of being passive receptors in the process (ITiCSE, 1997). Self-driven learning also enables organizations to make learning material available in a variety of formats. This in turn means users will have a choice of how they are taught, which has already been shown to be a necessary feature of information security education.

3.3.5 Users should be held accountable for their studies

Most information security standards make it clear that users should be held accountable for their information security responsibilities (ISO/IEC 17799,

2000, pp. 8-10, section 6). These responsibilities are normally spelt out in the organization's information security policies and procedures. In an organization, policies function in a similar fashion to laws. For laws, ignorance is not a valid defense. However ignorance of policy is an acceptable defense (Whitman & Mattord, 2003, p. 93). Thus, to be able to hold employees accountable for their actions, the organization should have proof, normally in the form of a signed form, that the employees have been educated regarding their responsibilities and that they understand and accept these responsibilities as laid out in the policies (Whitman & Mattord, 2003, p. 93). Wood (1997) suggests that all employees should be required, on an annual basis, to sign a statement saying that they have read and understood the information security policy manual. It should thus be clear that self-driven learning for information security purposes, as discussed previously, could only be used if the employees are also held accountable for their learning. Otherwise the organization could not legally hold the employees accountable for their actions.

3.3.6 Learners must receive feedback

According to NIST 800-16 (1998), **evaluation** of training is vital, and should be an integral component of any training programme (NIST 800-16, 1998, p. 157). This holds true for any form of education. Being able to assess progress and provide feedback to the learner is a prerequisite for any educational program to be successful. Fingar (1996) states that feedback, specifically in the form of knowledge regarding the outcomes of the learners' actions, is required for learning to take place. This feedback should be continuous and constructive (DOE, 2001). In a traditional classroom situation educators are responsible for helping the learners achieve the instructional objectives designated for their classes. These instructional objectives are that each learner should attain the learning outcomes by being able to demonstrate their mastery of the assessment standards. The purpose of assessment is to determine whether the learners have achieved these objectives (Cunningham, 1998). Assessment, in this case, should not be confused with *evaluation*. According to Siebörger (1998) assessment is similar to evaluation, but assessment is the measurement of the extent of learning in *individuals*, whereas *evaluation* is a process by which the *effects* and effectiveness of teaching are determined. Both assessment and *evaluation* should form part of any information security

program. The learners should thus receive feedback in two forms. First they should be assessed, which will tell them how well they as individuals have mastered the knowledge from a specific program. Secondly, they should be evaluated. *Evaluation* could serve as a metric towards measuring the overall success of the information security education program (a concept that will be explored in more depth in a later chapter). Such a metric could also be used as a key performance indicator to assist in holding users accountable for their studies.

As mentioned earlier, humans can be seen as the weakest link in information security. Information security depends on human knowledge and human attitude. The aim of an information security education program is to address a lack of information security knowledge. Due to financial constraints, most organizations cannot afford to spend money on educational programs if such programs are not going to provide a return on the organization's investment. In the case of information security education, adhering to the above requirements when designing the educational programs *should* increase the likelihood of such a program's success.

3.4 Conclusion

Many organizations have realized that their own employees are the biggest threat to their information systems (Von Solms, 2000). In order to address this problem it is vital for organizations that their employees have both the necessary knowledge and the right attitude to fulfil their required roles in the overall information security efforts of the organization. This chapter examined information security **education**, which is required to impart the needed **knowledge** to the employees. Current programs used to educate employees, fail to pay sufficient attention to aspects related to the behavioral sciences (Siponen, 2001). It would make sense to adhere to a formal educational methodology when constructing user education programs.

The methodology used should be suitable for the specific needs of an information security user education program. This chapter examined the scope of such a user education program. It then suggested a set of criteria that the chosen methodology would have to meet in order for it to be suitable

for use in information security education. The criteria identified included:

- Everyone should be able to "pass" the course
- Employees must know why they are taught a specific skill or have to behave in a specific way
- Learning materials should be customized to the learning style, or preferences, of the learner
- Users should be responsible for their own learning
- Users should be held accountable for their studies
- Learners must receive feedback

Since the aim of the user education program is not to prepare the users for further levels of formal education, but rather to help them achieve information security know-how for use in their everyday jobs, the educational methodology used should be chosen accordingly. Outcomes Based Education (OBE) is an educational methodology which has as its aim to help learners achieve a specific outcome, in this case information security awareness and the skills that enables the learners to behave in a secure manner. Preliminary investigations have shown that OBE might, in fact, be ideally suited for use in information security education programs. This methodology, and its suitability for information security education, will therefor be examined in more depth in the next chapter.

Chapter 4

OUTCOMES BASED EDUCATION

This chapter discusses Outcomes Based Education (OBE). It explains what outcomes are, discusses the basic premises of OBE, and explores curriculum design using OBE. Lastly, this chapter attempts to show that OBE matches the requirements for information security education, by linking OBE to the criteria defined in the previous chapter.

4.1 Introduction

Information security education differs from traditional school-, or university education. The aim of an information security user education program is not to prepare the users for further levels of formal education, but rather to help them achieve information security know-how for use in their everyday jobs. The educational methodology used should thus be chosen accordingly.

Outcomes Based Education (OBE) is an educational methodology with the aim to help learners achieve a specific outcome, in this case information security awareness and the skills that enable the learners to behave in a secure manner. Preliminary investigations have shown that OBE might in fact be ideally suited for use in information security education programs. This methodology, and its suitability for information security education, will therefor be examined in more depth in this chapter.

4.2 Outcomes Based Education Defined

Outcomes Based Education (OBE) is defined as an approach to teaching and learning which stresses the need to be clear about what learners are expected to achieve. The educator states beforehand what "outcome" is expected of the learners. The role of the educator is then to help the learners achieve that outcome (Siebörger, 1998). Outcomes Based Education means clearly focusing and organizing everything in an educational program around what is essential for the learners to be *able to do successfully at the end* of their learning (Spady, 1994, p. 1). In essence an OBE program is developed through three basic steps:

1. Developing a **clear** set of learning outcomes (Killen, 2000; Spady, 1994, pp. 1-2).

2. Establishing the conditions and opportunities that will enable learners to reach those outcomes (Killen, 2000; Spady, 1994, pp. 1-2).

3. Deciding on criteria to determine when learners have reached the desired outcomes (Killen, 2000).

This model forms the basis for many learning experiences outside formal educational institutes. Contemporary examples of outcomes based models include technical training programs in the military, flight schools, karate instruction, professional licensure of doctors or lawyers, and any other area of learning where **clearly defined competence** and **performance** are **essential** to carry out a role or perform a task effectively (Spady, 1994, p. 4). All of these examples have two features in common. Firstly, there is a clearly defined performance requirement that is not compromised. Secondly, **what** and **whether** a student learns are more important than **when** and **how** they learn it (Spady, 1994, p. 5).

In traditional educational systems, this clear focus on the desired end-result is sometimes lacking. To further clarify these differences, the next subsection will briefly compare OBE to traditional educational models.

4.2.1 OBE vs traditional education models

Several differences exists between OBE and traditional educational systems. The primary differences includes:

- OBE systems build the entire learning experience, including curriculum design, assessments and performance strategies, on a clearly defined framework of exit outcomes (Spady, 1994, p. 6). See also (Killen, 2000; Malan, 2000)

- Time in an outcomes based system is not treated as a fixed resource (Spady, 1994, p. 6). In fact, most of the factors that shape traditional education, namely; time, procedures, programs, teaching and curriculum, take a subordinate position to the desired outcomes (Malan, 2000; Spady, 1994, p. 3). As an example; in a traditional model, the curriculum might be planned around a fixed time period, one academic year, and the amount of learning that should take place in that time period is fixed for both students who learn fast and those who take longer to master the same concepts. In OBE, it is more important for a learner to achieve the desired outcome, than how long it takes to achieve. Thus, in an OBE model all learners have to achieve the same "amount" of learning, but some may do this faster, or slower, than others.

- Standards in an OBE system are clearly defined and criterion-based for all learners. This means that it is possible for all learners to receive full credit for achieving a given performance standard. Anyone can eventually achieve a 100% mark (Spady, 1994, p. 6), but not necessarily in the same time-frame (Malan, 2000).

- OBE focuses on increasing learning and ultimate performance for all learning areas to the highest possible levels (Spady, 1994, p. 6). In other words, learners have the opportunity to continuously re-visit areas of learning in order to further improve their skills, unlike traditional educational models where past performance becomes a permanent part of a learner's record (Spady, 1994, p. 6). This concept, also known as *mastery learning*, has several additional benefits in terms of learner motivation. According to Killen (2000) mastery learning and outcomes-based programming make all instruction purposeful for students.

As mentioned above, OBE places a major emphasis on the mastery of the expected *outcomes*. In order to fully understand the concept of an *outcome*, as used in OBE, the next subsection will briefly examine outcomes in more depth.

4.2.2 What are outcomes?

Outcomes are clear learning results that the learners should be able to demonstrate at the end of a significant learning experience (Spady, 1994, p. 2). Outcomes are what learners **can actually do** with what they know and have learned (Spady, 1994, p. 2). In addition to these definitions, Malan (2000) mentions that outcomes can be seen as actions and performances that embody and reflect learner competence in using content, information, ideas, and tools successfully.

In an information security education context, **one** possible outcome could thus be: *The learner must be able to successfully scan an electronic message for viruses.* This example outcome could also be called a competency outcome, which is one category of possible outcomes that can be defined. The categorization of outcomes may sometimes seem confusing to persons who are unfamiliar with OBE. These categories will be briefly examined in order to clarify this issue.

4.2.3 Types of outcomes

Outcomes can be categorized into many "sub-types", or "kinds" of outcomes. Spady (1994, p. 59) presents the following list:

- Content Focus: Outcomes are classified according to the discipline, or subject area, they represent.
- Time-Referenced: Outcomes are linked to time blocks they represent, e.g. semester outcomes.
- Curriculum Scope: Outcomes are classified according to the scope of the specific curriculum segment to which they are linked, e.g. a specific lesson.
- Jurisdictional Domain: Outcomes are linked to the organizational jurisdiction that defined the outcomes, e.g. departmental, provincial, etc. Such a classification is mainly useful for reporting purposes.
- Competency Scope: Outcomes are classified according to the nature, scope and complexity of the competence that must be used to demonstrate them, e.g. performing a virus check or encrypting a document.

- Operational Function: Outcomes are classified according to the function they serve within a curriculum design framework, e.g. culminating outcomes, enabling outcomes, and discrete outcomes.

For example, the South African Department of Education often define outcomes according to their operation function, as either cross-curriculum (general outcomes) or specific outcomes (DOE, 2001). A cross-curriculum outcome can be seen as the desired effect that attaining a specific competency should have within the general environment within which the learner operates. A specific outcome is one that directly demonstrates the mastery of the appropriate skill that the learner should gain from the OBE program.

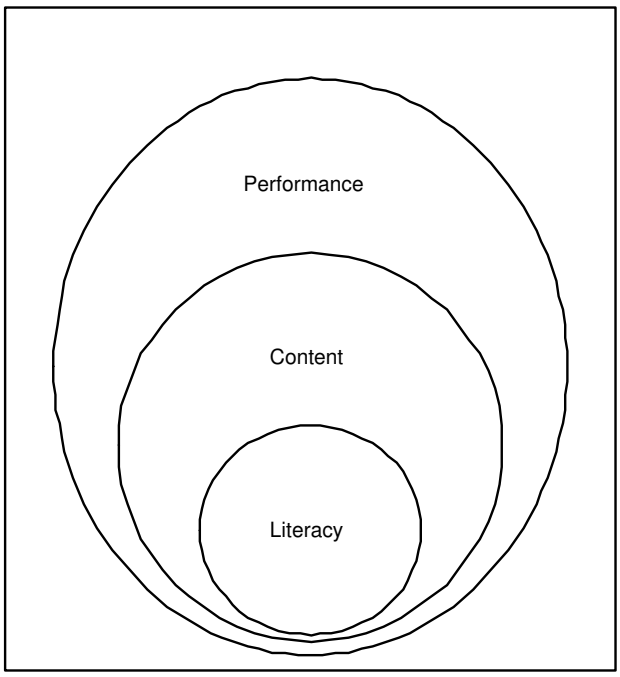

Figure 4.1: Three Critical Domains of Outcomes (adapted from Spady, 1994, p. 60)

The above classifications, and many others that exist, can at first seem confusing; however, all outcomes can essentially be classified into three, encompassing, "**critical domains**" of outcomes (Spady, 1994, pp. 60-61). The first, and largest, domain is a grouping of all outcomes relating directly to the **performance** abilities of the learners. The second is embedded within the first and deals with the **content** or subject matter, essentially a grouping of outcomes reflecting the core knowledge without which performance is

not possible. The final critical domain is embedded within the first two and groups all outcomes dealing with the basic **literacy** skills in a problem domain. These literacy skills are required in order to understand the content. Figure 4.1 illustrates the relationship between these three critical domains of outcomes.

As mentioned in 4.2, defining clearly what outcomes are expected from learners can be seen as the first step in the design of any outcomes based educational program. The second step is to establish the conditions and opportunities that will enable learners to reach those outcomes. These conditions and opportunities should be established in line with the basic premises and principles upon which OBE is based.

4.3 The Premises and Principles of OBE

Outcomes based education is based upon three basic premises, namely (Killen, 2000; Spady, 1994, p. 9):

1. All students can learn and succeed, but not all in the same time or in the same way.

2. Successful learning promotes even more successful learning.

3. Schools (and teachers) control the conditions that determine whether or not students are successful at learning.

From these basic premises four essential principles of OBE were developed. They are (Killen, 2000; Spady, 1994, pp. 10-11):

1. Clarity of focus, which means that all teaching activities must be clearly focused on the desired outcome that the learners should achieve.

2. Designing back, which means that the starting point for an OBE program's design should be a clear definition of the desired results. The rest of the curriculum should be designed according to this desired outcome.

3. High expectations for all students. OBE not only assumes that everyone can attain the desired outcomes, it also requires that high standards should be set. This is based on evidence that learners are more likely

to attain high standards when they are challenged by what is expected from them.

4. Expanded opportunities for all learners. This final principle of OBE is based on the idea that not everyone learns the same way or at the same pace. Thus, in OBE, learners are given many opportunities for learning. Achieving the desired outcome is deemed more important than how that outcome was reached.

In order for an educational program to be classified as being outcomes based, it has to adhere to **all four** of these principles (Killen, 2000). There are many ways in which a curriculum could be designed in line with these principles and premises. Spady (1994) presents a few examples. A full examination of these examples falls outside the scope of this dissertation. Instead, important concepts from these examples will be revisited where applicable.

The last generic step in the creation of an OBE program, as listed in 4.2, is the selection of assessment criteria. This selection should take place **during** the design of "learning experiences", and will often go hand-in-hand with the definition of the outcomes themselves.

4.4 Assessment in OBE

For each defined outcome a corresponding assessment standard should be defined. These assessment standards are necessary in order to provide feedback to the learners. According to Siebörger (1998) assessment is essential to OBE to measure the degree to which a learner has achieved an outcome. In fact being able to assess progress and provide feedback to the learner is a prerequisite for any educational program to be successful. Fingar (1996) states that feedback, specifically in the form of knowledge regarding the outcomes of the learners' actions, is required for learning to take place. Furthermore this feedback should be continuous and constructive (DOE, 2001). The purpose of assessment is not only to measure what learners have achieved, but also to help them to achieve more (Siebörger, 1998).

According to Spady (1994, p. 103) it is vital to have a criterion-based, consistently applied, system of assessments, performance standards, learner credentialing, and reporting that:

1. is tightly aligned with all the defined significant, future-focused outcomes. In other words the assessments should always keep the ultimate goal of the program in mind;

2. emphasizes **applied** learning in **relevant**, life-role contexts. The learner should thus be able to always **relate** the learning back to a role he/she performs in the course of his/her normal activities;

3. encourages learners to attain high performance levels on everything they pursue;

4. documents what students do successfully whenever they are able to do it;

5. enables learners to demonstrate and receive full credit for improved learning on a timely basis;

6. prevents and avoids comparisons among students.

Once all three the basic steps in creating an OBE program have been completed, the learning process for the "students" can begin. The educational process in general can be viewed as a system of teaching and learning activities that are tied together via various feedback loops. It also includes other functions such as assessment, admission, quality assurance, direction and support (Tait, 1997). All of these components can, and should, play a role in the creation of an effective Information Security education program.

OBE can be viewed in three different ways: as a theory of education, a systematic structure for education, or the creation of educational material, and lastly as a classroom practice (Killen, 2000). OBE can thus be seen as a complete educational system, which contains all the components such a system should have. The question of whether or not OBE fits the requirements for information security education, still needs to be answered.

4.5 OBE for Information Security Education

In section 3.3, this dissertation proposed a set of requirements that an educational methodology would have to meet, in order for it to be suitable for information security education. The following requirements were proposed:

- Everyone should be able to "pass" the course
- Employees must know **why** they are taught a specific skill or have to behave in a specific way
- Learning materials should be customized to the learning style, or preferences, of the learner
- Users should be responsible for their own learning
- Users should be held accountable for their studies
- Learners must receive feedback

The beginning of *this* chapter introduced OBE and briefly outlined the basic premises and the principles of this educational methodology. It will now attempt to show that OBE is in fact well suited to the needs of information security by comparing OBE to the requirements listed above:

Everyone should be able to "pass" the course.

The first requirement listed for information security education was that everyone should be able to "pass" the course. Clearly OBE fulfils this requirement since the very first premise upon which OBE is based is the assumption that all students can succeed and learn.

Employees must know *why* they are taught a specific skill or have to behave in a specific way.

For information security education to be successful, employees must know **why** information security is important and why a specific policy or control is in place. Course developers should be aware that adults have well-established values, beliefs, and opinions. Adults relate new information and knowledge to previously learned information, experiences, and values which might result in misunderstanding (NIST 800-16, 1998, p. 20). It is even possible that they understand correctly but still don't adhere to a security policy because it conflicts with their beliefs and values (Schlienger & Teufel, 2003). One of the fundamental differences between OBE and traditional educational models is the fact that rote learning is completely unacceptable in OBE. OBE requires the learner to identify and solve problems in which responses display that

responsible decisions using critical and creative thinking have been made (Olivier, 1998; Pretorius, 1998). This type of thinking requires not only knowledge but also insight. Insight requires the learner to know why they are doing something (NIST 800-16, 1998, p. 18). According to Killen (2000) each outcome based educational program must have a rationale to explain why the program exists.

Learning materials should be customized to the learning style, or preferences, of the learner.

The third requirement of information security education identified was that learning materials should be customized to the needs of individual learners. The first basic premise of OBE not only states that all students can learn and succeed, but it also states that all students cannot necessarily do this in the same time or in the same way. This premise is also expanded on in the fourth principle of OBE, which states that learners should be given many opportunities for learning. OBE thus recognizes that individuals learn in different ways and at different paces. For a program to be truly outcomes based it is vital that learning materials are provided in as customized a format as possible for individual learners. However, according to Killen (2000) the practical difficulties of providing expanded opportunities must be weighed against the long-term benefits of enabling all learners to be successful.

Users should be responsible for their own learning.

The fourth suggested requirement of information security education states that users should be responsible for their own learning. This, together with the next requirement, accountability, could also be summarized by stating that the users should take *ownership* of their own learning. Ownership of their learning and self-driven learning are central concepts to OBE. Because OBE recognizes that different students will learn at a different pace, OBE encourages self-driven learning. The ability to effectively manage one's own time, and learning abilities, are one of the critical cross curriculum outcomes identified for all South African students (SAQA, 2000). The OBE model strives to move away from teacher centeredness, towards learner-centered education (Malan, 2000). Thus, responsibility for their own studies can be seen to be central to OBE.

Users should be held accountable for their studies.

As mentioned above, *accountability* goes hand in hand with *responsibility*, and together these two concepts confer *ownership* of their learning to the learners. OBE places major emphasis on assessment as a tool to provide feedback on progress to the learner, and as a tool for measuring whether the desired outcomes have been reached (Killen, 2000; Malan, 2000). Assessment makes students accountable for their studies.

Learners must receive feedback.

The final requirement for information security education proposed in the previous chapter, is that the learners must receive feedback regarding their learning. In OBE, as in every other pedagogically sound model, feedback and assessment plays a *vital* role. As mentioned earlier; without feedback learning **cannot** take place (Fingar, 1996). According to Killen (2000) learners in an outcomes based program should be provided with feedback both to, *Enhance* their learning, and to provide information regarding their progress toward achieving the stated outcomes. In an outcomes based program there is no such thing as failure, only feedback and results. Success depends on how well learners process the feedback they get regarding their efforts (Killen, 2000).

The following is a brief summary of the relationships between OBE and information security education concluded thus far:

1. In terms of an organization's overall information security effort it is vital for all users to ultimately pass the information security course. OBE requires a high expectation for all learners to do well, and additionally requires that learners be given multiple opportunities to prove that they have achieved the desired outcomes.

2. Employees should be told **why** a specific information security policy, or control, that applies to them, is in place. In OBE memorization of concepts is not sufficient, OBE requires learners to have *insight* and thus to understand **why** they are doing something.

3. Due to the different levels of prior education, different organizational roles and different individual preferences of employees in an organization, learning materials used in an organization should be customized

to the needs of individual learners. Recognizing that individuals learn in different ways and at different paces are concepts central to OBE. Flexible learning material, to suit individual needs, is a pre-requisite in an outcomes based program.

4. In order to control costs, and to provide the above-mentioned flexibility in learning materials, organizational learners should be responsible for their own learning. The organization should supply the learning materials in formats that support as many learning styles as possible, but responsibility for using those materials should ultimately rest with the individual employees. Employees should thus take ownership of their learning. This concept of ownership and self-driven learning are central to OBE, which is essentially a learner centered educational methodology.

5. Hand-in-hand with ownership and responsibility is accountability. Organizations need to make employees accountable for their own learning, otherwise, they would not be able to hold them accountable for negligence stemming from a lack of education. In OBE, and other educational methodologies, assessment plays a vital role. Learners must be held accountable for their learning in order to get them to accept ownership of their learning.

6. Lastly, without feedback in **any** educational system, learning is not possible. This holds true for both information security education and OBE. In an outcomes based system, feedback is deemed even more important than in many traditional pedagogical models. Success, in OBE, **depends** on how well learners process the feedback they get regarding their efforts (Killen, 2000).

OBE can thus be seen to match all of the requirements for information security education identified by the previous chapter. In fact, a closer examination of the "results-based" educational framework advocated by NIST 800-16 (1998) for information security programs will reveal many elements that are common to OBE as well. For example, NIST argues that information security education programs should be "results-based" and should focus on job functions, or roles and responsibilities specific to individuals (NIST

800-16, 1998, p. iii). OBE aims to help learners achieve a specific outcome or attain a specific skill. These outcomes should reflect the complexities of the real life and the roles the learners would have to fulfill (Killen, 2000). In an organizational context this would mean that the outcomes would have to reflect skills needed in the individual's day-to-day job functions.

4.6 Conclusion

This chapter examined Outcomes Based Education (OBE). It introduced OBE as an educational methodology whose aim is to help learners achieve a specific *outcome*. At the end of an OBE program the learners have to be able to **successfully apply** the skills taught in the program. The design of an OBE program follows a top-down approach towards curriculum design. An OBE program's design starts with a clear and unambiguous statement of the desired outcomes. Based on these outcomes the content of the course is then created. Lastly a set of criteria is chosen to help evaluate whether or not a learner achieved the stated outcomes. The whole process, around which an OBE program is build, should always keep the basic premises, and principles, of OBE in mind.

OBE is based upon three basic premises, namely:

1. *All* students can learn and succeed, but not all in the same time or in the same way.
2. Successful learning promotes even more successful learning.
3. Schools (and teachers) control the conditions that determine whether or not students are successful at learning.

OBE is also based on four main principles, namely:

1. Clarity of focus
2. Designing back
3. High expectations for all students
4. Expanded opportunities for all learners

In order for an educational program to be outcomes based it has to adhere to *all four* of these principles. The chapter then discussed assessment in OBE programs, and listed some principles these assessment standards have to adhere to. Lastly this chapter compared OBE to the requirements for information security education, as proposed in chapter 3. It was shown that OBE fits the requirements for information security education well. OBE can thus be used as a pedagogical model for the design of user education programs to impart knowledge about information security to organizational end-users. It is, however, important to realize that outcomes are not values, beliefs, attitudes, or psychological states of mind (Spady, 1994, p. 2). OBE, and education in general, alone, cannot change the *attitudes* of users towards information security. In order to address user attitude, the second dimension to the "human factor" in information security, as discussed in chapter 2, it is necessary to cultivate an information security culture throughout the organization (Von Solms, 2000). The next chapter will examine the concept of such a culture in more detail.

Chapter 5

CORPORATE CULTURE

This chapter examines corporate culture. It defines corporate culture and then expands this definition towards an information security culture. This chapter further examines organizational learning theory in general. Lastly a process for changing corporate culture is presented, and a list of psychological factors that should be considered in a cultural change process is provided.

5.1 Introduction

Many organizations have realized that their own employees are the biggest threat to their information systems (Von Solms, 2000). Previous chapters analyzed this "human factor" in information security and introduced two dimensions to this human factor, namely; knowledge and attitude (or behavior). Chapter 3 suggested that the first of these dimensions, knowledge, can be addressed via an extensive information security user education program. Chapter 4 suggested outcomes based education (OBE) as a suitable educational methodology for such a program. It is, however, important to realize that outcomes are not values, beliefs, attitudes, or psychological states of mind (Spady, 1994, p. 2). In order to change a learner's values, beliefs, attitudes, or psychological states of mind, **more** than just education will be required. The "strength" of current beliefs and values will also have a major impact on how easy or difficult it will be to change these beliefs and values. It is therefor important to realize that the learners in a corporate information security education program will, in most cases, be **adults**.

Adults have well established values, beliefs, and opinions, as opposed to

the formative beliefs, values, and opinions of children. In addition to this, adults may have had differing education, varying years of experience, and a wealth of previously learned information (NIST 800-16, 1998, p. 21). Adults relate new information and knowledge to previously learned information, experiences, and values. This happens both consciously and unconsciously, and could lead to misperception and miscommunication (NIST 800-16, 1998, p. 21). In addition to this risk of the learners misinterpreting the "lessons", there is also a risk that they might understand the knowledge they are taught correctly, but still fail to comply to the information security policy, for example, because they disagree with the policy itself (Schlienger & Teufel, 2003). To counter this risk and thereby address the second dimension to the human factor, attitude, it is necessary to cultivate an organizational sub-culture of information security (Von Solms, 2000; Schlienger & Teufel, 2003).

Through the establishment of such a culture of information security, users can become a security asset instead of being a threat (Von Solms, 2000). Education of employees plays a very important role in the establishment of such a culture. It is paramount that the people are educated to *want to be* more secure in their day to day operation (Nosworthy, 2000). Such a change of attitude is of utmost importance, because a change in attitude automatically leads to a subsequent behavioral change (Nosworthy, 2000). Through the establishment of an information security culture, the employees can become the organization's most valuable assets.

Many recent studies have shown that the establishment of an Information Security "culture" in the organization is in fact **necessary** for effective information security (Eloff & Von Solms, 2000; Von Solms, 2000). Some of these studies have presented definitions of what an information security culture is. This dissertation presented an informal definition of such a culture in chapter 2, which defined a corporate culture of information security as; the predominating attitudes towards information security and security related behavior that characterize the functioning of the employees within the organization. However, since failure to pay sufficient attention to behavioral theories is one of the primary weaknesses of current security education programs (Siponen, 2001), this dissertation will use a more formal definition of corporate culture from the management sciences.

Once a more formalized definition of corporate culture has been provided,

this chapter will expand the formal definition, in order to make it more specific to an information security culture. Next, due to the importance knowledge plays in an organization's overall information security strategy, and in the establishment of an information security culture, the concept of organizational learning will be examined in more detail. Thirdly, this chapter will provide a process for changing, or introducing, a corporate culture. This process will be "borrowed" from the behavioral sciences, since failure to adhere to behavioral principles is one of the problems with current information security education (Siponen, 2001). The success of such a culture change process will, to a large extend, depend on several psychological factors being adequately addressed. Therefor, this chapter will conclude with an examination of these psychological factors that should be addressed as part of a culture change process.

5.2 Corporate Culture Defined

Every organization has a particular culture, comprising an omnipresent set of assumptions that is often difficult to fathom, and that directs the activities within the organization (Smit & Cronjé, 1992, p. 382). Such a culture could be defined as; the **beliefs** and **values** shared by people in an organization (Smit & Cronjé, 1992, p. 382). Beliefs and values, however, are both concepts that can be difficult to quantify. It is therefor often tempting to think of culture as just "the way we do things around here" (Schein, 1999a, p. 15), or that "something" that makes an organization more successful than others (Smit & Cronjé, 1992, p. 383). However, oversimplifying the concept of culture is the biggest danger to understanding it (Schein, 1999a, p. 15).

A better way to think about culture is to examine the different "levels" at which culture exists (Schein, 1999a, p. 15). Figure 5.1 illustrates these different levels. This way of thinking about corporate culture is already widely accepted in information security (Schlienger & Teufel, 2003). In order to clarify these levels of culture, each of the levels will now be briefly examined in more depth.

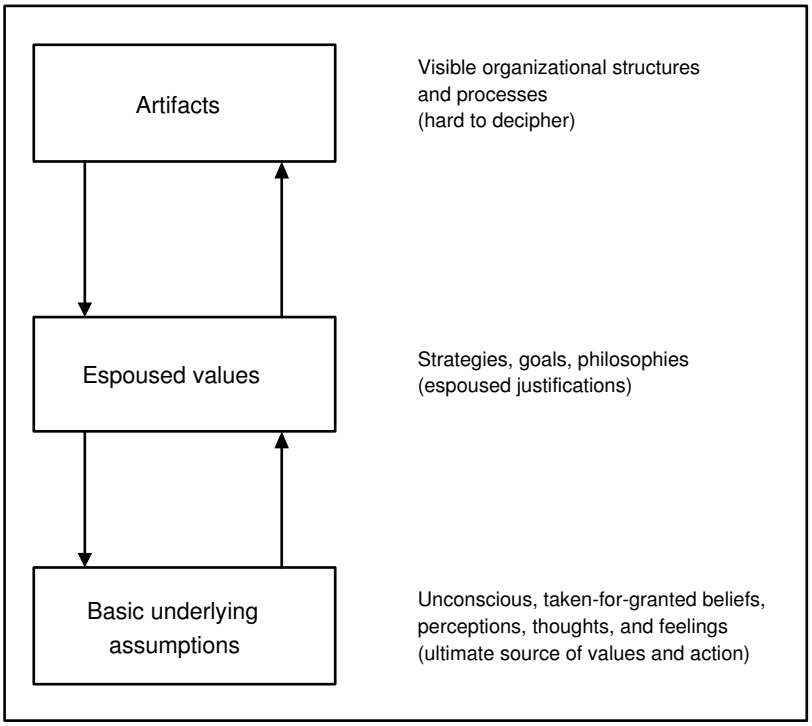

Figure 5.1: Levels of Culture (adapted from Schein, 1999, p. 16)

Level One: Artifacts

Artifacts are what you can observe, see, hear, and feel, in an organization (Schein, 1999a, p. 15). Artifacts would include visible organizational structures and processes. At the level of artifacts, culture is very clear and has an immediate emotional impact, which could be positive or negative, on the observer (Schein, 1999a, p. 16). Observing the artifacts alone, however, does not explain **why** the members of the organization behave as they do (Schein, 1999a, p. 16). In order to understand the reasons for the behavior patterns of organization members it is necessary to examine "deeper" levels of culture (Schein, 1999a, p. 16), such as the organization's espoused values.

Level Two: Espoused Values

An organization's *espoused values* are the "reasons" an organizational insider would give for the observed artifacts (Schein, 1999a, p. 17), for example; that the organization believes in team work, that everyone in the organization's view is important in the decision making process, etc. Espoused values generally consist of the organization's *official* viewpoints, such as mission-

or vision-statements, strategy documents, and any other documents that describe the organization's values, principles, ethics, and visions (Schein, 1999a, p. 17). However, it is possible for two organizations to have very different observable artifacts and yet share very similar espoused values (Schein, 1999a, pp. 18-19). This is because there is an even deeper level of thought and perception that drives the overt, or observable, behavior (Schein, 1999a, p. 19). The espoused values are values which the organization *wants* to live up to. The interpretation, and application, of these espoused values in the day to running of the organization depends on the shared tacit assumptions between the employees of that organization.

Level Three: Shared Tacit Assumptions (Basic Underlying Assumptions)

The *shared tacit assumptions* in an organization develop in any successful organization. Often these assumptions are formed in the organization's early years, *because* certain strategies have proven to be successful (Schein, 1999a, p. 19). If strategies based on specific beliefs and values continue to be successful, these beliefs and values gradually come to be shared and taken for granted. The beliefs and values become *tacit assumptions* about the nature of the world and how to succeed in it (Schein, 1999a, p. 19). These values, beliefs, and assumptions that have become shared and taken for granted in an organization, form the essence of that organization's culture. Beliefs, in this sense, refer to a group of people's convictions about *the world and how it works*, whilst values refer to a community's basic assumptions about *what ideals are worth pursuing* (Smit & Cronjé, 1992, p. 383). It is important to remember that the shared tacit assumptions resulted from a *joint learning process.*

The corporate *culture* of any organization, is a result of all three the above levels. At its most basic, and most difficult to quantify, level, the members of the organization share certain beliefs and values. These *shared tacit assumptions* act as a kind of "filter", which affects how individuals will carry out their normal day-to-day activities. It also influences how these individuals interpret the organization's policies, and how they implement its procedures. These policies and procedures form part of the organization's *es-*

poused values. The espoused values can be seen as the "visible" contribution of the organization's management towards the organization's culture. To a degree, espoused values provide cultural direction. The interpretation of this "direction", however, is extremely dependant on the underlying shared tacit assumptions.

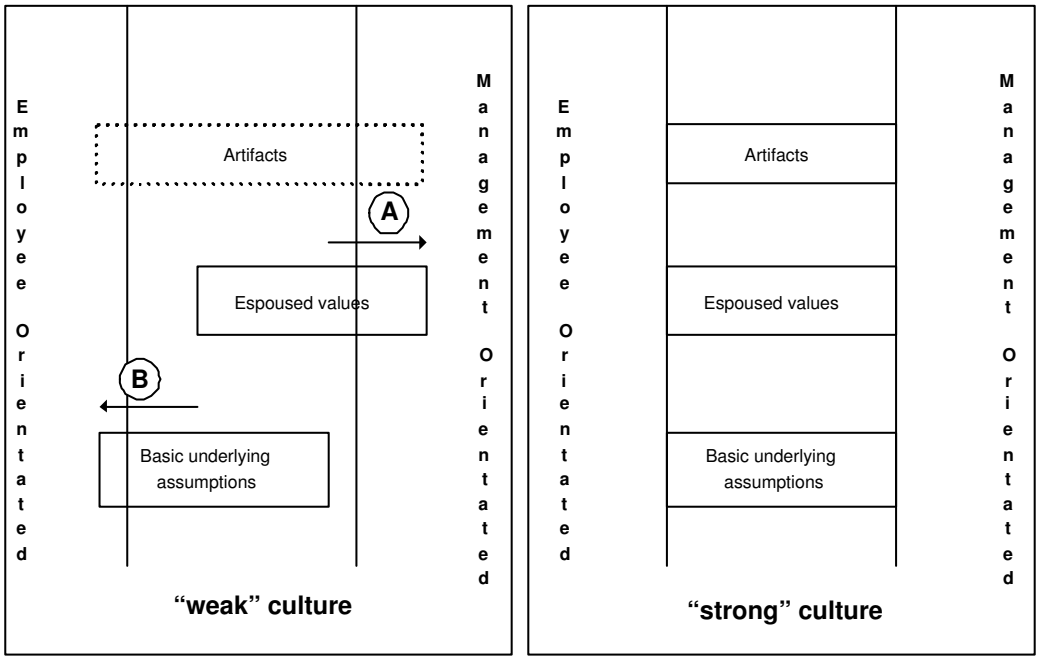

Figure 5.2: The Effect of the Combination of Culture Levels

The combination of the espoused values, and the "filtering effect" of the shared tacit assumptions on these espoused values, results in the visible, and measurable *artifacts.* This relationship is demonstrated in figure 5.2. In terms of figure 5.2 a *strong* culture would be a culture where the underlying beliefs and values of the employees are aligned with the policies and other espoused values, as laid down by the organization's management. In such a culture, the measurable artifacts would have a strong correlation to the espoused values **and** the underlying shared tacit assumptions. On the other hand, in terms of the "filtering effect" as illustrated by figure 5.2, a *weak* culture would be a culture where the shared tacit assumptions are **not** aligned with the espoused values. Such a culture would result in a weaker correlation between the espoused values and the measurable artifacts. In such a culture the underlying beliefs and values are not in line with management's vision for the organization. This misalignment results in two opposing forces,

indicated by the vectors A and B in figure 5.2, whose counter-acting effects result in artifacts which are not in line with management's vision. Vector A indicates that the espoused values are more "management orientated", or more authoritarian. Vector B indicates that the underlying beliefs and values of the employees are more "employee orientated", or less authoritarian. As shown in 5.2, the opposing forces in a *weak* culture could make it difficult, if not impossible, to accurately predict the artifacts. However, if the espoused values and the shared tacit assumptions are perfectly aligned, as shown on the right-hand side of 5.2, it should be possible to accurately predict the resulting artifacts. The terms *strong* and *weak*, as used above, do **not** refer to the actual stability of the culture, or to the magnitude of the impact the culture's impact on the visible artifacts, instead it refers to the desirability of the culture in terms of management's vision for the organization. A *strong* culture, in the context used above, is thus a culture where the measurable results of the *way things are done* in the organization, is both **predictable** and desirable. According to Schein (1999a, pp. 25-26) the magnitude of **any** organizational culture should not be underestimated. Schein (1999a, pp. 25-26) provides the following three basic facets of any organizational culture that should always be kept in mind when working with culture:

1. Culture is deep: If culture is treated as superficial any results to change it will always fail. Culture controls people more than people control culture. This is because culture is based on *tacit* assumptions that form part of the basic belief systems of people.

2. Culture is broad: **All** aspects of both internal and external relationships in an organization are affected by culture. Beliefs and values are formed about every aspect of daily life. Deciphering culture can thus seem like an endless task.

3. Culture is stable: Culture provides meaning to day-to-day activities and makes life more predictable. Humans do not like chaotic or unpredictable situations, and thus always try to "normalize" such situations. Attempts to change an existing culture is therefor always met with high levels of anxiety and resistance to change. Culture is one of the most stable facets in an organization.

For an organizational sub-culture of *information security*, an additional *dimension* to the culture needs to be considered if the employees are expected to behave in the correct way. This additional dimension is the relevant information security knowledge. An information security culture's definition would thus deviate slightly from the standard definition for corporate culture.

5.2.1 Information Security Culture Defined

As mentioned in 2.4, the two dimensions to the "human factor" in information security, namely knowledge and attitude, are very inter-related. Due to this co-dependency between knowledge and attitude, it is not possible to ignore the impact a lack of information security related knowledge would have on the organizational sub-culture of information security. In "normal" definitions of organizational culture, the relevant job-related knowledge are generally ignored, because it can be assumed that the average employee would have the needed knowledge to do his/her job. In the case of information security, the required knowledge is not necessarily needed to perform the employee's *normal* job functions. Knowledge of information security is generally only needed when it is necessary to perform the *normal* job functions in a way that is consistent with good information security practices. However, if an organization is trying to foster a sub-culture of information security, **all activities** would have to be performed in a way that is consistent with good information security practice. Having adequate **knowledge** regarding information security is a prerequisite to performing **any** security related activity successfully. Information security knowledge, or a lack thereof, would influence all three levels of culture in the following way:

Artifacts: At the artifact level, knowledge relating to **how** a specific task should be performed in a secure manner is required. Without the necessary skills and proficiencies, it would be impossible to perform security related tasks correctly.

Espoused Values: In order to create a security policy that is consistent with good security practices, and that fits the organization's specific security needs, a high level of security knowledge is required. To create the policy document, the person, or team, responsible for the drafting of the policy must know **what** to include in such a policy.

Shared Tacit Assumptions: Knowing **why** a specific control is needed, not only improves employee understanding about security, but can also play a vital role in changing beliefs. Employees who do not know why a control is there, might still disobey the policy even if they are aware of the policy (Schlienger & Teufel, 2003).

The co-dependency the levels of an information security culture have on knowledge, is illustrated in figure 5.3

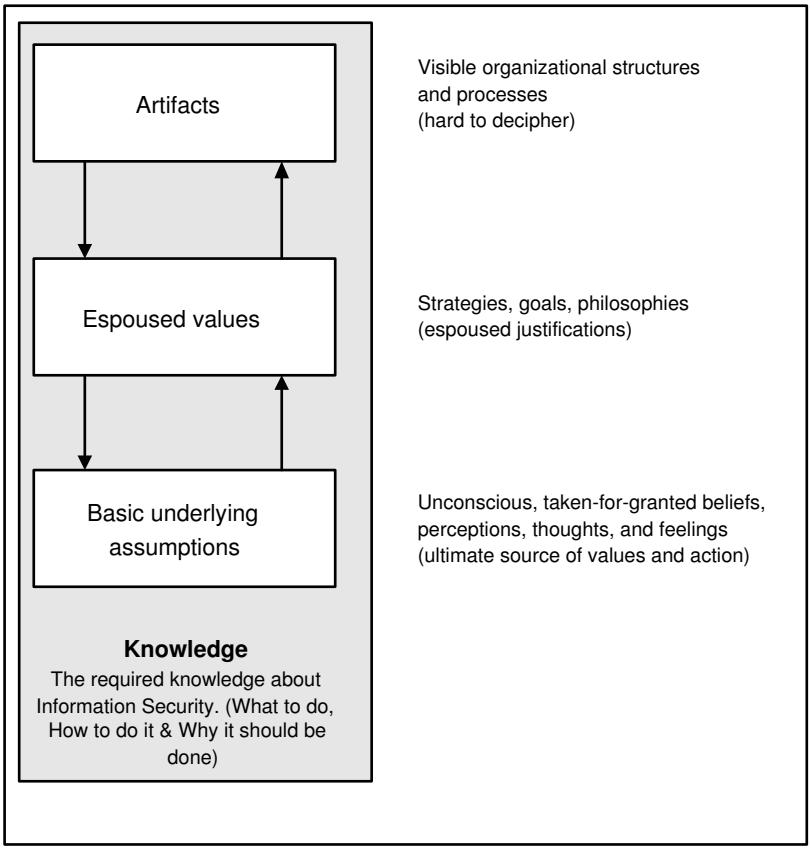

Figure 5.3: Information Security Culture

The co-dependency between the organization's information security culture, and the information security knowledge of its employees, could potentially have a detrimental effect on the organization's overall information security. In an organization where all three the levels of culture are consistent with the organization's information security needs, the measurable artifacts would still be influenced towards weaker security, *if* there is a lack of security related knowledge. In an organizational sub-culture of information security, a lack of

the necessary knowledge would effectively negate the positive impact such a culture would have on the overall information security efforts of the organization. Without adequate knowledge, even employees actively *trying* to behave securely, might inadvertently cause a breach in the organization's security. As mentioned in section 2.4.1, information security knowledge is a prerequisite, if a human is expected to behave securely. In the case of information security, the two dimensions of the human factor, namely knowledge and attitude, are **co-dependant** on each other and thus, *cannot* be dealt with in isolation. In the case of an organizational sub-culture of *information security*, this would imply that the culture as a whole, must be supported by the requisite knowledge. The negative effect that a lack of knowledge could have on such a culture is illustrated in figure 5.4.

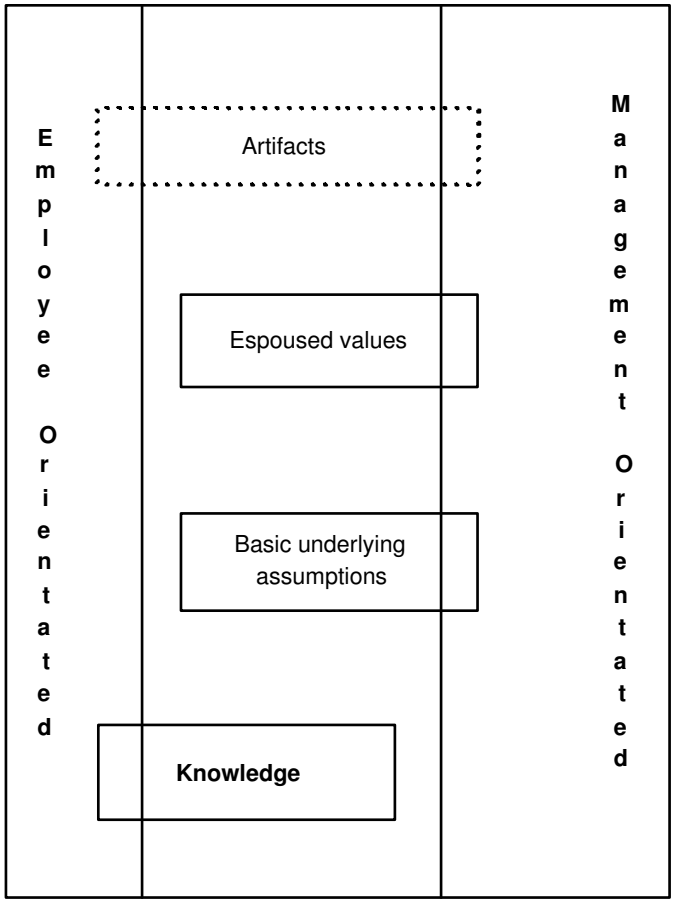

Figure 5.4: The Effect of Knowledge on an Information Security Culture

It is also possible for the organizational management to be unaware that the security is *weaker* than it should be. In order to "quality assure" the

organization's information security it is vital to implement **security metrics** to continuously and dynamically measure information security aspects in the organization. Such metrics can supply knowledge regarding how well the information security policies, procedures, etc are complied with (Von Solms, 2000). It is also necessary to ensure that the security policy is based on internationally accepted standards (Von Solms, 2000, 1999). If the security policy is based on internationally accepted standards, a security audit could be a useful tool to measure whether or not the artifacts are in line with the espoused values.

The very characteristics that make organizational culture difficult to work with, are also the characteristics that make a *strong* or *desirable* culture such a big asset to the organization. In an organization where the underlying beliefs and values of employees are in line with the values espoused by management, the visible artifacts will be both predictable and desirable. In an organization with such a culture, employees will behave in a desirable way because, that is simply *the way things are done*. It is thus worthwhile investigating how such a culture could be changed or manipulated. However, as mentioned earlier, culture is based on the underlying beliefs and values of employees, and is thus very *stable*. Any attempt to change culture, thus will have to change the shared tacit assumptions of employees. These shared tacit assumptions were formed as the result of years of *joint learning experiences* (Schein, 1999a, p. 19). In order to change the tacit assumptions, it is thus necessary to provide new joint learning experiences. In other words, the organization as a whole has to learn. If the aim is to establish an organizational sub-culture of information security, part of this organizational learning process would encompass the underlying knowledge required. The organization as a whole would also have to learn *new ways* of doing things. These *new ways* will be governed by variables which might need adjusting until a suitable level of information security has been obtained. Organizational learning theory, from the management sciences, is a field of study that could contribute to the management of such a learning process. The main principles of organizational learning will therefor be briefly examined.

5.3 Organizational Learning

Organizational learning, as a field of study, has existed for many decades. According to Malhotra (1996) organizational learning could be defined as the process within organizations by which knowledge about action-outcome relationships and the effect of the environment on these relationships is developed. Most current organizational learning theories stem from theories originally developed by Chris Argyris and Donald Schon (Smith, 2001a, 2001b). These theories were based on the idea that people have mental maps with regard to how to act in situations. These maps involve the way people plan, implement and review their actions. Argyris and Schon asserted that it is these maps that guide people's actions, rather than the theories they explicitly espouse (Smith, 2001b). Smith (2001b) describes the process involved using a model based on three elements:

- **Governing variables**: Those dimensions that people are trying to keep within acceptable limits. In information security this could refer to acceptable levels of risk. In terms of an information security culture, these governing variables could refer to the organization's espoused values.

- **Action strategies**: The moves and plans people use to keep the governing variables within the acceptable range. In information security these would include procedures outlining employee behavior in specific scenarios. Both action strategies and governing variables correspond to a large degree to an organization's espoused values.

- **Consequences**: What happens as the result of an action. These would include both intended and unintended results. In terms of corporate culture, the consequences correspond to the artifact level of culture.

In organizational learning theory, there are two main types of learning, namely, adaptive learning and generative learning. Currently most organizations focus on adaptive, also called single-loop, learning. Instead companies should be focussing on generative learning or "double-loop" learning (Malhotra, 1996; Rowe, 1996). Single-loop learning can be likened to a thermostat (Rowe, 1996). If a thermostat learns it is too hot or too cold it will turn the heat on or off. It can do this because it receives information about the

current temperature and it has the ability to take action through turning the heat on or off. Single-loop learning is usually present where the underlying governing variables, such as goals, values and frameworks, are taken for granted (Smith, 2001b).

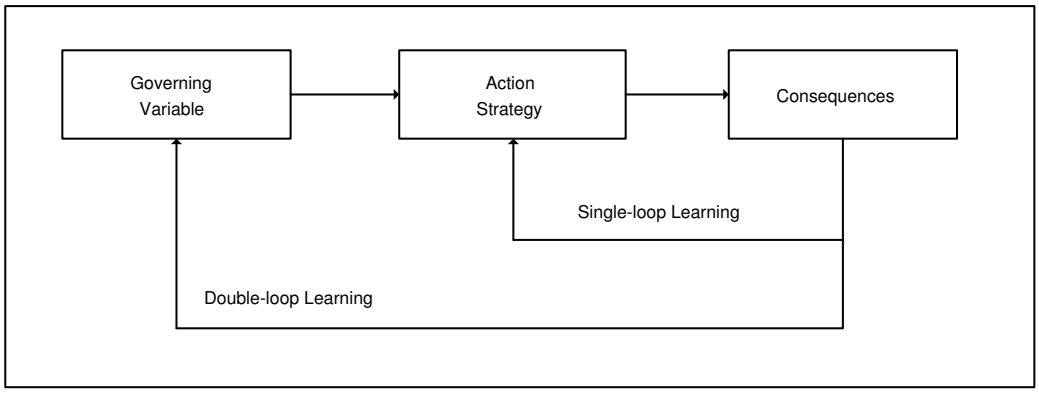

Figure 5.5: Single and Double Loop Learning

In order for organizational learning to take place, companies should be focussing on generative, or double-loop, learning (Malhotra, 1996). Generative learning emphasizes continuous experimentation and feedback in an ongoing examination of the very way in which organizations go about defining and solving problems. Thus, it can be likened to a thermostat that has the ability to ask why it is set at a specific temperature and can then explore whether another setting might be more effective (Rowe, 1996). Double-loop learning could thus result in the underlying governing variables being adjusted should they be found to be ineffective or unrealistic. Figure 5.5 demonstrates the relationship between the three elements of the model and the two types of learning.

Even though the concept of organizational learning is directly relevant to creating joint learning experiences, which could influence culture, organizational learning theory was not developed to address organizational culture *specifically*. On its own, organizational learning is not necessarily sufficient to change organizational culture. It can, however, play a role in the manipulation of culture, especially in the determination, and adjustment, of espoused values (governing variables). In order to change organizational culture, it is necessary to follow a structured change management process (Schein, 1999a, p. 132). Without such a structured process it will be difficult, if not impos-

sible, to change the underlying beliefs, values and principles of employees, to a "level" that matches the organization's espoused values. As argued earlier, a mismatch between the espoused values and the shared tacit assumptions operating in an organization, could result in unpredictable artifacts. Such a structured transformative change management process, for the management of an organizational culture change process, will thus be presented below.

5.4 Changing Corporate Culture

Corporate culture affects all aspects of the day-to-day business of an organization. As such, it is very important to understand the *current* culture in an organization, *before* trying to change it. Changing organizational culture should never be taken lightly. The impact of a planned change might be very far-reaching and could have undesirable consequences. The first step in any cultural change process should be to clearly define the desired or ideal future state of the culture.

5.4.1 Defining the Desired Future State

Sadri and Lees (2001) place the main responsibility for changing a corporate culture on the shoulders of management. Management need to provide a clear vision of where the organization would *like to be* in terms of the corporate culture. The definition for the desired future culture must be clear and concrete. Basically this phase of a culture change process should answer the question: "If you are to solve the business problem or achieve the ideals that are not being met, **what** are the **new ways of thinking** and working that will get you there?" (Schein, 1999a, p. 133). Without a clear definition of the behavioral changes that are ultimately needed, it is not possible to test the relevance of culture to the change process (Schein, 1999a, p. 134). In other words, the organization needs to know, *in cultural terms* what should change, otherwise they will not be able to measure the behavioral change. The obvious next step, once the desired state of the culture has been determined, is to assess what the *current* state of the culture is.

5.4.2 Assessing Corporate Culture

According to Schein (1999a, pp. 24-25) it is impossible to infer the shared tacit assumptions just from observing the behavior, or artifacts. However, if the shared tacit assumptions is understood, it is easy to predict the artifacts. The key to understanding an organization's culture is thus to gain understanding regarding the underlying shared tacit assumptions. According to Schein (1999a, pp. 86-87), culture should be assessed by means of individual and group interviews. Schein (1999a, p. 86) also warns that surveys or questionnaires should **not** be used to assess culture. Survey responses can be viewed as artifacts, but do not say anything about the deeper values or assumptions (Schein, 1999a). Schein (1999a, pp. 86-87) provides the following outline towards assessing corporate culture:

1. Before a culture assessment is done, a specific problem context for the assessment should be determined. A culture assessment has no value unless it is done in the context of a specific organizational problem or issue. Culture itself is too vast to accurately assess. The impact of culture on a specific goal can, however, be assessed meaningfully.

2. The cultural assumptions should be identified. These assumptions should then be categorized as either strengths or constraints in terms of the specific problem that the organization is trying to address.

3. If necessary, assessment should be done on any relevant sub-cultures that might influence the current problem.

5.4.3 Determine Work to be Done

Once the current state of the culture has been assessed, and the desired future state of the culture has been clearly defined, the amount of *work* to be done should be determined. The *present* should be assessed in terms of the *future* in order to quantify the amount of work needed to get from the present state to the future state (Schein, 1999a, p. 133). According to Schein (1999a, p. 136), identification of the gaps that need to be bridged should make the areas where cultural assumptions aid, or hinder, the change agenda more apparent. Once the gaps have been identified, processes to bridge these gaps, can be

introduced. In terms of psychodynamics, the process in a transformative change program consist of three basic steps (Schein, 1999a, pp. 116-126):

1. **Unfreezing: creating the motivation to change**. Essentially this step is a process of disconfirmation, which should make employees realize that the current way they are doing things is no longer working. During this step a certain level of survival anxiety will be instilled when employees recognize the need to change. This survival anxiety will generally be replaced by learning anxiety, once employees accept the need to change. It is very important to create psychological safety in order to overcome this learning anxiety. See section 5.5

2. **Learning new concepts**. This stage is where new ways of doing things are learned. Generally employees will identify and imitate role-models, and/or attempt to adjust to new requirements through trial-and-error learning. Effective employee education programs can play a major role during this phase of the change process.

3. **Internalizing new concepts and meanings**. During this phase new behavior becomes part of the employee's self-concept and identity. The new way of doing things is incorporated into ongoing relationships.

The above steps form the basis of a learning cycle in a culture change process. These three steps should however be supported by an underlying, formal, educational program.

5.4.4 Educate Employees

The change manager must think carefully about which *outcomes* he/she wants (Schein, 1999a). Decisions should be taken about whether entire groups, or units, should adopt the new way. In most culture change programs it will be necessary to get entire groups to adopt new ways of thinking and behaving. Therefor initial training activities should be aimed at groups, not individuals (Schein, 1999a, p. 129). It is important to remember that the shared tacit assumptions result from joint learning processes. If only key individuals adopt the changes, they will, over time, revert back to the norms of the group (Schein, 1999a, p. 129). The change manager also needs to

decide whether or not the new way of thinking and behaving can be standardized. In other words, consensus should be reached on the new way of behaving. If role models, and examples of correct behavior, can be provided it will speed up the learning process (Schein, 1999a, p. 129). The danger of standardizing, and thus prescribing, the behavior is that some learners might fail to internalize the *new ways* (Schein, 1999a, p. 130). Such learners will eventually revert to the *old way*, unless their behavior is continuously "policed". The alternative to standardizing the new ways of thinking, and behavior patterns, is to provide clear goals to learners, and to allow them to develop their own behavior patterns. This process is slower, but guarantees internalization of concepts learned (Schein, 1999a, p. 130). In this instance role models, and clear examples, should be withheld. Evolutionary learning and change go on all the time (Schein, 1999a, p. 130). Organizations are dynamic systems that interact with perpetually changing environments. If some part of the organization can learn an alternative way of thinking, and if the alternative can be shown to be **successful**, there will be less anxiety in introducing this alternative way to the rest of the organization (Schein, 1999a, p. 130). It can therefor be beneficial to introduce the educational, and culture change, program in a single department first. In terms of the psychodynamic processes outlined in the previous subsection, it should be clear that the **education** cycle in a culture change process is much more than just a formal "classroom" type of learning. It also includes learning that takes place in the employee's day to day activities. Shared tacit assumptions are formed as part of a joint learning process based on successful behavior. During a culture change, employees have to unlearn behavior patterns that *used to be* successful. These old behavior patterns then need to be replaced with new way of behaving. Most of the real learning will take place in the actual workplace where role-models can play a vital role. For example, in an information security context, the employee might try to imitate the behavior of someone he/she perceives to be more "security literate". However, if new tacit assumptions are to be formed based on these learning experiences, it is vital for employees to perceive the desired way of behaving as being successful. In order to show that this alternative way of operating is successful, some way of measuring the benefits would be needed.

5.4.5 Measuring and Feedback/Rewards

Corporate culture should start with proper visionary statements and should thereafter be **positively reinforced** through management behavior i.e. rewarding employees' successes and distributing newsletters and videos that reinforce the culture. Leadership from the very top of an organization is essential for major cultural change. However, even though middle managers do not initialize the cultural change, ultimately it is their actions that produce the changes (Brubakk & Wilkinson, 1996). Thus the culture change process has to be supported by a sound user education program **and** reinforced via continuous feedback. This feedback will come from the organization's middle management (Brubakk & Wilkinson, 1996). It is vital to remember that shared tacit assumptions are formed as the result of continuously **successful** past behavior (Schein, 1999a, p. 19). In the case of information security, it will be very difficult for employees to know that their new behavior patterns are successful, because successful information security is mostly tacit, and difficult to quantify. It is therefor vital to implement security metrics and to use these metrics to continuously provide feedback to employees. Employees must realize that their behavior is successful, or that the *old way* of doing things is not successful. Such metrics should thus, ideally, become part of the key performance indicators for employees. It is also important for management to show their commitment to this cultural change through **rewarding** employees that behave correctly (Brubakk & Wilkinson, 1996). Employees could be coerced into behaving in a specific way, but such a behavior change will be superficial and unstable (Schein, 1999a, p. 115). A reward system based on "impartial" metrics, in combination with a degree of coercion is likely to be more successful. However, without "impartial" metrics, a reward system could be viewed as biased or unfair and might result in employee dissatisfaction.

Most of the above steps would form part of a repetitive change management cycle. True culture change is a lengthy process. During the entire change process, the change team, and its leaders, *must* own the change process and *must* be held accountable for it (Schein, 1999a, p. 137). Lastly, it should be realized that any change, or learning process, will result in a certain degree of learning anxiety (Schein, 1999a, p. 122). It is extremely

important to address this learning anxiety, and other psychological factors which may arise during a culture change process. A culture change process that does not equitably involve the employees, and address their fears and needs, *cannot* be considered ethical (Woodall, 1996). The above process should thus be supported by processes which deals with such psychological factors. These psychological factors will thus, for the sake of completeness, be briefly discussed.

5.5 Psychological Factors

Several psychological factors could influence a culture change process. These factors need to be addressed by management during such a change process. A culture change process could result in learning anxiety amongst the employees. Such anxiety could be caused by several factors. Schein (1999a, pp. 122-123), presents the following list of causes for learning anxiety:

- Fear of temporary incompetence: Employees might feel anxiety because they have given up the old way of doing things, but feel they have not mastered the new way yet.

- Fear of punishment for incompetence: Employees might fear that they will be punished for being less productive because they spend too much time learning the new way of doing things. This might result in employees *never* mastering the new way of doing things, because they spend too much time trying to remain productive, and thus do not "take off" enough time to master the new skills.

- Fear of loss of personal identity: Employees might resist change because they strongly identify with the *old way* of doing things. Many people might not want to be the kind of person the new system requires them to be. As an example: In an information security context, a person who is used to always "helping" anyone who approach them, might resist the kind of "naturally suspicious" behavior required from them to counter the threat of social engineering.

- Fear of loss of group membership: The shared assumptions that make up culture also help people define who is "in" and who is "out" of the

group. If people are forced to change, they might fear being rejected by their group.

In response to learning anxiety people might act defensively. Schein (1999a, pp. 122-123), presents the following list of defensive responses:

- Denial: Individuals might convince themselves that the required changes are just temporary, or that management is "crying wolf".
- Scape-goating, or passing the buck: Individuals might convince themselves that the *new way* of doing things is someone else's responsibility. In information security, business users often "pass the buck" to the IT Department.
- Maneuvering or bargaining: People might want special compensation for the effort to make the change.

In order to address the above psychological factors, change managers should create psychological safety for employees. According to Schein (1999a, p. 124), two main priciples should govern transformative change:

1. Survival anxiety must be greater than learning anxiety.
2. Learning anxiety should be reduced, rather than increasing survival anxiety.

The reason why it is important to decrease learning anxiety, rather than increase survival anxiety, or coerce employees into changing, is that employees will simply increase their own defensiveness in response to a greater threat. Schein (1999a, pp. 124-125), presents the following list of ways to create psychological safety:

1. Provide a compelling positive vision.
2. Provide **formal** training.
3. Involve the learner.
4. Informally train relevant "family" groups and teams.
5. Provide "practice fields", coaches and feedback. In other words, hands on training is needed and must be reinforced via continuous feedback.

6. Management should be positive role models.

7. Support groups.

8. Consistent systems and structures.

Most transformative change programs fail because they do not provide psychological safety (Schein, 1999a, p. 126). Only if all the above factors are incorporated into a structured change management program can culture truly be changed.

5.6 Conclusion

This chapter focused on the concept of corporate culture. Earlier chapters have shown that the establishment of a corporate sub-culture of information security is necessary, in order to ensure the desired behavior of organizational employees towards information security. Without such a culture, it would be difficult, or impossible, to guarantee that employees have the correct attitude towards information security. A formalized definition of such a corporate culture was presented. This definition was based on the fact that culture consists of three levels, namely:

- Artifacts: The visible and measurable day-to-day behavior in the organization.

- Espoused Values: The written documents, such a vision or policy statements, that espouse the organization's *formal*values.

- Shared Tacit Assumptions: The underlying beliefs and values of the employees. These are the true drivers of employee behavior and were formed as the result of joint learning experiences based on successful past behavior.

This chapter also emphasized that any attempt to change the corporate culture *must* address the shared tacit assumption level of culture. The shared tacit assumption level of a corporate culture, consist of the beliefs, values, and principles of the employees. It is these beliefs, values, and principles that truly determine the behavior of employees. In the case of information security, it was argued that the three "normal" levels of corporate culture,

in isolation, would still not be sufficient to ensure the desired security levels. Any attempt to *ensure* employees behave in the desired way, *must* address both employee attitude, and employee knowledge. These two dimensions of the human factor in information security are co-dependent on each other. The definition for corporate culture was thus expanded to incorporate this co-dependency that an information security sub-culture would have on the level of information security related knowledge amongst employees. In order to learn the *new* attitudes, and to gain the required knowledge, the organization as whole would have to learn. Such a learning process would have to take organizational learning theory into account.

Organizational learning theory, which is applicable to any organization wide learning experience, was thus examined, since it *should* play a role in the creation of the joint learning experiences aimed at changing the shared tacit assumption layer of culture. Organizational learning theory on its own, however, is not sufficient to introduce, or change, the corporate culture of an organization. To change the organization's culture, a formalized transformative change management process, from the managerial sciences, would be needed. Such a formalized culture change process was briefly introduced. The ultimate aim of this culture change process is to change the underlying shared tacit assumptions of the organization's employees. These shared tacit assumptions are a very stable part of any organization's culture. Any attempt to change the shared tacit assumptions could thus result in psychological anxiety amongst the employees. A list of psychological factors that might negatively impact an attempted culture change was thus given. These psychological factors, and ways of dealing with them were briefly dealt with.

The next chapter will attempt to integrate all the concepts introduced in this chapter with the outcomes based educational model presented in chapter 4, in order to present a single holistic model to introduce a corporate subculture of information security into organizations.

Chapter 6

A FRAMEWORK FOR THE ESTABLISHMENT OF AN INFORMATION SECURITY CULTURE

This chapter combines the concepts introduced in previous chapters into a holistic, outcomes based, framework for the introduction of an information security sub-culture in organizations. The proposed framework is presented and argued in this chapter. The example of introducing a sub-culture of proper password security is used throughout this chapter to assist with the necessary explanations.

6.1 Introduction

Thus far this dissertation has introduced three distinct fields of study, namely, information security, outcomes based education, and corporate culture. In the discussion on information security the co-dependance of organizational information security on human cooperation was highlighted. This human factor is the weakest link in information security, and consists of two inter-related dimensions. Firstly, employees *must* have sufficient **knowledge** about information security in order to effectively implement and maintain the various information security controls. Secondly, the employees *must* have the correct **attitude** towards information security. Without the correct attitude,

even employees who have sufficient knowledge will still not behave in a secure manner (Schlienger & Teufel, 2003). Conversely, an employee who has the desired attitude, but, lacks the necessary knowledge, won't be *able* to behave securely. It is thus necessary to address both the above mentioned dimensions in order to ensure the security of an organization's information.

In order to address the knowledge dimension of the human factor in an organization's information security efforts, the organization's employees must be educated. In Chapter 3, this dissertation discussed information security education and identified several requirements an educational methodology would have to meet in order to be suitable for information security education. Outcomes based education (OBE), was introduced in chapter 4 as a methodology that could meet these predefined requirements. However, outcomes based education cannot change corporate culture, since outcomes are not values, beliefs, attitudes, or psychological states of mind (Spady, 1994, p. 2).

To instill the desired attitude towards information security amongst employees, a corporate sub-culture of information security needs to be established. The establishment of a corporate culture was discussed in the previous chapter. However, due to the above-mentioned co-dependence between the two dimensions of the human factor in information security, neither employee education, nor the establishment of a corporate sub-culture, should be dealt with in isolation. It is therefor necessary to combine the various methodologies and processes introduced thus far into a single holistic framework.

6.2 A Framework for Employee Education and Culture Change

This section will attempt to present a single holistic framework for the introduction of both an organizational information security sub-culture, and an information security education program. This framework will "borrow" concepts and processes from disciplines introduced in earlier chapters. In order to facilitate understanding, the teaching of correct password usage and the related fostering of a "secure password culture" will be used as a continuous example throughout the remainder of this chapter. This example, although

relatively detailed, should not be viewed as a *complete* solution, since it is intended only to clarify and illustrate the relevant steps. As with most other information security processes, the introduction of a corporate sub-culture of information security has to start with top-management.

6.2.1 Top Management Commitment

Firstly, top management will have to show its commitment to information security and to the "new" desired culture. This is done, firstly, by developing visionary statements and/or slogans (Sadri & Lees, 2001). This could be part of the corporate vision statement or an awareness campaign, for example; putting up, and endorsing, posters stating that the organization is committed to improving information security. For example, a poster, signed by the CEO, could be posted throughout the organization stating: *"At ABC we are committed to the integrity, availability and confidentiality of all our information"*.

Top management also has to visibly support the desired culture through its own behavior (Wallace, Hunt, & Richards, 1999), and through a commitment in terms of rewards for desirable behavior and punishment for undesirable behavior (Alpander & Lee, 1995). Rewarding desirable behavior and punishing undesirable behavior are both vital factors in shaping employee compliance in information security (Gonzalez & Sawicka, 2002). Once management has committed to the new culture, the *vision* for this information security culture has to be followed up by a corporate information security policy. This policy will form part of the organization's *espoused values*. The policy, in turn, is followed up by various sub-policies, each dealing with specific aspects of the desired culture.

Gaining complete top management commitment for the culture change process will thus be the first component to the integrated framework this chapter is presenting.

6.2.2 Define Problem in Business Context

According to Schein (1999a, pp. 86-87), culture change should always be done in a specific business context. Without such a context, culture change has no meaning. In terms of information security this would mean that each

specific security need should be addressed individually in order to ensure that both the dimensions to the human factor are dealt with. Defining the problem in a specific business context would consist of three steps. For each individual business problem:

- the current state, in terms of culture, should be assessed,
- the *ideal* future state should be defined and
- the steps needed to get from the current state to the ideal state should be defined.

Assess the Current State

The first step in defining the needed culture change is the assessment of the current state. This should be done at multiple levels. Firstly the current **espoused values**, or policy items and related business procedures, should be assessed. Secondly the current **artifacts** need to be assessed. In other words, measurements should be gathered to determine how well the current espoused values are implemented. Thirdly, the underlying **shared tacit assumptions** need to be assessed. This layer of underlying beliefs and values will generally be the most difficult to quantify. Several techniques, such as interviews and surveys, might contribute towards such an assessment (Martins & Eloff, 2002; Schein, 1999a, pp. 59-87). Lastly, in addition to the cultural layers, it is vital to assess the current underlying information security related **knowledge** of the employees. Several tools could be used to assess current knowledge levels, for example; questionnaires, online tests or interviews. In terms of password usage, it is thus, as an example, necessary to answer the following questions:

1. **Espoused Values**: What current policies and/or procedures exist regarding the authentication of employees?
2. **Artifacts**: How secure is the average password used by employees? How often do employees change their passwords? Do employees share their passwords with others? Do employees write their passwords down? Etc.
3. **Shared Tacit Assumptions**: How serious are employees about keeping their passwords confidential? Do employees believe that choosing

"easy" passwords for themselves could have a potentially negative impact on the organization as a whole? Etc.

4. **Knowledge**: Do all employees know *how* to change their passwords? Do employees know what would constitute a secure password? Do employees know the necessary techniques to create and remember secure passwords? Does each employee know what the consequences for him/her would be if a security breach results due to personal negligence regarding his/her password? Etc.

Once the current state has been assessed, the ideal future state should be defined in terms of the specific business process.

Define the Ideal State

The ideal future state for the specific business process should also be defined in terms of all three layers of the corporate culture, as well as the required employee knowledge. Such a definition should be specific and in terms of measurable outcomes. Without a clear definition of the behavioral changes that are ultimately needed, it is not possible to test the relevance of culture to the change process (Schein, 1999a, p. 134). For the password example, this definition could include:

- **Espoused Values**: One of the information security policy statements would be: *"All users of information must be authenticated before being allowed to use information resources".* This policy item, in turn, should be supported by a set of procedures dealing with the specific operational control. Thus, for password usage, these procedures could include:
  - All users must use passwords that is at least eight characters long and include at least two non-alphabetic characters
  - All users must change their passwords at least once every two weeks
  - Users may not write down their password or share their password with any other user
- **Artifacts**: In terms of the measurable artifacts clear metrics, supporting the relevant espoused values, need to be defined. For password usage these could include:

  - All passwords should withstand a standard brute force attack.
  - Administrative log-files should show that all passwords are changed at least once every two weeks.
  - Each and every user should have their own individual, not shared, user account.

- **Shared Tacit Assumptions**: Defining the desired underlying beliefs and values for an ideal future state will require a lot of insight into exactly what beliefs are needed. Basically this phase of a culture change process should answer the question: "If you are to solve the business problem or achieve the ideals that are not being met, **what** are the **new ways of thinking** and working that will get you there?" (Schein, 1999a, p. 133). For the password example these could include:

  - Every user must place as much value on the confidentiality of his/her user account's password, as he/she places on his/her personal bank account's pin-number. A user should never be willing to disclose his/her password, not even to the system administrator.
  - Every user should believe that the entire organization's wellbeing could depend on his/her password being secure.
  - Every user must *accept* personal responsibility for his/her password, and should **not** believe that security is the IT Department's responsibility.

- **Knowledge**: The knowledge required by individual employees should be clearly defined. This could be done in terms of the specific outcomes for the related employee education program. For the password example these specific outcomes could include:

  - The learner should be able to demonstrate that he/she is able to successfully change his/her own password
  - The learner should be able to successfully construct a secure password
  - The learner should be able to use mnemonic techniques to memorize and recall secure passwords

Once the *ideal* future state has been defined in terms of both the corporate information security sub-culture, and the required employee knowledge, the gap between the current state and the desired state needs to be analyzed for the specific business problem being addressed.

Determine the Steps Needed

The steps needed to get from the current state to the desired future state need to be clearly defined. In some cases it might be necessary to go through several intermediate "states" to eventually attain the desired *ideal* state. Culture is extremely stable and any attempt to change it will thus have to start with a disconfirmation process (See section 5.4.3). Employees will have to realize that the current way of doing things is no longer good enough. Without such an *unfreezing* of current values, employees will resist the change. Human systems tend toward trying to maintain a stable equilibrium. If change is to occur, this equilibrium must be upset by some new force. The recognition and management of these "change forces" creates the motivation for humans to change (Schein, 1999a, p. 117). The steps needed to get from the current state to the future state should thus cover all the psychodynamic steps of such a transformative change process (Woodall, 1996; Schein, 1999b, 1999a, pp. 116-139), as well as the required, formal, educational programs to impart the needed information security knowledge to employees. For the password example these steps could include:

- **Unfreezing/Disconfirmation**: Many employees currently believe that truly secure passwords are not necessary for them personally. This belief should be disconfirmed. Regular password audits should be run and disciplinary steps should be taken against employees whose passwords do not conform to the company policies. Regular internal propaganda programs should be used to emphasize that each and every password *must* be secure.

- **Learning**: Employees should be taught **what** would constitute a secure password. Employees should be taught techniques for constructing and memorizing such passwords, in other words, **how** to manage passwords. Employees should also be taught **why** it is necessary for each and every password to be secure.

- **Internalizing/Refreezing**: The average strength of each department's employees passwords should be included as a key performance indicator for that department's manager. Individual employees should receive continual feedback regarding their own password's strength. Employees should be rewarded for compliance, or disciplined for non-compliance.

To a certain extent, a culture change process will always be coercive (Woodall, 1996; Schein, 1999b). Schein (1999b) compares the processes needed for an enforced culture change to "brainwashing" techniques used in prisoner of war camps. Woodall (1996) argues that such a culture change process can only be considered ethical if there is an equitable balance between the degree of coercion used, and the rewards, and other positive spin-offs, for employees. It is also advisable to create communication conditions where employees have an equal say in the new cultural direction (Woodall, 1996). Involving employees at this planning stage should help to reduce resistance to change.

The above process of disconfirmation, learning, and internalization, is, to a large degree, dependent on the authority given to the person, or team, responsible for the culture change process, by top management. Without complete top management buy-in it would be difficult, or impossible, to apply the necessary degree of coercion and/or, give the needed rewards, to employees. It is thus advisable for the person, or team, responsible for the management of the culture change, to ensure that the steps outlined during this phase of the culture change process are possible, given the level of top management buy-in. As with "normal" organizational learning, it might be necessary to adjust the governing variables if the desired change is not possible. In other words, it might be necessary to opt for a less idealized but more realistic future state.

The above processes collectively comprise the second major component to the integrated framework this dissertation is presenting. The second component is thus the defining of the needed culture change in a specific business context. This definition process will repeat for each business process that need to be supported by the new culture, and consists of three subcomponents, namely:

- Assessing the current state of the culture in the context of the specific business problem.

- Defining the ideal future state of the culture in the context of the specific business problem.
- Determining the steps that should be taken to transform the culture *from* its current state *to* the defined, ideal future state for the specific business problem being dealt with. This will include analyzing the gap between the current, and ideal future states of the culture for the specific business problem, as well as outlining the strategies for unfreezing the culture, teaching employees the new culture, and refreezing, or internalizing, the new culture.

As discussed above, the success of the steps in this second component to the framework will depend on the degree to which top management has committed to the change process. Without top management authority, the necessary coercion and reward system would be difficult, if not impossible, to implement. Even though some degree of coercion, and some reward system, will always be needed during a culture change, it is also possible to use education as a source of disconfirmation (Schein, 1999a, pp. 120-121).

6.2.3 Educate The Employees

According to Schein (1999a, pp. 120-121) employees will often refuse to accept the need for new, responsible behavior patterns until they have been educated to the dangers inherent in environmental events, for example, the dangers inherent in using a weak password. Education is often the only way to convince employees and managers of the need to do things differently (Schein, 1999a, p. 120). For a culture change process it is thus vital to not only teach employees **what** to do, and **how** to do it, but also **why** it should be done. In the establishment of a corporate sub-culture of information security, education will thus play a role in changing attitude, as well as its role in conferring knowledge. As argued in previous chapters, it would be sensible to use a pedagogically sound methodology for such education. For information security education, outcomes based education (OBE) has been argued to be a suitable methodology. An outcomes based curriculum for the password example could be constructed as follows:

Step 1: Defining the outcomes

For the purposes of this example, outcomes will be defined in each of the three critical domains of outcomes, as discussed in section 4.2.3. These outcomes serve as an example only, and should not be considered a comprehensive list.

- **Performance:** These are outcomes relating directly to actual performance, for example:
  - The learner should change his/her password at least once every two weeks.
  - The learner should only use secure passwords. Such passwords should be at least eight characters long and should contain at least two non-alphanumeric characters. The password should also be able to withstand a "standard" brute force attack by auditing software.
  - The learner should be able to recall his/her password without needing to write it down.
  - The learner should understand **why** passwords need to be secure and **why** a password should be changed so often.
  - The learner should understand the consequences to him/her self as well as the organization as a whole if his/her password is compromised.
- **Content**: These are outcomes related to understanding of subject matter.
  - The learner should be able to demonstrate that he/she has the necessary skills to change his/her own password.
  - The learner should be able to discuss what would constitute a secure password. He/she should also be able to create secure passwords on a testing program.
  - The learner should be able to demonstrate that he/she can use mnemonics to construct and recall secure passwords.
  - The learner should be able to locate the information security policies and procedures dealing with password usage on the company

intranet. He/she should be able to discuss the implications of these policies and procedures for him/her self.

  - The learner should be able to discuss the consequences of his/her password being compromised.

- **Literacy**: These are basic literacy skills needed to understand the content level outcomes.

  - The learner should understand what a password is, and what role a password plays in authentication schemes.
  - The learner should know the difference between alphanumeric and non-alphanumeric characters.
  - The learner should have basic computer literacy skills.

Since education could play an important role in the process of disconfirmation, needed for a culture change, care should be taken that the outcomes defined for the educational program address the need for changing. Special care should be taken that all learners understand **why** they should behave in a specific way, as discussed in section 3.3.2. Once a clear set of outcomes has been defined, the next step in the creation of an OBE program is developing the actual learning opportunities.

Step 2: Develop learning opportunities

The learning opportunities should be developed in line with the basic premises, and principles, of OBE as outlined in section 4.3, as well as the criteria for information security education identified in section 3.3. Due to the relevance of these premises, principles, and requirements, to the development of the actual course content, the premises, principles, and requirements are briefly listed below.

- Premises of OBE:

  1. *All* students can learn and succeed, but not all in the same time or in the same way.
  2. Successful learning promotes even more successful learning.

3. Schools (and teachers) control the conditions that determine whether or not students are successful at learning.

- Principles of OBE:

  1. Clarity of focus.
  2. Designing back.
  3. High expectations for all students.
  4. Expanded opportunities for all learners.

- Requirements for Information Security Education:

  1. Everyone should be able to "pass" the course.
  2. Employees must know why they are taught a specific skill or have to behave in a specific way.
  3. Learning materials should be customized to the learning style, or preferences, of the learner.
  4. Users should be responsible for their own learning.
  5. Users should be held accountable for their studies.
  6. Learners must receive feedback.

The educational content developed will have to adhere to all of the above premises, principles and requirements. In addition to these, the educational programs will also have to be *cost effective*. This would mean that the "delivery mechanism", or media, used for such education should be chosen appropriately. Many organizations will not be able to afford sending each and every employee away to attend classroom based educational courses. Not only would the financial cost of such classroom training be prohibitive, but, the cost in terms of the time employees would be away from their jobs, would make classroom training unfeasible. This problem is compounded even further by the need for multiple opportunities for learning, as well as multiple opportunities for passing courses. Should an employee fail a course, that employee would have to be given another chance to attain the same learning. However, this does not mean classroom training is completely unsuitable for information security education. Whether or not classroom training can be

used will depend on the size of the organization, as well as the amount of resources available for information security education.

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

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

- The web is a very rich media. This means that educational material developed in this media is not restricted to simple text and static graphics, but can consist of a mixture of text, graphics, animations and even sound or video clips.

- Web-based training solutions are cheap to distribute organization wide and can easily be administrated from a centralized point.

- It is very easy to maintain, manage and update web-based training materials.

- Web-based training materials can include programmatic components. This makes it feasible to add automated assessment modules to such training materials, which means that learners can receive continuous feedback on their progress.

- It is also possible and feasible to create web-based material that will automatically adapt to the needs of the specific user being trained based on the predefined information security profile of the user.

- Most computer literate users will already be familiar with a web-based interface, which reduces additional training overheads that might be experienced should another form of computer based teaching solution be implemented.

In addition to web-based training, many other possible alternatives to classroom training exist. These include paper-based textbooks or manuals,

videos, instructional programs on CD, etc. The specific medium chosen for the development and presentation of the information security programs will depend on many factors, including the preference of the target learners, the level of computer literacy of the learners, the amount of hands-on practice required to develop the specific skills, etc. For example: executive managers might prefer reading through content instead of working through online examples, IT personnel could probably learn skills from technical manuals, whereas typical end-users would find it difficult to learn from such manuals, etc.

Which media, or training mechanism, is used will depend on many factors. It is, however, important to attempt to provide any educational material in as wide a variety of formats as possible in order to ensure the maximum amount of "customization" to individual learning preferences. The learning material should also be presented in formats that make it possible for individual learners to take responsibility for their own learning. For password usage subject matter could be constructed around the following outlines:

- **Classroom training for role-models**: An information security "role-model" should be identified in each department. These should, ideally, be individuals who have a high degree of computer literacy and who are willing to act as security role-models. These role-models will be sent on a one-day workshop where they will be taught the relative skills to effectively construct and manage secure passwords. The workshop should give the role-models sufficient knowledge regarding **all** aspects of password management, in order to enable these role-models to assist the other employees in his/her department should any of them require help during their own learning process. The workshop will include hands-on skills training. Participants will also be engaged in active debates regarding the organization's password policies, and will be asked to provide their own input into these policies. A lot of emphasis will be placed on *selling* the new policies and procedures to these role-models. Actual intrusion detection log-files will be used to help the role-models realize that hacking attempts against the organization is in fact a common occurrence. Password audit tools, like LC4 (http://www.atstake.com/research/lc/, 2003), will be used to show workshop attendees how vulnerable their own passwords are.

- **A web-based course for end-users**: A web-based course regarding password usage will be created for organizational end-users. This course will contain both reading material and interactive content. The course will contain links to all relevant policies and procedures, as well as content explaining the rationale behind these policies and procedures. Content will include sections on how to construct a secure password, mnemonic techniques to remember secure passwords, as well as sections explaining different techniques hackers might use to obtain an employee's password. Included in the online content will be video clips showing the learner *how* to change his/her own password. The course will be accessible from the organizational information security portal. Each employee will be required to successfully pass an online test on completion of this course. Users will be allowed to access the course material, or retake the test as often as they want to.

- **A password practice application for end-users**: An application will be developed for employees to test the strength of their own passwords. This application will use techniques and algorithms similar to those used by hackers, to attempt to "crack" the employee's password. It will also provide recommendations on how the employee can strengthen his/her password. A link to this application will be provided from the organizational information security portal. The web-based course for end-users will contain a section explaining the use of this application to the users.

- **Secure password usage booklet**: A booklet will be created regarding password usage. This booklet will contain all the relevant policy items and procedures dealing with passwords, as well as the rationale behind these policies and procedures. It will contain material explaining how to construct and remember secure passwords. This booklet will also be made available as a download from the organizational information security portal.

- **Awareness**: An awareness campaign will be launched to reinforce the other educational material regarding password usage. This will include posters, notice board email messages and reminders whenever a user logs in on the organization's information systems.

When creating the above "courses", care should be taken that all the previously identified outcomes are addressed. Once a comprehensive set of learning opportunities has been created, a set of assessment criteria for the various outcomes needs to be defined.

Step 3: Assessment and Feedback

For each defined outcome a corresponding assessment standard should be defined. These assessment standards are necessary in order to provide feedback to the learners. The importance of feedback in both OBE and information security education has been argued extensively in section 4.4 and section 3.3.6. Without assessment and feedback, learning cannot take place. According to Spady (1994, p. 103) it is vital to have a criterion-based, consistently applied, system of assessments, performance standards, learner credentialing, and reporting that is tightly aligned with all the defined significant, future-focused outcomes. This system must emphasize **applied** learning in **relevant**, life-role contexts. The learner should thus be able to always **relate** the learning back to a role he/she performs in the course of his/her normal activities. The feedback should also encourage learners to attain high performance levels on everything they pursue and enable learners to demonstrate and receive full credit for improved learning on a timely basis (Spady, 1994, p. 103).

The assessment standards for an OBE program must conform closely to the defined outcomes. In the case of the password example, this would mean that assessment criteria would have to be defined for all outcomes across each of the three critical domains in which outcomes have been defined. For example:

- **Performance:** These are outcomes relating directly to actual performance. The assessment criteria for these outcomes should thus also relate directly to actual performance. For example:
  - All password changes in the organization will be logged. Metrics based on these logs will be compiled and made available to all employees. In order to ensure all employees change their passwords at least once every two weeks, this metric will be made part of the employee's key performance indicators.

  - A password strength metric will be calculated and stored every time an employee changes his/her password. This metric will be based on an algorithm which takes into account many factors, such as, the length of the password, the number of non-alphanumeric characters it contains, etc. This metric will also become part of the employee's key performance indicators.
  - Occasional password audit will be conducted. Password auditors will do random spot-checks on employees to ensure they are able to log in without help from a written down password. Employees who write their passwords down will be penalized and will have to redo the course material dealing with mnemonic techniques to recall passwords.
  - The password auditors will also interview random employees in order to determine whether they understand the reasons behind the strict password policy. Based on the results of these interviews employees/departments might be rewarded or asked to attend additional classes.

- **Content**: These are outcomes related to understanding of subject matter. The assessment criteria for these outcomes should relate directly to the understanding of the specific subject matter dealt with.

  - The learner should be able to demonstrate that he/she has the necessary skills to change his/her own password. The employee should successfully use a "password change" simulation application five consecutive times in order to get a "passing" metric.
  - The learner should be able to achieve a score of 80% or more on a multiple choice test that measures knowledge about the elements that constitute a secure password.
  - The learner should be able to create secure passwords on an application testing password strength, five consecutive times.
  - The learner should be able to demonstrate that he/she can use mnemonics to construct and recall secure passwords. This component will be measured individually by password auditors for each

employee. Alternatively the employees can use an online forum to submit a mnemonic and password for auditing.

  - The learner should be able to locate the information security policies and procedures dealing with password usage on the company intranet. A link on the intranet pages containing the applicable policies can be used by the employee to "log" that he/she has actually visited the page.

- **Literacy**: These are basic literacy skills needed to understand the content level outcomes. The outcomes for these can be measured in a similar way normal computer literacy skills are tested. Some employees might be exempted from these tests, for example employees who have an International Computer Drivers Licence certificate.

  - The learner should be able to score 80% or more on a basic computer literacy test.

For the purposes of testing **knowledge**, assessment of the content level outcomes is the most important. However, in a culture change process the performance level outcomes will play a much larger role, since the metrics of these outcomes will also measure the cultural artifacts. The possible roles of performance level outcomes in a culture change process will be re-visited in later sections. Once the required assessments criteria have been defined, the final part of creating an outcomes based educational program is to ensure all the necessary components for the effective administration of such a program are in place.

Administration

The educational process in general can be viewed as a system of teaching and learning activities that are tied together via various feedback loops. It also includes other functions such as assessment, admission, quality assurance, direction and support (Tait, 1997). All of these components can, and should, play a role in the creation of an effective Information Security education program. Without proper administration it will be impossible to fairly reward/penalize employees for their performance. It will also be impossible to ensure that each and every employee has indeed successfully attained the

required learning. Proper administration plays a vital role, not only in OBE, but also in the culture change process in general.

The education of employees forms the third major component in the framework this dissertation is presenting. This component is outcomes based, and consists of several sub-processes in a repeating cycle. These sub-processes include:

- Defining the outcomes.
- Defining assessment standards for each outcomes.
- Creating the learning experiences that will enable employees to attain the defined outcomes.
- Educating the employees.
- Providing feedback, based on the defined assessment criteria, to employees, regarding their learning progress.
- The continuous administration and reviewing of components in the above steps.

Once employees have been educated, the next step in a culture change process, would be to define "cultural metrics" to measure the actual culture change.

6.2.4 Define Culture Change Metrics

Metrics play a vital role in both information security, and in any culture change process. Without accurate measurements it is very difficult to know the current status of the culture, or to quantify the desired status of the culture. It is vital to remember that shared tacit assumptions are formed as the result of continuously **successful** past behavior (Schein, 1999a, p. 19). In the case of information security, it will be very difficult for employees to know that their new behavior patterns are successful, because successful information security is mostly tacit, and difficult to quantify. It is therefor vital to implement security metrics and to use these metrics to continuously provide feedback to employees. Employees must realize that their *new* behavior is successful, or that the *old way* of doing things is not successful. If

OBE is used to develop the educational component for the culture change process, the problem of defining these "cultural metrics" becomes much easier. The **performance** level outcomes in an OBE program, can be translated directly to the relevant cultural artifacts the organization desires. The assessment metrics for these outcomes can thus be used as the cultural metrics.

The definition of culture change metrics, comprises the fourth component of the framework this dissertation is presenting. As mentioned above, some of these metrics can consist of the performance level outcomes from the educational process in the third component. These metrics should also include meaningful aggregates of these performance level metrics at various levels of the organizational hierarchy. In addition to these, other metrics that could contribute to the monitoring of the culture might be needed, for example, metrics regarding actual security incidents, like attempted intrusions on the organization's information network.

The culture change metrics should be used to provide feedback regarding the culture change process to both the employees, and management.

6.2.5 Feedback, Rewards and Punishments

Feedback plays a vital role in a culture change process. The visionary statements, provided by top-management, *must* be **positively reinforced** through management behavior. As argued earlier, without a combination of both coercion, and the rewarding of desired behavior, real change cannot take place. Commitment from the very top of an organization is essential for major cultural change. However, even though middle managers do not initialize the cultural change, ultimately it is their actions that produce the desired change (Brubakk & Wilkinson, 1996). Middle management behavior is vital in a culture change process, since middle management will be the ones providing feedback to the employees. In a case study of a successful culture change process at the Bangor Hydro-Electric Company, Alpander and Lee (1995) note that the management team had to go through the training program twice, to ensure they understood the new values that the organization was espousing. Management behavior is instrumental in creating the desired environmental conditions for change. If the behavior of a *learner* fits the expectations of important others, i.e. managers and colleagues, in the

learner's work and social environment, that behavior will become a stable part of the person, and eventually of the group (Schein, 1999a, p. 129). By providing the "correct" feedback, management is ultimately responsible for the internalization of the new values by employees.

Feedback provided by management can take many forms. On the one hand, employees can be rewarded/punished based on performance level metrics defined for the culture change process. Section, or departmental, level aggregates of these metrics can in turn be used as performance level metrics for middle-managers, etc. Secondly, feedback relating to actual security incidents taking place need to be given to both employees and management. According to Gonzalez and Sawicka (2002), risk **perception** is vital for human compliance in information security. Employees *must* perceive the risk, through their own, or reported, experiences, if they are expected to comply with secure practices (Gonzalez & Sawicka, 2002). Thus, in addition to measurements relating to performance outcomes, employees need to receive feedback regarding actual security incidents taking place, in order for them to *perceive* the risk. This feedback should be continuous, otherwise, even employees who have both the desired knowledge and the desired attitude, might become complacent regarding information security because they do not *perceive* the risk accurately.

Lastly, it should be remembered that employees could be coerced into behaving in a specific way, **but** such a behavior change will be superficial and unstable (Schein, 1999a, p. 115). A reward system based on "impartial" metrics, in combination with a degree of coercion is likely to be more successful. It might be beneficial to use such metrics in combination with an information security certification scheme. Such a scheme could have great value in a culture change process, especially if achieving a new level in the certification scheme is linked to an appropriate reward system, i.e. a monetary increase. The achievement of a specific level of certification could even be used as a pre-requisite for promotion. Such a certification scheme could be designed around the concept of mastery of learning (Malan, 2000; Killen, 2000), as used in OBE. In a mastery learning environment, learners are allowed to continuously improve their mastery of a specific concept. Learners are allowed the opportunity to be periodically re-assessed on their learning and, when applicable, receive credit for achieving higher levels of mastery

of the subject matter. In an information security environment this concept could be used to phase in a desired ideal level of knowledge and cooperation, through a scheme of security certification. Such a scheme, in combination with a reward system, could be very advantageous to the establishment of an information security sub-culture in the organization.

In terms of password usage, the following system of feedback, rewards and penalties could, for example, be implemented:

- A personal page on the organization's information security portal, which allows each employee to view his/her personal password metrics, as well as the combined effect of these metrics on his/her key performance indicators. Metrics could include:
  - How often the employee change his/her password on average.
  - How secure the employee's average password is.
  - How secure the employee's current password is.
  - What "level" the employee have attained in the organization's information security certification scheme.
  - A list of educational modules successfully completed.
  - A list of educational modules still to be completed.
- A departmental summary page on the organization's information security portal, accessible by the department's manager andhis/her superiors. Metrics on this page could include:
  - An aggregate indicating how often the average employee in the department changes his/her password.
  - An aggregate indicating how secure the average passwords of employees in the department is.
  - An aggregate indicating how secure the current average passwords of employees in the department is.
  - A comparison between the current departmental password metrics and the desired level, as defined in the organization's espoused values.

- An organizational summary page on the organization's information security portal. This page could be used by the person, or team, responsible for the culture change to manage overall progress.
- A summary of recent security incidents in the organization, as well as explanations of possible consequences had any of these attacks succeeded.

It should be remembered that a change in beliefs and values results from joint learning processes based on *successful* behavior. Feedback, rewards, and penalties, are the mechanisms management should use to ensure that employees understand *what* behavior would be considered successful.

The system of feedback, reward, and punishment mechanisms, comprises the fifth component of the framework this dissertation is presenting. This feedback should include all the defined culture change metrics. Individual employees should receive feedback regarding their own performance, as well as feedback regarding actual security incidents. This feedback should be part of both the formal education process, and the individual employee's key performance indicators. Without sufficient feedback, it will be very difficult for employees to learn new behavior patterns. If unwanted behavior patterns persist, even though management is actively trying to discourage them, it might be necessary to review the desired changes.

6.2.6 Review and Refinement

A basic principle of organizational change is the fact that governing variables might sometimes need to be adjusted (Section 5.3). Sometimes the changes required from employees are not feasible in practice, or employees might disagree with a policy and thus disregard the policy (Schlienger & Teufel, 2003). In a case where employees refuse to cooperate, due to a fundamental disagreement with the espoused values, management can either try to "bribe", or coerce, employees to comply through rewards, or punishments, **or** management can **negotiate** a more acceptable policy. In other words, instead of using rewards or punishments to change the shared tacit assumptions, the culture could be "strengthened" (section 5.2) by bringing the espoused values more in line with existing shared tacit assumptions. Ac-

cording to Woodall (1996), equitable involvement of employees in a culture change process is the only way such a process could be considered ethical. Periodical reviews of the current state of the culture and the ideal future state might thus be needed. Active management of organizational culture is a continuous process until the new values have been internalized. In the case of information security, the ideal future state would also need to be continuously reviewed and refined in order to cope with the fast changing nature of information technology itself.

The process of constantly reviewing and refining the culture change process comprises the sixth, and final, component of the framework presented in this dissertation. Continuous review of the ideal future state of the culture is especially important in the light of the fast changing nature of information technology. It is also a basic principle of organizational learning theory in general, that the governing variables in a learning process will occasionally need revision.

6.3 Framework Overview

In the previous section an integrated, holistic framework was presented for the fostering of an organizational sub-culture of information security. This framework "borrows" elements from several fields of study in the behavioral sciences, including; outcomes based education, organizational learning theory, and transformative change management. Figure 6.1 presents a graphical exposition of this framework. The following is a brief overview of this framework:

1. Attain top management commitment.
2. For each business problem, define the culture change in the context of the specific business problem. This step consist of the following sub-steps:
   (a) Assess the current state of the culture in terms of the specific business problem.
   (b) Define the *ideal* future state of the culture in terms of the specific business problem.

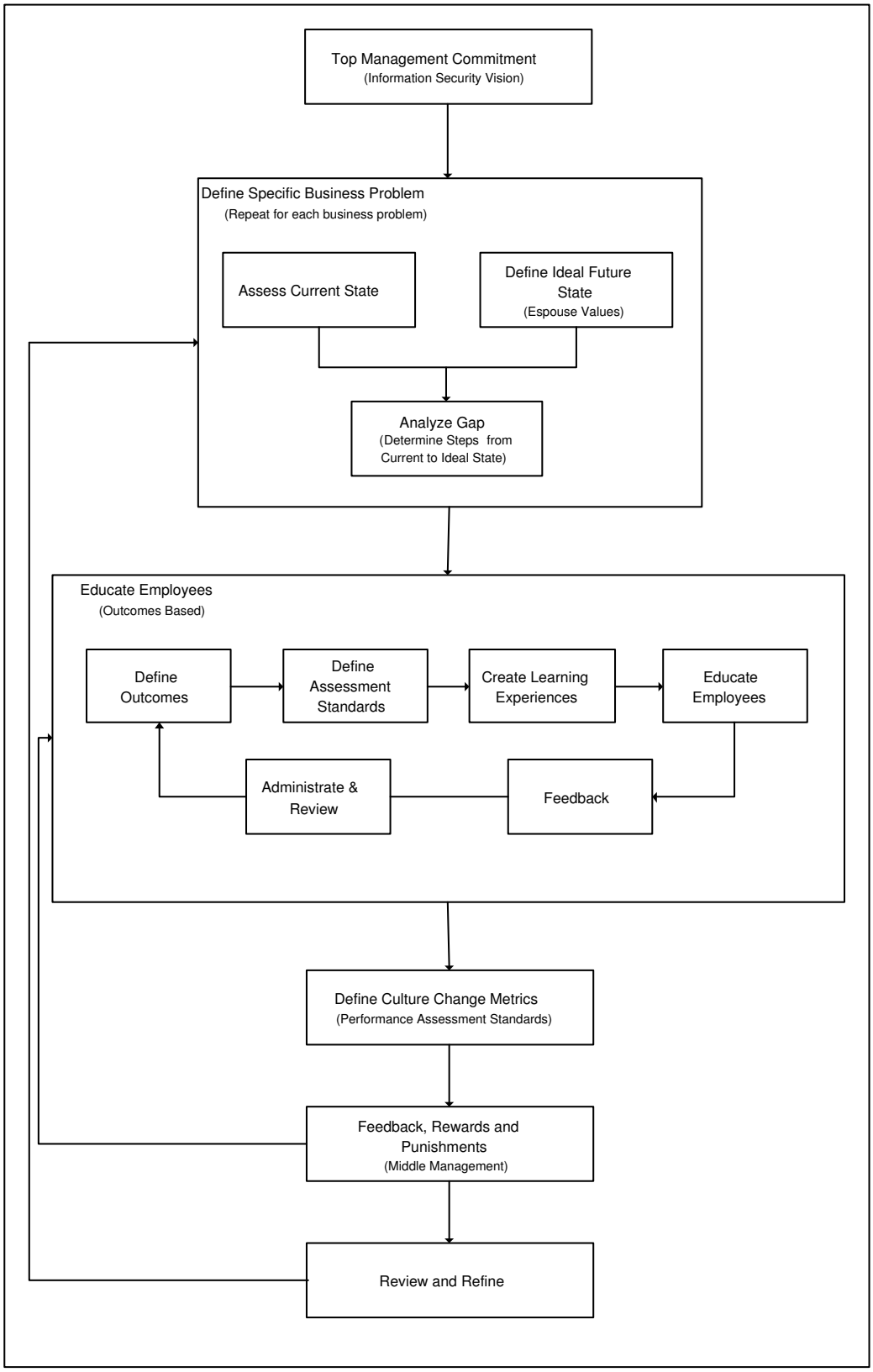

Figure 6.1: An Outcomes Based Framework for Culture Change

   (c) Analyze the gap between the current state and the desired future state and determine the *steps* needed to get *from* the current state *to* the ideal future state.

3. Educate the employees. For this step in the culture change process outcomes based education should be used. An outcomes based program will consist of the following cycle of steps that should be supported by a sound administrative process:

   (a) Define the desired outcomes.

   (b) Define assessment metrics for each outcome.

   (c) Create learning experiences that will enable learners to attain the desired outcomes.

   (d) Expose the learners to the learning experiences. (Educate)

   (e) Provide feedback to learners based on the defined assessment metrics.

   (f) Constantly review the learning experiences, and where necessary revise them.

4. Define culture change metrics. These could be based on the performance level metrics defined for the educational component.

5. Provide feedback to the employees. This feedback should be *backed* by both rewards and punishments, where necessary. Ideally, most feedback should come from middle management, since ultimately it is the consistent actions of middle management that will drive the culture change. The culture change metrics should also feed back into the educational process, which should be a continuous process that reinforces the *new way* of doing things. These metrics should also feed into a review process.

6. Review and refine the culture change process. Where needed, re-examine the governing variables (espoused values), in order to strengthen the culture and assist with the internalization of the new culture.

6.4 Conclusion

This chapter introduced an holistic framework for the introduction of a corporate sub-culture of information security. The framework combines elements from outcomes based education, organizational learning, and corporate culture, in order to address the two dimensions to the human factor in information security in a holistic fashion. The purpose of the presented framework is to demonstrate how the two dimensions to the human factor in information security, namely knowledge and attitude, *could* be addressed holistically.

Information security depends on both human knowledge, **and** human cooperation. A lack of knowledge can generally be addressed through education, whilst a lack of cooperation can be addressed through the fostering of an organizational sub-culture of information security in the organization. However, if employees have adequate knowledge, but lack the required attitude they will not necessarily behave securely. Conversely, employees who have the correct attitude, but do not have the necessary knowledge, will not be *able* to behave securely. This co-dependency between knowledge and attitude would mean that neither of these factors should be addressed in isolation. The framework presented in this chapter incorporates the educational components needed to impart information security knowledge to the employees, into the general culture change process, as presented in the previous chapter. Outcomes based education was used as an educational methodology, since this methodology was shown to be very well suited to information security education in chapter 4. Furthermore, the assessment metrics which should be defined for performance level outcomes in outcomes based courses, were incorporated into the culture change process as metrics that could be used to gauge the effects of the change process.

Through the definition, and motivation, of the framework presented in this chapter, this dissertation has demonstrated, firstly, that outcomes based education **can** be used for the design, implementation and administration of information security education programs. Secondly, the definition, and motivation, of this framework has demonstrated **how** sound behavioral principles can be applied to the fostering of a corporate sub-culture of information security. The integration of these components from both the educational,

and the behavioral, sciences into a single, holistic, outcomes based, framework for the fostering of a corporate sub-culture of information security in organizations thus, successfully achieved the objectives of this dissertation, as outlined in section 1.3.

The next chapter will briefly summarize the findings of this dissertation, and present possible future research directions leading from the work in this dissertation.

Chapter 7

CONCLUSION

This chapter concludes this dissertation

7.1 Introduction

The objective of this dissertation was to develop a holistic framework, based on sound educational, and behavioral, principles, for the establishment of a corporate sub-culture of information security compliance. This framework should use educational principles that directly contribute towards the establishment of such an information security sub-culture, and that will also produce a high level of user awareness and behavioral discipline. This framework should be based on a combination of various behavioral sciences as well as outcomes based educational principles. The framework should also provide guidelines for the creation and management of information security education programs. This objective would be accomplished by addressing the following sub-objectives:

- Identifying the educational needs specific to information security in a corporate environment.
- Identifying behavioral theories that could play a role in such educational programs.
- Evaluating outcomes based education to determine is suitability for the creation of such programs.

- Demonstrating, through arguing and critical evaluation techniques, that outcomes based is suitable for information security education.
- Identifying the major elements that should play a role in the active changing of a corporate culture.
- Where necessary, augmenting the above elements in order to make it more suitable for the specific needs of information security.
- Integrating the elements from various disciplines into a single holistic approach, through the use of modelling techniques, critical evaluation, and arguing.

As far as could be ascertained, there were no frameworks, or models, in existence which covered the same scope, nor which were founded on the same proven, behavioral principles, intended for use specifically in the field of information security, at the start of this dissertation. The framework presented in this dissertation could thus make a meaningful contribution towards the available knowledge in the field of information security.

7.2 Summary

The first part of this dissertation was devoted to determining the role humans play in the information security process. Two co-dependent dimensions to the human factor in information security were identified, namely, knowledge and attitude. Without adequate knowledge regarding information security, organizational employees would be unable to perform their security related roles and responsibilities. However, even if employees have the requisite knowledge, they still need to have the correct attitude towards information security. Without the desired "secure" attitude, even employees with the necessary knowledge might still disregard security policies or procedures, for example, because they disagree with a specific policy item. This part of the dissertation also established the need for incorporating the behavioral sciences into any programs which aims to address human factors in information security.

The second part of this dissertation dealt with information security education, which can be used to address the knowledge dimension to the human

factor in information security. A lack of attention to sound pedagogical principles was identified as one of the problems with current information security education programs. In order to address this lack of attention to pedagogical principles, an investigation was conducted into various current information security related standards. The aim of this investigation was to identify a set of requirements that a formal educational methodology would have to adhere to, in order for such a program to be suitable for information security education. The identified requirements were then proposed and argued.

The third part of this dissertation focussed on one such an educational methodology, namely, outcomes based education (OBE). OBE was investigated and then critically evaluated in order to determine its suitability for information security education. This critical evaluation showed that a strong correlation exists between the premises, and principles, of OBE, and the requirements for information security education, as argued earlier. It was then argued that OBE is indeed a suitable pedagogical methodology for the creation, and administration, of information security education programs. The use of OBE could thus assist to address the knowledge dimension of the human factor in information security. However, due to the co-dependency between human knowledge and human attitude in an organization's information security efforts, it was still necessary to find a way of addressing an undesired attitude towards information security, amongst organizational employees.

The fourth part of this dissertation, therefor, focussed on corporate culture. Many studies have shown that the fostering of a corporate sub-culture of information security in an organization, could successfully address human attitude, the second dimension to the human factor in information security. This part of the dissertation provided a formal definition of corporate culture, and then expanded this definition to include a knowledge level, in order to make the definition more specific to an information security culture. Knowledge was included in this definition due to the strong co-dependance the two dimensions to the human factor in information security have on each other. Various theories regarding organizational learning and culture change were then examined, in order to determine exactly how an organization culture could be established. This part of the dissertation also briefly examined the psychological factors that could play a role in such a culture change process.

The final part of this dissertation integrated all the previous parts into

a single, holistic, outcomes based framework for the establishment of an organizational sub-culture of information security. Various components were modelled into this integrated framework and there specific roles in the framework were argued, and explained with the use of a continuous example.

7.3 Possible Further Enhancements

It is important to realize that the establishment of a corporate sub-culture of information security is a long-term process. This process needs to be ongoing, and due to the fast evolving nature of information technology itself, such a process would need continuous revision. Empirical studies, to determine the effectiveness of the framework proposed in this dissertation, could make a significant contribution towards the knowledge available regarding the human factors in information security.

It would also be worthwhile to further investigate the possibilities offered by web-based technologies, as a delivery mechanism for information security education programs. Effective use of web-based technologies could also greatly enhance the requisite feedback, and administration, processes involved in a structured culture change process.

7.4 Conclusion

Information security is crucial to the continuous well-being of modern organizations. Humans play a significant role in the processes needed to secure an organization's information resources. Without an adequate level of user **co-operation** and **knowledge**, many security techniques, methods, controls, etc., are liable to be misused or misinterpreted by users. This may result in even an adequate security measure becoming inadequate. It is therefor necessary to educate the organization's employees regarding information security and also to establish a corporate sub-culture of information security in the organization, which will ensure that the employees have the correct attitude towards their security responsibilities. Without both the necessary knowledge, **and** the desired attitude amongst the employees, it will be impossible to guarantee that the organization's information resources are secure. It would therefor make sense to address both these dimensions to the human

factor in information security, using a single integrated, holistic approach. This dissertation presented such an approach.

References

Alpander, G. G., & Lee, C. R. (1995). Culture, strategy and teamwork: The keys to organizational change. *Journal of Management Development*, *14*(8), 4–18.

Barnard, L., & Von Solms, R. (2000). A formalized approach to the effective selection and evaluation of information security controls. *Computers & Security*, *19*(2), 185–194.

Brubakk, B., & Wilkinson, A. (1996). Agents of change? Bank branch managers and the management of corporate culture change. *International Journal of Service Industry Management*, *7*(2), 21–43.

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

Department of Education (DOE). (2001). Draft Revised National Curriculum Statement: Technology Learning Area. *[WWW document]. URL http://education.pwv.gov.za/. Sited 14 August 2003.*

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

Eloff, M. M., & Von Solms, S. H. (2000). Information security management: An approach to combine process certification and product evaluation. *Computers & Security*, *19*(8), 698–709.

Fingar, P. (1996). *The blueprint for business objects.* New York: SIGS Books & Multimedia.

Gonzalez, J. J., & Sawicka, A. (2002). A framework for Human Factors in Information Security. *Presented at the 2002 WSEAS International Conference on Information Security, Rio de Janeiro, 2002.*

Haag, S., Cummings, M., & Dawkins, J. (2000). *Management information systems for the information age* (2 ed.). Irwin/McGraw-Hill.

Horrocks, I. (2001). Security training: Education for an emerging profession? *Computers & Security*, *20*(3), 219–226.

ISO/IEC 17799: Code of Practice for Information Security Management. (2000).

ISO/IEC TR 13335-1:2004 Guidelines to the Management of Information Technology Security (GMITS). Part1: Concepts and models for IT security. ISO/IEC, JTC 1, SC27, WG 1. (2004).

ISO/IEC TR 13335-3:1998 Guidelines to the Management of Information Technology Security (GMITS). Part3: Managing and Planning IT Security. ISO/IEC, JTC 1, SC27, WG 1. (1998).

ITiCSE Working Group on the Web and Distance Learning. (1997). The web and distance learning: what is appropriate and what is not. *ITiCSE'97 Working Group Reports and Supplemental Proceedings*, 27–27.

Killen, R. (2000). Outcomes-based education: Principles and possibilities. *[WWW document]. URL http://www.schools.nt.edu.au/curricbr/cf/outcomefocus/killen_paper.pdf. Sited 10 March 2003.*

Laudon, K. C., & Laudon, J. P. (2002). *Management information systems: Managing the digital firm* (7 ed.). Prentice Hall.

LC4. (2003). LC4 - the password auditing and recovery application. *[WWW document]. URL http://www.atstake.com/research/lc/. Sited 17 September 2004.*

Malan, S. (2000). The 'new paradigm' of outcomes-based education in perspective. *Tydskrif vir Gesinsekologie en Verbruikerswetenskappe*, *28*(1), 22–28.

Malhotra, Y. (1996). Organizational learning and learning organizations: An overview. *[WWW document]. URL http://www.brint.com/papers/orglrng.htm. Sited 4 March 2004.*

Martins, A., & Eloff, J. (2002). Assessing information security culture. *Information Security South Africa (ISSA), Johannesburg, South Africa, 2002.*

Mitnick, K., & Simon, W. (2002). *The art of deception: Controlling the human element of security.* Wiley Publishing.

NIST 800-16: Information Technology Security Training Requirements: A Role- and Performance-Based Model. NIST Special Publication 800-16, National Institute of Standards and Technology. (1998).

Nosworthy, J. D. (2000). Implementing information security in the 21st century - do you have the balancing factors? *Computers & Security*, *19*(4), 337–347.

O'Brien, J. A. (1999). *Management information systems: Managing information technology in the internetworked enterprise* (4 ed.). Irwin/McGraw-Hill.

Olivier, C. (1998). *Educate and train: Outcomes-based.* Pretoria, South Africa: J. L. van Schaik Publishers.

Pretorius, F. (1998). *Outcomes-based education in South Africa.* Randburg, South Africa: Hodder and Stoughton Educational.

Rowe, C. (1996). Evaluating management training and development: revisiting the basic issues. *Industrial and Commercial Training*, *28*(4), 17–23.

Sadri, G., & Lees, B. (2001). Developing corporate culture as a competitive advantage. *Journal of Management Development*, *20*(10), 853–859.

Schein, E. H. (1999a). *The corporate culture survival guide.* Jossey-Bass Inc.

Schein, E. H. (1999b). Empowerment, coercive persuasion and organizational learning: do they connect? *The Learning Organization*, *6*(4), 163–172.

Schlienger, T., & Teufel, S. (2003). Information security culture - from analysis to change. *Proceedings of the 3rd Annual Information Security South Africa Conference, Information Security South Africa (ISSA), Johannesburg, South Africa, 2003*, 183–196.

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

Siponen, M. (2001). Five dimensions of information security awareness. *Computers and Society, June 2001*, 24-29.

Smit, P. J., & Cronjé, G. J. d. J. (1992). *Management Principles: A Contemporary South African Edition.* JUTA.

Smith, M. K. (2001a). Chris Argyris: Theories of action, double-loop learning and organizational learning. *[WWW document]. URL http://www.infed.org/thinkers/argyris.htm. Sited 4 March 2004.*

Smith, M. K. (2001b). Donald Schon: Learning, Reflection and change. *[WWW document]. URL http://www.infed.org/thinkers/et-schon.htm. Sited 4 March 2004.*

South African Bureau of Standards - Recommended Practice: Glossary of IT Security Terminology ARP 057. (2002).

South African Qualifications Authority (SAQA). The National Qualifications Framework and Curriculum Development. (2000).

Spady, W. G. (1994). *Outcomes-based education: Critical issues and answers.* USA: American Association of School Administrators.

Tait, B. (1997). Object orientation in educational software. *Innovations in Education and Training International*, *34*(3), 167–173.

The American Heritage Dictionary of the English Language (4 ed.). (2000). Houghton Mifflin Company, USA.

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

Tripathi, A. (2000). Education in information security. *IEEE Concurrency, October-December 2000*, 4–8.

Von Solms, B. (2000). Information security - the third wave? *Computers & Security*, *19*(7), 615–620.

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

Von Solms, R. (1999). Information Security Management: Why Standards are Important. *Information Management & Computer Security*, *7*(1), 50–57.

Wallace, J., Hunt, J., & Richards, C. (1999). The relationship between organisational culture, organisational climate and managerial values. *The International Journal of Public Sector Management*, *12*(7), 548–564.

Whitman, M. E., & Mattord, H. J. (2003). *Principles of information security.* Thompson Course Technology.

Wood, C. C. (1997). Policies alone do not constitute a sufficient awareness effort. *Computer Fraud & Security, December 1997*, 14–19.

Woodall, J. (1996). Managing culture change: can it ever be ethical? *Personnel Review*, *25*(6), 26–40.

Appendices

During the research conducted towards this dissertation, three peer-reviewed papers were presented at national, and international, conferences. These papers are:

1. Appendix A

    - Establishing an Information Security Culture in Organisations: An Outcomes Based Education Approach, *Information Security South Africa (ISSA), Johannesburg, South Africa, 2003*

2. Appendix B

    - Organizational Learning Models for Information Security, *Information Security South Africa (ISSA), Johannesburg, South Africa, 2004*

3. Appendix C

    - Corporate Information Security Education: Is Outcomes Based Education the Solution?, *10th IFIP WG11.1 Annual Working Conference on Information Security Management, World Computer Congress (WCC), Toulouse, France, 2004*

ESTABLISHING AN INFORMATION SECURITY CULTURE IN ORGANISATIONS: AN OUTCOMES BASED EDUCATION APPROACH

Johan van Niekerk[a] and Rossouw von Solms[b]

[a]Department of Business Information Systems, Port Elizabeth Technikon

[b]Department of Information Technology, Port Elizabeth Technikon

[a]johanvn@petech.ac.za, 041 5043048, Private Bag X6011, PORT ELIZABETH, 6000

[b]rossouw@petech.ac.za, 041 5043604, Private Bag X6011, PORT ELIZABETH, 6000

ABSTRACT

In today's business world information is a valuable commodity and such needs to be protected. This protection is typically implemented in the form of various security controls. In order for these controls to be effective the users in the organization needs to be educated about these controls. Many recent studies have shown that user education alone is not sufficient and that the emphasis should be on the creation of an organizational culture of information security. This paper examines the concept of organizational cultures and the role education plays in the establishment of such a culture. It then examines outcomes based education (OBE) and finally attempts to show how OBE can play a positive role in organizations wanting to establish a culture of information security.

KEY WORDS

Information Security, Information Security Culture, Outcomes Based Education, Awareness

ESTABLISHING AN INFORMATION SECURITY CULTURE IN ORGANISATIONS: AN OUTCOMES BASED EDUCATION APPROACH

1. INTRODUCTION

In today's business world information is a valuable commodity and such needs to be protected. It affects all aspects of today's businesses from top management right down to operational level. In order to avoid loss or damage to this valuable resource, companies need to be serious about protecting their information. This protection is typically implemented in the form of various security controls. However, it is very difficult to know exactly which controls would be required in order to guarantee a certain acceptable minimum level of security. Furthermore, managing these controls to see that they are always up to date and implemented uniformly throughout the organization is a constant headache to organizations.

There exist several internationally accepted standards and codes of practice to assist organizations in the implementation and management of an organizational information security strategy. Some of the better known examples would include the BS7799 (British Standards Institute, 1999) and the Guidelines for the Management of Information Technology Security (GMITS) (GMITS, 1995).

These standards and codes of practice provide organizations with guidelines specifying how the problem of managing information security should be approached. One of the key controls identified by all the major IT Security standards published to date is the introduction of a corporate information security awareness program. The purpose of such a program is to educate the users about Information Security or, more specifically, to educate users about the individual roles they play in the effectiveness of one type of control, namely, operational controls.

2 THE HUMAN SIDE OF INFORMATION SECURITY

Information Security controls can generally be sub-divided into three categories: Physical controls, Technical controls and Operational controls. Physical controls deal with the physical aspects of security, for example; a physical control might state that an office containing sensitive documents should have a lock on the door. Technical controls are controls of a technical nature, for example; forcing a user to authenticate with a unique username and password before allowing the user to access the operating system would be a technical control. The third category, operational controls, consists of all controls that deal with human behaviour.

Employees, whether intentionally or through lack of knowledge, are the greatest threat to Information Security (Thomson, 1998) and because these operational controls rely on human behaviour, hence employee behaviour, they can be seen as the weakest link in Information Security. Unfortunately both physical and technical controls rely heavily on these operational controls for effectiveness. As an example, an operational control might state that a user leaving their office must logoff from the operating system and lock their office door. If a user were to ignore this control, both the technical control forcing authentication and the physical control of having a lock on the door would be rendered useless. Thus anyone who thinks that security products, i.e. technical and physical controls, alone offer true security is settling for the illusion of security (Mitnick & Simon, 2002).

According to Dhillon (1999), the user education program is singled out because increasing awareness of security issues is the most cost-effective control that an organization can implement. This control is so cost-effective because it ensures that all users are aware of the operational controls without which all other controls cannot operate efficiently. Special care should be taken that the awareness program is presented in such a form that it do not go beyond the comprehension of the average user. The emphasis should be to build an organizational sub-culture of security awareness.

Many recent studies have shown that the establishment of an Information Security "culture" in the organization is in fact necessary for effective Information Security (Eloff & Von Solms, 2000; Von Solms, 2000). Some of these studies have presented definitions of what an Information Security culture is, but currently there exists very little knowledge on how such a culture can be established. It is however clear that the user education program will have to play a major role in the establishment of such a culture.

3 ESTABLISHING A CULTURE OF INFORMATION SECURITY

Before the task of establishing an Information Security culture can be tackled it is necessary to understand what such a culture is. According to The American Heritage Dictionary of the English Language (2000) a culture is:

- The totality of socially transmitted behavior patterns, arts, beliefs, institutions, and all other products of human work and thought

- The predominating attitudes and behavior that characterize the functioning of a group or organization.

In terms of Information Security a corporate culture of Information security can thus be seen as the predominating attitudes towards information security and security related behaviour that characterize the functioning of the employees within the organization. Thus, in an organization that has a culture of information security, the employees would adhere to proper security practices during execution of their day-to-day functions because that is simply the way things are done. It is obvious that in order for employees to be able to adhere to proper security practices the employees would have to know what proper security practices are. Therefore information security education would have to play a key role in the establishment of such a culture.

Even though user education is essential for the establishment of a successful corporate culture of information security, education on its own cannot change a corporate culture. Sadri and Lees (2001) place the main responsibility for changing a corporate culture on the shoulders of management.

Corporate culture should start with proper visionary statements and should thereafter be positively reinforced through management behaviour i.e. rewarding employees' successes and distributing newsletters and videos that reinforce the culture. Leadership from the very top of an organization is essential for major cultural change. However, even though middle managers do not initialize the cultural change, ultimately it is their actions that produce the changes (Brubakk & Wilkinson, 1996).

Thus, in order to establish a culture of information security, the top management of the organization will have to start the process via vision and mission statements, as well as policy changes. This process has to be supported by a sound user education program and reinforced via continuous feedback. This feedback will come from the organization's middle management (Brubakk & Wilkinson, 1996).

4 OUTCOMES BASED EDUCATION

Since the aim of the user education program is not to prepare the users for further levels of formal education, but rather to help them achieve information security know-how for use in their everyday jobs, the educational methodology used should be chosen accordingly. Outcomes Based Education

(OBE) might in fact be ideally suited for use in such programs since the aim of OBE is to help learners achieve a specific outcome, in this case information security awareness.

OBE is defined as an approach to teaching and learning which stresses the need to be clear about what learners are expected to achieve. The educator states beforehand what "outcome" is expected of the learners. The role of the educator is then to help the learners achieve that outcome (Siebörger, 1998).

Outcomes can be defined as either cross-curriculum (general outcomes) or specific outcomes. A cross-curriculum outcome can be seen as the desired effect that attaining a specific competency should have within the general environment within which the learner operates. A specific outcome is one that directly demonstrates the mastery of the appropriate skill that the learner should gain from the OBE program.

For each outcome an assessment standard should be defined. These standards are necessary in order to provide feedback to the learners. According to Siebörger (1998) assessment is essential to OBE to measure the degree to which a learner has achieved an outcome. In fact being able to assess progress and provide feedback to the learner is a prerequisite for any educational program to be successful. Fingar (1996) states that feedback, specifically in the form of knowledge regarding the outcomes of the learners' actions, is required for learning to take place. Furthermore this feedback should be continuous and constructive (DOE, 2001).

The educational process in general can be viewed as a system of teaching and learning activities that are tied together via various feedback loops. It also includes other functions such as assessment, admission, quality assurance, direction and support (Tait, 1997). All of these components can, and should, play a role in the creation of an effective Information Security education program.

5 OUTCOMES BASED EDUCTION FOR INFORMATION SECURITY

Up to this point this paper has shown that establishing a corporate culture will have to start with top management, be continuously reinforced via feedback from middle management to the employees and should be based on a sound user education program. It has also been suggested that this user education program should be outcomes based.

The following example will attempt to show how these components could be brought together in order to affect such a cultural change. Suppose the controls for which we want to change the users' behaviour deals with proper password usage.

Firstly, top management will have to show their commitment to information security by developing visionary statements and/or slogans (Sadri and Lees, 2001). This could be part of the corporate vision statement or simply some posters stating that the organization is committed to improving information security. For example, a poster, signed by the CEO, could be posted throughout the organization stating: "At ABC we are committed to the integrity, availability and confidentiality of all our information". These visionary statements have to be followed up by a corporate information security policy. One of the policy statements would be: "All users of information must be authenticated before being allowed to use information resources". The policy in turn should be supported by a set of procedures dealing with the specific operational control. Thus for password usage these procedures could include:

- All users must use passwords that is at least eight characters long and include at least two non-alphabetic characters
- All users must change their passwords at least once every two weeks
- A user may not write down their password or share their password with any other user

Secondly, a user education program should be constructed to educate the users about proper password usage. The specific outcomes for such a program could include:

- The learner (user) should know why using a properly constructed password is necessary
- The user should be able to demonstrate constructing their own passwords and recalling them with the aid of simple mnemonic techniques
- The user should be able to change their own passwords on the required system
- The user should know that they are accountable for any misdeeds that takes place using their authentication information and should be fully aware of the possible consequences to themselves and the organization.

General (cross-curriculum) outcomes could include:

- All users' passwords should be changed once per week
- All users' passwords should withstand a standard brute force dictionary attack.

Thirdly, middle management will have to positively reinforce any learning that took place by giving continuous feedback to the users. For the specific outcomes feedback can form part of the actual

education program, possibly in the form of a quiz or small workshop at the end of a learning session. Feedback for the general outcomes however, should be seen as drivers for the desired cultural change. It should be fairly easy to gather metrics such as the percentage of users in the organization that changed their passwords for a specific week and the percentage of passwords cracked by an in-house test attack. These metrics could be gathered per department, branch, etc. and can then easily be made part of the key performance indicators for the appropriate middle level manager. The old adage that what you measure is what you get will then play its part by ensuring that the appropriate line managers will feed this statistics back to their staff since it impacts on their own performance evaluations.

The process discussed in this section would have to be repeated for each control addressed in the corporate information security policy or sub-policies. Obviously separate visionary statements and/or slogans would not be required for each control. However, each control should be addressed specifically in an information security policy, and by supporting procedures. Each control would have to be included in an educational program. The outcomes and measurables for these outcomes would have to be clearly defined. Special care should be taken when defining the cross-curriculum or general outcomes, since in this approach these general outcomes act as *drivers* for the intended cultural change.

6 CONCLUSION

This paper discussed aspects that will contribute to the establishment of a corporate sub-culture of information security. It showed that establishing a culture will have to start with top management and should be continuously reinforced via feedback from middle management to the employees. It also suggested that a sound user education program should form this basis of such a cultural change. The concept of outcomes based education (OBE) was examined and then proposed as a very suitable methodology for use in the establishment of such a culture.

This paper forms part of an ongoing research project at the Port Elizabeth Technikon. In the paper a brief example of how OBE could be used to assist organizations in the establishment of an information security culture was given. This example is by no means complete at this stage and only served to illustrate the point that OBE *can* play a useful role in information security education. It should be obvious that several factors still need to be taken into account. For example:

- How should the educational material be presented and will this differ for users in different levels of the organization? I.e. end users vs. top management.

- What forms of user profiling would be needed to ensure the learning material is appropriate for the intended audience? Obviously not all controls available in a standard such as ISO/IEC 17799 should be taught to every user.

These and other issues are currently be examined and it is hoped that the research project this paper forms part of will be able to present a complete and holistic methodology for Information Security Education that will directly contribute towards the establishment of an culture of information security in organizations.

7 REFERENCES

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

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

Brubakk, B., Wilkinson, A. (1996). Agents of change? Bank branch managers and the management of corporate culture change. International journal of Service Industry Management, 7 (2), pp. 21-43.

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

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

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

Eloff, M.M., Von Solms S.H. (2000). Information security management: A hierarchical framework for various approaches. Computers and Security, 19(3): pp. 243-256.

Fingar, P. (1996). The blueprint for business objects. New York, New York : SIGS Books & Multimedia

Guidelines to the Management of Information Technology Security (GMITS). (1995). Part 1, ISO/IEC, JTC 1, SC27, WG 1.

Guidelines to the Management of Information Technology Security (GMITS). (1997). Part 2, ISO/IEC, JTC 1, SC27, WG 1.

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

King, S. (1998). Are you ready for a BS 7799 audit ?. BSI, UK.

Martins, A., Eloff, J.H.P. (2002) Assessing Information Security Culture. ISSA 2002, Muldersdrift, South Africa, 10-12 July 2002.

Mitnick, K.D., Simon, W.L. (2002) The art of deception: Controlling the human element of security. United States of America : Wiley Publishing, Inc.

Sadri, G., Lees, B. (2001) Developing corporate culture as a competitive advantage. Journal of Management Development, 20 (10). Pp. 853-859.

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

Tait, B. (1997). Object Orientation in educational software. Innovations in Education and Training International, 34 (3). pp. 167-173.

The American Heritage Dictionary of the English Language, Fourth Edition. (2000) Houghton Mifflin Company, USA.

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

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

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

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

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

Acknowledgement: We would like to thank the National Research Foundation for their financial support for research conducted towards this paper.

ORGANISATIONAL LEARNING MODELS FOR INFORMATION SECURITY

Johan van Niekerk[a] and Rossouw von Solms[b]

[a]Department of Business Information Systems, Port Elizabeth Technikon
[b]Department of Information Technology, Port Elizabeth Technikon

[a]johanvn@petech.ac.za, 041 5043048, Private Bag X6011, PORT ELIZABETH, 6000
[b]rossouw@petech.ac.za, 041 5043604, Private Bag X6011, PORT ELIZABETH, 6000

ABSTRACT

Humans today live in an emerging global information society, with a global economy that is increasingly dependent on the creation, management, and distribution of information resources. Information and its use permeate all aspects of modern society. Today, most organizations need information systems to survive and prosper. It is therefore imperative that modern organizations, operating in this global information society, take the protection of their information resources seriously. The protection of information resources is to a large extent dependent on human co-operated behaviour. This dependence on human behaviour makes it necessary to have a user education program to educate users regarding their roles and responsibilities towards information security. Recent studies have indicated that current user education programs fail to pay adequate attention to behavioural theories. There exist several organisational learning models that could be used for information security education. This paper will examine some of these models in terms of their applicability to information security education.

KEY WORDS
Information Security, Information Security Culture, Outcomes Based Education, Awareness, Double-loop Learning, Organisational Learning

ORGANISATIONAL LEARNING MODELS FOR INFORMATION SECURITY

1. INTRODUCTION

Humans today live in an emerging global information society, with a global economy that is increasingly dependent on the creation, management, and distribution of information resources (O'Brien, 1999, pp. 11). Information and its use permeate all aspects of modern society. Today, most organizations need information systems to survive and prosper (Laudon & Laudon, 2002, pp. 4). It is therefore imperative that modern organizations, operating in this global information society, take the protection of their information resources seriously.

This protection is typically implemented in the form of various security controls. Information security controls can generally be sub-divided into three categories: Physical controls, Technical controls and Operational controls (Thomson, 1998, p. 29; Van Niekerk & Von Solms, 2003). Physical controls deal with the physical aspects of security, for example; the lock on the door of an office containing sensitive documents. Technical controls are controls of a technical nature, usually software based, for example; forcing a user to authenticate with a unique username and password before allowing the user to access the operating system. The third category, operational controls, collectively including business-, administrative-, managerial-, and procedural controls, consist of all controls that deal with human behavior in one form or another. These controls would include those that deal with the creation of information security policies and procedures, and administration of other controls. Both physical and technical controls, even though they do not deal directly with operational issues, usually require some form of human involvement. In an organizational context, these controls would thus have to be supported by procedures outlining the employee's involvement in the use of these controls.

Employees, whether intentionally or through negligence, often due to a lack of knowledge, are the greatest threat to information security (Thomson, 1998, p. 12, Mitnick & Simon, 2002, p. 3). Operational controls rely on human behavior. This means that these controls are arguably some of the weakest links in information security. Unfortunately, both physical and technical controls rely to some extent on these operational controls for effectiveness. As an example, an operational control might state that a user leaving his/her office must logoff from the operating system and lock his/her office door. If a user were to ignore this procedure, both the technical control forcing

authentication and the physical control of having a lock on the door would be rendered useless. Thus, anyone who thinks that security products, i.e. technical and physical controls, alone, offer true security is settling for the illusion of security (Mitnick & Simon, 2002, p. 4).

Siponen (2001) describes this tendency of organizations to settle for the illusion of security as a general human tendency to often blindly ignore complications in IT related issues. Without an adequate level of user co-operation and knowledge, many security techniques are liable to be misused or misinterpreted by users. This may result in even an adequate security measure becoming inadequate (Siponen, 2001) Organizations cannot protect the integrity, confidentiality, and availability of information in today's highly networked systems environment without ensuring that each person involved understands his/her roles and responsibilities and is adequately trained to perform them (NIST, 1998, p. 3).

Teaching employees their roles and responsibilities relating to information security requires the investment of company resources in a user education program. However, budgetary requirements for security education and training are generally not a top priority for organizations (Nosworthy, 2000). Organizations often spend most their information security budget on technical controls and fail to realize that a successful information security management program requires a balance of technical and business controls (Nosworthy, 2000). Business controls in this sense refer to operational controls. According to Dhillon (1999), increasing awareness of security issues is the most cost-effective control that an organization can implement. However, in order to ensure that the maximum return on investment is gained, special care should be taken to ensure the success of the user education programs used. For educational programs this would mean ensuring adherence to proper pedagogical principles when these educational programs are compiled.

Most current user education programs fail to pay adequate attention to behavioral theories (Siponen, 2001). The emphasis of user education programs should be to build an organizational sub-culture of security awareness, by instilling the aspects of information security in every employee as a natural way of performing his or her daily job (Von Solms, 2000). Recent studies have indicated that the establishment of an information security "culture" in the organization is desirable for effective information security (Von Solms, 2000). Such a culture should support all business activities in such a way that information security becomes a natural aspect in the daily activities of every employee (Schlienger & Teufel, 2003). Such a culture would require employees

to have knowledge of their information security responsibilities as well as commitment towards these responsibilities (Siponen, 2000). A detailed examination of how such a culture could be established in an organization falls outside the scope of this paper. Instead this paper will focus only on user education, one of the components needed to establish such a culture. The rest of this paper will examine, and then briefly discuss, three learning models, which are arguably pedagogically sound, in an attempt to identify common principles an information security education program should adhere to if such a program is to be useful in the establishment of an organisational sub-culture of information security. In other words, this paper will try to examine pedagogically sound learning models. These models were selected based on the premise that information security involves standards, policies and user behaviour and that the selected models should be useable in an attempt to modify employee behaviour. The following three models will be examined:

- The American National Institute of Standards and Technology (NIST) model: "Information Technology Security Training Requirements: A Role- and Performance-Based Model" (Available online at http://www.nist.org as NIST special publication 800-16). This model is included because it is the American standard for information security training, and as such warrants closer examination.
- Organizational learning, including both single-, and double-loop learning. Organizational learning theories deal specifically with the idea of the organization as a whole learning and adapting its behaviour. These theories are widely used in the management sciences specifically to change employee behaviour, see e.g. (Rowe, 1996; Smith 2001:1; Smith 2001:2). Organizational learning theories are included in this study since they deal with both policies and employee behaviour.
- Outcomes based education (OBE). OBE is a pedagogical model used in schools in many countries world-wide. OBE is included in this paper due to the fact that it has been previously suggested as a driver for change in establishing an information security culture, see (Van Niekerk & Von Solms, 2003).

2. THE NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST) MODEL

The American National Institute of Standards and Technology (NIST) provides an information security specific training model, see (NIST, 1998). This model provides a framework that serves as the American standard for information security training. The NIST model, entitled: "Information

Technology Security Training Requirements: A Role- and Performance-Based Model", is currently the only standard that focus exclusively on learning as related to information security. The rest of this section will provide a brief overview of the NIST model.

The NIST model is based on the premise that learning is a continuum. Specifically, learning in this context starts with awareness, builds to training, and evolves into education (NIST, 1998, p.14). Furthermore the model is role-based. Meaning that it defines the IT security learning needed as a person assumes different roles within an organization and different responsibilities in relation to IT systems (NIST, 1998, p.14).

The premise that information security learning is a continuum consisting of awareness, training and education is fairly widely accepted see e.g. (Horrocks, 2001, Schlienger & Teufel, 2003). The three levels of learning in this continuum can be described as follows:

Awareness: The purpose of awareness programs is simply to focus attention on security issues. In awareness activities the learner is simply the recipient of information and do not actively participate (NIST 1998, p.15). Awareness campaigns often make use of tools such as posters, videos and promotional slogans.

Training: The learner has to know how he/she can behave securely. This level strives to produce relevant and needed security skills and competency by practitioners of functional specialties other than IT security (e.g., management, auditing). Training of special security tools or features within applications must be offered (NIST, 1998, p.16; Schlienger & Teufel, 2003).

Education: The "Education" level integrates all of the security skills and competencies of the various functional specialties into a common body of knowledge. It also adds a multi-disciplinary study of concepts, issues, and principles (technological and social).This level strives to produce IT security specialists and professionals capable of vision and pro-active response (NIST, 1998, p.16). An important characteristic of education is that the employee must understand why information security is important for the organization (Schlienger & Teufel, 2003).

The model in NIST special publication 800-16 deals primarily with the training part of this learning continuum. The NIST document uses this continuum to identify the knowledge, skills, and abilities an individual needs to perform the IT security responsibilities specific to each of his or her roles in the organization. According to this model all employees would need awareness. Training would only be required by individuals whose roles in the company indicates a need for specific

knowledge of security threats and risks, as well as the safeguards against these threats and risks. Lastly, according to this model, education would only be needed by information security specialists. Thus, the type of learning that individuals need starts simplistic and then becomes more comprehensive and detailed towards the top of the continuum. (NIST, 1998, pp. 13-14)

Once the specific information security related roles of an employee has been determined, the NIST document can be used to identify the specific learning requirements of that employee. The document also emphasizes that all learning materials should match individual learner preferences (NIST, 1998, p. 19). According to NIST, individuals learn in several ways, but each person, as part of his/her personality, has a preferred or primary learning style. Instruction can positively, or negatively, affect a student's performance, depending on whether it is matched, or mismatched, with a student's preferred learning style (NIST, 1998, p. 19). Thus, what should be taught to a specific individual user and how it should be taught, will depend on both the user's preferred learning style, and the specific role that user plays within the organization. Finally the document provides a framework for the planning of information security training curricula and the evaluation of training effectiveness. According to NIST special publication 800-16, evaluation of training is vital, and should be an integral component of any training programme (NIST, 1998, p. 157).

3. ORGANIZATIONAL LEARNING

According to Malhotra (1996) organizational learning could be defined as the process within organizations by which knowledge about action-outcome relationships and the effect of the environment on these relationships is developed. Most current organizational learning theories stem from theories originally developed by Chris Argyris and Donald Schon (Smith, 2001:1;Smith, 2001:2) These theories were based on the idea that people have mental maps with regard to how to act in situations. These maps involve the way people plan, implement and review their actions. Argyris and Schon asserted that it is these maps that guide people's actions, rather than the theories they explicitly espouse (Smith, 2001:2). Smith (2001:2) describes the process involved using a model based on three elements:

- Governing variables: Those dimensions that people are trying to keep within acceptable limits. In information security this could refer to acceptable levels of risk.
- Action strategies: The moves and plans people use to keep the governing variables within the acceptable range. In information security these would include procedures outlining employee behaviour in specific scenarios.

- Consequences: What happens as the result of an action. These would include both intended and unintended results.

Currently most organizations focus on adaptive, or single-loop, learning. Instead companies should be focussing on generative learning or "double-loop" learning (Malhotra, 1996, Rowe, 1996). Single-loop learning can be likened to a thermostat (Rowe 1996). If a thermostat learns it is too hot or too cold it will turn the heat on or off. It can do this because it receives information about the current temperature and it has the ability to take action through turning the heat on or off. Single-loop learning is usually present where the underlying governing variables, such as goals, values and frameworks, are taken for granted (Smith, 1996:2).

In order for organizational learning to take place, companies should be focussing on generative, or double-loop, learning (Malhotra, 1996). Generative learning emphasizes continuous experimentation and feedback in an ongoing examination of the very way in which organizations go about defining and solving problems. Thus it can be likened to a thermostat that has the ability to ask why it is set at a specific temperature and can then explore whether another setting might be more effective (Rowe, 1996). Double-loop learning could thus result in the underlying governing variables being adjusted should they be found to be ineffective or unrealistic. Fig 3.1 demonstrates the relationship between the three elements of the model and the two types of learning.

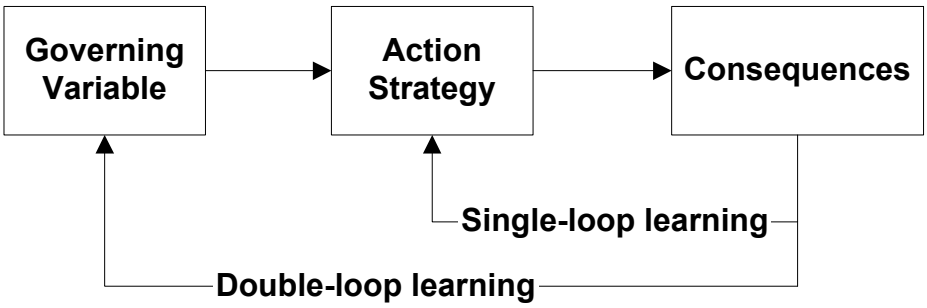

Figure 3.1: Organizational Learning (Adapted from Smith 2001:1)

4. OUTCOMES BASED EDUCATION (OBE)

OBE is defined as an approach to teaching and learning which stresses the need to be clear about what learners are expected to achieve. The educator states beforehand what "outcome" is expected of the learners. The role of the educator is then to help the learners achieve that outcome (Siebörger, 1998).

Outcomes can be defined as either cross-curriculum (general outcomes) or specific outcomes. A cross-curriculum outcome can be seen as the desired effect that attaining a specific competency should have within the general environment within which the learner operates. A specific outcome is one that directly demonstrates the mastery of the appropriate skill that the learner should gain from the OBE program.

For each outcome an assessment standard should be defined. These standards are necessary in order to provide feedback to the learners. According to Siebörger (1998) assessment is essential to OBE to measure the degree to which a learner has achieved an outcome. In fact being able to assess progress and provide feedback to the learner is a prerequisite for any educational program to be successful. Fingar (1996) states that feedback, specifically in the form of knowledge regarding the outcomes of the learners' actions, is required for learning to take place. Furthermore this feedback should be continuous and constructive (DOE, 2001).

The educational process in general can be viewed as a system of teaching and learning activities that are tied together via various feedback loops. It also includes other functions such as assessment, admission, quality assurance, direction and support (Tait, 1997). All of these components can, and should, play a role in the creation of an effective information security education program. OBE can be viewed in three different ways: as a theory of education, a systematic structure for education, or the creation of educational material, and lastly as a classroom practice (Killen, 2000). OBE can thus be seen as a complete educational system, which contains all the components such a system should have.

According to Killen (2000), OBE is based upon three basic premises, namely:

1. All students can learn and succeed, but not all in the same time or in the same way.
2. Successful learning promotes even more successful learning.
3. Schools (and teachers) control the conditions that determine whether or not students are successful at learning.

From these basic premises four essential principles of OBE were developed (Killen, 2000). They are:

1. Clarity of focus, which means that all teaching activities must be clearly focused on the desired outcome that the learners should achieve.
2. Designing back, which means that the starting point for an OBE program's design should be a clear definition of the desired results. The rest of the curriculum should be designed according to this desired outcome.
3. High expectations for all students. OBE not only assumes that everyone can attain the desired outcomes, it also requires that high standards should be set. This is based on evidence that learners are more likely to attain high standards when they are challenged by what is expected from them (Killen, 2000).
4. Expanded opportunities for all learners. This final principle of OBE is based on the idea that not everyone learns the same way or at the same pace. Thus, in OBE, learners are given many opportunities for learning. Achieving the desired outcome is deemed more important than how that outcome was reached.

In order for an educational program to be classified as being outcomes based, it has to adhere to all four of these principles (Killen, 2000).

5. DISCUSSION

The previous sections provided a brief overview of three pedagogically sound models that could be applicable to corporate information security education. This paper will now attempt to identify, and briefly discuss, common characteristics and principles from these models.

Firstly, it should be clear that a proper learning program, even if it is aimed at corporate users, as opposed to students or scholars, requires a lot of planning. The NIST model provides extensive templates for planning training programs. OBE requires one to start with a clear view of the desired outcomes and then to design the curriculum based on the desired outcomes, taking into consideration the backgrounds and learning preferences of individuals. Organizational learning requires both the governing variables and desired action strategies to be taken into account when constructing learning programs. Efforts revolving around posters, videos or once-off classroom sessions can be said to fall within the awareness level of the continuum, which, though necessary, is not sufficient. It is therefore imperative for an organization to follow a formalized methodology, like e.g. the NIST templates and training matrixes, when constructing learning programs.

Secondly, in all three the models the outcome or the goal of the learning experience needs to be clearly defined. In the NIST model, templates for training programmes all start with clear goal statements, OBE has a clear statement of the desired outcomes as one of its core elements and organizational learning requires a definition of the desired consequences in order to evaluate the action strategies. In organizational learning, efforts focussing only on the immediate consequences, as opposed to a defined long-term outcome, can be described as single-loop learning. Single-loop learning is not sufficient instead organizations should focus on double-loop learning (Malhotra, 1996, Rowe, 1996). Training program organizers for organizational learning efforts have to set programme objectives and, on the basis of this, plan, implement, and review a program (Rowe, 1996).

Thirdly, evaluation, or assessment, is critical to all three these models. According to the NIST model evaluation is the only way to ensure that training efforts is meaningful (NIST, 1998, p.155). OBE requires continuous and constructive feedback to learners, without which learning cannot take place (Fingar, 1996;DOE, 2001). Lastly, Organizational learning requires an evaluation of the consequences of actions. Without such an evaluation, the "mind maps" determining action strategies cannot be adapted. Thus no learning can take place without evaluation of some form.

Fourthly, learners must know **why** they should behave in a certain way or follow a specific policy. The NIST model reserves this level, where learners are taught why for information security specialist. But, according to NIST (1998, p.20) course developers should be aware that adults have well-established values, beliefs, and opinions. Adults relate new information and knowledge to previously learned information, experiences, and values, which might result in misunderstanding (NIST, 1998, p. 20). It is even possible that they understand correctly but still don't adhere to a security policy because it conflicts with their beliefs and values (Schlienger & Teufel, 2003). Therefore it is imperative for learners to know why they are learning something (Schlienger & Teufel, 2003). OBE requires the learner to identify and solve problems in which responses display that responsible decisions using critical and creative thinking have been made (Olivier, 1998; Pretorius, 1998). This type of thinking requires not only knowledge but also insight. Insight requires the learner to know why they are doing something (NIST, 1998, p. 18). According to Killen (2000) each outcome based educational program must have a rationale to explain why the program exists. Double-loop learning does not directly require learners to know why they are taught something. But it does require the governing variables to be re-examined if the desired consequences has not been reached. Which, in turn, can be construed as knowing why a specific action strategy is taught.

Lastly, learning material should be customized for individual learners. The NIST model is role-based. The specific training needs of individuals should be identified based on their role within the organization. Specifically, training is to be provided to individuals based on their particular job functions (NIST, 1998, p. 43). Furthermore, according to NIST, individuals learn in several ways, but each person, as part of his/her personality, has a preferred or primary learning style. Instruction can positively, or negatively, affect a student's performance, depending on whether it is matched, or mismatched, with a student's preferred learning style (NIST, 1998, p. 19). The first basic premise of OBE not only states that all students can learn and succeed, but it also states that all students cannot necessarily do this in the same time or in the same way. This premise is also expanded on in the fourth principle of OBE, which states that learners should be given many opportunities for learning. OBE thus recognizes that individuals learn in different ways and at different paces. For a program to be truly outcomes based it is vital that learning materials are provided in as customized a format as possible for individual learners.

6. CONCLUSION

According to Siponen (2001), most current user education programs fail to pay adequate attention to behavioral theories. Since the emphasis of user education programs should be to build an organizational sub-culture of security awareness (Von Solms, 2000), the programs used to educate users should be suitable for modifying user behaviour. This paper examined three pedagogical models that are based on behavioural theories and attempted to identify common characteristics between these models. The aim of this paper is not to provide a complete solution to current problems with information security education, but rather to introduce some elements that could improve the effectiveness of such programs. The following key elements, that should be considered when constructing programs aimed at modifying employee behaviour, have been identified:

- Programs should be thoroughly planned using a formalised methodology, which takes into consideration aspects relating to both the learners and the environment in which they operate.
- Programs should be designed around a clearly defined outcome or goal, in terms of the desired results, for example: the desired change in employee behaviour.
- Evaluation, or assessment, is critical for the success of a learning program. Learners **must** receive feedback if learning is supposed to take place.

- Learners must not only be taught how to behave in a specific situation but should also be taught **why** they should behave in that specific way.
- Learning materials should be customized to individual learners

A lot of additional research would be required in order to provide a complete solution to all current information security education problems. For example, the link between the establishment of an information security culture and double-loop learning, which requires one to re-examine, and possibly modify, the underlying governing variables, warrants further investigation. This paper only examined the common characteristics of the three models. Furthermore, it only focused on "positive" aspects of these models. Future research should also include an examination of the weaknesses of each approach. Many other models for information security education exist. A rigorous scientific examination of such models, dealing with both common elements and weaknesses, would be very beneficial. However, any additional research would have to take into account both the goal of a user education program, to help establish a culture of information security awareness, and sound pedagogical principles.

7. REFERENCES

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

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

Fingar, P. (1996). The blueprint for business objects. New York, New York : SIGS Books & Multimedia

Horrocks, I. (2001). "Security Training: Education For an Emerging Profession?" Computers & Security 20(3): 219-226.

Killen, R. (2000). Outcomes-Based education: Principles and Possibilities. Unpublished manuscript, University of Newcastle, Faculty of Education. [WWW document]. URL http://www.schools.nt.edu.au/curricbr/cf/outcomefocus/killen_paper.pdf. Sited 20 August 2003.

Laudon, K. C., Laudon, J. P. (2002). Management Information Systems: Managing the Digital Firm (7th ed). New Jersey, USA: Prentice Hall.

Malhotra, Y. (1996) Organizational Learning and Learning Organizations: An Overview [WWW document]. URL http://www.brint.com/papers/orglrng.htm. Sited 4 March 2004.

Mitnick, K.D., Simon, W.L. (2002) The art of deception: Controlling the human element of security. United States of America : Wiley Publishing, Inc.

National Institute of Standards and Technology (NIST). (1998) Information Technology Security Training Requirements: A Role- and Performance-Based Model. NIST Special Publication 800-16. U.S. Government Printing Office, Washington.

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

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

Olivier, C. (1998), Educate and Train : Outcomes-Based. Pretoria, South Africa. J.L. van Schaik.

Pretorius, F. (1998) Outcomes-based Education in South Africa. Randburg, South Africa: Hodder and Stoughton Educational.

Rowe, C. (1996) Evaluating management training and development: revisiting the basic issues. Industrial and Commercial Training, 28 (4), Pp. 17-23.

Schlienger, T., Teufel, S. (2003) Information Security Culture – From Analysis to Change. Proceedings of the 3rd Annual Information Security South Africa Conference, 9-11 July 2003, Sandton, South Africa, pp. 183-196.

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

Siponen, M.T. (2000) A Conceptual Foundation for Organizational Information Security Awareness. Information Management & Computer Security. 8 (1), pp. 31-41.
Siponen, M.T. (2001). Five Dimensions of Information Security Awareness. Computers and Society, June 2001. Pp. 24-29.

Smith, M., K. (2001:1). Chris Argyris: Theories of action, double-loop learning and organizational learning. [WWW document]. URL http://www.infed.org/thinkers/argyris.htm. Sited 4 March 2004.

Smith, M., K. (2001:2). Donald Schon: Learning, Reflection and change. [WWW document]. URL http://www.infed.org/thinkers/et-schon.htm. Sited 4 March 2004.

Tait, B. (1997). Object Orientation in educational software. Innovations in Education and Training International, 34 (3). Pp. 167-173.

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

Van Niekerk, J., Von Solms, R. (2003). Establishing an Information Security Culture in Organisations: An Outcomes Based Education Approach. Proceedings of the 3rd Annual Information Security South Africa Conference, 9-11 July 2003, Sandton, South Africa, pp. 3-12.

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

ACKNOWLEDGEMENTS

The financial assistance of National Research Foundation (NRF) towards this research is hereby acknowledged. Opinions expressed and conclusions arrived at, are those of the author and are not necessarily to be attributed to the National Research Foundation.

CORPORATE INFORMATION SECURITY EDUCATION: Is Outcomes Based Education the Solution?

Johan van Niekerk[a] and Rossouw von Solms[b]

[a]Department of Business Information Systems, Port Elizabeth Technikon
[b]Department of Information Technology, Port Elizabeth Technikon

[a]johanvn@petech.ac.za, 041 5043048, Private Bag X6011, PORT ELIZABETH, 6000
[b]rossouw@petech.ac.za, 041 5043604, Private Bag X6011, PORT ELIZABETH, 6000

ABSTRACT

Today's global economy is increasingly dependent on the creation, management, and distribution of information resources. Information and its use permeate all aspects of modern society. Most modern organizations need information systems to survive and prosper. Information has become a valuable commodity and as such needs to be protected. This protection is typically implemented in the form of various security controls. In order for these controls to be effective, the users in the organization need to be educated regarding these controls. Recent studies have indicated that current user education programs fail to pay adequate attention to behavioral theories. This paper examines the educational principles an information security user education program should adhere to. It then introduces outcomes based education (OBE) and finally argues that OBE is ideally suited for the needs of information security.

KEY WORDS

Information Security, Information Security Culture, Outcomes Based Education, Awareness

CORPORATE INFORMATION SECURITY EDUCATION: Is Outcomes Based Education the Solution?

1. INTRODUCTION

In today's business world, information is a valuable commodity and as such, needs to be protected. Information affects all aspects of today's businesses, from top management right down to the operational level (Turban, et al., 2002. pp 3-37). In order to avoid loss or damage to this valuable resource, companies need to be serious about protecting their information. This protection is typically implemented in the form of various security controls (Barnard & Von Solms, 2000). However, it is very difficult to know exactly which controls would be required in order to guarantee an acceptable minimum level of security. Furthermore, managing these controls to see that they are always up to date and implemented uniformly throughout the organization is a constant headache to organizations.

When selecting the controls to implement in an organization, it is important to refer to accepted international standards (Von Solms, 1999). There exist several internationally accepted standards and codes of practice to assist organizations in the implementation and management of an organizational information security strategy. Some of the better known examples would include the ISO/IEC 17799 (British Standards Institute (BSI), 1999) and ISO/IEC 13335 also known as GMITS (Guidelines to the Management of Information Technology Security (GMITS), 1995).

These standards and codes of practice provide organizations with guidelines specifying how the problem of managing information security should be approached (Von Solms, 1999). One of the primary controls identified by many of the major IT security standards published to date is the introduction of a corporate information security awareness program (BSI, 1999; GMITS, 1995). The purpose of such a program is to educate the users about information security or, more specifically, to educate users about the individual roles they should play in the effective execution and maintenance of these controls. Most security controls, whether physical, technical, managerial or administrative in nature, requires some form of human involvement. This paper will examine this dependence of information security on human involvement with specific emphasis on the role user education has to play in a corporate information security strategy. It will then propose outcomes based education (OBE) as a pedagogical methodology suitable for the information security education needs of organizations.

2. THE HUMAN SIDE OF INFORMATION SECURITY

Information security controls can generally be sub-divided into three categories: Physical controls, Technical controls and Operational controls (Thomson, 1998, p. 29). Physical controls deal with the physical aspects of security, for example; the lock on the door of an office containing sensitive documents. Technical controls are controls of a technical nature, usually software based, for example; forcing a user to authenticate with a unique username and password before allowing the user to access the operating system. The third category, operational controls, collectively including business-, administrative-, managerial-, and procedural controls, consist of all controls that deal with human behavior in one form or another. These controls would include those that deal with the creation of information security policies and procedures, and administration of other controls. Both physical and technical controls, even though they do not deal directly with operational issues, usually require some form of human involvement. In an organizational context, these controls would thus have to be supported by procedures outlining the employee's involvement in the use of these controls.

Employees, whether intentionally or through negligence, often due to a lack of knowledge, are the greatest threat to information security (Thomson, 1998, p. 12, Mitnick & Simon, 2002, p. 3). Operational controls rely on human behavior. This means that these controls are arguably some of the weakest links in information security. Unfortunately, both physical and technical controls rely to some extent on these operational controls for effectiveness. As an example, an operational control might state that a user leaving his/her office must logoff from the operating system and lock his/her office door. If a user were to ignore this procedure, both the technical control forcing authentication and the physical control of having a lock on the door would be rendered useless. Thus, anyone who thinks that security products, i.e. technical and physical controls, alone, offer true security is settling for the illusion of security (Mitnick & Simon, 2002, p. 4).

Siponen (2001) describes this tendency of organizations to settle for the illusion of security as a general human tendency to often blindly ignore complications in IT related issues. Without an adequate level of user co-operation and knowledge, many security techniques are liable to be misused or misinterpreted by users. This may result in even an adequate security measure becoming inadequate (Siponen, 2001) Organizations cannot protect the integrity, confidentiality, and availability of information in today's highly networked systems environment without ensuring that each person involved understands his/her roles and responsibilities and is adequately trained to perform them (National Institute of Standards and Technology (NIST), 1998, p. 3).

Teaching employees their roles and responsibilities relating to information security requires the investment of company resources in a user education program. However, budgetary requirements for security education and training are generally not a top priority for organizations (Nosworthy, 2000). Organizations often spend most their information security budget on technical controls and fail to realize that a successful information security management program requires a balance of technical and business controls (Nosworthy, 2000). Business controls in this sense refer to operational controls. According to Dhillon (1999), increasing awareness of security issues is the most cost-effective control that an organization can implement. However, in order to ensure that the maximum return on investment is gained, special care should be taken to ensure the success of the user education programs used. For educational programs this would mean ensuring adherence to proper pedagogical principles when these educational programs are compiled.

Most current user education programs fail to pay adequate attention to behavioral theories (Siponen, 2001). The emphasis of user education programs should be to build an organizational sub-culture of security awareness, by instilling the aspects of information security in every employee as a natural way of performing his or her daily job (Von Solms, 2000). Recent studies have indicated that the establishment of an information security "culture" in the organization is desirable for effective information security (Von Solms, 2000). Such a culture should support all business activities in such a way that information security becomes a natural aspect in the daily activities of every employee (Schlienger & Teufel, 2003). A detailed examination of how such a culture could be established in an organization falls outside the scope of this paper. Instead this paper will focus only on user education, one of the cornerstones required for the establishment of such a culture. For more information on the establishment of such a culture see e.g. (Van Niekerk & Von Solms, 2003; Schlienger & Teufel, 2003).

3. ELEMENTS OF INFORMATION SECURITY EDUCATION

The user education programs needed for information security purposes differ from traditional educational programs. Unlike traditional educational programs, these programs will primarily be aimed at teaching adults. Adults have well established, not formative, values, beliefs, and opinions (NIST, 1998, p. 20). The educational methodology used should thus be suitable for adult education. Furthermore, there are several other requirements specific to the role that such a program will play in the overall organization's information security efforts. In the following sections, this paper will

suggest and attempt to motivate some of the features that should typically constitute such an information security education program.

3.1 Everyone should be able to "pass" the course.

Nosworthy (2000) states that each person in the organization from the CEO to House Keeping staff must be aware of, and trained to exercise their responsibilities towards information security. However in traditional educational models there are usually a percentage of the learners who do not pass the course, or in other words, successfully meet the assessment criteria. In order for an organization's information to be secure, everyone needs to not only be trained, but to "pass" the training. Unlike traditional education, failing an information security educational program cannot be accepted. Workers at every level, even those who do not use a computer, are liable to be targeted (Mitnick & Simon, 2002, p. 39). This means that having even a single person who does not know his/her information security responsibilities should be unacceptable.

3.2 Employees must know why information security is important and why a specific policy or control is in place.

Recent studies have suggested that current information security awareness programs are failing (Siponen, 2001). This failure is due to many reasons. Schlienger & Teufel (2003) have shown that even employees who know their responsibilities with regards to information security will still disobey security policy if they disagree with the policy. They suggest that the mere awareness of the policies and procedures is in fact not sufficient, the users also need to know why a specific policy or control is in place (Schlienger & Teufel, 2003). In information security, being taught why a specific policy or control is in place is generally considered to be a feature of education, and not of awareness (Schlienger & Teufel, 2003; NIST, 1998, pp. 16-17). Information security "education" is generally sub-divided into three levels, namely; awareness, training and education. Awareness simply focuses attention on information security. Training is more interactive and tries to instill the necessary skills and competencies. Education integrates all of the security skills and competencies of the various functional specialties into a common body of knowledge and adds a multi-disciplinary study of concepts, issues, and principles (NIST, 1998, pp. 15-16). A feature of the educational level is that the user must understand why information security is important (Schlienger & Teufel, 2003; NIST, 1998, pp. 16-17). Obviously end-users do not require the same level of understanding as information security professionals (NIST, 1998, p. 14). You don't need to understand why procedures are in place or how the technologies work to use them effectively

(Tripathy, 2000; NIST 1998, p. 15). However, in information security, if a user asks why, it should always be explained (Tripathy, 2000).

3.3 Learning materials should be customized to the needs of individual learners.

In an organizational context, users of information exist at several levels. There are essentially three categories of users that need to be educated in information security awareness namely: The End User, IT Personnel and Top Management (Thompson, 1998). The National Institute for Science and Technology (NIST) expands on this classification by stating that training and education are to be provided selectively, based on individual responsibilities and needs. Specifically, training is to be provided to individuals based on their particular job functions (NIST, 1998, p. 43). The ISO/IEC 17799 states that the information security policy should be communicated throughout the organization to users in a form that is relevant, accessible and understandable to the intended reader (BSI, 1999, p. 3). According to NIST, individuals learn in several ways, but each person, as part of his/her personality, has a preferred or primary learning style. Instruction can positively, or negatively, affect a student's performance, depending on whether it is matched, or mismatched, with a student's preferred learning style (NIST, 1998, p. 19). Thus, what should be taught to a specific individual user and how it should be taught, will depend on both the user's preferred learning style, and the specific role that user plays within the organization.

3.4 Users should be responsible for their own learning.

In today's organizations it is crucial to maximize return on investment. Through its very nature classroom training requires the availability of highly trained specialists to present the courses. It also requires that the learners take time off from their regular duties to attend classes. These factors make classroom training very expensive. One of the most cost-effective substitutes for traditional classroom training is to provide employees with intranet-based instruction (O'Brien, 1999, p.361). Such web-based instructional programs require individual learners to be responsible for their own acquisition of knowledge instead of being passive receptors in the process (ITiCSE Working Group on the Web and Distance Learning, 1997). Self-driven learning also enables organizations to make learning material available in a variety of formats. This is turn means users will have a choice of how they are taught, which has already been shown to be a necessary feature of information security education.

3.5 Users should be held accountable for their studies.

Most information security standards make it clear that users should be held accountable for their information security responsibilities (BSI, 1999, pp. 8-10). These responsibilities are normally spelt out in the organization's information security policies and procedures. In an organization, policies function in a similar fashion to laws. For laws, ignorance is not a valid defense. However ignorance of policy is an acceptable defense (Whitman & Mattord, 2003, p. 93). Thus, to be able to hold employees accountable for their actions, the organization should have proof, normally in the form of a signed form, that the employees have been educated regarding their responsibilities and that they understand and accept these responsibilities as laid out in the policies (Whitman & Mattord, 2003, p. 93). Wood (1997) suggests that all employees should be required, on an annual basis, to sign a statement saying that they have read and understood the information security policy manual. It should thus be clear that self-driven learning for information security purposes, as discussed previously, could only be used if the employees are also held accountable for their learning. Otherwise the organization could not legally hold the employees accountable for their actions.

Many organizations have realized that their own employees are the biggest threat to their information systems (Von Solms, 2000). However, through the establishment of a culture of information security, users can become a security asset instead of being a threat (Von Solms, 2000). Education of employees plays a very important role in the establishment of such a culture. It is paramount that the people are educated to want to be more secure in their day to day operation (Nosworthy, 2000). Such a change of attitude is of utmost importance, because a change in attitude automatically leads to a subsequent behavioral change (Nosworthy, 2000). The employees can then become the organization's most valuable assets. Current programs used to educate employees, fails to pay sufficient attention to aspects related to the behavioral sciences (Siponen, 2001).

It would make sense to adhere to a formal educational methodology when constructing such educational programs. The methodology used should be suitable for the specific needs of an information security user education program. Since the aim of the user education program is not to prepare the users for further levels of formal education, but rather to help them achieve information security know-how for use in their everyday jobs, the educational methodology used should be chosen accordingly. Outcomes Based Education (OBE) is an educational methodology that might in fact be ideally suited for use in such programs. The aim of OBE is to help learners achieve a specific outcome, in this case information security awareness and know-how.

4. OUTCOMES BASED EDUCATION

OBE is defined as an approach to teaching and learning which stresses the need to be clear about what learners are expected to achieve. The educator states beforehand what "outcome" is expected of the learners. The role of the educator is then to help the learners achieve that outcome (Siebörger, 1998).

Outcomes can be defined as either cross-curriculum (general outcomes) or specific outcomes. A cross-curriculum outcome can be seen as the desired effect that attaining a specific competency should have within the general environment within which the learner operates. A specific outcome is one that directly demonstrates the mastery of the appropriate skill that the learner should gain from the OBE program.

For each outcome an assessment standard should be defined. These standards are necessary in order to provide feedback to the learners. According to Siebörger (1998) assessment is essential to OBE to measure the degree to which a learner has achieved an outcome. In fact being able to assess progress and provide feedback to the learner is a prerequisite for any educational program to be successful. Fingar (1996) states that feedback, specifically in the form of knowledge regarding the outcomes of the learners' actions, is required for learning to take place. Furthermore this feedback should be continuous and constructive (Department Of Education (DOE), 2001).

The educational process in general can be viewed as a system of teaching and learning activities that are tied together via various feedback loops. It also includes other functions such as assessment, admission, quality assurance, direction and support (Tait, 1997). All of these components can, and should, play a role in the creation of an effective information security education program. OBE can be viewed in three different ways: as a theory of education, a systematic structure for education, or the creation of educational material, and lastly as a classroom practice (Killen, 2000). OBE can thus be seen as a complete educational system, which contains all the components such a system should have.

According to Killen (2000), OBE is based upon three basic premises, namely:

1. All students can learn and succeed, but not all in the same time or in the same way.
2. Successful learning promotes even more successful learning.
3. Schools (and teachers) control the conditions that determine whether or not students are successful at learning.

From these basic premises four essential principles of OBE were developed (Killen, 2000). They are:

1. Clarity of focus, which means that all teaching activities must be clearly focused on the desired outcome that the learners should achieve.
2. Designing back, which means that the starting point for an OBE program's design should be a clear definition of the desired results. The rest of the curriculum should be designed according to this desired outcome.
3. High expectations for all students. OBE not only assumes that everyone can attain the desired outcomes, it also requires that high standards should be set. This is based on evidence that learners are more likely to attain high standards when they are challenged by what is expected from them.
4. Expanded opportunities for all learners. This final principle of OBE is based on the idea that not everyone learns the same way or at the same pace. Thus, in OBE, learners are given many opportunities for learning. Achieving the desired outcome is deemed more important than how that outcome was reached.

In order for an educational program to be classified as being outcomes based, it has to adhere to all four of these principles.

5. OUTCOMES BASED EDUCTION FOR INFORMATION SECURITY

Up to this point this paper has shown the requirements an educational methodology would have to meet in order for it to be suitable for information security education. It has also introduced OBE and briefly outlined the basic premises and the principles of this educational methodology. It will now attempt to show that OBE is in fact well suited to the needs of information security.

The first requirement listed for information security education was that everyone should be able to "pass" the course. Clearly OBE fulfils this requirement since the first premise upon which OBE is based is the assumption that all students can succeed and learn.

Secondly, for information security education to be successful, employees must know why information security is important and why a specific policy or control is in place. Course developers should be aware that adults have well-established values, beliefs, and opinions. Adults relate new information and knowledge to previously learned information, experiences, and values which might

result in misunderstanding (NIST, 1998, p. 20). It is even possible that they understand correctly but still don't adhere to a security policy because it conflicts with their beliefs and values (Schlienger & Teufel, 2003). One of the fundamental differences between OBE and traditional educational models is the fact that rote learning is completely unacceptable in OBE. OBE requires the learner to identify and solve problems in which responses display that responsible decisions using critical and creative thinking have been made (Olivier, 1998; Pretorius, 1998). This type of thinking requires not only knowledge but also insight. Insight requires the learner to know why they are doing something (NIST, 1998, p. 18). According to Killen (2000) each outcome based educational program must have a rationale to explain why the program exists.

The third requirement of information security education identified was that learning materials should be customized to the needs of individual learners. The first basic premise of OBE not only states that all students can learn and succeed, but it also states that all students cannot necessarily do this in the same time or in the same way. This premise is also expanded on in the fourth principle of OBE, which states that learners should be given many opportunities for learning. OBE thus recognizes that individuals learn in different ways and at different paces. For a program to be truly outcomes based it is vital that learning materials are provided in as customized a format as possible for individual learners. However, according to Killen (2000) the practical difficulties of providing expanded opportunities must be weighed against the long-term benefits of enabling all learners to be successful.

The fourth and fifth suggested requirements of information security education state that users should be both responsible and accountable for their own learning. In other words, the users should take ownership of their own learning. Ownership of their learning and self-driven learning are central concepts to OBE. Because OBE recognizes that different students will learn at a different pace, OBE encourages self-driven learning. The ability to effectively manage one's own time, and learning abilities, are one of the critical cross curriculum outcomes identified for all South African students (South African Qualification Authority (SAQA), 2000). The OBE model strives to move away from teacher centeredness, towards learner-centered education (Malan, 2000). Thus, responsibility for their own studies can be seen to be central to OBE. Hand in hand with responsibility is accountability. OBE places major emphasis on assessment as a tool to provide feedback on progress to the learner, and as a tool for measuring whether the desired outcomes have been reached (Killen, 2000; Malan, 2000). Assessment makes students accountable for their studies.

The following is a brief summary of the relationships between OBE and information security education concluded thus far:

1 In terms of an organization's overall information security effort it is vital for all users to ultimately pass the information security course. OBE requires a high expectation for all learners to do well, and additionally requires that learners be given multiple opportunities to prove that they have achieved the desired outcomes.

2 Employees should be told why a specific information security policy, or control, that applies to them, is in place. In OBE memorization of concepts is not sufficient, OBE requires learners to have insight and thus to understand why they are doing something.

3 Due to the different levels of prior education, different organizational roles and different individual preferences of employees in an organization, learning materials used in an organization should be customized to the needs of individual learners. Recognizing that individuals learn in different ways and at different paces are concepts central to OBE. Flexible learning material, to suit individual needs, is a pre-requisite in an outcomes based program.

4 In order to control costs, and to provide the above-mentioned flexibility in learning materials, organizational learners should be responsible for their own learning. The organization should supply the learning materials in formats that support as many learning styles as possible, but responsibility for using those materials should ultimately rest with the individual employees. Employees should thus take ownership of their learning. This concept of ownership and self-driven learning are central to OBE, which is essentially a learner-centered educational methodology.

5 Hand-in-hand with ownership and responsibility is accountability. Organizations need to make employees accountable for their own learning, otherwise, they would not be able to hold them accountable for negligence stemming from a lack of education. In OBE, and other educational methodologies, assessment plays a vital role. Learners must be held accountable for their learning in order to get them to accept ownership of their learning.

OBE can thus be seen to match all of the requirements for information security education identified by this paper. In fact, a closer examination of the "results-based" educational framework advocated by NIST (1998) for information security programs will reveal many elements that are common to OBE as well. For example, NIST argues that information security education programs should be "results-based" and should focus on job functions, or roles and responsibilities specific to individuals (NIST, 1998, p. iii). OBE aims to help learners achieve a specific outcome or attain a specific skill. These outcomes should reflect the complexities of the real life and the roles the

learners would have to fulfill (Killen, 2000). In an organizational context this would mean that the outcomes would have to reflect skills needed in the individual's day-to-day job functions. Several other such similarities exist, but a detailed examination of these falls outside the scope of this paper. Instead, the contextual role of OBE in the establishment of a corporate culture of information security will be briefly examined.

According to Van Niekerk and Von Solms (2003), establishing a corporate culture will have to start with top management, who has to show commitment to information security via vision statements, policies and their own behavior. Secondly, a user education program should be constructed to educate the users about these policies and the behavior expected from them. Thirdly, middle management will have to positively reinforce any learning that took place by giving continuous feedback to the users. This feedback could take the form of performance metrics, e.g. key performance indicators, for individual employees. Ultimately, it will be this continuous reinforcement by middle management that produces the change in behavior.

If OBE is to be used in this process, the cross-curriculum outcomes and measurables for these outcomes would have to be clearly defined. The programs to teach employees the necessary skills to attain these outcomes would then have to be drawn up and made available in a variety of learning formats. These could for example include a set of online tutorials, security manuals, videos or even lunch-hour workshops. This will ensure that each user has a choice in terms of how they learn, which satisfies the third requirement as outlined previously. Part of these programs would have to discuss the possible consequences to both the individual and the organization as a whole, should an employee fail to comply to the taught procedures. This will satisfy the requirement that user should know why they are taught a skill.

Finally, to ensure that the users take ownership of their own learning, and to hold them accountable for their own learning, compliance metrics should be gathered. These metrics could then be used as part of individual user's key performance indicators. This can fulfill the role of the continuous feedback from middle management that is required to change behavior. These metrics could be gathered per department, branch, etc. and can then also be made part of the key performance indicators for the appropriate middle level manager. The old adage that what you measure is what you get will then play its part by ensuring that the appropriate line managers will feed this statistics back to their staff since it impacts on their own performance evaluations. Since the learning material should always be available and the employees are measured against their compliance, eventually all the users should reach a level of compliance that indicates they have "passed" the

course. It should thus be very possible to integrate all the requirements of information security education, as identified in this paper, into the process aimed at introducing a change in the organizational culture, as outlined by Van Niekerk and Von Solms (2003).

6 CONCLUSION

Humans today live in an emerging global information society, with a global economy that is increasingly dependent on the creation, management, and distribution of information resources. Information and its use permeate all aspects of modern society. Today, most organizations need information systems to survive and prosper. It is therefore imperative that modern organizations, operating in this global information society, take the protection of their information resources seriously.

This paper has pointed out that this protection of information resources are to a large extent dependent on human co-operated behavior. It also pointed out that this dependence on human behavior makes it necessary to have a user education program to educate users regarding their roles and responsibilities towards information security. This paper proposed several "elements", or properties such an information security education program should have in order for it to suit the needs of modern organizations. These included:

- Everyone should be able to "pass" the course.
- Employees must know why information security is important and why a specific policy or control is in place.
- Learning materials should be customized to the needs of individual learners.
- Users should be responsible for their own learning.
- Users should be held accountable for their studies.

Each of these proposed elements were argued in earlier sections of this paper.

The same elements were shown to be present in OBE, an existing pedagogical methodology. The possible role of OBE in the context of attempting to change organizational culture, were also briefly examined. This paper argued that OBE could be seen to be an excellent fit for the needs of information security education and is definitely a solution to these needs. It has been suggested that information security, because it depends on human behavior, should look at the human sciences when attempting to solve problems relating to the roles humans play in information security. This paper aims to reinforce that suggestion. Educationalists spend many years developing models such

as outcomes based education (OBE). These models have been extensively tested and critically examined in the literature. It is the contention of this paper that instead of "re-inventing the wheel" when designing user education programs, information security practitioners should "borrow" methodologies, like OBE, from the educational sciences. Future researchers who wish to solve information security education problems should be basing their work on sound pedagogical models.

7 REFERENCES

Barnard, L., Von Solms, R. (2000). A Formalized Approach to the Effective Selection and Evaluation of Information Security Controls. Computers and Security, 19(2): pp. 185-194.

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

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

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

Fingar, P. (1996). The blueprint for business objects. New York, New York : SIGS Books & Multimedia

Guidelines to the Management of Information Technology Security (GMITS). (1995). Part 1, ISO/IEC, JTC 1, SC27, WG 1.

ITiCSE Working Group on the Web and Distance Learning (1997). The Web and distance learning:what is appropriate and what is not. ITiCSE'97 Working Group Reports and Supplemental Proceedings, pp. 27-37.

Killen, R. (2000). Outcomes-Based education: Principles and Possibilities. Unpublished manuscript, University of Newcastle, Faculty of Education. [WWW document]. URL http://www.schools.nt.edu.au/curricbr/cf/outcomefocus/killen_paper.pdf. Sited 20 August 2003.

Laudon, K. C., Laudon, J. P. (2002). Management Information Systems: Managing the Digital Firm (7th ed). New Jersey, USA: Prentice Hall.

Malan, S.P.T. (2000) The 'new paradigm' of outcomes-based education in perspective. Tydskrif vir Gesinsekologie en Verbruikerswetenskappe (28), South Africa.

Martins, A., Eloff, J.H.P. (2002) Assessing Information Security Culture. ISSA 2002, Muldersdrift, South Africa, 10-12 July 2002.

Mitnick, K.D., Simon, W.L. (2002) The art of deception: Controlling the human element of security. United States of America : Wiley Publishing, Inc.

National Institute of Standards and Technology (NIST). (1998). Information Technology Security Training Requirements: A Role- and Performance-Based Model. NIST Special Publication 800-16. U.S. Government Printing Office, Washington.

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

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

Olivier, C. (1998), Educate and Train : Outcomes-Based. Pretoria, South Africa. J.L. van Schaik.

Pretorius, F. (1998). Outcomes-based Education in South Africa. Randburg, South Africa: Hodder and Stoughton Educational.

South African Qualifications Authority (SAQA) (2000). The National Qualifications Framework and Curriculum Development. Retrieved on 10 September 2003 from URL http://www.saqa.org.za

Schlienger, T., Teufel, S. (2003) Information Security Culture – From Analysis to Change. Proceedings of the 3rd Annual Information Security South Africa Conference, 9-11 July 2003, Sandton, South Africa, pp. 183-196.

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

Siponen, M.T. (2001). Five Dimensions of Information Security Awareness. Computers and Society, June 2001. Pp. 24-29.

Tait, B. (1997). Object Orientation in educational software. Innovations in Education and Training International, 34 (3). Pp. 167-173.

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

Tripathi, A. (2000) Education in Information Security. IEEE Concurrency, October-December 2000, pp. 4-8.

Turban, E., Mclean, E., Wetherbe, J. (2002). Information technology for management: Transforming business in the digital economy (3rd Ed).United States of America. John Wiley & Sons, inc.

Van Niekerk, J., Von Solms, R. (2003). Establishing an Information Security Culture in Organisations: An Outcomes Based Education Approach. Proceedings of the 3rd Annual Information Security South Africa Conference, 9-11 July 2003, Sandton, South Africa, pp. 3-12.

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

Von Solms, R. (1999) Information Security Management: why standards are important. Information Management & Computer Security, 7 (1), pp. 50-57.

Whitman, M. E., Mattord, H. J. (2003) Principles of Information Security. Canada: Thomson Course Technology.

Wood, C.C. (1997) Policies alone do not constitute a sufficient awareness effort. Computer Fraud & Security, December 1997, pp. 14-19.

ACKNOWLEDGEMENTS

The financial assistance of the National Research Foundation (NRF) towards this research is hereby acknowledged. Opinions expressed and conclusions arrived at, are those of the author and are not necessarily to be attributed to the National Research Foundation.