FOSTERING INFORMATION SECURITY CULTURE THROUGH INTEGRATING THEORY AND TECHNOLOGY

by

Johannes Frederick van Niekerk

FOSTERING INFORMATION SECURITY CULTURE THROUGH INTEGRATING THEORY AND TECHNOLOGY

by

Johannes Frederick van Niekerk

Thesis

submitted in fulfillment
of the requirements
for the degree

Philosophiae Doctor

in

Information Technology

in the

Faculty of Engineering, the Built Environment and Information Technology

of the

Nelson Mandela Metropolitan University

Promoter: Prof. Rossouw Von Solms

August 2010

Declaration

I, Johannes Frederick van Niekerk, hereby declare that:

- The work in this thesis is my own work.
- All sources used or referred to have been documented and recognized.
- This thesis has not previously been submitted in full or partial fulfillment of the requirements for an equivalent or higher qualification at any other recognized educational institute.

Johannes Frederick van Niekerk

Abstract

Today information can be seen as a basic commodity that is crucial to the continuous well-being of modern organizations. Many modern organizations will be unable to do business without access to their information resources. It is therefor of vital importance for organizations to ensure that their information resources are adequately protected against both internal and external threats. This protection of information resources is known as *information security* and is, to a large extent, dependent on the behavior of humans in the organization.

Humans, at various levels in the organization, play vital roles in the processes that secure organizational information resources. Many of the problems experienced in information security can be directly contributed to the humans involved in the process. Employees, either intentionally or through negligence, often due to a lack of knowledge, can be seen as the greatest threat to information security. Addressing this *human factor* in information security is the primary focus of this thesis.

The majority of current approaches to dealing with the human factors in information security acknowledge the need to foster an information security culture in the organization. However, very few current approaches attempt to adjust the "generic" model(s) used to define organizational culture to be *specific* to the needs of information security. This thesis firstly proposes, and argues, such an adapted conceptual model which aims to improve the understanding of what an information security culture is.

The thesis secondly focuses on the underlying role that information security educational programs play in the fostering of an organizational information security culture. It is argued that many current information security educational programs are not based on sound pedagogical theory. The use of learning taxonomies during the design of information security educational programs is proposed as a possible way to improve the pedagogical rigor of such programs. The thesis also argues in favor of the use of blended and/or e-learning approaches for the delivery of information security educational content. Finally, this thesis provides a detailed overview demonstrating how the various elements contributed by the thesis integrates into existing transformative change management processes for the fostering of an organizational information security culture.

Acknowledgements

My grateful thanks goes to the following people:

My promoter, Professor Rossouw von Solms, whose knowledge, guidance, support and patience have played a major role in both my career and the completion of this thesis.

My wife, Ezanne, who had to spend a lot of time without me while I was working on this thesis.

Contents

List of Tables

List of Figures

Chapter 1

INTRODUCTION

This chapter introduces the research problem, research questions and research objectives of the thesis.

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 (B. Von Solms, 2000).

It is therefor of vital importance for organizations to ensure that their information resources are adequately protected against both internal and external threats. The protection of organizational information resources is typically accomplished through the implementation of various information security controls. These controls are usually selected with the aid of internationally accepted standards such as ISO/IEC 27002 (2005) and ISO/IEC TR 13335-1 (2004).

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 (M. Thomson, 1998). Humans, at various levels in the organization, play a vital role in the processes that secure organizational information resources. Many of the problems experienced in information security can be directly contributed to the humans involved in the process. Employees, either intentionally or through negligence, often due to a lack of knowledge, can be seen as the greatest threat to information security (Mitnick & Simon, 2002, p. 3). Addressing this *human factor* in information security will be the primary focus of this thesis.

Information security standards, such as ISO/IEC 27002 (2005) and ISO/IEC TR 13335-1 (2004), recommend the use of information security awareness campaigns to help address the human factor in information security. According to ISO/IEC 27002 (2005) **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 27002, 2005, p. 11 section 6.2.1). The standard does **not** provide any guidance as to how this training should be done.

Exactly how to educate organizational users regarding their information security related roles and responsibilities has been the focus of many studies. Chapter 4 provide an in depth overview of such studies. However, education alone cannot completely address the human factor in information security. As shown in section 4.3, the majority of current research studying the human factor in information security acknowledges that behavioral aspects are equally important when dealing with the role(s) humans play in information security. In fact, many recent studies have shown that the establishment of an *information security culture* in the organization is necessary for effective information security (Eloff & Von Solms, 2000)(B. Von Solms, 2000).

A lot of knowledge exits in the management sciences regarding organizational 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 a user education program will have to play a major role in the establishment of such a culture. The aim of this thesis is to contribute to the field of information security by improving the understanding of the concept of an information security culture, and by addressing the role that education would play in the fostering of such a culture in a holistic way.

The rest of this chapter will provide a brief outline of the research aims of this thesis. This outline will be presented according to the format recommended by Hofstee (2006, pp. 80-90).

1.2 Fields of Study

The work in this thesis falls primarily in the fields of *information security education* and *organizational culture*.

1.3 Problem Statement

As mentioned earlier, information security is dependent on the behavior of humans in order to be effective. It has been argued that the establishment of an organizational culture of information security would be the ideal way to ensure desirable user behavior. A lot of knowledge exits in the management sciences regarding organizational culture in general, but very little knowledge exists regarding the applicability of this knowledge to information security specifically. It is, however, clear that a user education program will have to play a major role in the establishment of such a culture. An extensive analysis of current approaches towards dealing with the human factor in information security has been performed as part of this thesis. This analysis is presented in chapter 4. A summary of the results of this analysis is presented in section 4.3. This analysis has shown that:

- Most current approaches recognize the importance of the behavioral aspects in dealing with the human factor in information security

- Most current approaches acknowledge the need to foster an information security culture in the organization
- Very few current approaches attempt to adjust the "generic" model used to define organizational culture to be specific to the needs of information security
- Less than a quarter of current approaches uses a formal, pedagogical approach to information security educational programs
- Only one current approach mentions the use of learning taxonomies to improve the design of information security educational programs, none provides guidance on how to use such a taxonomy for information security education
- Less than a third of current approaches mentions the use of e-learning and/or technological platforms to improve the delivery of information security education

This analysis of current literature addressing the human factor in information security has shown that current approaches, which focus on the fostering of an organizational information security culture, rarely modify existing theory to be specific to the needs of information security. Furthermore, current approaches towards educating organizational users regarding information security are mostly not based on sound pedagogical principles. The problem which this thesis will address can thus be summarized as follows:

Most current approaches towards dealing with the human factors in information security do not have a sound theoretical basis.

1.4 Thesis Statement

Theory from the human and social sciences **can** be adapted and/or used to address the human factors in information security.

1.5 Delineation

The human factor in information security consists of two closely inter-related dimensions, namely knowledge, and behavior. These dimensions are discussed in depth in section 3.4. The establishment of an organizational culture of information security will address both of these dimensions. In order to establish such a culture organizational users should be educated and motivated. This thesis will firstly focus on the overall concept of an information security culture, and will secondly deal with the requisite information security educational programs to establish such a culture in depth. However, to address the requisite motivational aspects in equal depth would require an in depth knowledge of the underlying psychological factors that could play a role. *This thesis will not attempt to address these psychological factors in depth.* Instead, motivational aspects will be dealt with only in sufficient detail to highlight their relative role(s) during the fostering of an information security culture, and to highlight the closely inter-related nature of the dimensions of the human factor in information security.

1.6 Research Questions

The primary research question this thesis will answer is:

How can existing theory be adapted and/or used to address the human factors in information security?

In order to answer this primary research question, the following sub-question will be answered:

1. How can the *generic* definition of organizational culture be **adapted** *to be specific* to the needs of information security?

2. How can a learning taxonomy be used to plan the contents of an information security educational program?

3. How should information security educational activities be delivered to organizational learners?

4. How can the various theoretical and technical elements be integrated into transformative change management processes in order to foster an organizational information security culture?

1.7 Research Objectives

The primary objective of this thesis is to *demonstrate* ***how*** *existing theory can be modified and/or used when addressing the human factor in information security.*

In order to achieve this objective, the following secondary objectives have been identified:

1. Adapt the *generic* model which defines organizational culture, as presented by Schein (1999a, pp. 15-16) to be specific to the needs of information security.

2. Demonstrate how the use of a learning taxonomy can be used to add pedagogical rigor to information security educational programs.

3. Demonstrate the suitability of e-learning as a delivery medium for organizational information security educational programs.

4. Provide a detailed overview demonstrating how the various elements contributed by this thesis integrates into existing transformative change management processes for the fostering of an organizational information security culture.

1.8 Layout of the Thesis

This thesis has been laid out in accordance to the general guidelines provided in (Hofstee, 2006, pp. 35-43). Figure 1.1 provides a graphical overview of the thesis layout.

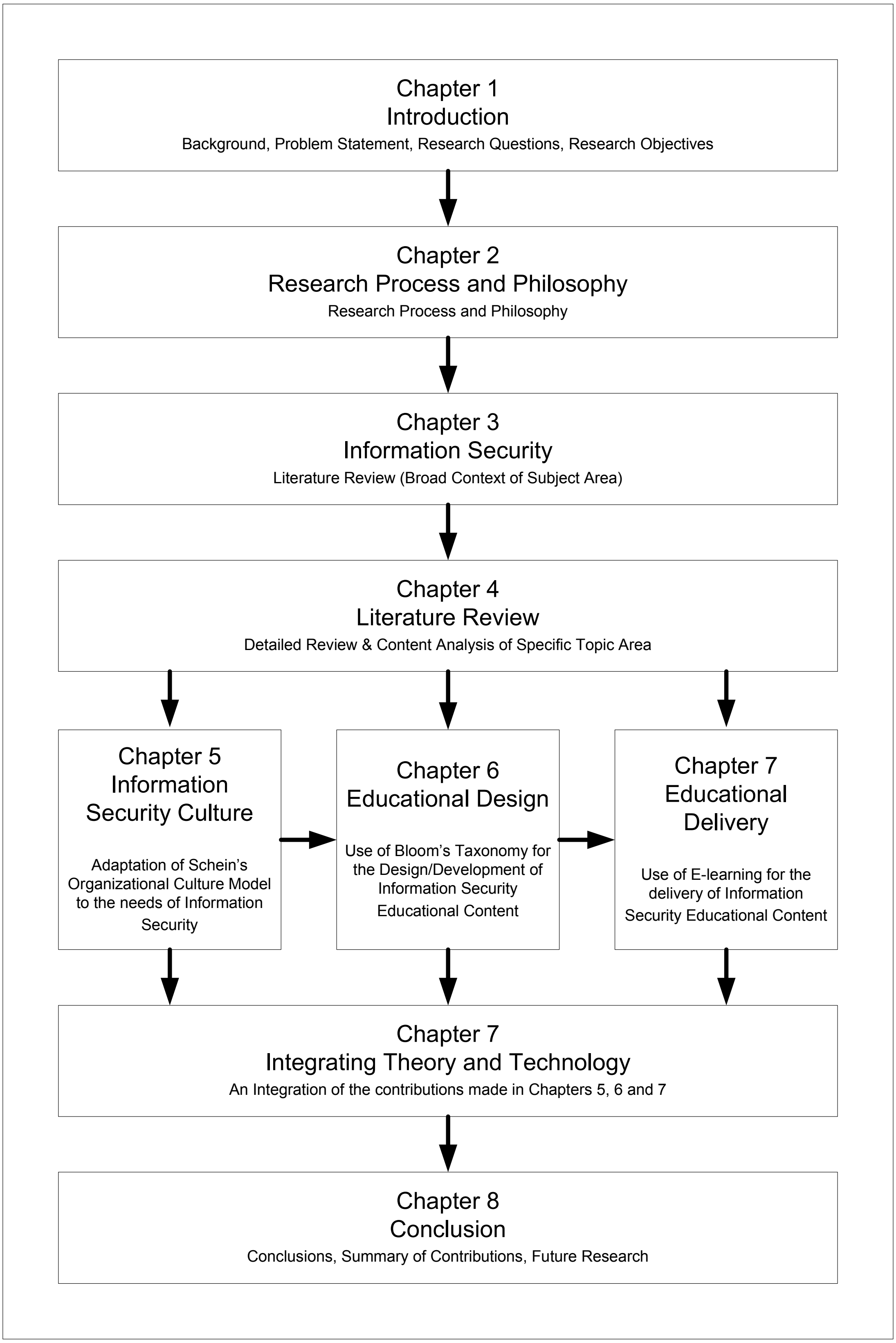

Chapter 1
Introduction
Background, Problem Statement, Research Questions, Research Objectives
Chapter 2
Research Process and Philosophy
Research Process and Philosophy
Chapter 3
Information Security
Literature Review (Broad Context of Subject Area)
Chapter 4
Literature Review
Detailed Review & Content Analysis of Specific Topic Area
Chapter 5
Information Security Culture
Adaptation of Schein's Organizational Culture Model to the needs of Information Security
Chapter 6
Educational Design
Use of Bloom's Taxonomy for the Design/Development of Information Security Educational Content
Chapter 7
Educational Delivery
Use of E-learning for the delivery of Information Security Educational Content
Chapter 7
Integrating Theory and Technology
An Integration of the contributions made in Chapters 5, 6 and 7
Chapter 8
Conclusion
Conclusions, Summary of Contributions, Future Research

Figure 1.1: Layout of the Thesis

Chapter 2

RESEARCH PROCESS AND PHILOSOPHY

This chapter provides a high level overview of the research process followed in this study. Philosophical considerations which influenced the choice of the research paradigm and methodologies are briefly discussed.

2.1 Introduction

The aim of this chapter is to describe the research process that was followed during the work conducted in this thesis, and to provide insight into the philosophical assumptions of the author in order to ensure the trustworthiness of the results of the work. The chapter will not attempt to provide a *treatise* on various research methodologies. As such the discussion of methodological considerations will focus on material that provides insight into the underlying factors that influenced the decisions that were made during the choice of appropriate methodologies. The chosen research methodologies themselves are briefly introduced in the specific chapters where each methodology is used. For more detail the reader should refer to the relevant authors of methodological texts referenced for each of the used methodologies.

In order to choose a suitable methodological approach for the work in this thesis, the author conducted an extensive investigation into research methods used by other researchers in the field of information security. The author examined publications over a three year period ranging from the beginning of 2006 to the end of 2008, in both the journal ”Computers & Security” and the

"Proceedings of the IFIP TC 11 International Information Security Conference". These two publication forums were chosen since, in the author's opinion, they represent the foremost research in the field of information security. The methodology for this examination can be described as interpretive content analysis, as described in Krippendorff (2004, pp. 87-88). The analysis was not exclusively empirically grounded, like some forms of content analysis, but rather examined the literature with a specific goal in mind, namely to determine the methodologies espoused by the published articles and papers. However, since this analysis was largely a process of *systematic content analysis of large bodies of text*, it still has some clearly quantitative, hence empirical, roots.

The analysis examined a total of 284 articles and papers. This included all papers and articles over the three year period but excluded editorials. Of the analyzed articles and papers 216 were found to be primarily positivist, design orientated, or empirical based. The remaining 68, equal to 23.9% of the total, were deemed to be interpretive and/or qualitative in nature.

Based on this analysis *design science* was chosen as an appropriate methodology for the development/adaptation of the *generic* model which defines organizational culture, as presented by Schein (1999a, pp. 15-16) to be specific to the needs of information security (the first research objective of this thesis). However, the remainder of the work in this thesis is primarily of a qualitative nature. The research was primarily conducted in an inductive way during which research questions were continuously evolved (refer to section 2.6 for a discussion of this process) as increased understanding of the subject matter/research needs were gained. Due to the interpretive nature of qualitative work, it is important to ensure the trustworthiness of the research by providing either guarantors of objectivity, or via reflexive methods (Easterby-Smith, Golden-Biddle, & Locke, 2008)(Meyrick, 2006)(Mays & Pope, 2000).

This thesis used a continuous process of publication/presentation of results at *relevant*, *peer-reviewed*, *subject specific conferences* as its primary guarantor. Research work was continuously updated and/or improved based on feedback received from such peer-review. This process of verifying research results via publication will continue for all sections of this thesis that have not yet been published. A full outline of all publications that have thus far stemmed from the work in this thesis is presented in section 9.4 of chapter 9.

The rest of this chapter will briefly outline the philosophical assumptions that led to the choice of a qualitative research paradigm. Secondly, considerations which could influence the quality of such qualitative work will be briefly examined, followed by an explicit overview of the researcher's philosophical and methodological choices. Finally an outline of the actual research process according to which the work was conducted will be presented.

2.2 Research Philosophy and Paradigm

All research begins with philosophical assumptions. Even if the researcher him/her self is unaware of these assumptions, they still exist. Every person has a certain world view or philosophy and to a certain extent this world view will influence his/her research. The choice of a research paradigm and methodology will also be influenced by this philosophy. Figure 2.1 shows the core ontological assumptions which might stem from a researcher's primary choice of philosophy.

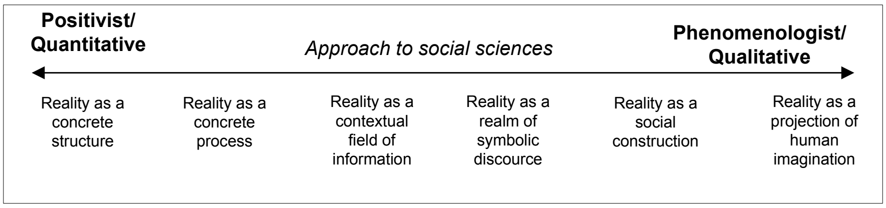

Positivist/ Quantitative
Approach to social sciences
Phenomenologist/ Qualitative
Reality as a concrete structure
Reality as a concrete process
Reality as a contextual field of information
Reality as a realm of symbolic discource
Reality as a social construction
Reality as a projection of human imagination

Figure 2.1: Continuum of core ontological assumptions (adapted from (Collis & Hussey, 2003, p. 51))

Researchers whose primary philosophy leans towards the quantitative side of the continuum view reality as a concrete structure and believes that it is possible to objectively measure this reality. This extreme of the philosophical continuum has been widely used and accepted in the natural sciences. At the other extreme, researchers leaning towards the qualitative side interpret reality as a projection of human imagination. In such a qualitative world view the subjective nature of the human doing the research is acknowledged and this form of research tends to focus more on the *interpretation* of the research than on the *measurement* of results (Collis & Hussey, 2003, p. 53).

Even though it is widely accepted that qualitative research can help information systems researchers to understand human thought and action in both social and organizational context (Klein & Myers, 1999), researchers studying such phenomena in an organizational context might still choose to not use such methods if they clash with their own research philosophy.

The following five categories of philosophical assumptions can lead to an individual's choice to do qualitative work (Creswell, 2007, pp. 16-19), (Ritchie & Lewis, 2003, pp. 11-23):

1. Ontological: The researcher believes in "multiple realities". In other words, the researcher believes that even supposedly objective studies are still influenced by the person doing these studies' subjective interpretation of the results. There can thus be more than one interpretation of the same reality. Research subjects being interviewed might also experience the same reality in different ways.

2. Epistemological: The researcher believes that getting as close as possible to the subjects being studied will result in a "better" study.

3. Axiological: The researcher tries to make his/her "values" explicit. In other words, the researcher admits to being subjective, and tries to "actively report their own values and biases as well as the value-laden nature of the information gathered from the field" (Creswell, 2007, p. 18).

4. Rhetorical: Qualitative researchers tend to write in a more personal and literary form. They might employ terms such as "credibility" instead of "objectivity". The language used in the study is often based on definitions that evolved during the study, as opposed to definitions the researcher him/her self brought to the study.

5. Methodological: Qualitative researchers use inductive logic, as opposed to the deductive logic used by quantitative researchers. They usually study the topic within its context, and continually revise questions based on experience gained.

The above philosophical assumptions might lead to a researcher doing qualitative work. As mentioned earlier many research works make no clear distinction between ”qualitative” and ”interpretive” work (Klein & Myers, 1999). However, these terms are not synonymous; **qualitative work may or may not be interpretive** and will generally fall into one, or more, of the following four main research paradigms (Creswell, 2007, pp. 19-23)

1. Postpositivism - This is mainly a scientific approach and the researcher will likely view inquiry as a series of logically related steps. This research usually espouses rigorous methods of data collection and analysis. Postpositivst approaches strongly resemble quantitative approaches.

2. Constructivism (**Interpretivism**) - In this form of research, subjective meanings are formed through interaction with others. ”Rather than starting with a theory (as in postpositivism) inquirers generate or inductively develop a theory or pattern of meaning” (Creswell, 2007, p. 21). These researchers often address processes of interaction among individuals. The findings of these researchers are ”shaped” by their own interpretations.

3. Advocacy/Participatory - This type of research contains an action agenda that might change the lives of participants. Action research as a methodology is probably the best known example of work in this paradigm.

4. Pragmatism - Pragmatism focuses on the **outcomes** of the research more than the antecedent conditions. In other words, in pragmatism the application(s) of the research is more important than focusing on rigorous methods. In practice, the researcher will often employ multiple methods to best answer the research question (Creswell, 2007, p. 23).

From the above paradigms and philosophies it should also be clear that qualitative methods are not always easy to classify. However, it should be clear that ”the criterion of confirmation through data should be played down relative to what books on method normally suggest, and conceptions of the nature of empirical material should be changed as compared to traditional epistemology” (Alvesson & Sköldberg, 2000, pp. 275-276). That does not imply that empirical material is unimportant. But it should be consigned a considerably less clear-cut and robust character. Empirical data is still ”*an expression on negotiable, perspective-dependent interpretations*” and is conveyed in an ambiguous language. "*Empirical material should be seen as an argument in efforts to make a case for a particular way of understanding social reality...*" (Alvesson & Sköldberg, 2000, pp. 275-276).

The above philosophies and paradigms can lead to many distinct approaches towards qualitative studies. Some of these methodologies have strong empirical grounding, e.g. postpositivist, while others might be more interpretive. It is even possible for one methodology to borrow from more than just one of the qualitative paradigms. This wide array of choices available to qualitative researchers not only makes it difficult for the researcher him/her self to choose a specific philosophy, ontological stance and methodology, but also makes it very difficult for future researchers who want to build on such a researcher's work to judge the compatibility of published work with their own philosophies and methods.

To fully evaluate the applicability of another researcher's work to his/her own work, a researcher must be able to understand the philosophical choices made by that prior researcher. This is especially true in qualitative work, which is inherently biased. Without insight into the prior researcher's possible biases a future researcher might be unable to ascertain the applicability of the prior work as a basis to his/her own work.

2.3 The Researcher's Dilemma

All researchers are to varying degrees dependent on the work done by other researchers before them. Sir Isaac Newton, one of the foremost scientists of the last few centuries, is often quoted as having said: "*If I have seen further it is only by standing on the shoulders of giants*". This is true of most research. A researcher's work is often judged by the credibility of his/her argument, which is based on a *specific* philosophical stance and which is supported by the arguments of earlier researchers (included as citations in his/her work). Even the best research results might be discredited if they were based on prior research of doubtful integrity, or if they were based on prior work from an incompatible philosophical stance. Learning how to judge the credibility of sources is one of the first skills a new researcher has to master.

When faced with a publication that could potentially support his/her own work, a researcher has to ask him/her self two basic questions in order to judge the "value" of the work for his/her own research,

1. "Can I trust the integrity of this research?"

2. "Can this research be integrated with, or used in support of, my own research?"

To a certain extent it has become the norm to answer the first of the above questions based on the reputation of the forum on which the research was published. Obviously, the forum of publication is not the only important factor when answering this question, but it is one of the most useful overall indicators. Usually the integrity of any work published in a credible and peer-reviewed journal can be viewed as trustworthy. Similarly the integrity of work referenced from a forum like Wikipedia is often distrusted. Thus, even though the actual information provided about a specific topic on Wikipedia might in fact be correct, a credible researcher would still avoid using it as a primary reference because the integrity of the forum in general is distrusted.

Answering the second question can be more difficult and requires a lot of insight into the research work's underlying philosophical, ontological and methodological assumptions. It is especially important to ascertain whether the methodologies used in the different studies are compatible. According to Mason (1996, pp. 34-36) the following factors should be considered when determining the compatibility of different methods:

1. Technical integration: Are the units of analysis used in the research similar or complimentary? In other words, will you be "comparing apples with apples"?

2. Ontological integration: Are the works based on "similar, complementary or comparable assumptions about the nature of social entities and phenomena?" (Mason, 1996, p. 35).

3. Integration at the level of knowledge and evidence: Do the different methods or forms of data stem from the same epistemologies? "Are they based on similar, complementary or comparable assumptions about what can legitimately constitute knowledge or evidence?" (Mason, 1996, pp. 35-36).

4. Integration at the level of explanation: Integration at this level also depends on the epistemologies but focuses on the ways in which theories are constructed or the ways in which results can be generalized. Can the "different data sources and methods usefully contribute to some kind of coherent and convincing argument...?" (Mason, 1996, p. 36). According to (Collingridge & Gantt, 2008) "qualitative studies that do not follow a coherent qualitative framework and are poorly executed lack generalizable results".

It might be tempting to disregard, or under-estimate, the seriousness of such concerns regarding the compatibilities of various methods. However, researchers whose own philosophical stances lie at one of the extremes of the continuum shown in Figure 2.1 often question the validity of the work of researchers operating at the opposite extreme. Such concerns regarding the validity of work done by researchers with a different philosophical or ontological stance are not restricted to researchers at one of the extremes of the continuum only. **All** researchers have to be able to make critical judgements regarding the validity of work done by other researchers. Because quantitative and positivistic work have a long standing tradition of adhering to the "scientific method" and are less prone to interpretive biases of the researcher, this is less of a problem at the quantitative end of the continuum. Certain fields of study, especially those where most researchers adhere to the same, clearly established, methodological traditions, might also be less prone to the effects of such compatibility concerns. However, in information security this is not the case. Information security researchers often use methods varying from the quantitative/positivistic side of the continuum all the way through to the qualitative/phenomenological side. It is therefor vital that researchers in information security not only accurately assess the general validity of research sources, but also pay specific attention to questions regarding methodological compatibility. As argued earlier, this is especially true when dealing with qualitative work. Many studies have addressed the general issues researchers face to assess the validity of qualitative work . These issues will be briefly examined.

2.4 Assessing the Validity/Quality of Qualitative Research

Many authors have focused on issues regarding the assessment of research quality, or validity, in qualitative research. This section will provide a very brief overview of this issue. Meyrick (2006) provides a step-by-step framework to enable readers to make a "value judgement about rigour and quality" for qualitative research. The following steps are listed (Meyrick, 2006):

- **Researcher epistemological and theoretical stance**. "Good quality research ensures that the epistemological and theoretical stance of the researcher is **stated clearly in the study**" (Meyrick, 2006)(Amis & Silk, 2008). The distance between the researcher(s) and the subject(s) need to be clearly established via either guarantors of objectivity, or reflexive methods (Easterby-Smith et al., 2008)(Meyrick, 2006)(Mays & Pope, 2000).

- **Methods**. The research objectives and the methods used to reach these objectives should be stated clearly in order to enable the reader to "make judgements on the appropriate selection of methodology and whether they meet the criteria" (Meyrick, 2006). The reader should be able to answer the question "would a different method have been more appropriate?" (Mays & Pope, 2000). According to Collingridge and Gantt (2008) the entire concept of **reliability** in qualitative research revolves around the adoption of "research methods that are accepted by the research community as legitimate ways of collecting and analyzing data" (Collingridge & Gantt, 2008).

- **Sampling**. The rationale and theory behind sampling techniques used should be clearly established (Meyrick, 2006). It is also important, if appropriate, to demonstrate that efforts were made to obtain contradictory data (Mays & Pope, 2000). Sampling should also be done in a fashion that ensures results can be generalized (Collingridge & Gantt, 2008).

- **Data Collection**. How data was collected should be described with sufficient transparency for the reader to "judge if the methods used and decisions made during data collection were reasonable" (Meyrick, 2006). A future researcher should be able to repeat the same data collection process (Mays & Pope, 2000).

- **Analysis**. It is important to provide sufficient insight into the route that was followed from the data to the conclusions (Meyrick, 2006). The exact "route" might vary from study to study but the reader should have sufficient information to "follow the process and judge how fair, reasonable or regular the process or steps taken were" (Meyrick, 2006).
- **Results and Conclusions**. In order to reinforce the link between the data and the conclusions, insight should be provided on exactly how the data shaped the conclusions (Meyrick, 2006).

To a certain extent, the utility of most research depends on how generalizable the research results are. According to Collingridge and Gantt (2008) "qualitative studies that do not follow a *coherent qualitative framework* and are poorly executed lack generalizable results". In order to be generalizable, qualitative studies should "build on existing theoretical concepts through comprehensive literature reviews, employ theory-based sampling procedures, follow well-defined data analysis procedures, clearly define how the findings apply to other contexts, and integrate results into existing research in a coherent fashion" (Collingridge & Gantt, 2008). In light of the above listed step-by-step framework for ascertaining the quality, or validity, of qualitative research it should be clear that a reader of qualitative research will be unable to judge whether or not a *coherent qualitative framework* was followed, if the researcher's epistemological and theoretical stance, as well as the research methods, have not been explicitly espoused. One possible guideline for researchers who wish to publish work based on qualitative research methods is to describe their research approach with the help of a construct like the "research onion" presented by Saunders et al. (2007)

2.5 The Research Onion

Saunders et al. (2007) provide a layered approach towards explaining research choices known as the "research onion". This is a popular way (and perhaps one of the easiest) to understand, and present, the plethora of choices a researcher has to make. Figure 2.2 depicts this research onion.

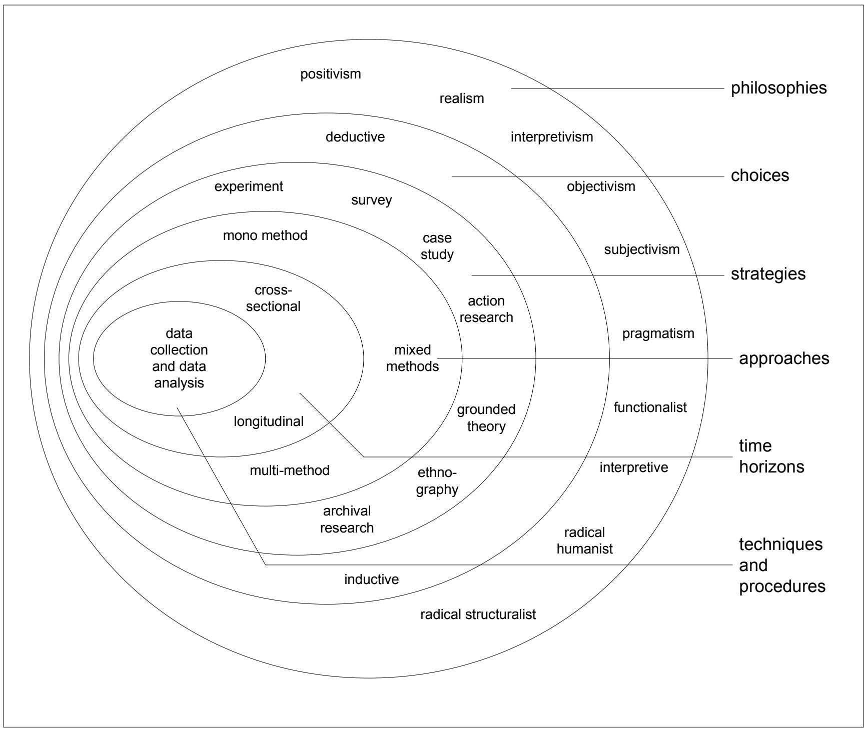


Figure 2.2: Research Onion. Adapted from (Saunders et al., 2007)

When using the research onion the research would start at the outer layers and proceed inwards in the espousing of their research choices. At the first layer lies the philosophical stance of the researcher. To a certain extent, the choice of philosophy will determine whether the researcher's work will be primarily deductive (in which a theory and hypothesis is developed), or inductive (in which data is collected and a theory developed as a result of the data analysis). This choice will in turn lead to the choice of research strategy which could include case studies, action research, surveys, etc. Research strategy choices lead to an overall research approach, including mono method, multi-method, or mixed method approaches. The research approach helps to determine the time horizons of the research (longitudinal or cross-sectional), which in turn leads to specific techniques and procedures (including focus group research, interviewing, questionnaires, etc). It is not the author's intention to recommend the use of the research onion as *the solution* to the discussed problem of determining the quality/validity of qualitative work.

The use of a construct *similar to this research onion*, as a form of checklist, could ensure that the necessary information is available to allow the reader to make an informed judgement of the validity and/or applicability of the research to his/her own research needs. Such a list does not necessarily have to include all aspects outlined by the research onion. Instead **it should only list all aspects which are *applicable* to the specific study**. The following list serves to espouse the philosophical choices made for this thesis, in terms of the general framework provided by the research onion:

- Philosophy: The work in this thesis was conducted based on a **pragmatic** philosophy. The author does not prescribe to either a strict positivist, or a strict interpretive viewpoint. Instead, the author believes that methods should be chosen based on their *suitability for the specific task at hand.*

- Choices: The work in this thesis is primarily of an **inductive** nature. Research questions were continuously evolved as increased understanding of the subject matter/research needs were gained. The process of this ”evolution” is discussed in the next section.

- Strategies: **Design science** was selected as the primary research strategy. The guidelines for this research strategy, as presented by Hevner, March, Park, and Ram (2004), are discussed in more depth in chapter 5. This strategy was extensively supported by **evidential and narrative argumentation**.

- Approaches: A **triangulated approach** was used. Various methods, techniques and procedures were used to establish the validity of results.

- Techniques and Procedures: The research methods, techniques, and procedures used for specific elements of this study are espoused in the specific chapters to which those methods, techniques and procedures apply.

As mentioned earlier, the primary method of **verification** of results used for the work in this thesis was a process of **extensive peer-review and publication** (this also meets guideline 7 for design science as specified by Hevner et al. (2004) and discussed in section 5.2). The following section will briefly describe the research process that was followed during this study in a narrative manner.

2.6 Research Process

The work in this thesis was preceded by a Master's degree dissertation in the field of information security education. Initially the author focused on the possible role(s) that e-learning, and specifically adaptive technologies, could play in information security education. This initial work led to the publication of Van Niekerk and Von Solms (2006a) at the E-learn 2006 conference. Feedback stemming from this initial work, and extensive additional literature work, led the author to belief that the use of e-learning on its own would not solve the problems associated with the human factor in information security. Education on its own cannot address all behavioral aspects related to this human factor. Instead, the focus of attempts to address this human factor should be on the fostering of an organizational information security culture.

The need for an adaptation of the existing generic model defining organizational culture, in order to make it more suited to the specific needs of information security, was determined. This led to an initial version of the conceptual model presented in chapter 5. This initial version was published as Van Niekerk and Von Solms (2006b). During the next three years this initial version of the conceptual model defining information security culture was subjected to several cycles of peer-review and eventually refined into the final version presented in chapter 5. This conceptual model is seen as one of the primary research contributions of this thesis and has been published in the journal "Computers & Security" as Van Niekerk and Von Solms (2010).

The education of employees regarding their information security related roles and responsibilities plays a *major* role in the fostering of an organizational information security culture. Due to the importance of information security educational programs for the fostering of such a culture, these educational programs have to be dealt with as an integral part of the fostering of such a culture. Concurrent to the further development of the conceptual model, the work in this thesis therefor focused on the underlying educational programs. An extensive investigation into current information security awareness, training, and educational approaches was conducted and a need for more pedagogical rigor in current approaches was identified. Extensive examination of pedagogical theory identified the important role learning taxonomies could play in information security education. This work was published at the Information Security South Africa conference as Van Niekerk and Von Solms (2008). After extensive peer-review and feedback, a second paper focusing more on the actual use of the taxonomy in information security was published at the World Information Security Education conference as Van Niekerk and Von Solms (2009).

Finally, the above elements were integrated into existing and transformative change management process to show how these elements could form part of a holistic approach towards the fostering of an organizational information security culture. Further publication of work in this thesis is ongoing.

2.7 Conclusion

This chapter outlined the philosophical assumptions which influenced the work in this thesis. A discussion of the nature of qualitative research was presented with the specific purpose of demonstrating how the author of this thesis ensured research rigor in the work in this thesis. Finally, a brief overview of the research process that was followed during the work in this thesis was presented. The work in this thesis is based on a *pragmatic and inductive approach towards design formulation through qualitative methods, which is supported by peer-review and publication as its primary verification methods.* The next chapter will provide a broad overview of the field of information security in general, in order to highlight the importance of the specific area on which the work in this thesis focuses.

Chapter 3

INFORMATION SECURITY

This chapter discusses information security in general. It defines information security and discusses the different elements and services required for effective information security. It will then examine the process of information security with specific emphasis on the role humans play in this process. The purpose of this chapter is to provide additional background information in order to establish the overall context of the primary literature study in the following chapter. The chapter also aims to further clarify the need to address the human factors in information security.

3.1 Introduction

Humans today live in an emerging global information society. This society has 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 work groups creating, using, and distributing information (O'Brien, 1999, p. 11).

Today information can be seen as a basic *commodity*, similar to electricity, without which many businesses simply **cannot** operate (Carr, 2003). In the interconnected world we live in, information is a lot more vulnerable than many other basic commodities. It is highly unlikely that the actions of a discontent teenager on another continent can affect a company's electricity supply. The same cannot necessarily be said about the *supply* of information resources. It is *vital* for organizations to ensure their continued access to this commodity by protecting their information assets. Many of these information assets reside in information systems.

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 collect, transform, and disseminate information in an organization (O'Brien, 1999, p. 9),(Whitman & Mattord, 2009, p. 14). The advent of information technology 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.

3.2 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 more than one way, as highlighted below.

3.2.1 Information Security

The international standard ISO/IEC 27002 (2005) defines information security as the preservation of the **confidentiality**, **integrity** and **availability** of information (ISO/IEC 27002, 2005, p. 1). Information, in the context of the ISO/IEC 27002 (2005) 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 27002, 2005, p. 1).

Whitman and Mattord (2009) define information security as "the protection of information and its critical elements, including the systems and hardware that use, store, and transmit that information" (Whitman & Mattord, 2009, p. 8). Whitman and Mattord (2009) also identify several critical characteristics of information that give it value in organizations. The identified characteristics include the **confidentiality**, **integrity** and **availability** of information, as mentioned in the definition provided in ISO/IEC 27002 (2005), but are not restricted to only these three characteristics. According to Whitman and Mattord (2009, p. 8) ensuring the **confidentiality**, **integrity** and **availability** of information, which is also known as the CIA triangle in information security, has traditionally been the *industry standard.* "The security of these three characteristics of information is as important today as it has always been, but the CIA triangle model no longer adequately addresses the constantly changing environment of the computer industry" (Whitman & Mattord, 2009, p. 8). Whitman adds the characteristics of **accuracy**, **authenticity**, **utility**, and **possession** to the list of characteristics of information that needs to be protected.

A few concepts in the above 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 information security is commonly defined in terms of the properties, or characteristics that secure **information** should have. These usually include the confidentiality, integrity and availability of information, but sometimes also include additional characteristics.

It is also important to note that there is a difference between information security and information technology security.

3.2.2 Information and Communication Technology Security

Information and communication technology security deals with the protection of the actual information technology based systems on which information is commonly stored and/or transmitted. The international standard ISO/IEC TR 13335-1 (2004) defines information and communication technology security, or ICT 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. 3). Since information security also includes the protection of the underlying information resources, it can be argued that *information technology security is a sub-component of information security.* The definition of information technology security is thus very similar to the one for information security. However, additional characteristics, which in this context could also be better described as services that should be provided by secure **information resources**, are added to the definition. These include **non-repudiation**, **accountability**, **authenticity**, and **reliability**. Dhillon (2007, p. 19) also refers to the concept of *data security* to refer to the protection of the actual data in an information system. Since the given definition in Dhillon (2007, p. 19) includes most of the characteristics from the definition for information technology security, and because the security of underlying data is to a large extent reliant on the overall security of the information system on which the data resides, it can be argued that the term *data security* was in fact used in Dhillon (2007) to refer to the same concept which ISO/IEC TR 13335-1 (2004) calls information and communication technology security.

From the definitions discussed in sections 3.2.1 and 3.2.2 it should be clear that there is a difference between *secure information resources* and *secure information technology resources.* A secure information resource could include **any** entity from which information was received or to which information was sent. A secure information technology resource is a secure information resource that happens to reside on an information technology system. It is also important to note that, in terms of information technology based systems, the information alone **cannot** be deemed secure unless all resources, and processes, dealing with that information, are secure as well. Although the work in this thesis is conducted within the School of Information and Communication Technology at the Nelson Mandela Metropolitan University, the term *information security*, as used in this thesis, does not refer only to the security of information *technology* resources. Instead, the term information security, as used in this thesis, is meant to deal with the *all encompassing field of information security which covers both information technology based, as well as non-technological, information resources.*

All the definitions discussed thus far in this chapter define secure information in terms of its underlying characteristics. As mentioned earlier, 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, 2009, p. 8). The additional characteristics were added to the definition to address the additional security needs of organizations in today's inter-networked business environment. A clear understanding of the meaning of all the above mentioned characteristics (and/or services) is essential to an understanding of information-, and information technology security, and consequently the following sub-sections will briefly discuss each of these characteristics individually.

3.2.3 Confidentiality

Confidentiality is defined by both ISO/IEC TR 13335-1 (2004) and ISO/IEC 27002 (2005) as *the property that information is not made available or disclosed to unauthorized individuals, entities, or processes* (ISO/IEC 27002, 2005, p. 1)(ISO/IEC TR 13335-1, 2004, p. 2). 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, 2009, pp. 10-11). Confidentiality deals with *privacy*, or the "for your eyes only" property of information. Confidentiality should apply equally to information residing in a system, or during the transmission of data between systems (Dhillon, 2007, p. 19). If a person, entity, or process, gains access to information that he/she/it is 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, 2009, p. 13).

3.2.4 Integrity

Both ISO/IEC TR 13335-1 (2004) and ISO/IEC 27002 (2005) define integrity as *the property of safeguarding the accuracy and completeness of assets* (ISO/IEC 27002, 2005, p. 1)(ISO/IEC TR 13335-1, 2004, p. 3). Another definition would be that the integrity of information is *the quality or state of being whole, complete, and uncorrupted* (Whitman & Mattord, 2003, p. 12). According to Dhillon (2007, p. 20) "integrity refers to an unimpaired condition, a state of completeness and wholeness, and adherence to a code of values". 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). All data is present and accounted for, irrespective of whether or not the original data was accurate or correct (Dhillon, 2007, p. 20). The integrity of information is threatened when the information is exposed to corruption, damage, destruction, or other disruption of its authentic/original 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, 2009, p. 12).

3.2.5 Availability

Availability, the third part of the CIA triangle, is defined in ISO/IEC TR 13335-1 (2004) and ISO/IEC 27002 (2005) as *the property of being accessible and usable upon demand by an authorized entity* (ISO/IEC 17799, 2000, p. 3, Section 2.1),(ISO/IEC TR 13335-1, 2004, p. 2). 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, 2009, pp. 9-10). However, availability, as defined above by the two international standards, does not imply that the information should be accessible to any user

(Whitman & Mattord, 2009, pp. 9-10). 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, 2009, pp. 9-10). 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. To a certain extent it can be argued that availability of information in an information system is dependent on the *reliability* of the information system itself (Dhillon, 2007, p. 21).

3.2.6 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 (ISO/IEC TR 13335-1, 2004, p. 3). 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. Usually, non-repudiation is achieved through cryptographic means (Dhillon, 2007, p. 22). The South African standard SABS ARP 057 (2002) defines the following sub-categories of non-repudiation services (SABS ARP 057, 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 play an integral role in establishing trust between parties who have never met in person. Furthermore, non-repudiation services are dependent on the confidentiality (privacy), where applicable, of the underlying non-repudiation tokens. Thus, in a digital signature scheme, the use of a private key relies on the owner of that key maintaining the privacy of the key (Dhillon, 2007, pp. 22-23).

3.2.7 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 (2004) defines accountability as a property that ensures that the actions of an entity may be traced uniquely to the entity (SABS ARP 057, 2002, p. 1). 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 his/her actions. Accountability in this sense should not be confused with accountability **for** information security. Accountability **for** information security deals with the role(s) individuals play in the information security process and will be discussed in more detail in a later section.

3.2.8 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 (2004) 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 (ISO/IEC TR 13335-1, 2004, p. 2). 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. During an ongoing information exchange between two parties authentication would take place at two levels. Firstly, to determine that both entities are who they claim to be, and secondly to ensure that no third party starts to masquerade as one of the parties **during** the exchange (Dhillon, 2007, p. 21).

3.2.9 Reliability

Reliability is defined in the ISO/IEC TR 13335-1 (2004) standard as the property of consistent intended behavior and results (ISO/IEC TR 13335-1, 2004, p. 4). This property basically means that an information resource should be *consistent* (predictable), 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.

3.2.10 Accuracy, Utility, and Possession

The remaining three characteristics of secure information were identified by Whitman and Mattord (2009). It might be argued that these characteristics will automatically be ensured if all characteristics identified by the standards, ISO/IEC 27002 (2005) and ISO/IEC TR 13335-1 (2004), have been ensured. However, since the purpose of this chapter is to provide a comprehensive overview of the concept of information security, and insight into these characteristics might improve the overall understanding of information security, these characteristics will be briefly examined. Firstly, Whitman and Mattord (2009, p. 10) defines accuracy as how correct (free of mistakes) the information is. If information is modified, whether intentionally or unintentionally, it might no longer be accurate. Inaccurate information is of less use to the user than accurate information. Secondly, the utility of information is a characteristic that deals with it having some value or purpose (Whitman & Mattord, 2009, p. 12). Information does not only have to be available, it often also has to be in a specific format in order to be useful. The final characteristic of secure information identified by Whitman and Mattord (2009) is possession. The possession of information deals with the state of ownership, or control, one has over the information (Whitman & Mattord, 2009, p. 21). As mentioned earlier, the confidentiality of information is not necessarily breached when possession is compromised.

Without the **confidentiality, integrity, availability, non-repudiation, accountability, authenticity,** and **reliability** of information resources, information cannot be deemed secure. All of the above (also including the accuracy, utility, and possession of information) 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.

3.3 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. A *control* can be defined as "the use of *interventions* by a controller to promote a preferred behavior of a system being controlled" (Dhillon, 2007, p. 5). In other words, through the use of controls an organization can *intervene* and thereby *reduce the risk* posed by a certain threat to one or more of its information assets. Various *risk management* approaches exist to guide the selection of a specific set of controls to protect the information assets of an organization. An in-depth examination of these processes falls outside the scope of this thesis. However, when selecting the security controls to implement in an organization, it is important to refer to accepted international standards (Von Solms, 1999). The set of information security controls used by an organization will be contained in an *information security policy.* Such a policy can be supported by a hierarchical system of sub-policies and procedures outlining various lower-level controls. 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 exist 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 27002 (2005) and the 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 (M. Thomson, 1998, p. 29) (Van Niekerk & Von Solms, 2004). An understanding of the interrelationships between these three categories of controls is needed in order to understand the role(s) humans play in the information security process. Each of these categories will thus be briefly examined.

3.3.1 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, 2009, p. 4).

3.3.2 Technical Controls

With the introduction of computer networks, databases, shared memory, etc, physical controls alone were no longer deemed sufficient protection (Whitman & Mattord, 2009, p. 6). 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, 2009, 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 B. 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 (B. Von Solms, 2000). At this stage, aspects like information security policies, information security awareness of users etc., were not deemed important (B. 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 (B. Von Solms, 2000). This management involvement eventually came, with the advent of distributed computing, in the form of information security policies (B. 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, namely, operational controls.

3.3.3 Operational Controls

Operational controls (also referred to as; business-, administrative-, managerial-, and/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 (B. Von Solms, 2000).

This wave is characterized by management involvement in information security, and generally improved information security (B. Von Solms, 2000). The above-mentioned three categories of controls, together with the information security policy, form 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 the three broad categories of controls, as well as the dependence on human involvement during this process, is of vital importance for the purposes of this thesis and will thus be examined in more detail.

3.4 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 (Mitnick & Simon, 2002, p. 3). Operational controls rely on human behavior. Both physical and technical controls, in turn, rely to some extent on operational controls for effectiveness. It should thus be clear that humans play a **very** important role in the information security process.

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). Without adequately addressing the human factor in information security, organizations **cannot** be sure that their information resources are safe.

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 primary dimensions to the *human factor* in information security, namely **knowledge** and **behavior**.

The first dimension to the human factor in information security 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. This requirement for adequate knowledge is very important for the purposes of this thesis and will be examined in depth in the next section.

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

3.4.1 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). 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 first step in the creation of such programs would be to determine exactly **what** users should be taught.

ISO/IEC 27002 (2005) 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 27002, 2005, 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 27002 (2005).

According to ISO/IEC TR 13335-1 (2004, p. 25) each employee should know his or her **role** and **responsibility**, his or her **contribution to ICT security**, and should be entrusted to achieving the organization's ICT security goals. 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. NIST 800-16 (1998) presents such a role-based approach towards information security awareness, training and education.

According to M. 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 implementation 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 a variety of factors. These factors would probably include the user's category and the specific departmental role which that user plays within the organization, but would not necessarily be limited to only these two factors. It should be clear that the determination of the exact content for an information security user education program should not be done in an unplanned, or haphazard, fashion. A lack of relevant information security knowledge amongst organizational end-users could compromise the security of information assets. It is **vital** that organizations ensure that the humans in the information security process have the requisite information security knowledge. The design of information security educational content should thus be done in a systematic and/or formal way in order to ensure that the content addresses the specific educational needs of the intended target audience. The extent towards which current approaches to the human factor in information security utilize such a formal, pedagogically sound, approach in user education programs will be examined in depth in chapter 4.

Once the appropriate content for an organization's information security user education program has been determined, this content needs to be *delivered*. Simply providing information security training to individuals does not necessarily ensure that learning has occurred (NIST 800-16, 1998, p. 6). 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* in both the creation and delivery of these programs. 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. The educational approach should also be practical, affordable and should meet all other possible requirements for organizational end-user education.

Few, if any, modern organizations can afford to send each and every staff member on extensive classroom based information security educational courses. 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 alterative to traditional classroom training is to provide employees with e-learning alternatives. Chapter 4 will examine the extent towards which e-learning is being used and/or recommended in current approaches dealing with the human factor in information security. The specific suitability of e-learning as an educational delivery channel for information security education will be dealt with in depth in a later chapter.

Through properly designed and delivered educational programs organizations can address the need for organizational end-users to have the requisite information security knowledge relevant to their jobs. However, as mentioned earlier, there are two dimensions to the human factor in information security. Once the 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 thus imperative to also ensure that the users have the correct attitude, beliefs and values, and thus desired *behavior*, towards information security.

3.4.2 Behavior

As mentioned earlier, ensuring that employees have the requisite knowledge does not guarantee that the employees will use the knowledge to act more securely. In fact, studies have shown that users might disregard a specific control because they disagree with the control, or disagree about the necessity of adhering to the control (Schlienger & Teufel, 2003). "Even the simplest security procedure demanded by security guidelines, such as the correct use of a password, is often ignored" (Siponen, 2000). Information security policies can also be misinterpreted by employees as attempts to interfere with their way of getting the job done (Kabay, 2002, p. 35.2). It thus becomes necessary to not only educate employees about their information security roles and responsibilities, but to also address the underlying factors which could influence their behavior. Layton (2005, pp. 46-54) identifies six psychological factors that can contribute towards an individual's behavior. These factors include motivation, attitude, beliefs, personality, morals, and ethics.

In order to ensure the desired user behavior, it is thus necessary to also consider behavioral theories. Most current user education programs fail to pay **adequate** attention to behavioral theories (Siponen, 2001). Section 4.5 of this thesis clearly shows that the importance of behavioral theories in dealing with the human factors in information security is widely recognized. However, most current approaches that do deal with the behavioral aspects, only do so at an abstract level (Siponen, 2000). One approach towards addressing the behavioral aspects of the human factor in information security is to foster an organizational sub-culture of information security.

According to B. Von Solms (2000), the emphasis of user education programs should be to build an organizational 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.* Recent studies have indicated that the establishment of an information security "culture" in the organization is desirable for effective information security (B. 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 theory from the behavioral sciences. This approach has become widely accepted in current approaches towards the human factor in information security. Section 4.5 will show that the majority of current approaches recognize the need for the establishment of an organizational information security sub-culture. However, section 4.5 will also show that very few of these current approaches have made any efforts at adapting the *generic* model used to define organizational culture to be specific to the needs of information security.

The two dimensions to the human factor in information security, knowledge and behavior, are tightly interwoven. Without adequate knowledge it is not possible to behave correctly. Even if a user has the desired attitude and is properly motivated, a lack of the requisite knowledge would prevent that user from behaving securely. Similarly, having the requisite knowledge still does not guarantee the desired behavior. A user who has the requisite knowledge but who views security as a hindrance to performing his/her job, or as not being very important, might still behave insecurely. Any attempt to address the human factors in information security should thus address both these dimensions holistically.

It is also imperative to realize that approaches intent on addressing the knowledge dimension of the human factors in information security, would have to consider pedagogical theory. Similarly, approaches towards fostering an information security culture would have to consider organizational culture theory from the management sciences. When dealing with the *human* factor in information security, information security researchers need to take cognisance of relevant theories from the human and social sciences. This thesis will address various components of such an holistic approach towards the human factor in information security through the integration of both the relevant theory and, where appropriate, technology.

3.5 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 operational controls. The first two of these categories of controls depend 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, knowledge and behavior, constitute 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. Both the education of users, and the establishment of an information security sub-culture in the organization, need to be done in a way that is theoretically sound. The next chapter will provide an overview, and perform a detailed analysis, of current approaches towards dealing with the human factor in information security. This detailed analysis will clearly show the specific areas where current approaches are still lacking. It is the intention of this thesis to address some of these areas in a theoretically sound way.

Chapter 4

LITERATURE REVIEW

This chapter reviews existing information security awareness, training and educational approaches. The aim of the chapter is to provide both an overview of existing programs, and to perform a qualitative content analysis on existing approaches. The purpose of the qualitative content analysis is to demonstrate the relevance of, and need for, the specific research objectives of this thesis.

4.1 Introduction

This chapter provides an overview of existing approaches to dealing with the human factor in information security. These approaches include all current work dealing with either *information security awareness, training and education*, or with the *fostering of an organizational culture of information security*. The primary purpose of the review is twofold. Firstly, the review aims to provide a comprehensive overview of the current state of approaches dealing with the human factor in information security. Secondly, a *qualitative* content analysis will be conducted in order to establish the relevance of the specific research objectives of this thesis, as discussed in section 1.7.

The aims of the qualitative content analysis is thus to determine the extent towards which:

- reviewed literature recognizes the importance of dealing with the **behavioral aspects** of information security education (including dealing with user attitude and/or motivation), as opposed to exclusively focussing on the transfer of skills and/or knowledge. This could also be interpreted as a focus on the so-called "content category" of awareness education programs (Siponen, 2001).

- current literature acknowledges the need for an information security **culture**.
- current approaches have **adapted** the more generic **definition(s) of organizational culture** used in the human and social sciences to be specific for the needs of information security.
- formal, pedagogically sound, methods were followed in the creation of actual information security learning content.
- learning taxonomies were used to plan the learning activities in information security awareness, training, and education approaches.
- technology based channels (e-learning) are used in order to deliver learning content.

The following sections will briefly discuss what a qualitative content analysis is and will clearly delineate the scope of the conducted literature review and content analysis. A comprehensive overview of existing approaches to dealing with the human factor in information security will then be presented. Finally the chapter will present and discuss the results of the qualitative content analysis performed on the reviewed sources.

4.2 Methodology

Content analysis "is a research technique for making replicable and valid inferences from texts (or other meaningful matter) to the contexts of their use" (Krippendorff, 2004, p. 18). Content analysis is essentially an empirically grounded method. However, the main focus of content analysis is to examine data, texts, images, etc, in order to interpret or understand what they *mean* to people. Content analysis tries to determine what the information conveyed by the content *does*, and what it *enables* or *prevents* people from doing. "Contemporary content analysis *transcends notions of symbols, contents, and intents*" (Krippendorff, 2004, pp. xvii-xviii). A researcher making use of content analysis usually starts with data sources that was meant to be *read, interpreted and understood by people other than the analysts.* This methodology differs from techniques such as hermeneutics in that the analyst usually starts the reading with a specific research question in mind. Content analysts who start the research with a specific question in mind *read the text for a purpose*, not for what the author might lead them to in an abstract (Krippendorff, 2004, p. 33)

This method is often employed because direct observable evidence and/or validation might be difficult or unfeasible in practice. In such a case the texts, and other data sources, provide the empirical grounding for the researcher's work (Krippendorff, 2004, pp. 39-40). However, it is important to note that content analysis is not necessarily empirical in nature, it could be seen as *either* quantitative or qualitative, depending on how the techniques are used. Qualitative researchers will often support their interpretations by weaving quotes from the analyzed texts and literature into their arguments and conclusions, by constructing parallelisms, by engaging in triangulations, and by elaborating on any metaphors they can find (Krippendorff, 2004, pp. 87-88).

4.3 Scope of the review and content analysis

One of the aims of this review of current approaches to dealing with the human factor in information security is to provide as comprehensive an overview of these current approaches as possible. It was deemed essential to *attempt* to include every *current* source that could be deemed relevant in this review. Source material for the review was collected using a careful and systematic process. This process included the exploration of as many information systems and information security journals as possible. The search process included extensive searching through the contents of online electronic databases, including: ACM digital library, EBSCOhost, Elsevier Science Direct, Emerald Library, IEEE/IEE Electronic Library, and Springer Link. Secondly, international information security standards were evaluated, and where relevant content which focused on information security awareness, training and education was found the standards were included in this review. Standards that simply stated the importance and/or scope of such information security awareness, training and education programs (for example (ISO/IEC 27002, 2005)) were **not** included in the review, but were considered throughout the rest of the thesis.

Specific attention was also given to the journal "Computers & Security" and the "Proceedings of the IFIP TC 11 International Information Security Conference". These two publication forums were emphasized since, in the author's opinion, they represent the foremost research in the field of information security. Additional searches were conducted using online search engines. Finally, as many academic textbooks dealing with information security related topics as possible were obtained and, where relevant content was found, were included in this review.

In order to ensure the currency of the results, **all sources older than ten years (published pre 1999) were excluded from the review and content analysis**. These sources were, however, considered throughout the rest of thesis.

4.4 An overview of existing approaches to dealing with the human factor in information security

Albrechtsen and Hovden (2009) examine the divergence between how information security managers view and interpret information security related issues, and how organizational users view and interpret these issues. The study identifies and explores the "digital divide" between information security users and information security managers and describes this digital divide as being either social, socio-technical, or both. A social digital divide is defined as "differences in self-efficacy, individual skills and perceptions, cultural aspects, and interpersonal relationships". A socio-technical digital divide is defined as "differences with regard to information security skills and knowledge, perceptions of information security, social norms, and interpersonal relationships, any or all of which can result in differences in information security performance between individuals" (Albrechtsen & Hovden, 2009). The study explores various aspects relating to the management of human aspects in information security. According to Albrechtsen and Hovden (2009) information security managers surveyed prefer to deal with technological solutions to prevent users from taking insecure actions, whether intentional or unintentional. Technology is seen as more sound and reliable than users. Most managers agree that users should be kept informed regarding security policies and guidelines. However, the surveyed managers believe that few users actually read the documents and that such policy documents contributed little towards overall information security awareness. Several popular forms of awareness campaigns, including use of the intranet, e-mail, leaflets, screen savers and interactive training were found to be mostly ignored by users due to lack of motivation, or a lack of awareness of the need for information security awareness. Both managers and users believe that user participation in security work (ranging from dialogue during policy creation to active involvement in risk analysis, etc) is the most effective way to improve user adherence to information security principles (Albrechtsen & Hovden, 2009).

Alnatheer and Nelson (2009) focus on information security culture in the Saudi environment. The paper briefly discusses information security in general and then provides some insight into the Saudi environment. Specific attention is given to the Saudi government's national IT plan which aims to transform the country into an information society and digital economy. The adoption of an information security culture within this national context is the main focus of the paper. Several issues and factors that should be considered for the adoption of such an information security culture are briefly examined. These issues includes *corporate citizenship*, the *legal and regulatory environment*, *corporate governance*, and *cultural factors* (including an overview both national and organizational cultures). A conceptual framework for using these factors in the cultivation of an information security culture is briefly outlined. The future aims of the authors are to use the presented framework in the examination of information security culture in Saudi. In its current form the research lacks depth.

Ashenden (2008) examines the extent of the "human challenge" in information security. The study specifically focuses on the **management** of the human aspects of information security. The paper argues that this challenge goes beyond the management of just the organizational role(s) of the humans involved and should also include the individual's attitudes, beliefs and perceptions. This holistic view of humans in the organization is described as organizational culture. A brief definition of organizational culture, and the role it plays is then examined. The paper discusses the management of information security in general and then provides more detail on specific challenges when dealing with the human aspects of security. These include the changing of organizational culture (which is briefly discussed), the development of the information security manager's identity, effective communication, and skills development (Ashenden, 2008). The discussion of skills development focuses on the skills needed for the effective management of humans in information security, as opposed to the skills needed *by* humans in information security. The ability to manage culture change is emphasized as essential in the management of the human aspect in information security (Ashenden, 2008). The definition of organizational culture used by Ashenden (2008) does not adapt the generic definition of organizational culture to the specific needs of information security.

Atkinson, Furnell, and Phippen (2009) focus on the raising of young people's awareness regarding security whilst online. The paper firstly outlines the risks associated with the quick adoption of new technologies by young people. The authors then point out that the parents or other older role-models like school teachers, who in other situations would have been expected to provide guidance to the younger generation, often themselves lack awareness or do not have the technological know-how to help ensure e-safety awareness. Purely technological solutions, which mainly restrict the range of online activities young people can engage in, are briefly examined and found to be inefficient. Peer education, where learners "build upon the knowledge and sophistication that they already have, thus making the encouraging of safe online behaviors much more likely", is cited as a possible solution and discussed as the primary focus of the paper (Atkinson et al., 2009). The paper outlines the results of a research project which evaluated such peer education initiatives within UK secondary schools. The paper discusses perceptions that exist regarding online safety amongst young people. This is followed by an examination of the dominant threats as perceived by the young people in the study. An important concept in the research was the introduction of E-safety ambassadors, who were recruited from amongst the young people to provide peer support. The E-safety ambassadors were given the freedom to develop their own materials, or to tailor existing material to their needs. A forum was provided online to assist these E-safety ambassadors by allowing them to communicate with each other and to disseminate information. The study found that this peer-driven approach did not improve the security related knowledge of the young people (who was already fairly technologically ”savvy”) much, but was still successful in changing their actual online behavior. It is also noted that this ”peer support approach” should not be used in isolation. ”Peer ambassadors may be effective agents for influencing behaviors, but they are not the only mechanism and should be viewed as forming part of a wider toolkit” (Atkinson et al., 2009).

Aytes and Connolly (2003) present a model of user behavior relating to information security. The paper firstly emphasizes the role(s) humans play in the implementation/support of technical information security measures. Aytes and Connolly (2003) secondly state that many existing approaches to dealing with humans in information security only focus on two primary factors, namely **awareness** of a specific security threat and having adequate **training** in the use of the security counter measure to such a threat. It is then argued that this ”somewhat simplistic approach to human behavior ignores the fact that in many situations, users may choose to not implement countermeasures” (Aytes & Connolly, 2003). It is thus deemed necessary to pay adequate attention to behavioral theories. The paper then presents a model of user behavior based on various literature sources. The model's primary focus is both the factors that contribute to the users perception of risk and the factors relating to the subsequent choices users make based on the perceived risk. In the presented model various information sources can contribute to the user's knowledge. These sources includes training received, news/media, friends and coworkers, policies and procedures and personal experience. The user subsequently has knowledge regarding threats and vulnerabilities, countermeasures, potential consequences to him/her self and/or others as well as the cost of secure behavior in terms of time, effort, etc. The user's knowledge leads to the user's perception of the availability and usability of safe practices, the probability and significance of negative consequences, the ease of recovery and the user's beliefs regarding peer behavior. Perception, in combination with the individual's attitude towards risk, leads to the user's behavioral choice (i.e. to use, or disregard, the appropriate security counter measure) (Aytes & Connolly, 2003). The outcome of the user's choice, whether positive or negative, in turn feeds back and influences future behavior as an information source. This model does to a certain extent adapt behavioral theories for use in information security. However, its primary focus is to assist in predicting user behavior and the study thus does not make use of pedagogical theories. It should also be noted that this paper focuses only on one aspect of behavior and not on the more holistic concept of an information security culture.

Bryce and Klang (2009) examine online practices of young people with regards to the disclosure of private information. The research examines a variety of types of personal information, as well as the risk perceptions and associated disclosure practices existing amongst young people in an online environment. It is suggested that educational strategies should more clearly focus on encouraging young people to protect their online privacy. These strategies should also focus on raising awareness with regards to both commercial and non-commercial use of their private information amongst young people. A call is made for more empirical research towards the development of such educational strategies.

Chang and Lin (2007) examine the relationship between organizational culture and information security management (ISM). The research presents a model of the influence that organizational culture traits (including cooperativeness, innovativeness, consistency, and effectiveness) have on information security management principles (including confidentiality, integrity, availability, and accountability) (Chang & Lin, 2007). These traits and principles are selected after conducting a review of current literature. The influence of each cultural trait on each information security management principle is then measured empirically via regression analysis. It is concluded that "there are significant relationships between organizational culture and ISM" (Chang & Lin, 2007). The evidence provided in Chang and Lin (2007) strongly supports the importance of fostering an information security culture to help address the human factors in information security.

Chen, Medlin, and Shaw (2008) study the effect that cultural perspectives might have on situational information security awareness. The study focuses specifically on situational awareness, which makes users aware of various elements and their contextual meanings in their own working environments. This form of awareness allows the users to "form a mental model to both understand the current risks of a situation and to predict and possibly prevent the potential adverse effects of these risks" (Chen et al., 2008). The effects of four cultural traits (as described by Hofstede (1991)) individualism, power distance, masculinity and uncertainty avoidance are studied. The research uses a computerized animated information security awareness program that was developed based on "Endsley (1995)'s Situational Awareness Dynamic Decision Making Model and Situation Awareness Global Assessment Techniques" (Chen et al., 2008) to present the awareness material. It is found that the individualism cultural trait has a particularly strong influence on the effectiveness of situational information security awareness.

Choi, Kim, Goo, and Whitmore (2008) provide empirical evidence that managerial information security awareness influences managerial action towards information security. The study builds on previous theoretical work done by other authors and specifically tries to provide empirical support for theories regarding this relationship as proposed by Straub and Welke (1998). The study validates that, not only does higher levels of information security awareness amongst management lead to improved managerial action towards information security, but also that improved managerial action towards information security leads to improved organizational information security performance (Choi et al., 2008). The study thus does not address how awareness should be increased, but rather provides additional reasons why awareness is important.

Cohen (1999) presents an argument that awareness is only effective if the intended target audience of the awareness already is favorably predisposed to the subject matter. This argument is backed by anecdotal evidence based on the author's own experiences. The paper indirectly highlights the importance of the motivational aspects of awareness campaigns.

Cone, Irvine, Thompson, and Nguyen (2007) present a video game that is successfully being used in information security training and awareness campaigns. The use of a video game for information security awareness and training is briefly justified. It is argued that the "tacit knowledge gained by applying concepts in a virtual environment can significantly enhance student understanding" (Cone et al., 2007). A brief overview of several current training and awareness techniques is provided, followed by an overview of the discussed video game itself. This overview presents the major components of the game as well as information on how it was developed and tested. The paper also explains how scenarios for the game are constructed. An in depth view of the process of analyzing awareness and training requirements and creating game scenarios based on the gathered requirements is presented. The presented process provides clear insight and justification for the specific content created, but does not make use of an explicitly espoused learning taxonomy. It can be argued that the video game itself **can** be a form of E-learning.

Da Veiga and Eloff (2009) present a framework for an information security culture. This framework is supported by validating statistical analysis which is also published as Da Veiga, Martins, and Eloff (2007). Current research into information security culture is briefly examined, and it is noted that existing information security research does not integrate organizational culture and organizational behavior into an holistic framework for the cultivation and assessment of such an information security culture. The presented framework attempts to address this shortcoming. The framework is presented in three levels of increasing detail. The first level provides an overview of how *information security components* (for example policies) influence *information security behavior*, and how behavior, in turn, eventually leads to the cultivation of an *information security culture* (Da Veiga & Eloff, 2009). The second level breaks these three major elements of the framework down into further levels of granularity. The *information security components* are split into groupings that influence one of three major *behavioral* groupings, namely; organizational, group or individual behavior. These *behavioral* groupings in turn cultivate *information security culture* by influencing basic assumptions, values, or artifacts and creations. The final level presented further decomposes the framework into seven categories of *information security components*. Each of these categories once again is classified as being at an organizational, group or individual tier in terms of its influence on the information security culture. These tiers indicate the main sphere of the control's influence. However, components can also influence other tiers to a lesser extent (Da Veiga & Eloff, 2009). The influence of specific information security components at each of the tiers themselves is also broken down into more detail to further clarify the framework. The presented framework not only uses established theory relating to organizational culture, but also adapts it for the specific needs of information security.

Dhillon (2007, pp. 219-237) discusses information security culture from various perspectives. Information security culture is firstly discussed according to Schein's model (Schein, 1999a) for organizational culture. Information security specific *interpretations* of the three levels of Schein's model are provided (Dhillon, 2007, p. 223). Dhillon (2007) secondly explores security culture as a web of communication processes, as proposed by Hall (1959). In this view of culture Hall (1959) identified ten streams of culture (interaction, association, subsistence, gender, territoriality, temporality, learning, play, defense, and exploitation) and argued that the interaction between these streams leads to a pattern of behavior (Dhillon, 2007, pp. 224-229). The third view of culture presented is a framework by Cameron and Quinn (1999). This framework organizes Hall's ten streams along two dimensions. The first dimension differentiates *flexibility, discretion and dynamism* from *stability, order and control.* The second dimension differentiates *internal orientation, integration and unity* from *external orientation, differentiation and rivalry* (Dhillon, 2007, pp. 229-233). According to this framework an organization's culture can fall into one of four primary classes. An organizational culture could be an adhocracy culture (individual initiative and freedom is stressed, fewer security controls might actually improve security), hierarchy culture (a formalized and structured organization, security privileges models the same hierarchy), clan culture (a strong focus on people, security is largely ensured via ethics and loyalty), or market culture (focuses on achieving long-term goals and targets, security is seen as a hindrance) (Dhillon, 2007, pp. 230-231). The perspective of an information security culture provided is based on the nine principles presented by OECD (2002). The four presented perspectives are seen as being complimentary in terms of providing insight into an organization's culture. Despite interpreting these perspectives from an information security viewpoint, Dhillon (2007) does not **adapt** any of the models to be specific to information security.

Dodge, Carver, and Ferguson (2007) use phishing e-mails to test the level of awareness amongst learners. The results of the study indicate that learners "*continue to disclose information that should not be disclosed to an unauthorized user and expose themselves to malicious code by opening attachments*" (Dodge et al., 2007). The methods used in this study could conceivably be used in other awareness campaigns to help assess the success of specific aspects of such campaigns. One could argue that the focus of this research is on the behavioral aspects of information security. However, for the purposes of the qualitative content analysis this focus will be disregarded because the authors intended to focus on user knowledge. There was no attempt to directly measure, or address, concepts like user attitude and/or motivation.

Drevin, Kruger, and Steyn (2007) introduce a value-focused thinking approach to information security awareness. Value focused thinking starts with the identification of stakeholders that will be impacted by a decision. The values and principles, in the context of the specific scenario, of these stakeholders are then determined. These values are converted into objectives, which can be either *fundamental* or *means objectives.* A *means objective* is one which helps to achieve another objective. The inter-relationships between objectives are then analyzed for cause-effect relationships, and to generate possible decision opportunities. This approach is used by Drevin et al. (2007) to help "identify key areas of concern to ICT security awareness". The study also briefly discusses the positive influence such an approach can have on an organization's information security culture. It can be argued that this approach incorporates formal theory into the creation of information security awareness material. However, for the purposes of the qualitative content analysis conducted in this thesis, this value based approach will not be viewed as a formal *pedagogical* approach.

Du, Shang, and Xu (2006) focus on computer security education as part of formal tertiary education. The *Minix* operating system is used as a basis for laboratory exercises to provide students with ”hands on” practice. Du et al. (2006) provide brief insight into the pedagogical approach used in the course. The paper firstly describes the features of the *Minix* OS that makes it favorable for use in computer security education, and then describes how these features were used to form the basis of laboratory exercises. Finally the results of a brief teaching experiment by the authors are presented. Since Du et al. (2006) focus on computer security in a formal tertiary education environment, as opposed to information security in an organizational environment, the applicability of their work to this thesis is debatable. However, it was decided to include the work in this review based on the rigorous approach to the instructional design described in this paper.

Finne (1996) describes the entire *chain* of ”elements” in organizational information security (ISEC). Part of this *chain* is the element of ”personnel security”. Information security education for personnel is briefly mentioned, and it is suggested that each employee should have a written information security manual. Finne (1996) also addresses the element of ”attitudes towards ISEC issues”. To address employee attitudes it is necessary to establish an information security culture (Finne, 1996). According to Finne (1996) it should be possible to measure employee attitudes towards, and adherence to, information security policy. These measurements could be used to include ”security accountability” in job descriptions and performance appraisals. Such accountability ”is the only sustainable motivator and then only if managers strongly support and carry out this provision” (Finne, 1996). The paper also briefly introduces the idea of rewarding employees for good security behavior in order to help maintain such an information security culture.

Furnell (2008) examines the ”insecure” online behavior of end-users. The paper argues for the utilization of more channels in order to reach the users with awareness messages. It also argues that relevant awareness needs should be more actively pushed to the relevant user communities in both domestic and workplace contexts (Furnell, 2008). The paper does not specifically focus on organizational information security culture, or on organizational information security awareness. Instead, the focus is on the wider societal need for information security awareness and the establishment of an information security culture in society as a whole.

Furnell, Gennatou, and Dowland (2001) and Furnell, Gennatou, and Dowland (2002) both describe a prototype implementation of a software tool that allows self-paced information security training. Furnell et al. (2002) appear to be a more comprehensive version of Furnell et al. (2001). This overview will thus focus on the second paper only. The research first outlines the need for appropriate information security training and awareness in order to help establish an information security culture. Various ways in which security awareness could be promoted in organizations are briefly examined and it is pointed out that many of the current approaches would be inappropriate for smaller organizations. Smaller organizations have less staff capacity and less financial resources available for information security training and awareness programs. It is argued that computer based training solutions for information security training and awareness would be of particular importance for smaller organizations. Such tools would allow for flexible and personalized information security training. Employees could determine their own training schedule according to individual training needs. A prototype computer based training tool for information security training and awareness is then presented. Neither paper provides empirical evidence regarding the effectiveness of the presented tool.

Furnell and Thomson (2009a) provide an in depth examination of corporate culture and how it influences information security compliance within an organization. The paper firstly discusses Schein's (see also (Schein, 1999a)) model of corporate culture and how the three levels of this model interact to govern employee behavior. It then categorizes employee behavior with regards to information security according to an eight step scale reflecting the extent to which the employees are committed to security. The scale ranges from active non-compliance, through ignorance, to active compliance (secure culture). According to this scale employee behavior is either compliant or non-compliant with security policy, and this compliance or non-compliance could be either conscious (active choice), or unconscious. The scale does not represent clear boundaries but should rather be viewed as a "useful frame of reference" (Furnell & Thomson, 2009a). The various levels of the presented scale are related directly back to interactions between the three levels Schein's corporate culture model. Furnell and Thomson (2009a) next examine how information security compliance can be influenced by management, through the fostering of an information security culture. Senior management should not only espouse the importance of information security, but should also consistently behave in a way that supports this message (Furnell & Thomson, 2009a). The paper also examines the importance of awareness programmes and suggests that the success of such programmes could be improved by providing such training and education in a context sensitive fashion. It is suggested that factors such as the **role** of the user, the **current task** in which the user is engaged, the user's "normal" **behavior** patterns, **psychology**, and **current events** within the organization should all be considered when deciding on the applicability of specific information security awareness messages.

Furnell and Thomson (2009b) deal with people's perception of security and how the need for security compliance should be promoted. The paper first introduces the idea of "security fatigue". It is argued that staff will become prone to disobeying security policy as the "novelty" of taught secure behavior wears off. The research then examines specific information security controls and the potential for "security fatigue" inherent in each of these specific controls. It is suggested that the potential for "security fatigue" could be estimated through examining the **effort** needed by users to achieve compliance, the degree of **difficulty** to provide this effort in practice, and how **important** the user deems the securing of the specific information asset to be (Furnell & Thomson, 2009b). The argument is made that a highly motivated employee, for example a person with a higher degree of loyalty to an organization, could potentially behave more secure than one who is more educated about information security. "Security fatigue" is identified as just one of many possible reasons for a lack of motivation to behave securely. Furnell and Thomson (2009b) do not directly mention the concept of an information security culture; however, the work clearly focuses on some of the same behavioral aspects such a culture should help address.

Gaunt (1998) describes the "installation" of an information security policy in a large hospital. The paper describes an initial risk analysis during which surveys revealed a lack of information security awareness. In order to counter this problem, an approach was followed that included "extensive user consultation and involvement in the preparation of the security policy and proposed countermeasures" (Gaunt, 1998). This involvement also helped to obtain user buy-in into the security process and assisted in the gauging of the training needs of users. Users were given guidance in the form of self-administered questionnaires and leaflets. The policy included a contractual obligation on staff to adhere to the information security policy. All staff must complete appropriate training before being given Internet access. Gaunt (1998) argues that proper emphasis on the human factors in information security during such a project is vital to the success of the project. Furthermore, it is argued that continual education and reinforcement of security best practices will eventually lead to the formation of an information security culture.

Gaunt (2000) examines various practical ways in which an information security culture could be fostered in a health care environment. The paper starts by elaborating briefly on the various stakeholders in the health care system's need for information security. It then examines various factors that could prevent a change towards a more secure culture. These include staff **attitudes**, **ignorance** of security measures (lack of awareness), **conflicts** between the demand for direct access to patient data to improve health care versus the need to protect data, **inadequate** (poorly designed) security systems and controls, and **inconsistent policies**. Gaunt (2000) proceeds by examining some problems in establishing a security culture which could help address security problems caused by the aforementioned factors. Finally a list of recommendations is given to address these problems. The recommendations were made by a committee after examining various information flows in the health care environment. Gaunt (2000) concludes by stating that the ideal of attaining a "genuine security culture" is still a long way off.

Goucher (2008) briefly outlines common mistakes that are made with information security awareness training and presents a strong argument in favor of non-traditional training methods for information security education. Common mistakes listed include having long, expensive training sessions, confusing a lack of enthusiasm for the security awareness training with resistance to security awareness, irrelevant (or out of context) security training, inappropriate (too much technical jargon) training delivery, and including too many people in a single training session (Goucher, 2008). The paper does not elaborate in depth on any topic but the use of e-learning for security training is briefly advocated. The paper does not deal directly with the behavioral aspects of information security, but it does deal with behavioral aspects **during** information security education.

Grimson et al. (2000) present a campaign to raise awareness about information and communication technology in general amongst health care professionals. The campaign makes extensive use of multimedia and web technology in the presentation of the information. Information security awareness is incorporated as part of the overall campaign. Since security is not a major focus of the presented research this paper is of limited importance for the purposes of this overview. However, it is of importance to note that information security is not dealt with as an afterthought, but rather incorporated in the general user education programmes from the start.

Guenther (2001) presents an actual social engineering awareness campaign in the form of a slide presentation. The presentation contains clearly defined instructional outcomes, as well as an example case study. Due to the publication format, and probable lack of formal review, this work is considered to be of limited importance to this study, although the use of technology in the presentation of the material is noted. It is also important to note that the overall structure of the work does imply some adherence to formal pedagogics. However, in view of the lack of more explicit evidence, this probable adherence to formal pedagogics will be disregarded for the purposes of the content analysis conducted in this chapter.

Hagen and Albrechtsen (2009) present empirical evidence regarding the effectiveness of an e-learning based information security campaign. The study documents and compares pre- and post-training assessments of employee knowledge about information security, as well as employee attitudes towards information security. The paper first justifies the need for awareness and then introduces the e-learning awareness program itself. A theoretical model is provided, showing how the specific content to be presented to an employee was chosen, for the purpose of influencing employee behavior, based on the employee's current attitudes and knowledge. This is followed by the design and results of the empirical experiment itself. The research conclusively shows that the e-learning awareness program "had a significant short-term effect on employee security knowledge, awareness and behavior" (Hagen & Albrechtsen, 2009). Finally it is argued that individual information security awareness training, such as the presented e-learning program, is a "good starting point for building a corporate security culture based on common values and attitudes" (Hagen & Albrechtsen, 2009).

Hentea (2005) discusses issues in the security education model that need attention. The paper first discusses the need for an information security culture "in all aspects of information systems, from designing and planning through to everyday use, and among all participants, from government down through business to consumers" (Hentea, 2005). The paper then examines several issues with current information security awareness education in tertiary educational institutions. These issues include, firstly, the fact that information security education is not integrated with other aspects of information technology education. Learners should not be taught how to use computers without being taught how to do so securely and ethically. According to Hentea (2005) it is "becoming obvious that information security awareness has to be provided to students at an earlier age". The second issue examined is the fact that information security education is still not seen as a part of basic computer literacy skills, but is usually offered as an optional extra course. Thirdly, both end-users and IT professionals have a need for continuing information security education in order to remain secure in the fast changing IT arena. Fourthly, there is currently no standard integration between information security and other computer related subjects. A final identified issue is the fact that industry expects newly qualified security experts to be progressively more able in terms of both knowledge and skills (Hentea, 2005). Hentea (2005) proceeds by providing some guidelines that could assist in the addressing of the mentioned issues. The need for **both** information technology graduates and non-IT professionals to have information security knowledge is once again highlighted. It is argued that introductory information security should become a mandatory subject in all curricula. Several other recommendations regarding the teaching of information security in formal tertiary education is briefly argued. These arguments focus on the need to integrate security into other curricula and to ensure the teaching of "ethics and social responsibility in the information age" to all students.

Herold (2005) presents a very comprehensive framework for information security awareness and training. The book starts by establishing the importance of information security training and awareness and also provides a comprehensive overview of legal and regulatory requirements for such training and awareness. This overview covers both US and European regulatory requirements and lists, and briefly discusses, seventeen different laws and regulations that might be applicable. This is followed by a discussion on the incorporation of information security training and awareness into job responsibilities and appraisals (Herold, 2005, pp. 35-53). Herold (2005) also recommends rewarding employees for meeting the information security training and awareness goals specified for them. Common mistakes made in corporate education programs are discussed (Herold, 2005, pp. 55-60). Herold (2005) presents a detailed step-by-step approach to the development of an information security training and awareness program. These steps include (Herold, 2005, pp. 61-303):

- reviewing current awareness activities,
- establishing a baseline,
- getting executive support,
- identifying information security training and awareness methods,
- identifying information security training and awareness topics and audiences,

- defining specific messages,
- budgeting and obtaining funding,
- designing and developing training activities,
- designing and developing awareness material,
- communicating,
- delivering in-person training,
- launching awareness activities,
- and evaluating education effectiveness

Herold (2005) concludes with an overview of current leading practices. The primary weakness of the approach presented by Herold (2005) is lack of supporting references. It is very difficult, if not impossible, to judge the validity of the framework without insight into the underlying theories used and/or prior research on which the framework was based. The work does appear to adhere to a formal pedagogical approach towards the design and creation of content, however the specific theoretical basis of the approach is not explicitly mentioned. No mention is made of the fostering of a security culture. A brief but extensive overview of e-learning options as delivery mechanism for learning content is provided.

Hu and Meinel (2004) present an e-learning tool to teach IT security as part of formal tertiary education. The target audience of this e-learning tool is IT students and the primary focus of the subject matter is on the technical side of security. However, some of the material, for example how to digitally sign email, would also be of use in end-user information security education. The tool is provided to students on a CD which implements both a tutoring system and provides a virtual environment for hands-on laboratory exercises. All tools needed by students to complete the exercises are also provided on the CD. Though not explicitly mentioned, it is clear that some degree of formal pedagogics form the basis of the content developed on this tool.

Johnson (2006) provides a comprehensive overview of factors that should be considered in an information security awareness program. These include the direct and indirect costs of such a program, the benefits of a security awareness program, and the role(s) of other organizational functions and/or departments in the support of an awareness program. These identified other functions and/or departments, whose role(s) in support of an awareness campaign is discussed, includes executive management, the help desk, safety department, public relations, facilities, privacy, audit, and legal. Johnson (2006) also briefly discusses which topics should, as a minimum, be discussed and how to determine the appropriate target audiences for such topics. The paper briefly looks at various methods of delivering the awareness training, these include both traditional methods (i.e. posters) and technology based methods (i.e. online learning modules). How to measure the effectiveness of campaigns is briefly discussed. The paper concludes with a brief examination of IT governance principles.

Kabay (2002) discusses the use of social psychology to improve information security by changing the beliefs, attitudes, and behavior, of both individuals and groups. It is argued that rational arguments are not enough to convince people of the need to change behavior and that ”people can get very angry about what they perceive as interference with their way of getting the job done” (Kabay, 2002, p. 35.2). Kabay (2002) provides social psychological explanations to explain certain types of insecure behavior amongst users. These include *schemas* (to explain why people would share sensitive information with co-workers), *theories of personality* (interpersonal conflict might lead to resistance to conforming to a security culture), *explanations of behavior* (to help interpret employee behavior during culture change), *errors of attribution* (misinterpretation of other's behavior might prevent acceptance of a new culture), *intercultural differences* (people from different cultural backgrounds might behave differently in the same scenario), and *framing reality* (information security has to become part of people's framework of reality) (Kabay, 2002, pp. 35.3-35.8). Kabay (2002) also presents some practical recommendations for information security awareness program instructors and facilitators. In order to change employees' schemata when presenting security information, Kabay (2002) discusses the importance of initial exposure, counterexamples, and choice of wording (Kabay, 2002, pp. 35.9-35.10). A distinction is made between employee beliefs (”cognitive information that need not have an emotional component”) and attitudes (”an evaluation or emotional response”) (Kabay, 2002, p. 35.10). Kabay (2002) argues that the current structure of *beliefs* amongst employees and managers must be explored if security practitioners wish to foster an information security culture (Kabay, 2002, p. 35.10). It is also suggested that employees should be praised for exhibiting ”secure attitudes” and should be challenged (in private) about attitudes that dismiss the importance of security (Kabay, 2002, p. 35.10). Some evidence is presented in favor of rewarding employees for secure behavior, as opposed to only focusing on punishment of insecure behavior. Kabay (2002) also discusses how to change attitudes using persuasion, the use of various communication channels, the encouragement of initiative, and the impact of conformity, compliance and obedience on changing the views of individuals (Kabay, 2002, pp. 35.11-14). The role of group behavior is briefly dealt with. Kabay (2002) concludes with a very detailed summary providing specific, practical ideas on how these social psychology theories could be incorporated into information security awareness approaches. These ideas will be further explored in a later chapter. In terms of addressing the behavioral aspects of humans in information security the work published in Kabay (2002) is deemed very significant for the purposes of this thesis.

Katsikas (2000) discusses a methodology to identify the awareness training needs of health care staff. The presented methodology sub-divides security learning into awareness, training and education. This is similar to the security learning continuum presented in NIST 800-16 (1998). The presented methodology uses a training matrix to identify the specific educational needs of the target learners. A current security awareness education program in use in the health care environment is evaluated against the derived learning needs of the specific target audience. The course was found to be mostly sufficient, however, several small gaps in the content of the current course are highlighted.

Knapp, Marshall, Rainer, and Ford (2006) use a combination of qualitative and quantitative methods to provide evidence of the influence top management support has on both the level to which information security policy is enforced as well as the overall organizational information security culture. The studys results indicate that "top management support positively impacts security culture and policy enforcement" (Knapp et al., 2006). Both the rigorous methods followed in this research, as well as the research instrument developed in this study, could be of possible future use for assessing beliefs and attitudes regarding information security.

Kraemer, Carayon, and Clem (2009) identify and describe how human and organizational factors could cause computer and information security vulnerabilities. The study uses two focus groups to map out various "pathways" that could lead to vulnerabilities using causal network analysis. The paper first examines existing research regarding human and organizational factors in computer and information security. This literature overview is done from a multidisciplinary perspective. Secondly, the design of the research is described. The methods used are of a qualitative nature and make use of red teaming, an advanced form of assessment, to identify weaknesses with the help of focus groups consisting of experts. The results of this process are described in two causal network analysis and via examples. These results are further discussed and categorized. Categories include external influences, human error, management, organization of computer and information security, performance management, resource management, policy issues, technology, and training. The results indicate that vulnerabilities are often the result of not just one, but rather a combination of organizational conditions, such as management support or decisions made by designers. The study does not focus solely on awareness issues, however, several vulnerabilities that stem from problems in awareness programs are identified. The study could be useful to ensure adequate, and comprehensive coverage of specific topics during a formal approach to designing learning content in an information security educational program.

Kritzinger and Smith (2008) present a conceptual model for information security retrieval and awareness. The purpose of the conceptual model is to enhance information security awareness amongst employees. The first "building block" of the presented model is the collection of information security documentation, such as standards, best practices, etc. However, these contain too much detailed information to be used as a basis for information security awareness in industry. Kritzinger and Smith (2008) argue that there is a need for a common (global) body of information security knowledge aimed at the less technical end-users, as opposed to such bodies of knowledge aimed at technical information security experts. This common body of knowledge forms the second "building block" of the model. The third "building block" is the various IT authority levels. Each of these these authority levels consists of a grouping of stakeholders who have a role in ensuring the continued survival of the organization. The three "building blocks" combine to form a set of three information security retrieval and awareness dimensions. These dimensions collectively form the first part of the model. The second part of the model consists of various methods of retrieving information from the underlying dimensions, and using this information to enhance information security awareness. The final part of the model consists of methods to monitor and measure the current state of information security awareness in the organization.

Kruger and Kearney (2006) present a prototype model for measuring information security awareness in an international mining company. The paper first describes the current information security awareness program being used within the mining company. This program was developed after identifying six critical information security risk areas during an in depth risk analysis. The program focuses on these six areas and presents awareness content to the end-users using a variety of media formats. The model to measure the success of this information security awareness program was based on techniques from the field of social psychology which "proposes that learned predispositions to respond in a favorable or unfavorable manner to a particular object have three components: affect, behavior and cognition" (Kruger & Kearney, 2006). The model attempts to measure user knowledge, attitude and actual behavior. This measurement is done via the use of a simple scorecard approach. A prototype of the model was implemented in the above mentioned company and results were categorized according to a three category awareness scale. The overall awareness according to this scale, good, average, or bad, is derived through the combination of percentage scores for the underlying categories of knowledge, attitude, and behavior. The results of this prototype implementation were regarded as successful. However, it is recommended that future implementations develop a more comprehensive question bank, weigh specific underlying factors according to their relative importance, use practical system data, and make use of an automated tool.

Kruger and Kearney (2008) investigate the application of two existing management science methodologies to obtain consensus ranking from various role-players regarding priorities in an information security awareness program. Both a distance-based approach and a heuristic approach is used to perform the consensus ranking. These methodologies are applied in a large international mining company. The work in this paper supports earlier work published in Kruger and Kearney (2006). A simple questionnaire is used as a data collection instrument to obtain the various importance rankings regarding awareness priorities. It was found that this technique not only saves time and money in determining awareness priorities, but also provides better understanding of the relative importance of specific factors influencing the information security awareness program. The use of the technique described in this paper could assist educators in answering the so-called *learning question*, i.e. "what is the most important for learners to learn in the limited time available" (Anderson et al., 2001, pp. 6-10). The *learning question*, as well as the rest of the four so-called *organizing questions* in education, is discussed in depth in chapter 6.

Layton (2005) focuses on six *key psychological aspects of people's behavior* and how these "phenomena relate to, and impact, an information security program" (Layton, 2005, p. vii). Layton (2005) examines *motivation*, *attitude*, *beliefs*, *personality*, *morals*, and *ethics* and combines these aspects into a psychological-based framework for information security awareness. Layton (2005) starts by presenting arguments to establish why psychology is relevant to information security. These arguments are followed by an overview of information security awareness from the organization's perspective. Layton (2005) argues that most organizations currently "tell" users what to do via policy and then "push" these policies at the users without further explanation (Layton, 2005, p. 24). It is argued that information security awareness should rather be treated as an *attitude*. Users should be *asked* to change behavior, and should *understand* the risks, if they are to consistently behave in the desired way without supervision (Layton, 2005, pp. 24-25). Layton (2005), to a large extent, bases his theoretical model on *organizational citizenship behavior* theory. Organizational citizenship behavior is used to explain the connection between *behavior* and *motives* (Layton, 2005, pp. 30-45). User motivation is examined in depth in chapter 5 of Layton (2005) through an examination of various theories dealing with motivation. This includes need theory, two-factor theory, the operant model, goal-setting theory, expectancy theory, and equity theory (Layton, 2005, pp. 46-73). The in-depth examination of motivation is followed by an examination of user attitude, personality, and beliefs. Attitude is examined as a psychological phenomenon which can be defined as the ”feelings, beliefs, and predispositions forcing our behaviors” (Layton, 2005, p. 75). Layton (2005) does not relate these to an underlying discussion of corporate culture like most other information security research reviewed in this chapter, but rather relates these concepts to *organizational citizenship behavior* theory. Finally, the influence of morals and ethics on a user's information security behavior is discussed, before an approach to awareness which builds on the underlying psychological aspects is briefly introduced. The insight provided by Layton (2005) on the underlying psychological phenomena's influence on information security behavior is very valuable. Layton's (2005) summary, and discussions, of various theories regarding these phenomena could also be of great value to future researchers in information security awareness.

Leach (2003) discusses factors that influence user security behavior and how organizations can improve user security behavior. The paper first examines the threat posed to information security by organizational insiders. The various factors that influence user information security behavior is then investigated. These factors include what employees are told, what the see in practice around them, the user's security common sense and ability to make decisions, personal values, the user's sense of obligation, and how easy or difficult compliance is (Leach, 2003). The paper next discusses various ”keys to better user security behaviour”. These includes the behavior of other employees (principles, policies and procedures will be negatively influenced if employees see behavior contrary to these espoused values around them), the user's own security common sense and decision making ability (organizations should focus on improving the users ability to make security related decisions), and the user's psychological contract with their employer (the organizational culture). Leach (2003) concludes by stating that leadership is key to successfull behavior change; "After all, if senior management can't be bothered, then why should staff?" (Leach, 2003).

May (2008) provides seven guidelines for the development of more effective information security awareness programmes, the first of which is to "make it personal". The premise of this guideline is that staff members need to identify with information security messages if they are to remember them. The second guideline is to match the message to the target audience. Both the amount of technical detail, and the delivery style itself should be matched to the intended target audience's preferences. Thirdly May (2008) recommends that awareness messages should be short. Presentations should not exceed ten to fifteen minute sessions. Fourthly awareness education should be made interesting. The fifth guideline which ties in with the fourth is that examples should as far as possible be confined to real-life examples and should avoid speculation on what *might* happen if security is breached. The sixth guideline presented is that awareness sessions should be made part of a daily routine. A ten to fifteen minute daily awareness "break" is recommended. It is also argued that such a daily awareness session would help with the fostering of an information security culture in the organization. The final guideline is to use the right delivery method. These could include e-learning, informative (yet entertaining) leaflets, or even personalized presentations.

Mitchell, Marcella, and Baxter (1999) report on a study into corporate information security management. The paper first discusses information security in general. This discussion includes an overview of different types of threats, as well as an examination of certain baseline information security controls. The study gathered data through the use of both telephonic interviews and a questionnaire. Amongst other findings, it was found that half the respondents viewed information security as an IT function and thus not their responsibility. A large portion of respondents viewed themselves, or their employees, as "not very aware" of information security. And a "very low" portion of the surveyed companies had ongoing information security awareness, training and education programmes. "Statistically, there was no connection between training provision and whether or not a company had an information security policy document. In other words, the existence of a formal policy document did not mean that the company was translating policy into action" (Mitchell et al., 1999). The paper briefly discusses survey results regarding employees' perception of threats. More detail on attitudes towards information security is provided by the discussion of the telephonic interviews which found that four primary factors influenced these attitudes. The factors included whether or not the company was owned by a foreign parent company, a lack of perceived cost benefit in investing in information security, a lack of resources, and the (false) assumption that not having had major information security incidents in the past is an indication that none will happen in the future.

Mitnick and Simon (2002) argue that an ongoing information security awareness campaign is needed by organizations in order to protect the organizations against social engineering attacks. According to Mitnick and Simon (2002, p. 4) security products only offer the *illusion of security* unless these products are supported by a *human firewall.* Mitnick and Simon (2002) provide extensive insight into the roles humans can play in an organization's information security efforts through the use of example scenarios. According to Mitnick and Simon (2002) a successful information security awareness campaign should start with an understanding of how attackers take advantage of humans (Mitnick & Simon, 2002, pp. 246-249). It is important that *everyone* in the organization receives awareness education and that this education focuses on influencing employees to change their behavior and attitudes by motivating employees to *want to* protect the information assets of the organization (Mitnick & Simon, 2002, pp. 249-250). Mitnick and Simon (2002) recommend the use of role-playing, exposure to, and discussion of, recent media reports of information security incidents, as well as the use of videos as possible training methods. Mitnick and Simon (2002) also argue that information security should be made a part of every employee's job responsibility (Mitnick & Simon, 2002, p. 256). Finally, the use of rewards and punishments to help change behavior, as well as widely publicizing actual security incident is advocated (Mitnick & Simon, 2002, pp. 257-258).

Mitnick and Simon (2006) present detailed discussions of numerous actual computer security incidents. These discussion are in many cases based on interviews with the actual perpetrators of the "crimes". Mitnick and Simon (2006) reiterate the message presented in Mitnick and Simon (2002), namely that *humans are the weakest link in information security.* Mitnick and Simon (2006) concludes by presenting guidelines, similar to those presented in Mitnick and Simon (2002), for the training of employees in order to help prevent future information security vulnerabilities.

NIST 800-16 (1998) is published by the American National Institute of Standards and Technology (NIST). This document provides an information security specific training model.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", together with the complementary document "Building an Information Technology Security Awareness and Training Program" (NIST 800-50, 2003) (NIST 800-50 (2003) will be discussed as the next item in this overview), forms the only standard that currently focuses exclusively on the learning needs related to information security. As such this model is seen as extremely important for the purposes of this literature review and will be dealt with in depth. 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 and several other publications reviewed are based on this continuum. The three levels of learning in the NIST 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 specialities 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).

- Education: The "Education" level integrates all of the security skills and competencies of the various functional specialities 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.

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 consists 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.

NIST 800-16 (1998) does not make use of a learning taxonomy, however, the approach to content development specified in this document is very formal and clearly adheres to sound pedagogical principles.

NIST 800-50 (2003) is a companion to NIST 800-16 (1998) and provides a higher, strategic level discussion than NIST 800-16 (1998). The focus of NIST 800-50 (2003) is on *how to build* an information security awareness and training *program*, whilst the focus of NIST 800-16 (1998) is on the mechanics of the specific role-based information security training model. NIST 800-50 (2003) thus focuses on the overall program whilst NIST 800-16 (1998) focuses on how the content of the program should be developed. NIST 800-50 (2003) outlines four stages in the development life cycle of an information security awareness and training program. These include a design, development, implementation, and post-implementation phase. The document firstly briefly discusses the role an information security policy plays in the establishment of an information security awareness education program. This is followed by the identification of the various organizational structures/role players who *should be* responsible for the task of establishing such a program. The document clearly establishes the roles and responsibilities of the "agency head" (board of directors), the chief information officer, the information security manager, various line managers, and end users themselves. The introduction is followed by a brief discussion of the same learning continuum as described in NIST 800-16 (1998), after which each of the various stages in the life-cycle of an information security awareness program is discussed individually. The first stage in the life-cycle of an information security awareness and training program is a program design phase. This section discusses the structure of an awareness and training program, how to determine specific awareness and training needs, the development of an awareness and training strategy/plan, the setting of priorities, how to determine an appropriate level of complexity for learning material, and finally issues around the funding of an awareness and training program. The second life-cycle phase discussed by NIST 800-50 (2003) is the development phase. According to NIST 800-50 (2003) awareness specific material should be developed with a focus on the desired employee behavior, whilst training material should focus on the specific skill the target audience would need in order to have the ability to behave securely (NIST 800-50, 2003, p. 23). The development section of the document provides guidance on the selection of specific awareness topics, possible sources for awareness material, the development of training material (which focuses primarily on the use of NIST 800-16 (1998)), and possible sources for training courses and material. The implementation phase of an awareness and training program as discussed by NIST 800-50 (2003) starts with the communication of the awareness and training plan to various organizational role players. The document then discusses techniques for delivering awareness material (posters, screen-savers, video, etc) and techniques for delivering training (ranging from face-to-face instructor led training, to web-based training and other forms of e-learning). None of the training and awareness delivery mechanism is discussed in depth. The post-implementation phase is the final phase in the life-cycle of an information security awareness and training program. This phase consists of the monitoring of compliance, formal evaluation and feedback mechanisms, change management,and continuous program improvement. NIST 800-50 (2003) also briefly discusses various indicators for a successful program (NIST 800-50, 2003, p. 39).

OECD (2002) presents "Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security". The OECD consists of more than 30 member countries and adopted OECD (2002) "as a Recommendation of the OECD Council at its 1037th Session on 25 July 2002". The adoption of this guideline by the OECD clearly shows the importance of developing an information security culture. The document presents several aims, including the promotion of an information security culture "as a means of protecting information systems and networks", to raise risk awareness, to foster confidence in information systems (due to better security), to create a frame of reference for the understanding of security issues, to promote sharing of information in the creation of information security policies, practices, measures, and procedures, and to promote the consideration of information security in the development and implementation of standards (OECD, 2002). In order to help achieve these aims nine guiding principles are provided, namely; awareness, responsibility, response, ethics, democracy, risk assessment, security design and implementation, security management, and reassessment. Each of these principles is briefly discussed.

Power and Forte (2006a) present a "powerful, unique and comprehensive awareness and education program for a global entity" in the form of a case study. The case study outlines how a mandate from a large global entity resulted in a very successful awareness and education campaign aimed at fostering a culture of information security in the organization. The campaign took place in three phases. During the first phase it was attempted to engage all staff in a manner which is both economic and effective. During this phase an awareness and education task force with roll-players from various departments was formed, a bi-monthly security newsletter was launched, a security responsibility presentation was incorporated into the orientation sessions for new staff, a global annual security day was established, and an e-learning module for both new staff and remedial training was created. The second phase focused on technical security training seminars for IT staff. The third phase entailed the deliverance of vital security related intelligence and early warning regarding threats to executives. The program in the case study was very successful and Power and Forte (2006a) provide evidence of this success. However, due to a change in top-level attitudes the "mandate shriveled up and blew away" (Power & Forte, 2006a). The success of the program made top-management realize that they would prefer an environment which is less aware of all the information security threats and risks out there.

Power and Forte (2006b) discuss social engineering and countermeasures to social engineering. The paper sub-divides social engineering attacks into two categories; technology-based deception or human-based deception. The paper provides brief case study examples of actual social engineering attacks and then proceeds to discuss how such attacks should be handled. The discussion includes how to recognize elicitation, how to handle the caller, and incident reporting. Finally a brief checklist of how to handle social engineering attacks is presented.

Puhakainen (2006) introduces three design theories to help improve information security related behavior amongst users. The study firstly overviews and analyzes fifty-nine current approaches towards information security awareness. This analysis clearly shows that a significant lack of theory based approaches exist amongst current information security awareness approaches. A large overlap between the sources examined by Puhakainen (2006) and those reviewed in this chapter exists. However, several of the sources examined by Puhakainen (2006) were deemed not recent enough (older than ten years) for the purposes of this study and were thus excluded from the current study. Most of the approaches reviewed by Puhakainen (2006) lack a theoretical basis (Puhakainen, 2006, p. 62). Those approaches that were found to have a theoretical basis, and were recent enough (published during of after 1999), have all been included in this review. Out of the approaches reviewed by Puhakainen (2006), only (Aytes & Connolly, 2003), (Banerjee, Cronan, & Jones, 1998), and (Siponen, 2000), had both theoretical bases and were published recently enough for inclusion in the current study's review. The first of the three *new* theories presented by Puhakainen (2006) is a design theory for information security awareness based on the *universal constructive instructional theory* and the *elaboration likelihood model.* The universal constructive instructional theory "provides a framework for designing situational instructional theories to be used in creating customized instruction" (Puhakainen, 2006, p. 71). Puhakainen (2006) combines this framework with the *elaboration likelihood model*, which encourages attitude change via both *cognitive processing* of persuasive arguments and *cues* (Puhakainen, 2006, pp. 72-73). *Cues* are "non-argument elements of the message that can influence attitude change without any active thinking about the issue" (Puhakainen, 2006, p. 72). This theory is verified by Puhakainen (2006) through two action research interventions (Puhakainen, 2006, pp. 91-137). This proposed theory will be examined in more depth in chapter 6.

The second theory proposed by Puhakainen (2006) focuses on the design of information security campaigns. This theory is based on the *convergence model of communication.* The *convergence model of communication* explains how information is interpreted by different individuals according to their own personal perceptions, and how these varying beliefs and understandings can eventually converge through processes of feedback and information sharing (Puhakainen, 2006, pp. 78-79). Based on this model, Puhakainen (2006) proposes an approach to information security campaign design that is based on active communication and information sharing between all parties (Puhakainen, 2006, pp. 79-80). This theory is verified only via argument.

The final theory proposed by Puhakainen (2006) focuses on *reward and punishment* as a means to encourage information security behavior change. The proposed theory is based on the theory of *operant conditioning.* The theory of *operant conditioning* shows that an individual's future behavior can be influenced if environmental variables are manipulated (person is rewarded or punished) as a consequence of current behavior (Puhakainen, 2006, p. 85). Puhakainen (2006) presents a six step process which outlines how this theory could be applied in an organization (Puhakainen, 2006, p. 86-87). This theory presupposes that the current information security behavior of employees can in fact be monitored.

The theories presented by Puhakainen (2006) have a strong theoretical basis and are thus deemed very important for the purposes of the current thesis. However, Puhakainen (2006) does not focus directly on the fostering of an information security culture, or on the pedagogical basis for determining the actual contents of an information security educational campaign. Instead, Puhakainen (2006) focuses on theory dealing with the *structuring* of specific information security messages in order to enable learning, theory on *how* information should be distributed through the organization, and theory on *how* behavior change should be encouraged by the organization. These theories can play a supporting role in the current thesis but do not overlap with the primary focus of this thesis.

Rezgui and Marks (2008) explore factors affecting information security awareness amongst the staff at a higher education institution. The paper first examines several known security incidents that occurred at higher education institutions and also briefly focuses on risks that are specific to such institutions. Related publications are briefly examined and the authors subdivide current work on information security awareness into two broad categories, namely; studies where the term awareness is meant "to attract users' attention to information security issues" (this is the same meaning assigned to this term by NIST 800-16 (1998)), or studies where the term awareness means both the users' understanding of information security and ,optimally, the users' commitment to information security. The paper next presents the results of an interpretive case-study that was used to explore the levels of information security awareness at a university. The data for the case study was collected via questionnaires, interviews, direct observation, and documents. The study found that many respondents did not believe information security to be a problem and did not see themselves as part of the solution. In general staff was uniformed and unaware regarding information security issues. Most staff believed that manuals and documentation for information systems are available, yet the study found that the university had poor manuals and documentation. The university mostly had contract staff and this also contributed towards a lack of conscientiousness regarding information security. Three main awareness issues were identified. Firstly there was a lack of information security training and staff consequently behaved insecurely. Secondly, there was a lack of awareness campaigning. This lead to most staff being unaware that they lack training, or that there is a problem. Thirdly, it was found that the university had no security policy, and hence there were no rewards for secure behavior and also no punishment for insecure behavior. Rezgui and Marks (2008) conclude by providing some recommendation that could assist the university in improving information security awareness.

Rheea, Kimb, and Ryuc (2009) use self-efficacy, a construct from social cognitive theory, and model and test various aspects of information security against this construct. Self-efficacy is described as a "form of self-evaluation which is a proximal determinant of individual behavior" (Rheea et al., 2009). People with a high level of self-efficacy have more confidence in their own ability to "mobilize motivation, cognitive resources, and courses of action needed to successfully execute a task" (Rheea et al., 2009). The presented study extends the use of this social cognitive theory to information security. The paper contends that the users' belief in their own ability to perform their information security related role(s) can explain their actual security practices and their intention to persist in these practices. The research uses statistical methods to test whether or not individuals with higher self-efficacy use more security protection software, demonstrate more security conscious behavior, and have stronger intentions to improve their information security. Statistical methods are also used to test; whether or not more computer related experience leads to higher self-efficacy in information security, whether more security incidents lower self-efficacy in information security, and whether the perception that security threats are controllable increase self-efficacy in information security. The study found that a positive relationship exists in all the tested cases. Self-efficacy in information security thus leads to both improved security practice and improved motivation to behave securely.

Roper, Grau, and Fischer (2005) present a comprehensive guideline to security education, training and awareness in *general*. The book does not focus specifically on the needs of *information* security. However, it is included in this review because many of the problems experienced in security education in general, as well as many of the theories applicable to such education, could be applicable to information security too. The primary focus of Roper et al. (2005) is on actual security *performance* (i.e. employee actions), and all other aspects such as employee knowledge and/or attitude, are addressed in terms of the possible impact these aspects could have on actual behavior. Roper et al. (2005) present an educational model consisting of training (to provide the actuals skills needed to perform security roles), education (to allow people to understand the underlying security principles), awareness (to promote the consideration of security aspects during normal tasks), and motivation (to convince employees that it is worth their effort to adhere to security requirements). Roper et al. (2005) addresses security education as an important part of a person's *employment life cycle*. They stress the importance of ensuring that every employee *understands security as a job responsibility* (Roper et al., 2005, p. 41). Roper et al. (2005) also advise educators to tailor security educational material to specific employee groups, and to try to understand human behavior in order to establish a rapport with employees. Guidelines are provided relating to various aspects of the training, education, awareness, and motivation model presented in the book. Some information specific to information security, including security whilst online, is presented as appendixes to the main text.

Rudolf, Warshawsky, and Numkin (2002) start by examining the critical success factors for an information security awareness campaign. The first of these critical success factors is having an information security policy that clearly establishes that everyone must participate in an awareness program, that ensures everyone is given sufficient time to participate in awareness education, and that clearly establishes who is responsible for conducting awareness program activities. The second critical success factor is senior management support, which should include sufficient budget allocation, setting an example, and supporting (backing) security personnel. The third is having an awareness program that focuses on people (not technology). The fourth critical success factor is that the awareness program should have specific, realistic and measurable goals (Rudolf et al., 2002, p. 29.4). The fifth is that awareness education should be focused according to specific target audience groups (in terms of needs, roles and interests), and the final critical success factor listed is that the awareness program should seek to change behavior via *motivation*. Rudolf et al. (2002) briefly discuss the general approach towards a media campaign and plan for awareness activities. This is followed by an overview of awareness principles, possible content, presentation techniques, delivery tools, and finally measurement and evaluation. No specific mention is made of the pedagogical basis of these presented principles. E-learning based tools are briefly discussed.

Ruighaver, Maynard, and Chang (2007) view the concept of an information security culture from a management perspective. The paper adopts an eight dimensional organizational culture model from the management sciences. Each of the dimensions in this model is discussed in terms of its use to model an information security culture. The adoption of this model for information security culture is performed based on past case studies. The first dimension in this model deals with the *basis of truth and rationality.* The authors argue that the beliefs that decision makers in an organization have about the organization's current information security, is more important than those of end-users. The ability of both managers and end-users to be critical of their own existing beliefs is what distinguishes a good culture from a bad one. The second dimension in the model is the *nature of time and time horizon.* It is important to not only focus on immediate concerns, but also to have a long term strategy to develop security skills. The presented model's third dimension is motivation. "In an ideal security culture, end-users, security administrators and managers will be motivated to reflect on their behavior at all times, to assess how their behavior influences security and what they can do to improve security" (Ruighaver et al., 2007). The fourth dimension is *stability versus change, innovation, and/or personal growth.* According to Ruighaver et al. (2007) periodic processes of change and innovation should purposely be built into an information security culture. This would help the organization to be proactive in its security efforts, rather than reactive. The fifth dimension of the model is *orientation to work, tasks, and coworkers.* This dimension deals with finding the right balance for employees between information security and the ability to freely perform their duties. Education of employees can also contribute significantly to this dimension. Through information security education employees would be more able to determine the limits of 'acceptable use' of information. The sixth dimension is *isolation versus collaboration/cooperation.* It is important for organizations to include people from all facets of the organization in both the creation of information security policies, and the management of information security processes on a day-to-day basis. Information security should not be an isolated process handled by a small group of specialists (Ruighaver et al., 2007). The seventh dimension is *control, coordination and responsibility.* This dimension deals with the need for information security governance in the organization. The final dimension is *orientation and focus - internal and/or external.* This dimension deals with how much focus is given to the internal (inside the organization) versus the external security environments. The authors believe that an organization with a secure culture should have a balanced focus. This model does not adapt existing theory, but rather uses theory from the management sciences *as is* for the purposes of information security.

Schlienger and Teufel (2003) present a framework for the analysis of the information security culture of an organization. This framework is discussed in terms of a case study implementation. The paper firstly provides a definition for an information security culture based on Schein's corporate culture model. This is followed by a discussion on the cyclical nature of managing such a culture. During this process evaluation of the current culture plays an important role. The paper briefly discusses the difficulties inherent in performing such an evaluation. The evaluation process should be followed by the identification of areas that could be improved. Data is provided on the areas that were identified during the case study implementation. Schlienger and Teufel (2003) next present the process that was followed to affect the identified changes. This process started with strategic planning sessions during which a clear target culture was determined and organizational members were segmented according to the similarity of their attitudes towards the cultural targets. Strategic planning was followed by operative planning. During this phase internal communication, management buy-in, and the security awareness and training program was planned. Proper planning is vital for the success of security awareness, training and education. "The security awareness and training program leads from become aware to stay aware and ends up in be aware, which changes a security culture definitively." (Schlienger & Teufel, 2003). This operative planning phase was followed by an implementation phase. During this final phase an internal marketing exercise was conducted to ensure buy in from all role-players.

Schultz (2004) calls for more information security training and awareness research. The argument is made that awareness should not just consist of posters, or coffee cups and pens with slogans. It is also argued that "one size fits all" awareness programs are not suitable.

Sharma and Sefchek (2007) describe a hands-on information systems security curriculum forming part of formal tertiary education for information technology students. The described approach focuses on technical education of IT specialists, and not on end-user awareness education. The paper first justifies the need for information security education and then briefly overviews applicable literature. The authors sub-divided the curriculum into three separate under-graduate courses in order to ensure adequate coverage of the field of information systems security. The structure and content of the three courses are discussed. It is emphasized that the target learners are information systems students who wish to specialize in security. Next Sharma and Sefchek (2007) elaborate on the available lab infrastructure, followed by some insight into the underlying pedagogy of the courses. Some detail of actual content in assignments and tutorials is provided, followed by a section on lessons that were learned during the creation of the described curriculum. The authors assert that students performed best in laboratory exercises where they had some prior knowledge of the subject material, or where they were able to perform the tasks on their home PCs. One criticism of the approach mentioned by Sharma and Sefchek (2007) is that one could argue the same exercise is enabling students to become computer criminals. No mention is made of e-learning modules, however, technology is used extensively during the actual courses.

Shaw, Chen, Harris, and Huang (2009) use statistical methods to study the impact of information richness on the effectiveness of information security awareness training. The paper briefly discusses the need for information security awareness and for the fostering of an information security culture. This discussion is followed by a brief overview of problems with current awareness education. Specific attention is paid to how awareness education should be delivered and the lack of a fully developed methodology for the deliverance of awareness education is cited as a major problem. The study is based on various conceptual foundations. The first of these is the growing importance of security awareness programs in organizations. The second conceptual foundation was the major challenges existing awareness programs have in changing user perception, comprehension, or the ability to anticipate future security incidents. The third conceptual foundation was that e-learning systems is a feasible alternative for the delivery of security awareness, and the final foundation was the influence of media richness on the effectiveness of online information security education. Hypothesis testing was used to evaluate various theories. The findings indicated that;

- users with a higher perception of security risk are more likely to have a high comprehension of these risks,
- users with a higher comprehension of security risks are better able to project these risks (predict future incidents),
- hypermedia-based programs are more effective than multimedia-based ones in enhancing both users' comprehension of security issues, and their projection ability with regards to security incidents, but are not better than multimedia to enhance risk perception,
- and finally that multimedia-based programs are better than hypertext-based ones in enhancing both users' comprehension of security issues, and their projection ability with regards to security incidents.

Hypermedia is thus better for security awareness education than multimedia, which in turn is better than hypertext. There is thus clear indication that media richness plays a significant role in enhancing security related learning.

Siponen (2000) provides a conceptual foundation for information security awareness. The paper argues that problems with awareness programs can be classified as either framework related, or content related. The framework category consists of issues that can be approached from an *engineering discipline* perspective. These issues can be researched in a quantitative and structural fashion. The content category consist of issues that is better researched from a qualitative perspective. According to Siponen (2000) there exists a great need for research in the content category of information security awareness, for example, "how to motivate people to comply with security guidelines" would lie in the content category. Siponen (2000) asserts that most research in this content category of awareness tend to be descriptive in nature and hence lacks adequate foundations. It is also argued that many current authors recognize the need for attention to the behavioral aspect of information security awareness but that the current publications only consider these issues from an abstract viewpoint and lack theoretical basis (Siponen, 2000). The paper attempts to partially address this problem. Firstly a theoretical framework is provided for information security awareness approaches to deal with motivation and attitude. This framework makes use of the theory of reasoned action (intention leads to behavior), the theory of planned behavior (TPB) (intention consists of attitude, subjective norms, and perceived behavioral control), the theory of intrinsic behavior (people want to determine their own choices),and the technology acceptance model (TAM) (the intention to use "systems" depends on both its perceived usefulness and how easy it is to use). It is argued that the *ease of use* aspect of TAM and the *perceived behavioral control* issues from TPB should be dealt with via technical education and thus needs not be considered when trying to persuade users towards secure behavior. Siponen (2000) also considers the way in which people respond to awareness methods. Such responses can be either positive (leading towards more acceptance and internalization of security messages), or negative (leading towards resistance against the security message). It is argued that qualitative measurement of such attitudes must be considered during awareness efforts. A final part of the theoretical basis provided deals with the reconsideration of current methods in light of the theoretical framework provided earlier. The behavioral issues around current awareness should be examined in order to ensure these issues are considered. Siponen (2000) proceeds to argue that information security awareness should be *prescriptive*: "users often know the guidelines, but they fail to apply them correctly" (Siponen, 2000). There should thus be both a role responsibility to apply security controls, as well as a moral responsibility. This moral states "this obligation should be internal, coming from within the individual" (Siponen, 2000), hence an information security culture is needed. Various approaches that reflect these prescriptive requirements are briefly discussed. It is recommended that awareness program attempting persuasive strategies should consider the following principles;

- logic (action should be logical, do not act inconsistently),
- emotions (security measures should aim to appeal to positive emotions),
- morals and ethics (secure behavior should be viewed as the *right thing to do*),
- well-being (users should be aware of the threat to themselves, organizations and society),

- feeling of security (people should want to achieve a feeling of safety by behaving securely),
- and rationality (people should know why they need to behave in a certain way (rational explanations)).

This paper is one of the earliest papers to seriously address the behavioral aspects of information security education.

Siponen (2001) examines information security awareness as more than just an organizational issue. It is argued that information security awareness should also be the concern of society at large. Siponen (2001) presents five dimensions of information security awareness. The first is the organizational dimension. In the organizational dimension five target groups for awareness education is identified. These include top management, IT/IS management, information security staff, computing/IS professionals, and end-users. Third parties are also mentioned as a possible target group external to the organization. It is argued that the information security needs of each of these groups will be different. Awareness needs for the different categories of organizational users are briefly examined. The second identified dimension is the general public dimension. Two categories of target groups are identified, namely end users, and IT/computer/IS professionals. It is argued that there are several central information security issues that every citizen using IT should be aware of. Hence the need for general public information security awareness. The third dimension discussed is the socio-political dimension. Target groups in this dimension include lawyers, public relations people, politicians and other government employees. The need for information security awareness at this dimension is based on the overall well-being of society and its dependance on proper legislatury frameworks for information security. It is also important that the moral conceptions underlying IT law is realized by politicians. The fourth dimension Siponen (2001) identifies is the computer ethical dimension. This dimension should target the (computer) ethics scholars. Its purpose is to focus on the creation of a body of knowledge such scholars can draw upon. The final dimension identified is the institutional education dimension. This dimension deals with society-driven processes of education that are "aimed at making individuals proper members of society"

(Siponen, 2001). This dimension could thus also be interpreted as the need for the fostering of an information security culture in society at large. The ideas presented in this paper are, in the opinion of the author of this thesis, of great importance to the field of information security education. However, due to the specific focus of this thesis, only the organizational dimension will be dealt with in this thesis.

Theoharidou, Kokolakis, Karyda, and Kiountouzis (2005) examine the possible enhancements that could be made to the ISO17799 standard (now the (ISO/IEC 27002, 2005)) through the consideration of criminology theory. The paper specifically focuses on the aspect of an *insider threat* and the criminology theories that deal with such a threat. The paper discusses the possible role(s) of the general deterrence theory, the social bond theory, the social learning theory, the theory of planned behavior, and the theory of situational crime prevention. The paper does not specifically address the implications of these theories for information security awareness, training and education programs. Instead the focus is on an analysis of the ISO17799 standard, to determine the theoretical basis of this standard in terms of criminology. However, since these theories deal with the behavioral aspects of information security, the paper is included in this review to ensure that the possible impact of these theories on information security educational programs is also considered.

K. Thomson and Von Solms (2005) discuss the commonalities and relationships between the fields of corporate governance, information security and corporate culture. The role of each of these fields, and how the "other two" influences information security, are first discussed individually. Once the respective roles are identified K. Thomson and Von Solms (2005) examine the area of "overlap" between these three fields. The paper advocates the use of the term *information security obedience* to describe the area where all three of these fields overlap in the support of each other and in support of information security. It is argued that staff would behave in an obedient way in terms of information security if all three areas support each other. Firstly top management has to be committed to information security and must espouse this commitment through policies and procedures. Secondly a culture of information security should exist through which employees would want to behave securely.

K. Thomson and Von Solms (2006) present an information security competence maturity model as a possible method to evaluate the extent to which information security is entrenched in an organization's culture. The paper firstly discusses the significance of corporate culture and then briefly mentions various methods of knowledge creation. Bloom's Taxonomy is mentioned but not discussed. This is followed by the presentation of the conscious competence learning matrix. The conscious competence learning matrix views learning as a four stage process. At the first stage the learner has *unconscious incompetence.* In an information security context this would mean that the users are completely unaware of their security role(s) and responsibilities. The second stage of learning is *conscious incompetence.* At this stage users would be aware of the existence and relevance of security tasks but do not yet have the requisite knowledge or skills to perform these tasks. The third stage of this learning matrix is *conscious competence.* At this stage users will have the necessary knowledge or skills, but would still have to consciously think about it in order to perform security related duties. The final stage is unconscious *competence.* At this stage the task will become "second nature" to a user. K. Thomson and Von Solms (2006) present a maturity model which is derived from the conscious competence learning matrix for information security related knowledge. In the presented maturity model end users can be moved from unconscious incompetence, through to unconscious competence through the use of firstly awareness programs (to gain conscious incompetence), then training (to gain conscious competence), and finally experience (which will lead to eventual unconscious competence).

K. Thomson, Von Solms, and Louw (2006) present a model for the cultivation of an organizational information security culture. The paper starts by discussing *what* an information security culture is in depth. Reference is made to the idea of information security obedience, as discussed in K. Thomson and Von Solms (2005), as an amalgamation of corporate culture, corporate governance and information security. The paper then outlines a Model for Information Security Shared Tacit Espoused Values (MISSTEV). The first component of this model is the conscious competence learning model (K. Thomson & Von Solms, 2006). The second component is Nonaka's Modes of Knowledge Creation, which identifies existing knowledge and "converts" it to new knowledge. This is done through socialization (one person's tacit knowledge is transfered to another person), externalization (tacit knowledge is made explicit), combination (explicit knowledge is transferred through the organization via documents, etc), and internalization (an individual "absorbs" the explicit knowledge). The presented MISSTEV model details the progression of knowledge from an initial information security policy, via the mentioned learning models, to being realized as information security obedience. K. Thomson et al. (2006) do not significantly modify the commonly used definitions of organizational culture to be specific to information security. However, the presented model does adapt existing theory about culture change for the specific purposes of information security. Because the concept culture change, or the establishment of a "new" culture, forms an integral part of the theory about organizational culture in general, this will be counted as a modification of culture theory for the purposes of the qualitative content analysis done in this chapter.

Valentine (2006) presents a multi-phased methodology for information security awareness education. The paper firstly discusses, through the use of specific example cases, some common failures of "one-size-fits-all" information security awareness education programs commonly used by organizations. The paper then presents the multi-phased methodology which can be used to tailor information security awareness programs to be more specific to the need of the intended target audience. This methodology consists of three phases. The first phase is an *assessment phase*. During this phases the organization has to "scope" exactly what should be protected, and how educational needs can assist in this protection. Employees need to know what they are protecting and what the consequences of failure to protect this resource would be for the organization. The second phase is an *identification phase*. All employees who interact with each resource that must be protected should be identified. Employees should only be educated about information security roles applicable to themselves. The final phases in the methodology is an *education phase*. Due to the preceding assessment and identification phases, organizations should now have enough information to create educational materials that are specific to the needs of the identified users. Educational material can be partly scenario based and should include incident response procedures. The approach presented in Valentine (2006) is definitely a more formal pedagogical approach than most other current approaches reviewed in this thesis. However, no formal references to current pedagogical theories were provided to establish the credibility of this approach.

Van Niekerk and Von Solms (2004) examine the suitability of outcomes based education as a pedagogical basis for information security education. The paper firstly discusses the role humans play in information security and justifies the need for user education. A list of requirements that should be met by an educational program, specific to the need of information security education, is proposed. Each of the proposed elements is briefly justified by means of argument. The requirements include:

- ”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.” (Van Niekerk & Von Solms, 2004)

A comparative analysis between the ”features” of outcomes based education and the identified requirements of information security education is performed. The paper concludes that outcomes based education would be a suitable pedagogical basis for information security education.

B. Von Solms (2000) discusses the various *waves* characterizing information security through the ages and argues that the *third wave* will be one where information security becomes institutionalized. One of the aspects of institutionalized information security discussed in B. Von Solms (2000) is the cultivation of an information security culture. B. Von Solms (2000, p. 618) states that "a culture of information security must be created in a company, by instilling the aspects of information security to every employee as a natural way of performing his or her daily job".

B. Von Solms (2006) further explores the themes first discussed in B. Von Solms (2000). A fourth wave in information security is introduced in this paper. The fourth wave is characterized by a relationship between information security and corporate governance and this amalgamation is termed *information security governance.* One of the aspects that is seen as integral to *information security governance* is "full user awareness and commitment towards good information security" (B. Von Solms, 2006, p. 167). It is argued that this fourth wave in information security is not a technical wave and that "other (non-technical) issues like awareness and compliance management, ensuring that the stakeholders conform to all relevant policies, procedures and standards" (B. Von Solms, 2006, p. 168) form the core of good information security governance.

R. Von Solms and Von Solms (2004) present an hierarchical structure to demonstrate how information security policies could lead to eventual behavioral change amongst employees. The paper firstly examines *what* a policy is. Secondly, the concept of corporate culture is examined and the role policies play in such a culture is discussed. The ten commandments from the Christian Bible is then used as an analogy to present the hierarchical structure through which policies could lead to changed behavior. How these commandments influenced religious beliefs and led to laws in many countries, which in turn ultimately provide directives for daily behavior in these countries is discussed in depth. The paper then argues that the vision of top management should be structured into a proper policy and procedure framework. This will ensure that the conceptual ideas of management (vision) are entrenched in a set of logically structured documents. The contents of these documents should then be communicated to all employees via a "well defined process of education, reminders, refresher courses, etc" (R. Von Solms & Von Solms, 2004, p. 279). If the education is successful it will become entrenched in daily behavior which will ultimately change the organizational culture.

Vroom and Von Solms (2004) explore problems an organization would face if they wanted to audit the information security behavior of employees. The paper firstly examines auditing in general and then explores IT auditing and information security auditing. This is followed by a discussion of the human factors in information security and the possible problems that might prohibit the auditing of user behavior. After a detailed examination it is concluded that the auditing of end-user information security behavior would not be a plausible approach towards ensuring behavioral compliance. Vroom and Von Solms (2004) proceed to argue that the fostering of an information security culture in organizations would be a better approach towards ensuring behavioral compliance. The paper briefly presents a definition of such a culture and finally provides some suggestions on the changing of organizational culture.

Werlinger, Hawkey, and Beznosov (2008) use empirical methods to identify and then describe challenges that information security practitioners face. The study focuses on the interplay among human, organizational, and technological factors. The paper briefly discusses the need to examine the various factors and then presents the methodology used to gather the primary data in the study. Three of the challenges identified are classified by the authors as forming part of the human factor in information security. These include a lack of security training, a lack of an organizational information security culture, and challenges with the communication of security issues. Communication (and education) about information security issues were found to be particularly problematic where various stakeholders had different perceptions of the underlying risks. The paper continues to present a framework to assist with the understanding of the interplay between various identified factors. The paper does specifically discuss the need for an information security culture but does not discuss the underlying motivational/behavioral issues.

White House (2003b) presents a national strategy for information security training and awareness. The document identifies a lack of familiarity, knowledge and understanding of information security issues, as well as a lack of adequately trained IT staff to manage secure systems as major barriers to the improvement of the USA's *cybersecurity*. The document aims to firstly promote a national information security awareness program amongst all sectors, including home users and small business, large enterprizes, institutes of higher education, private sectors, state and local governments. Secondly, the document aims to foster adequate training and educational programs to support the country's cybersecurity needs. It also aims to improve the efficiency of existing programs, and finally to promote private sector support for information security certifications. This document does not directly address how these aims will be met, it only justifies the need for them. The similarities between this high level strategy and the earlier call for information security awareness to be dealt with as a problem for society as a whole by Siponen (2001) is noteworthy. The actions and recommendations in support of the aims outlined in White House (2003b) is presented in White House (2003a). Once again these are at a strategic level and primarily deals with the establishment of various task teams and/or committees, as well as calls upon various agencies to participate in national strategies.

Williams (2008) examines user needs when dealing with information security in a health care environment. The paper firstly outlines several information security related problems in the health care environment. These include the sensitive nature of the information, a lack of conceptual understanding of information security amongst health care professionals, the underestimation of threats (lack of awareness), and too much focus on technological solutions as opposed to addressing the lack of an information security culture amongst health care professionals. The study shows that health care professionals are often trusted with sensitive information, and that they are also trusted to be aware of the necessary security measures. However, despite this trust there exists a lack of knowledge, a lack of the capability to perform security related tasks, and an attitude that security issues are not a day-to-day priority. The study also found cost and time constraints, inconsistent security practices, and poorly implemented controls.

Wylder (2004) suggests incorporating information security responsibilities into employees' job performance criteria (Wylder, 2004, p. 100). From a human resource management perspective this would bring the task ensuring compliance into existing policies and procedures. Wylder (2004) elaborates on this idea through the suggestion of creating a personal security plan for every employee (Wylder, 2004, pp. 100-106). This approach towards addressing the human side on information security is unique amongst the approaches reviewed in this chapter in that it directly involves the human resource department in the management of the human factor in information security. One of the important aspects of this personal security plan is that every employee would, on an annual basis, have to ”sign a notice that he understands and complies with the corporate information security manual” (Wylder, 2004, p. 103). Wylder (2004) does not elaborate on how this *understanding* should be fostered, and is thus of limited use for the purposes of this thesis. However, the uniqueness of the approach justifies its inclusion in this review.

4.5 Summary of the content analysis

The results of the qualitative content analysis conducted as part of this literature review are presented in tables 4.1 and 4.2.

Table 4.1: Summary of qualitative content analysis regarding the extent of adaptation of organizational culture theory to the specific needs of information security.

Study	**Mentions Importance of Behavioral Aspects *(Content Category)***	**Specifically mentions Information Security Culture**	**Adapts Existing Culture Theory**
Alnatheer and Nelson (2009)	X	X	
Albrechtsen and Hovden (2009)	X		
Ashenden (2008)	X	X	
Atkinson et al. (2009)	X		
Aytes and Connolly (2003)	X		
Bryce and Klang (2009)	X		

Continued on next page

Table 4.1 – continued from previous page

Study	**Mentions Importance of Behavioral Aspects *(Content Category)***	**Specifically mentions Information Security Culture**	**Adapts Existing Culture Theory**
Chang and Lin (2007)	X	X	
Chen et al. (2008)	X		
Choi et al. (2008)	X		
Cohen (1999)	X		
Cone et al. (2007)			
Da Veiga and Eloff (2009)	X	X	X
Dhillon (2007)	X	X	
Dodge et al. (2007)			
Drevin et al. (2007)		X	
Du et al. (2006)			
Finne (1996)	X	X	
Furnell (2008)		X	
Furnell et al. (2001)		X	
Furnell et al. (2002)		X	
Furnell and Thomson (2009a)	X	X	X
Furnell and Thomson (2009b)	X		
Gaunt (1998)		X	
Gaunt (2000)	X	X	
Goucher (2008)	X		
Grimson et al. (2000)			
Hagen and Albrechtsen (2009)	X	X	
Hentea (2005)	X	X	
Herold (2005)	X		
Hu and Meinel (2004)			
Johnson (2006)	X	X	
Kabay (2002)	X	X	
Katsikas (2000)			
Knapp et al. (2006)	X	X	
Kraemer et al. (2009)		X	
Kritzinger and Smith (2008)		X	
Kruger and Kearney (2006)	X	X	
Kruger and Kearney (2008)	X		

Continued on next page

Table 4.1 – continued from previous page

Study	Mentions Importance of Behavioral Aspects *(Content Category)*	Specifically mentions Information Security Culture	Adapts Existing Culture Theory
Layton (2005)	X		
Leach (2003)	X	X	
May (2008)	X	X	
Mitchell et al. (1999)	X		
Mitnick and Simon (2002)	X		
Mitnick and Simon (2006)	X		
NIST 800-16 (1998)	X	X	
NIST 800-50 (2003)	X		
OECD (2002)	X	X	
Power and Forte (2006a)	X	X	
Power and Forte (2006b)	X		
Puhakainen (2006)	X	X	
Rezgui and Marks (2008)	X	X	
Rheea et al. (2009)	X		
Roper et al. (2005)	X		
Rudolf et al. (2002)	X		
Ruighaver et al. (2007)	X	X	
Schlienger and Teufel (2003)	X	X	
Schultz (2004)			
Sharma and Sefchek (2007)			
Shaw et al. (2009)	X	X	
Siponen (2000)	X	X	
Siponen (2001)	X		
Theoharidou et al. (2005)	X		
K. Thomson and Von Solms (2005)	X	X	
K. Thomson and Von Solms (2006)	X	X	
K. Thomson et al. (2006)	X	X	X
Valentine (2006)			
Van Niekerk and Von Solms (2004)	X	X	
B. Von Solms (2000)	X	X	
B. Von Solms (2006)	X	X	
R. Von Solms and Von Solms (2004)	X	X	

Continued on next page

Table 4.1 – continued from previous page

Study	**Mentions Importance of Behavioral Aspects *(Content Category)***	**Specifically mentions Information Security Culture**	**Adapts Existing Culture Theory**
Vroom and Von Solms (2004)	X	X	
Werlinger et al. (2008)		X	
White House (2003b) and White House (2003a)		X	
Williams (2008)	X	X	
Wylder (2004)			

Table 4.2: Summary of qualitative content analysis determining the extent of the use of formal pedagogics in the creation of information security educational content.

Study	**Formal Approach to Creating Learning Content *Pedagogics***	**Mentions use of a Learning Taxonomy**	**Uses Technology and/or E-Learning for content Delivery**
Alnatheer and Nelson (2009)			
Albrechtsen and Hovden (2009)			X
Ashenden (2008)			
Atkinson et al. (2009)			X
Aytes and Connolly (2003)	X		
Bryce and Klang (2009)			
Chang and Lin (2007)			
Chen et al. (2008)	X		X
Choi et al. (2008)			
Cohen (1999)			
Cone et al. (2007)			X
Da Veiga and Eloff (2009)			

Continued on next page

Table 4.2 – continued from previous page

Study	**Formal Approach to Creating Learning Content *Pedagogics***	**Mentions use of a Learning Taxonomy**	**Uses Technology and/or E-Learning for content Delivery**
Dhillon (2007)			
Dodge et al. (2007)			
Drevin et al. (2007)			
Du et al. (2006)	X		X
Finne (1996)			
Furnell (2008)			
Furnell et al. (2001)			X
Furnell et al. (2002)			X
Furnell and Thomson (2009a)			
Furnell and Thomson (2009b)			
Gaunt (1998)			
Gaunt (2000)			
Goucher (2008)			X
Grimson et al. (2000)			X
Guenther (2001)			X
Hagen and Albrechtsen (2009)	X		X
Hentea (2005)	X		
Herold (2005)	X		X
Hu and Meinel (2004)	X		X
Johnson (2006)			X
Kabay (2002)			
Katsikas (2000)	X		
Knapp et al. (2006)			
Kraemer et al. (2009)			
Kritzinger and Smith (2008)			
Kruger and Kearney (2006)	X		X
Kruger and Kearney (2008)	X		
Layton (2005)			
Leach (2003)			
May (2008)			X
Mitchell et al. (1999)			
Mitnick and Simon (2002)			

Continued on next page

Table 4.2 – continued from previous page

Study	**Formal Approach to Creating Learning Content *Pedagogics***	**Mentions use of a Learning Taxonomy**	**Uses Technology and/or E-Learning for content Delivery**
Mitnick and Simon (2006)			
NIST 800-16 (1998)	X		
NIST 800-50 (2003)	X		X
OECD (2002)			
Power and Forte (2006a)			X
Power and Forte (2006b)			
Puhakainen (2006)			
Rezgui and Marks (2008)			
Rheea et al. (2009)			
Roper et al. (2005)			
Rudolf et al. (2002)			X
Ruighaver et al. (2007)			
Schlienger and Teufel (2003)			
Schultz (2004)			
Sharma and Sefchek (2007)	X		X
Shaw et al. (2009)	X		X
Siponen (2000)	X		
Siponen (2001)			
Theoharidou et al. (2005)			
K. Thomson and Von Solms (2005)			
K. Thomson and Von Solms (2006)		X	
K. Thomson et al. (2006)			
Valentine (2006)	X		
Van Niekerk and Von Solms (2004)	X		X
B. Von Solms (2000)			
B. Von Solms (2006)			
R. Von Solms and Von Solms (2004)			
Vroom and Von Solms (2004)			
Werlinger et al. (2008)			
White House (2003b) and White House (2003a)			
Williams (2008)			

Continued on next page

Table 4.2 – continued from previous page

Study	**Formal Approach to Creating Learning Content *Pedagogics***	**Mentions use of a Learning Taxonomy**	**Uses Technology and/or E-Learning for content Delivery**
Wylder (2004)			

A total of 75 sources were included in the review conducted in this chapter. A summary of the results of the qualitative content analysis is presented in table 4.3. The majority of the reviewed sources acknowledge the importance of the behavioral aspects of the human factor in information security. The fostering of an information security culture, as a way to address the behavioral aspects of the human factor in information security, is also widely acknowledged. However, only 3 of the reviewed sources **adapt** the generic definition of organizational culture to be more specific to the needs of information security. This clearly *demonstrates the need for the first research objective of this thesis*, namely to provide a model to specifically define an information security culture, as discussed in section 1.7. The results also show that less than a quarter of the reviewed approaches is based on, or recommends the use of, a formal, pedagogically sound, approach for the creation of information security educational material. One approach which could possibly improve the quality of information security educational content, is the use of a learning taxonomy. Only one of the reviewed sources mentioned the use of such a taxonomy. This demonstrates the relevancy and significance of *the second research objective of this thesis*, namely to demonstrate how a learning taxonomy can be used to design and develop information security educational material.

Finally, despite the fact that the field of information security has its roots in technology, very few of the current approaches towards dealing with the human factors in information security leverages/or recommends the use of technology in delivering educational content. This demonstrates the relevancy and significance of *the third research objective of this thesis*, to demonstrate how technology can be used in a pedagogically sound way as a channel for the delivery of learning content.

Topic evaluated	**Number of Sources**	**Percentage of Total**
Acknowledges the importance of the behavioral aspects of the human factor in information security	56	74.6 %
Mentions the need for an information security culture	43	57.3 %
Adapts the *generic* definition for organizational culture to be specific for information security	3	4 %
Uses and/or proposes a formal pedagogical approach to create information security educational content	17	22.7 %
Mentions the use of a *learning taxonomy* to design information security educational content	1	1.3 %
Advocates and/or mentions the use of technology based (e-learning) media channels to deliver information security educational content	22	29.3 %

Table 4.3: Summary of results for the qualitative content analysis of literature sources

4.6 Conclusion

This chapter provided a detailed literature review of current approaches towards the human factor in information security. An extensive overview of current approaches was provided. The purpose of this overview was to provide insight into *current thinking* in the field of study. The overview was done in conjunction with a qualitative content analysis of the reviewed approaches. The primary purpose of this content analysis was to clearly establish the need for, and hence the relevance of, the research objectives of this thesis. The analysis showed a clear need for these objectives. Firstly, it showed that very few current authors adapted the *generic* model, as presented by Schein (1999a, pp. 15-16), which is commonly used to define organizational culture, *to be specific to the needs of information security.* Such an adaptation is the first objective defined in section 1.7. Secondly, it was found that no current authors used a learning taxonomy during the planning/design of information security educational programs. The second objective of this thesis, namely to *demonstrate how the use of a learning taxonomy can be used to add pedagogical rigor to information security educational programs*, is thus relevant. Thirdly, the analysis showed that less than a third of current approaches advocates *any* form of electronic delivery channel for the delivery of information security education. The third objective, which is to *demonstrate the suitability of e-learning as a delivery medium for organizational information security educational programs*, is thus also relevant. It can be argued that the relevance of the final research objective listed in section 1.7, which is to *demonstrate how the various elements contributed by this thesis integrates into existing transformative change management processes for the fostering of an organizational information security culture*, is a natural extension of the first three and would be necessary in order to show the relationship between the first three objectives. Having established the relevance of the research objectives, the remainder of this thesis will focus on addressing these research objectives. The next chapter will address the first of the listed research objectives, namely, to adapt the generic definition of organizational culture to the specific needs of an information security culture.

Chapter 5

INFORMATION SECURITY CULTURE

This chapter firstly examines corporate culture. It defines corporate culture and then expands the definition of corporate culture towards a specific definition for information security culture. Finally, a conceptual model of information security culture is presented in order to facilitate improved understanding of such a culture.

5.1 Introduction

Most current information security 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 culture of information security, by instilling the aspects of information security in every employee as a *natural* way of performing his or her daily job (B. Von Solms, 2000). Studies have indicated that the establishment of an information security culture in the organization is desirable for effective information security (B. 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). In order to better understand exactly *what* an information security culture is, it is necessary to first understand the concept of culture in general, and then the more specific idea of an organizational culture.

As mentioned in chapter 3, The American Heritage Dictionary of the

English Language (2000) defines a culture as:

- 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 first 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. Such an approach would also require a formal definition of exactly what an information security culture is. This thesis already presented an informal definition of such a culture. However, since failure to pay sufficient attention to behavioral theories is one of the primary weaknesses of current security education programs (Siponen, 2001), this thesis will use a more formal definition of corporate culture from the management sciences, as presented by Schein (1999a, p. 16). The aim of this chapter is to firstly adapt the ”generic” model which Schein (1999a) uses to define corporate culture, to a model which is more specific to the needs of information security culture. Secondly, this chapter will present a conceptual model, based on the adapted definition, to facilitate improved understanding of an information security culture. Since, the aim of establishing an information security culture would be to manage employee behavior, it would be sensible to also "borrow" the necessary methodologies and/or definitions from the human and social sciences.

5.2 Research Methodology and Process

This chapter adapts the *generic* model which is used to define organizational culture, as presented by Schein (1999a, pp. 15-16), to the specific needs of information security. The adapted model is then used as basis for a conceptual model which aims at to facilitate improved understanding of an information security culture. The work in this chapter is based on qualitative, or phenomenological-, research methods, as described in Creswell (1998), as well as the guidelines for *design science*, as described by Hevner et al. (2004). The process followed should thus be seen as "an inquiry process of understanding based on distinct methodological traditions of inquiry that explore a social or human problem" (Creswell, 1998, p. 15). The research presented here does not attempt to define *new* knowledge, but rather to provide a more in-depth understanding of the phenomenon described as "information security culture".

In order to achieve this aim a conceptual model was developed over a period of three years. The primary methodology followed in the design of this model was *design science*, as discussed by Hevner et al. (2004). Design science is "fundamentally a problem solving paradigm" (Hevner et al., 2004). The following outline demonstrates how the design process followed for the work in this chapter adheres to the guidelines provided by Hevner et al. (2004):

- **Guideline 1: Design as an Artifact**. The developed conceptual model satisfies all the requirements of a valid artifact as described by Hevner et al. (2004).

- **Guideline 2: Problem Relevance**. The need for a model that specifically defines information security culture, as opposed to the generic model of organizational culture used in most current literature, was established in section 4.5.

- **Guideline 3: Design Evaluation**. The design was evaluated by means of argument, as discussed in Mason (1996, pp. 187-189), and the utility of the design has been illustrated by means of examples.

- **Guideline 4: Research Contributions**. The designed model, which *defines* an information security culture, is the primary contribution of the design process. This model was accepted for publication in the journal *Computers & Security* as Van Niekerk and Von Solms (2010).
- **Guideline 5: Research Rigor**. Strict adherence to the guidelines provided by Hevner et al. (2004), as well as adherence to guidelines for phenomenological research methods, as described in Creswell (1998), ensured the research rigor of the design process.
- **Guideline 6: Design as a Search Process**. The process through which the model was designed occurred over a 3 year period. An initial design was was created and argued. This initial design was then presented at the Information Security South Africa conference as Van Niekerk and Von Solms (2006b). Based on the feedback received from both reviewers and the audience at this conference the design was further refined and submitted to the Journal of Computers & Security. This version of the design went through four review and improvement cycles before it was finalized and published as Van Niekerk and Von Solms (2010).
- **Guideline 7: Communication of Research**. As mentioned above, the design was published as Van Niekerk and Von Solms (2010). This satisfies the criteria for communicating the research.

5.3 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 therefore 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).

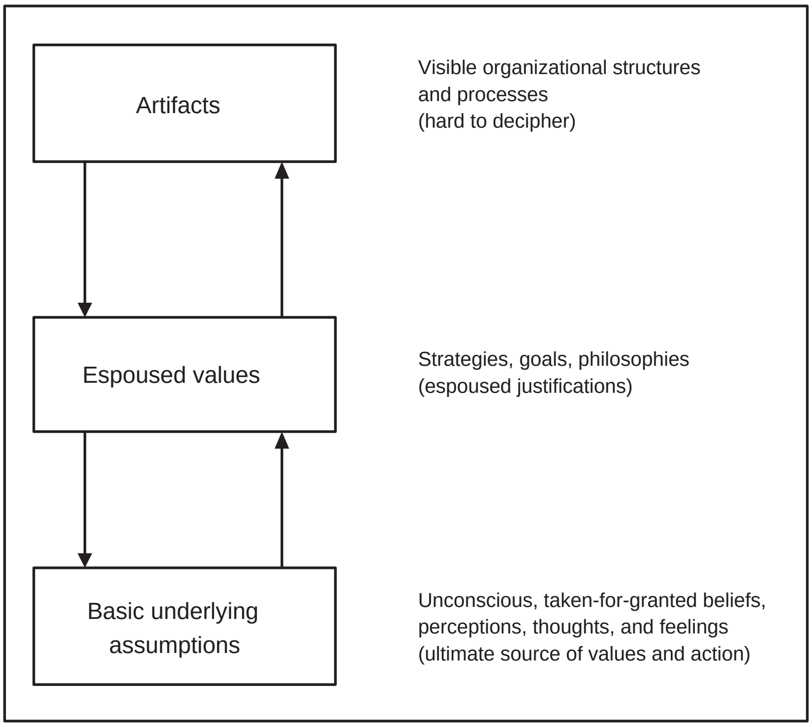

Artifacts
Visible organizational structures and processes (hard to decipher)
Espoused values
Strategies, goals, philosophies (espoused justifications)
Basic underlying assumptions
Unconscious, taken-for-granted beliefs, perceptions, thoughts, and feelings (ultimate source of values and action)

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

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.

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 day running of the organization depend on the shared tacit assumptions between the employees of that organization.

Level Three: Shared Tacit Assumptions (Basic Underlying Assumptions)

In any successful organization, *shared tacit assumptions* will eventually develop. 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 *espoused 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.

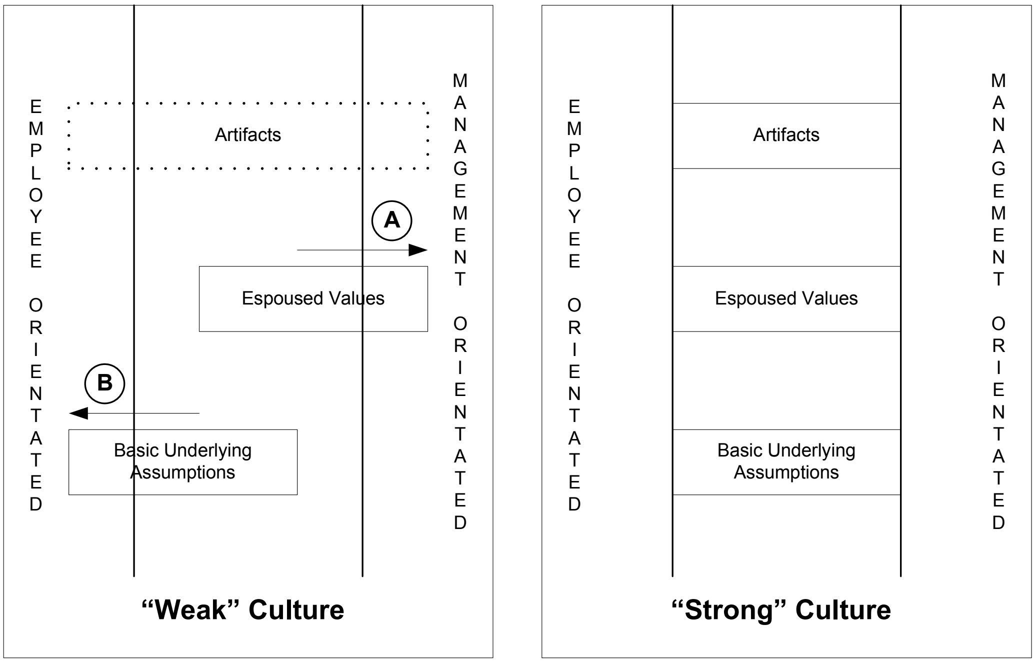


Figure 5.2: The Effect of the Combination of Culture Levels

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 Figure 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 Figure 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 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, are 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 (Van Niekerk & Von Solms, 2010). An information security culture's definition would thus deviate slightly from the standard definition for corporate culture (Van Niekerk & Von Solms, 2010).

5.4 Information Security Culture

In "normal" definitions of organizational culture, the relevant job-related knowledge is generally ignored, because it can be assumed that the average employee would have the requisite 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. It **cannot be assumed** that the average employee has the necessary knowledge to perform his/her job in a secure manner. 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** normal activity in a secure manner. Information security knowledge, or a lack thereof, could therefor be seen as a fourth level to an information security culture that will affect each of the other three layers. For example:

Artifacts: Artifacts are *what actually happens* in the organization. Without the necessary skills and proficiencies, it would be impossible to perform information related tasks securely. Thus, for the day-to-day task to happen in a secure way, the users would have to have sufficient knowledge of **how** to perform their tasks securely.

Espoused Values: 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 in order to adequately address the organization's security needs.

Shared Tacit Assumptions: This layer consists of the beliefs and values of employees. If such a belief should conflict with one of the espoused values, knowing **why** a specific control is needed, might play a vital role in ensuring compliance (Schlienger & Teufel, 2003).

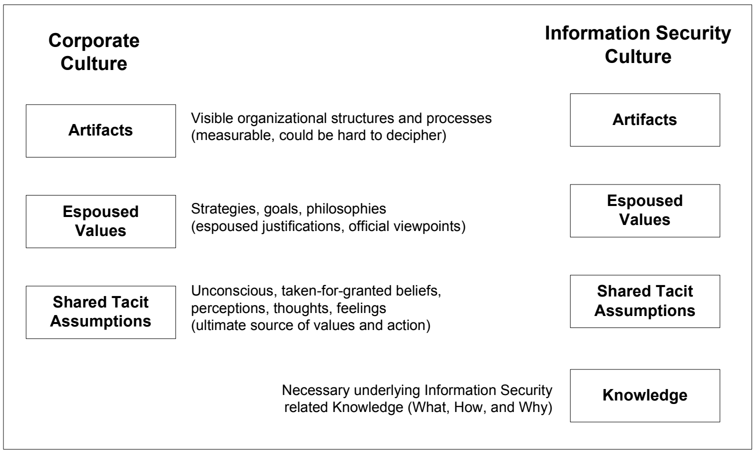

Corporate Culture
Information Security Culture
Artifacts
Visible organizational structures and processes (measurable, could be hard to decipher)
Artifacts
Espoused Values
Strategies, goals, philosophies (espoused justifications, official viewpoints)
Espoused Values
Shared Tacit Assumptions
Unconscious, taken-for-granted beliefs, perceptions, thoughts, feelings (ultimate source of values and action)
Shared Tacit Assumptions
Necessary underlying Information Security related Knowledge (What, How, and Why)
Knowledge

Figure 5.3: Levels of Culture (adapted from Schein, 1999, p. 16)

It should be clear that in an information security culture, knowledge **underpins** and **supports** all three the "normal" levels of corporate culture. Without adequate knowledge, information security cannot be ensured. The co-dependency between the three "normal" levels of an organization's information security culture, and knowledge, the "fourth level", implies that each of these four levels will have an impact on how "secure", or desirable, the overall information security culture will be. The first part of the model presented in this chapter is thus an adaptation of Schein's model. This adaptation incorporates the underlying need for information security related knowledge into Schein's model. Knowledge is added as a fourth level of culture that is specific to an information security culture. This adaptation is necessary because in an information security culture the requisite knowledge **cannot be assumed to be present**. Figure 5.3, provides a graphical exposition of this adaptation. In this presented conceptual model, knowledge is dealt with as an additional level to culture, as opposed to viewing knowledge as a sub-component of each of the original three levels. This is done solely because modeling knowledge as an additional level makes it easier to clearly show the effect that knowledge, or a lack thereof, would have on the overall information security culture.

In order to ensure an adequate level of information security knowledge, international standards such as ISO/IEC 17799 (ISO/IEC 17799, 2000) recommend the creation of an organizational information security awareness campaign. Awareness campaigns address the problems that a lack of knowledge could lead to. These campaigns help to create a culture of information security, by instilling the aspects of information security in every employee as a natural way of performing his or her daily job (B. Von Solms, 2000). Awareness campaigns are **the** key elements in ensuring that the knowledge level of an information security culture is of adequate "strength".

Before the interactions between the above levels of an information security culture can be examined in more depth, a final "tool" is needed. The conceptual model presented later in this chapter also needs to borrow the concept of *elasticity* from the economical sciences.

5.5 Elasticity in Information Security Culture

Elasticity is a general economic concept that measures the *change in one variable caused by changes in other, related variables* (Acs & Gerlowski, 1996, p. 49). In other words, elasticity measures how *sensitive* a variable is *to change* in another variable. In the presented model, the concept of elasticity will be borrowed, but instead of attempting to **measure** the change the concept will simply be used to explain the fact that change will be inherent in any such system and that the speed at which such change takes place depends on the *degree of elasticity* in the system. In order to provide more clarity of exactly what is meant by elasticity, another basic idea will first be borrowed from the economic sciences. Figure 5.4 shows a basic supply and a basic demand curve. According to economic theory (Acs & Gerlowski, 1996, p. 45) the market will be in *equilibrium* if the quantity of goods or services demanded in the market is matched perfectly by the quantity of goods or services supplied in this market. In such a system, assuming all other variables are fixed, the price that could be asked for the goods or services would be perfectly static **and predictable**.

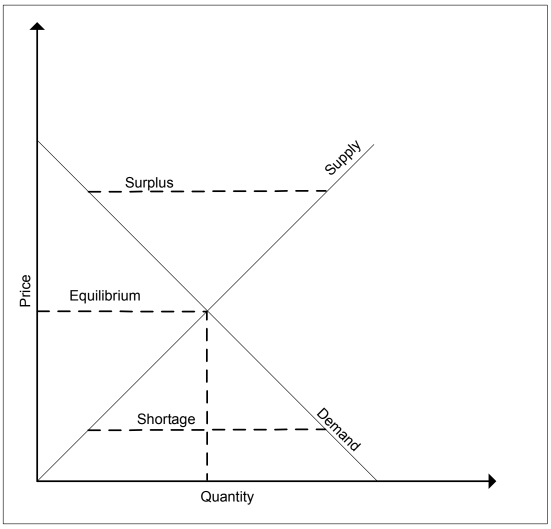


Figure 5.4: Market Equilibrium. Adapted from (Acs & Gerlowski, 1996, p. 47)

If, however, one of the variables in such a market was to change, for example if an increase in the quantity of goods or services demanded was to occur, the equilibrium would be disturbed. In such a case the other variable, the quantity of goods or services supplied would have to increase to match the increase in demand in order to bring the system back into equilibrium. While this situation of *disequilibrium* exists, the price that could be asked for the goods or services supplied, would be more dynamic and **difficult to predict**. In Figure 5.5, the price could fall anywhere in the shaded area, due to the increase in demand.

The term **elasticity** is used in economics to describe the relationship, shown in the above system, whereby increased demand would **cause** an increase in supply to eventually bring the system back into equilibrium. How-

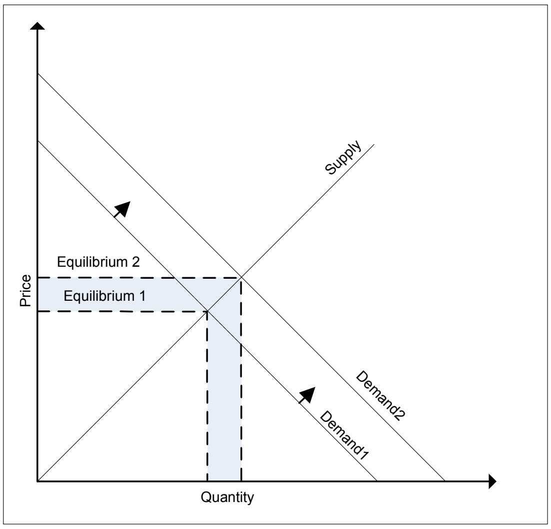


Figure 5.5: Change in Equilibrium caused by Increased Demand. Adapted from (Acs & Gerlowski, 1996, p. 48)

ever, not all systems would have the same inherent *degree of elasticity*. Elasticity could in fact range from systems that are *infinitely elastic* to systems that are completely *inelastic*. In an infinitely elastic system, shown in Figure 5.6, an increase in supply would have no effect on either the demand or the price people would be willing to pay. Figure 5.6 thus does not even show the supply curve since its position in such a perfectly elastic system is irrelevant in determining the price. On the other hand, in a completely inelastic system, shown in Figure 5.7, the variables would be "locked together". The supply and demand would thus always stay in equilibrium (Acs & Gerlowski, 1996, p. 51). An example of such an inelastic system would be certain types of life saving medicines. People who need such medicines would be willing to pay **any** price for such medicines. For the purposes of this chapter it is also important to note that in such an inelastic system consumers would be willing to pay any price but can only do so *if they have the necessary means.* Without the necessary means even consumers who are willing to pay any price would still be unable to do so.

A very **similar** situation to the one demonstrated above also exists when one looks at the human factors in an organization's information security environment. As discussed earlier, two of the basic "levels" of an information security culture would be the company's espoused values and the employees'

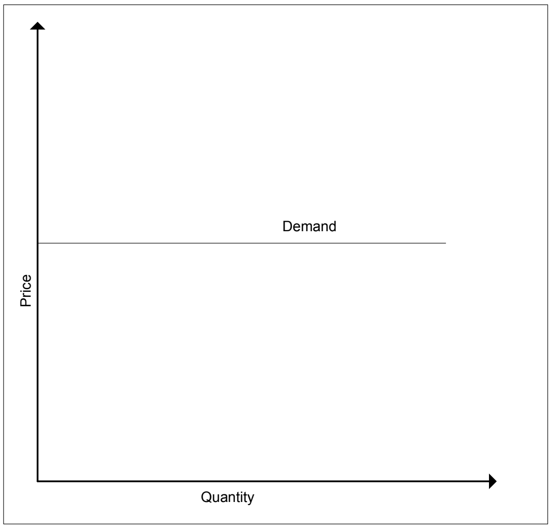


Figure 5.6: Perfectly Elastic Demand Curve. Adapted from (Acs & Gerlowski, 1996, p. 52)

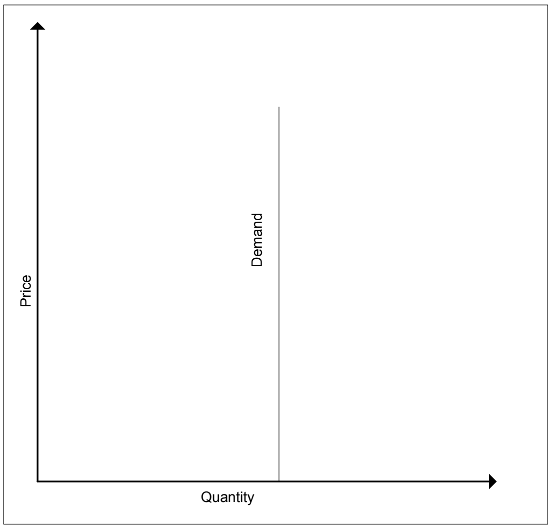


Figure 5.7: Perfectly Inelastic Demand Curve. Adapted from (Acs & Gerlowski, 1996, p. 52)

shared tacit assumptions. To a certain extent, it can be argued that the policies and procedures comprising the espoused values in an information security culture are an indication of how much security management is "demanding" from employees. Similarly, the shared tacit assumptions can be seen as a reflection of how much "compliance" employees are willing to "supply". If one were to model these two "supply" and "demand" curves, the intersection of these curves would be an indication of the actual amount of effort employees are willing to give. In other words, the "price" in this case would be the measurable employee participation in the organization's security efforts. Similarly, having the requisite knowledge to be able to participate in these security efforts is analogous to having the means to pay the required price. Such a system is modeled in Figure 5.8. If the management expectations are in perfect equilibrium with the employees' shared tacit assumptions, the resulting effort employees expended on behalf of the organization's information security would be perfectly predictable (Figure 5.8). Should management expect more than employees are willing to provide, it would be less easy to predict the actual amount of effort employees would expend towards the overall security goals (Figure 5.9). It should also be clear that employees who are in fact willing to perform their security related roles would only be able to do so if they have the requisite knowledge.

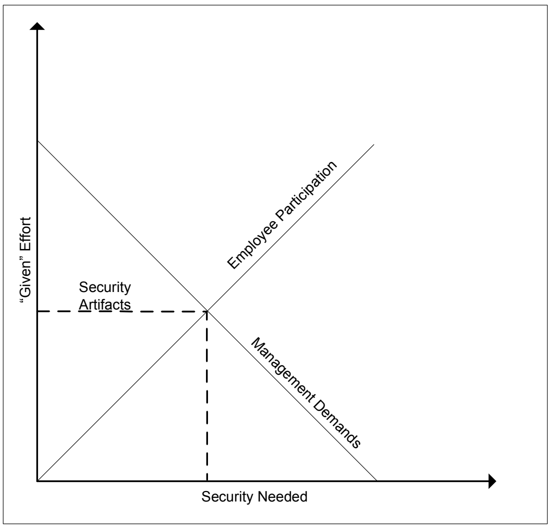


Figure 5.8: Management Expectations in Equilibrium with Employees Security Contribution. Adapted from (Acs & Gerlowski, 1996, p. 47)

In an information security culture there exists a causal relationship between the artifact level and the other three levels. In other words: the visible artifacts or, "how the employees *actually* behave towards information security", is caused by the combined effects of the espoused values, the shared tacit assumptions and the underlying information security knowledge. In Figure 5.8 the artifact level is represented by the intersection of the lines. In

Figure 5.9 the artifact level is represented by the shaded area between the two possible intersection points. This reflects the fact that it would be difficult to predict how employees will actually behave (artifacts) in a scenario where management demands (espoused values) and the effort employees are willing (shared tacit assumptions), or able (knowledge), to supply are not in equilibrium. In such a causal relationship elasticity plays an important role. More "demanding" espoused values will have an elastic effect on the artifacts, and will require a matching increase in the shared tacit assumptions and/or the knowledge level(s). Thus, if an organization's management increases the "strength" of the organization's security related policies and procedures, the "demand" (security needed) will increase in Figures 5.8 and 5.9. Such an increase will in turn require an increase in how much "security effort" employees are willing to give, or an increase in the security related knowledge of employees, or an increase in both. Without such matching increases in the other levels of the security culture, the culture will not be in equilibrium and it would thus become more difficult to predict the resulting employee behavior (artifacts).

In order to simplify the representation of the elasticity concept, it should be noted that the dynamic system represented in Figures 5.8 and 5.9 currently does not explicitly show the knowledge level. The knowledge level should, however, be assumed present in all cases. As mentioned above, this level can be seen as representing the ability to "pay" the demanded "price", and as such will have an equally important effect on the resulting employee behavior (artifacts) as the other two levels. The conceptual framework presented in the rest of this chapter will attempt to clarify this causal relationship between the artifact level and the other three levels of an information security culture.

5.6 Information Security Culture: A Conceptual Model

The overall effect of an organization's information security culture can be seen as an accumulation of the effects of each of the culture's underlying levels. Each of these levels can either positively or negatively influence the information security culture. In order to clearly demonstrate the interactions

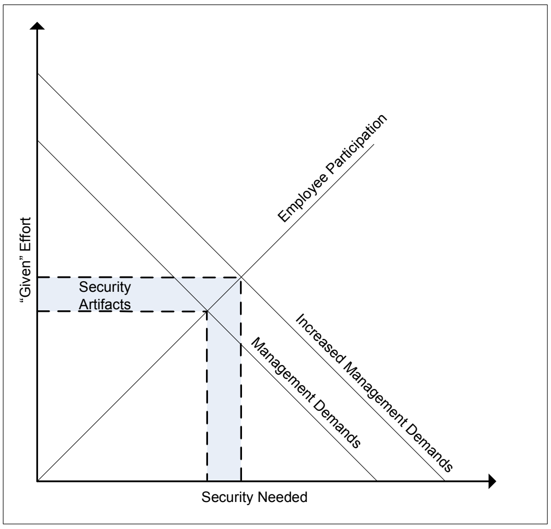
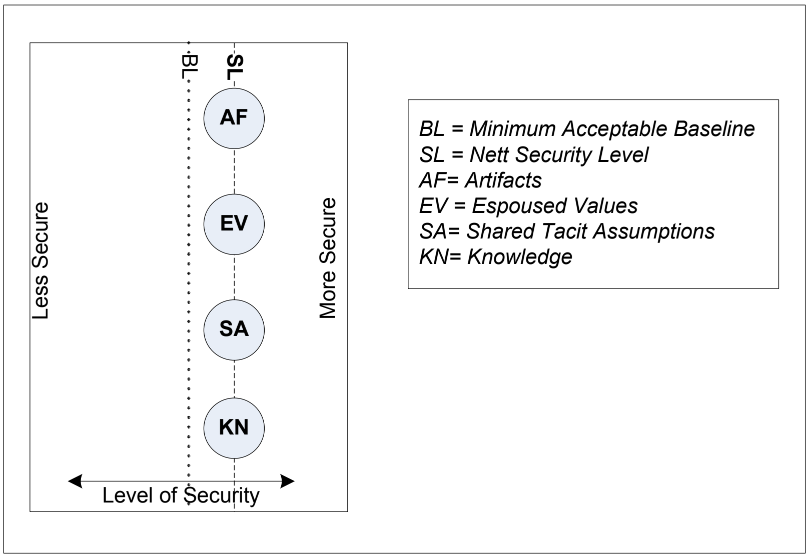


Figure 5.9: Increased Management Expectations require Increased Employee Participation. Adapted from (Acs & Gerlowski, 1996, p. 48)



BL = Minimum Acceptable Baseline
SL = Nett Security Level
AF= Artifacts
EV = Espoused Values
SA= Shared Tacit Assumptions
KN= Knowledge

Figure 5.10: Basic Elements of the Conceptual Framework.

between these four levels, and their effects on the overall security efforts, it is necessary to first provide a basic reference framework.

5.6.1 Basic Elements and Terminology of the Conceptual Model

The basic elements of this framework are depicted in Figure 5.10. The representation in this and subsequent Figures was chosen over the basic curves used in Figures 5.4 and 5.5, because it is easier to model all the interactions in this way, rather than adding an additional dimension to the model used to examine the concept of elasticity. The elements in Figure 5.10 can be described as follows:

- BL: Minimum Acceptable Base Line - This line indicates what would be an acceptable minimum security baseline; in other words, a culture whose net effect would meet the minimum requirements for some industry standard.

- SL: Nett Security Level - This line indicates the actual nett effect of the culture on the overall security effort. This line can be seen as the cumulative effect of the four underlying levels of the culture. The nett security level (SL) can either be more secure (to the right), less secure (to the left), or just as secure (overlapping) as the minimum acceptable baseline (BL).

- AF: Artifacts - This node represents the relative *strength* of the artifact level (AF) of the culture. If this node is to the left of the minimum acceptable baseline (BL), it indicates that the measurable artifacts are not as secure as they should be. A node to the right of the baseline (BL) would indicate artifacts that are even more secure than the acceptable minimum. A node exactly on the baseline (BL) would indicate artifacts that are just as secure as required by this baseline.

- EV: Espoused Values - This node represents the relative *strength* of the organization's espoused value level (EV). The various policies and procedures comprising this level could be more, less, or just as comprehensive than those recommended as the minimum acceptable baseline.

- SA: Shared Tacit Assumptions - This node represents the relative *strength* of the organization's shared tacit assumption level (SA). The underlying beliefs or values of the employees could be either more, less, or just as in favor of good secure practices as required by the minimum acceptable baseline.

- KN: Knowledge - This node represents how much knowledge the organization's employees have regarding information security. Employees can be more knowledgeable than a certain minimum level needed to perform their jobs securely, they could be less knowledgeable, or they could have exactly the minimum requisite level of knowledge.

As mentioned above, the horizontal alignment of the nodes representing the various cultural levels, AF, EV, SA and KN, in comparison to the minimum acceptable baseline, should be interpreted as an indication of the relative *strength* of each level. In a similar fashion, the horizontal alignment of the nodes in comparison to the same horizontal alignment of the **other** levels should be interpreted as an indication of how *stable*, or predictable, the culture is. The nett security level line (SL) is an indication of the average strength of the culture, or the nett combined effect of all four the levels. The culture depicted in Figure 5.10 should thus, firstly, be interpreted as a *strong*, or secure culture. All four levels in Figure 5.10 have a strength greater than the baseline, which also result in a nett security level that is positive, or greater than the baseline. Secondly, all four levels are perfectly aligned with each other. This results in a culture that should be completely *stable*, or predictable. One could also say that this would be perfect cultural *equilibrium*. The culture depicted in Figure 5.10 could thus be said to be the *ideal* culture in terms of information security since it is both *strong* and *stable*.

The terms *strong*, and *stable*, as used above, should not be confused as being indicative of how pervasive or resistent to change the culture might be. According to Schein (1999a, pp. 25-26), corporate culture is always strong in the sense of affecting every single aspect of daily life in an organization at a more than superficial level. Culture is also always stable, in the sense that it resists attempts at changing it. In that sense, culture is one of the most stable facets in an organization (Schein, 1999a, p. 26). When referring to an **information security culture**, the term *strong*, as used in this chapter, should be interpreted as a **desirable** culture that is conducive to information security. The term *stable*, as used in the same context, should be interpreted as an indication of how **predictable** the resulting artifacts, or nett security level of the culture would be for any specific scenario.

All of the factors mentioned above would contribute to the overall desirability of an information security culture. How *strong* and *stable* an organization's information security culture is, would depend on the interaction between the various levels of culture.

5.6.2 Interpreting the Conceptual Model

Each of the underlying cultural levels will contribute towards the overall strength and stability of such a culture. For example, if an organization has espoused values that are in line with recommended best practices for security, this would make the overall security better. Conversely, should the espoused values fail to address all relevant security related issues, the overall security would be weaker.

The combination of the espoused values, and the "elasticity effect", of the shared tacit assumptions and the user knowledge on these espoused values, results in the visible, and measurable *artifacts*. From a security viewpoint, the artifact level is a very good indication of the overall security of the organization's information, since this level reflects what *actually happens* in the day to day operations. In cases where the various levels are not in equilibrium this artifact level becomes more difficult to predict. In such cases the degree of elasticity in the specific system would determine how long it would take before the system "settles" into equilibrium. In infinitely elastic systems this equilibrium might never be attained, whilst completely inelastic systems would always be in equilibrium. In terms of the degree of elasticity in a security culture, the knowledge level also plays a very specific role in that it can act as an "inhibitor" of the elastic effect. A lack of knowledge can prevent employees who want to act securely from doing so. For the specific areas where the necessary security knowledge is lacking, this lack results in an infinite degree of elasticity in the security culture. The visible behavior (artifact level) **cannot** move towards equilibrium because the employees lack the means to provide the desired behavior.

Figures 5.11 to 5.15 show a few possible effects interactions between the various levels of culture could have on the overall state of the organization's information security.

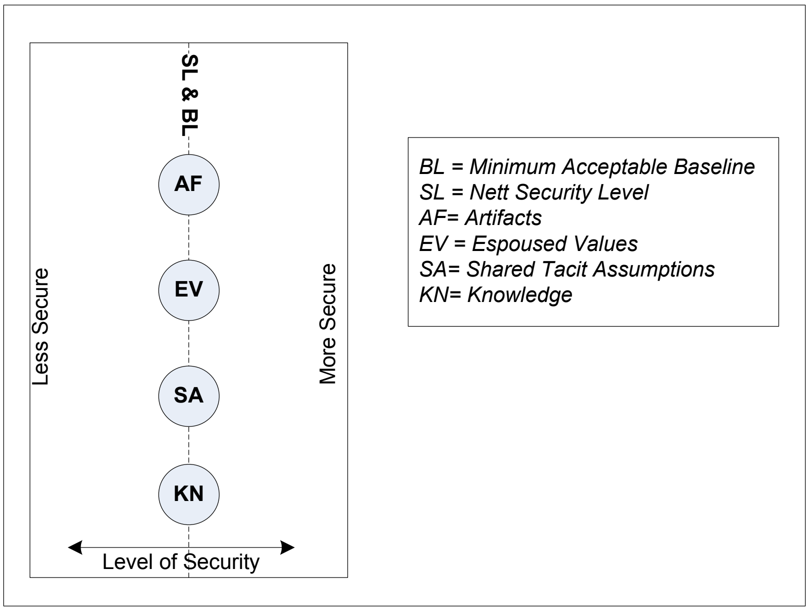


Figure 5.11: "Neutral" and Stable Culture.

The examples in Figures 5.11 to 5.15 assume that the desirability of the various levels can be quantified and normalized to the same scale. In other words, it is assumed that, for example, the desirability of the relevant espoused values can be measured and expressed as a value that indicates the contribution of this level towards the overall security. It is also assumed that the other levels can be expressed in the same way, and that the scale of such measurements can be normalized in such a way that these values will indicate the relative desirability of that level when compared to the other levels. The line marked **SL**(*Security Level*) represents the nett effect of the interactions between various levels of the culture. The five examples can be interpreted as follows:

Figure 5.11: "Neutral" and Stable. The desirability of the various levels of culture is "neutral", or average. In other words the *strength* of each level neither exceeds, nor falls short, of the minimum acceptable baseline standards. The Nett Security Level (SL) perfectly overlaps the Baseline (BL). Since all the levels have the same level of desirability, the various levels will neither negate nor reinforce the effects of other levels on the overall security. The effects of such a culture would thus be predictable and stable.

Figure 5.12: Insecure and "Mostly Stable". Both the espoused values and the shared tacit assumptions in this culture are of sufficient *strength*

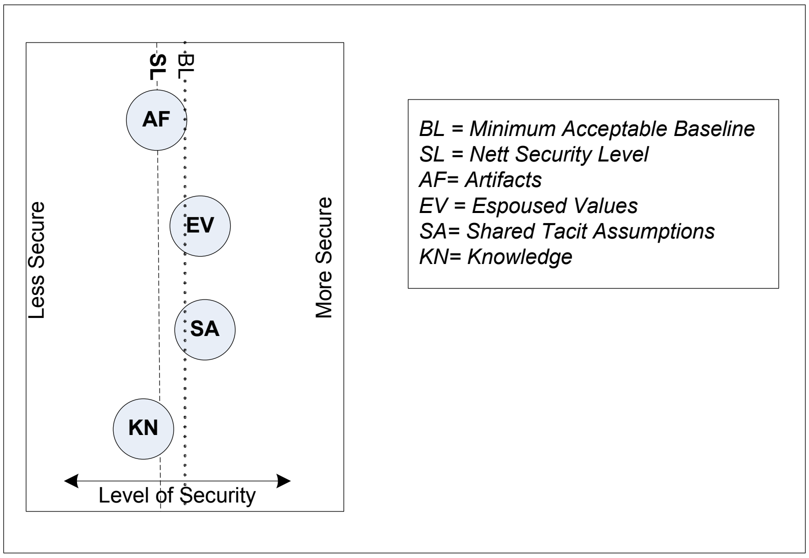


Figure 5.12: Insecure and ”Mostly Stable” Culture.

to meet the minimum acceptable baseline standard. However, in this culture, the employees do not have the requisite level of information security related knowledge. It is thus possible for the measurable artifacts to fall short of the minimum acceptable baseline. For example, either the policy dealing with a specific control might be lacking because the person(s) responsible for creating the policy lacks the necessary knowledge, or the knowledge needed to implement this control in day-to-day operations might be lacking amongst the responsible employees. In both such cases, the resulting artifacts *might* be weaker than expected. This misalignment between the various levels also means that it would be difficult to predict the exact relative strength of the overall security level. In this case one could probably assume that the culture will be mostly predictable, hence stable, because the lack of knowledge would probably not apply equally to all controls. This culture would also have an almost infinite degree of elasticity and the artifacts would thus never perfectly align with the espoused values and shared tacit assumptions. This is due to the lack of supporting information security knowledge. The lack of knowledge acts as an ”anchor” and prevents the artifacts from aligning with the other layers. By addressing the lack of knowledge the degree of elasticity inherent in this culture could be reduced. This would increase the rate at which a more desirable state is reached where the artifacts align with the shared tacit assumptions and espoused values.

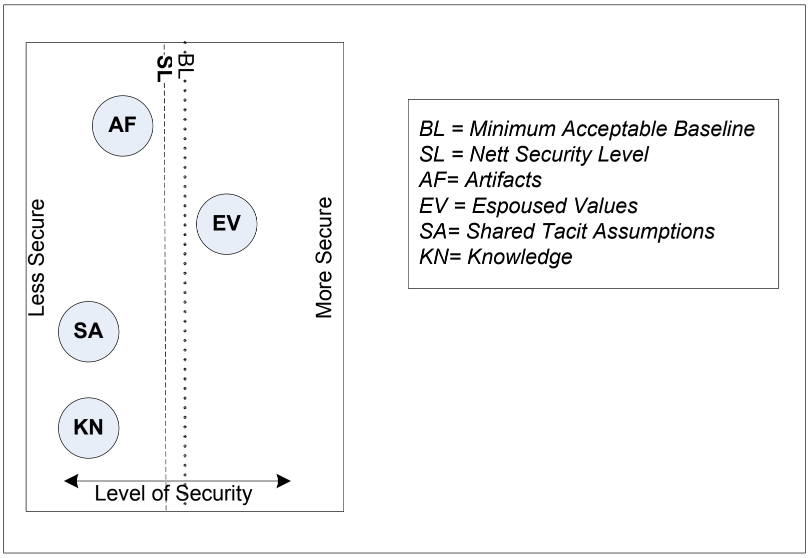


Figure 5.13: Insecure and Unstable Culture.

Figure 5.13: Insecure and Unstable. The various levels contributing to the culture are not aligned. This would mean that the nett effects of the culture might be unpredictable, due to the opposing forces at play in this culture. The espoused values are very desirable, but the users lack the requisite knowledge and do not have the desired beliefs and values, resulting in a measurable artifact level that is not secure. For any specific security control, a user may, or may not, have the requisite knowledge to fulfill his/her role in the implementation of that specific control. That same user could also agree with the relevant espoused value, or could have beliefs that are contrary to that espoused value. It would thus be very difficult to predict the nett security level of this culture. Such a culture would not be a desirable culture. In order to make this culture more desirable it would be necessary to address both the lack of knowledge and the underlying shared tacit assumptions of the employees. Once these aspects have been addressed the various levels of the culture will re-align to become more ”stable”. The rate at which this re-alignment will take place would be dependent on the degree of elasticity present in the system.

Figure 5.14: Secure and Unstable. The various levels contributing to the culture are not aligned. The espoused values are desirable, and the users have adequate knowledge. The high level of user knowledge in this case somewhat negates the fact that the users do not have the desired beliefs and

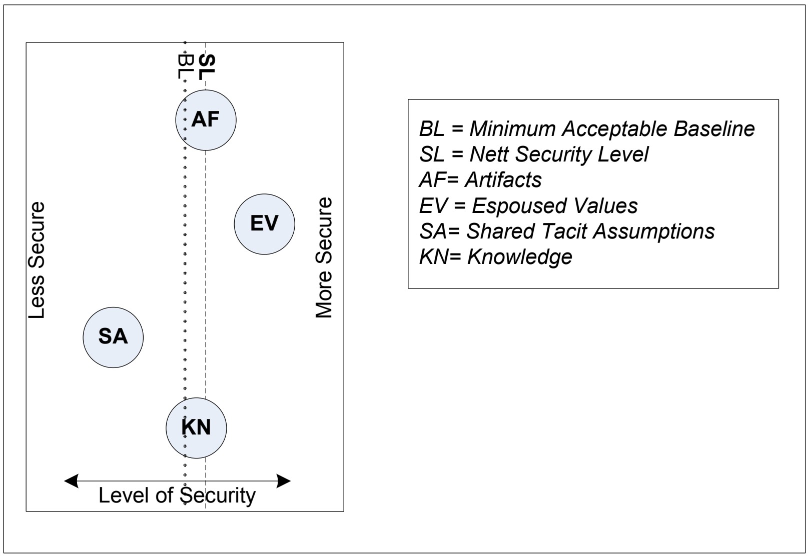


Figure 5.14: Secure and Unstable Culture.

values, resulting in an overall culture that is more secure than the minimum acceptable baseline. However, this culture should be considered not desirable, because its effects cannot always be predicted. It might be possible for the users to behave insecurely with regards to a specific security control because the specific control conflicts with their beliefs (Schlienger & Teufel, 2003). In this culture the knowledge level is already sufficient to enable employees to behave securely. However, there is still a gap between the knowledge level and the espoused values. This gap will have to be addressed before the culture could possibly align with the espoused values. The degree of elasticity in this culture could be reduced by addressing the shared tacit assumptions of employees. If employees can be convinced of the importance of their respective roles and responsibilities towards the organization's information security the culture *should* start to align itself.

Figure 5.15: Secure and Unstable. As in Figure 5.14 the various levels contributing to the culture are not aligned. In this case the figure models the scenario where the organization is small and all staff are skilled IT professionals who have both the requisite knowledge levels and the personal belief systems that enable secure behavior. In such a case it is quite likely to have a secure artifact level **despite** the fact that there is little or no espoused values. This is still not a desirable culture. Without adequate security policies (espoused values) in place, there can be no guarantees of

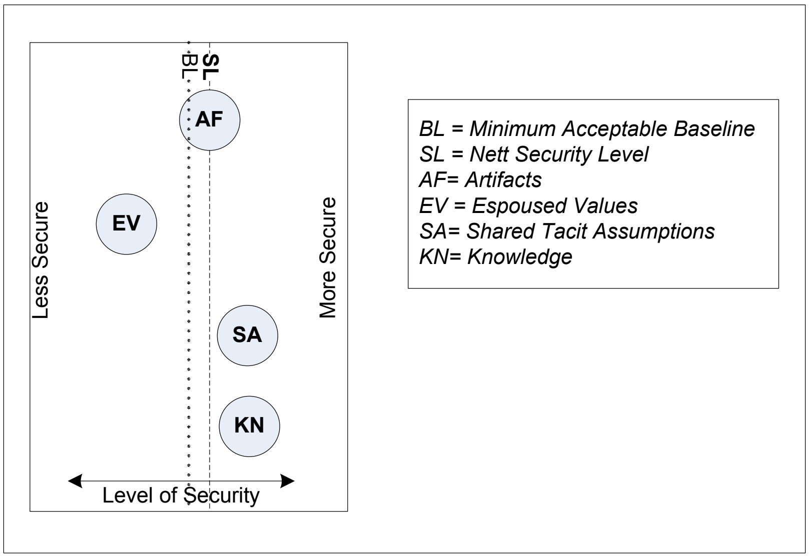


Figure 5.15: Secure and Unstable Culture.

desirable behavior. The appointment of additional staff members who might lack the underlying security knowledge can easily move the observable artifacts in this model back towards the less secure side. Unless the organization actively addresses the lack of espoused values, this culture will have an infinite degree of elasticity. The espoused values will never align themselves without active intervention.

The above examples only reflect a few possible scenarios. It should, however, be clear that the nett effect of any information security culture can be influenced, either positively, or negatively, by how ”secure” the underlying levels of such a culture is. In such a model it might also be possible to deduce the relative state of one or more of the cultural levels. For example, if the organization has *good* espoused values, but the measurable artifacts indicate *bad* security, it might be inferred that the employees lack either the required knowledge or the desired attitude. In the cultures represented by Figure 5.14 and Figure 5.15 the culture can probably be ”improved” by involving employees in the process of creating the espoused values. In both these cultures involving the employees in a ”negotiation” process when creating espoused values could reduce the ”gap” between the espoused values and shared tacit assumption layers. In both cases this would make the culture more predictable, and thus more desirable. In all cases insight into the degree of elasticity inherent in the culture can help guide decisions as to what course would be most appropriate to help manage the culture. If a system has infinite elasticity it will never align itself unless the underlying cause for this infinite elasticity is addressed. If management wants to see faster changes at the artifacts layer, i.e. how people behave on a day to day basis, steps should be taken to decrease the degree of elasticity. From a management perspective, the "perfect security culture" would be one that is completely inelastic. Such a culture will always instantly reflect changes in the espoused values of the organization.

5.7 Conclusion

This chapter suggested that, for an effective information security culture, the requisite information security knowledge amongst an organization's users could be seen as a fourth layer to Schein's (Schein, 1999a) model for corporate culture. The various interactions between the layers of such an information security culture were then presented conceptually.

The conceptual model presented showed that the nett overall effect that an information security culture would have on the organization's information security efforts would depend on the relative desirability, or *strength*, of each underlying level in such a culture. Furthermore, the alignment of the strengths of the individual underlying culture levels relative to the other levels, would to a large extent determine how predictable, hence *stable*, the effects of such a culture would be. The ideal culture would thus be one where all four underlying levels are stronger than the minimum acceptable baseline, and are also perfectly aligned relative to each other. The example in Figure 5.10 would be such an *ideal* culture.

The model also attempted to show that management demands and employees' participation are strongly interrelated. In an information security culture the visible artifacts are thus dependent on both the supporting knowledge as well as this relationship between espoused values (management demands) and shared tacit assumptions (employees' underlying beliefs and values). In any information security culture a certain degree of elasticity will be present. This elasticity will determine whether or not the shared tacit assumptions will over time align themselves to the espoused values of the organization. It will also determine how fast changes will occur if the system is not infinitely elastic. The lower the degree of elasticity in the system, the faster it would take for a possible re-alignment to happen. From a management perspective it would thus be highly desirable to reduce the degree of elasticity in such a culture as much as possible.

In its current form, the model's primary contribution is at a *conceptual* level where it aids in the understanding of information security culture. The current model has limited "hands-on" use. In a scenario where an organization's measurable artifacts are undesirable, a manager who is sure that the organization's espoused values are of adequate strength and who is also certain his/her staff members have adequate knowledge, might infer that the employees' beliefs and values are not in line with the espoused values. Based on the presented model, such a manager will also be able to deduce that he/she can make the artifacts easier to predict by addressing the shared tacit assumptions, for example by trying to convince the employees to buy into the espoused values. Through campaigns aimed at improving the employees' attitude towards security, management can reduce the degree of elasticity inherent in the culture and thus speed up the pace at which the measurable artifacts become more in line with the espoused values. Alternatively the espoused values could be "relaxed" to be more in line with the shared tacit assumptions, similar to the idea of adjusting the governing variables in a double-loop learning system (Smith, 2001). This might result in a culture that is slightly less secure but more predictable.

In either of the above mentioned approaches, use of the current model would only provide very vague guidance to someone wanting to manage an information security culture. In order for this model to become useful as a "hands-on" cultural management tool additional research would be required. If one could accurately quantify and normalize the various levels at play in this conceptual model it should be possible to use the model to manage specific aspects of an information security culture more precisely. The assumption, made when presenting the example, namely that the desirability of the various levels can in fact be quantified and normalized to the same scale, should by no means be taken as an assertion made by this chapter. The aim of the chapter was not to present such metrics and normalization processes but rather to show, at a certain level of abstraction, how this conceptual model could be used to reason about information security culture. It should, however, be possible to quantify and normalize the various factors for certain subsets of controls. For example, it might be possible to turn the presented conceptual model into a working model for a smaller sub-problem such as mapping the relationships between the four levels for password usage. If the required processes and metrics are developed, the conceptual framework might also play a valuable role in the management of an information security culture. For example; a metric that quantifies the actual degree of elasticity in an information security culture would be a very useful tool to have. This type of usage for the presented model could possibly be addressed by future research efforts. For the present, the contention of this thesis is simply that the conceptual model presented, *could* assist in improving the understanding of an information security culture. The work in this chapter should thus be seen as an attempt to lay a solid foundation on which future research could be built.

Finally, this chapter highlighted the important role relevant information security knowledge plays in an information security culture. From an information security viewpoint, it is vital for organizations to ensure that organizational employees have the requisite information security knowledge to perform their day-to-day activities in a secure manner. An appropriate information security educational approach is thus a vital *building block* towards the fostering of an information security culture. The next chapter will focus on a pedagogically sound approach towards the design of such an information security educational program.

Chapter 6

EDUCATIONAL DESIGN

This chapter focuses on the design of educational content for information security educational programs. The chapter firstly provides a brief overview of information security education in general. This is followed by an in-depth discussion on formal pedagogics and how these could be used in information security education. The chapter concludes by demonstrating how Bloom's taxonomy of the cognitive domain could be used as a theoretical basis for the design of information security educational content.

6.1 Introduction

The need for information security education is well established. Education is *central* to any attempt at addressing the human factor in information security. Section 3.4 of this thesis has shown that the human factor in information security consists of two inter-related, and co-dependant, dimensions, namely **knowledge** and **behavior**.

In order for an organization to have an acceptable level of information security, the users in that organization need to have both the requisite information security related knowledge and the desired *secure* behavior. Most current approaches to addressing this human factor agree that the fostering of an organizational information security culture can help to address the behavioral aspects of the human factor in information security. The previous chapter, chapter 5, focused on the concept of an organizational culture of information security. Chapter 5 also argued that the generic organizational culture model used by most current approaches to information security is not necessarily specific to the needs of information security practitioners. An adaptation to Schein's model for organizational culture was drafted and presented as a conceptual model to enhance the understanding of an information security culture. One of the primary adaptations made to Schein's model was the incorporation of knowledge as an additional level in such a culture (section 5.4). This adaptation was necessary because in an information security culture the requisite knowledge **cannot be assumed to be present**. The previous chapter also demonstrated that a lack of knowledge can effectively act as a kind of "anchor" which could prevent users from behaving in a secure manner even if every other level of the organization's information security culture is conducive to the desired secure behavior. The concept of elasticity was "borrowed" from the economic sciences to explain this effect (section 5.5). Ensuring that organizational users have the requisite information security knowledge is vital to the overall security efforts of an organization. According to Dhillon (2007, p. 7), increasing awareness of security issues is the most cost-effective information security control an organization can implement. Without adequate information security related knowledge, users cannot behave securely.

In order to convey the necessary knowledge to an organization's users, it is necessary to **educate** the users. This chapter will address issues relating to the selection/design of content for information security educational programs.

6.2 Research Paradigm and Rationale

The work in this chapter is based on qualitative, or phenomenological-, research methods, as described in Creswell (1998). This chapter should thus be seen as "an inquiry process of understanding based on distinct methodological traditions of inquiry that explore a social or human problem" (Creswell, 1998, p. 15). The research presented here does not attempt to define *new* knowledge, but rather to provide a more formalized understanding of information security *awareness*, *training* and *education*. As far as could be determined, the application of Bloom's Taxonomy, both the original and the revised versions, specifically to *information security* education has never been published before. It is the author's belief that the use of this taxonomy could improve the understanding of the pedagogical issues that **should** be considered in any educational program, amongst information security specialists.

Since education, as a field of study, is normally seen as a "human science" it was deemed fitting to also "borrow" the research paradigm used in this chapter from the humanities. Most current work dealing with information security education sees this education as a continuum consisting of three main levels, namely; awareness, training and education (Schlienger & Teufel, 2003),(Van Niekerk & Von Solms, 2004),(NIST 800-16, 1998, pp. 15-17). This continuum is used by many information security specialists when constructing information security educational campaigns. These specialists may not necessarily be educationalists. In order to ensure a rigorous research approach, this chapter will revisit all concepts it introduces, including those with a seemingly "obvious" meaning. The description and discussion of these concepts are deemed necessary because there might exist differences between the ontologies commonly adhered to by information security specialists and researchers from the educational sciences. It can be argued that for most security education programs more knowledge of the underlying theoretical background can help both practitioners and scholars to understand why a particular information security awareness approach is expected to have the desired impact on users' security behavior (Puhakainen, 2006, p. 139). It is believed that adherence to sound pedagogical principles when constructing information security educational campaigns, could improve the efficiency of such campaigns.

In order to ensure research rigor, the work in this chapter has been verified by means of peer-review and through publication at appropriate forums. An initial version of the work was presented at the Information Security South Africa conference as Van Niekerk and Von Solms (2008). This conference was chosen as an appropriate platform specifically because it is the foremost information security specific conference in South Africa and has many international attendees. Based on feedback received at this conference a second paper was prepared providing more insight into the use of Bloom's taxonomy for information security education. This second paper was presented at the World Information Security Education conference as Van Niekerk and Von Solms (2009). This conference was chosen because, in the author's opinion, it is the foremost international publication forum specific to information security education.

By demonstrating how Bloom's taxonomy of the cognitive domain can be used to introduce pedagogical rigor into the design of information security educational programs this chapter will answer the second research question posed in section 1.6. This will also meet the second research objective of this thesis as identified in section 1.7. Before demonstrating the use of Bloom's taxonomy for information security, the areas where current approaches are lacking will first be examined.

6.3 Current Information Security Awareness, Training and Education

The need for affordable and effective information security education has 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 means 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 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. The first step towards determining such a match is to delimitate the boundaries of such programs clearly.

6.3.1 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 two 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 in the next chapter.

According to ISO/IEC 27002 (2005, p. 9, section 6.2.1), "**All employees** of the organization and, where relevant, **third party users**, should receive appropriate training ... **before** access to information or services is granted". 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 ISO/IEC 27002 (2005). According to ISO/IEC TR 13335-1 (2004, p. 25), each employee should know his or her **role** and **responsibility**, his or her **contribution to ICT security**, and should be entrusted to achieving the organization's ICT security goals. It is therefore necessary to tailor the information security educational material used to the needs of the individual user.

As mentioned in 3.4.1, 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 3.4.1 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). This American standard NIST 800-16 (1998) is the only major information security standard dealing specifically with **role-based** information security education. NIST 800-16 (1998), together with NIST 800-50 (2003), is also the only current international standard that specifically deals with the creation/selection of content for information security educational programs. Section 4.4 provided a brief overview of this standard. However, due to its specific relevance to the work in this chapter, the NIST model will be examined in more depth in the next section.

6.3.2 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", together with the complementary document "Building an Information Technology Security Awareness and Training Program" (NIST 800-50, 2003), 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 consists 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. Table 6.1 illustrates such a training matrix.

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 ...							

Table 6.1: Training Matrix adapted from NIST 800-16, p. 14

The entries in the first column of each row in Table 6.1 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 **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 education 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. The following section will briefly demonstrate how such an adaptation could be made.

6.3.3 An organizational information security education matrix

For the purposes of this thesis 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 TR 13335-1 (2004), 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). The term education is used in an *encompassing sense* in this thesis because education is the highest level of the continuum. It could thus be argued that education would include aspects of both awareness and training. The use of the word awareness to also refer to programs and that includes both training and educational components could be construed to indicate a lack of rigor in the use of terminology. This will be discussed in more depth in the next section.

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.

Table 6.2 illustrates an example of how such an educational needs matrix might look.

Training Areas	Top Management		Finance				IT		
	Manage	Info Sec Officer	Manage	Accounting	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..	...	...	...	...	...	...	...	...	...

Table 6.2: Information Security ”Educational Needs Matrix”

In Table 6.2, 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 6.2 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.

From the example in Table 6.2 it should be clear that the model presented in NIST 800-16 (1998) could be used to identify the awareness, training and/or educational needs of an organization's users *to a certain extent.* Using this model an information security educationalist would, for example, be able to identify the specific controls from a standard such as ISO/IEC 27002 (2005) for which various levels of organizational users would require education. However, it is the contention of this thesis that using the NIST model exclusively, without attention to additional pedagogical theory, would not address all the needs of information security educational design. The NIST model provides guidance on the **applicability** of education/training for specific information security controls for specific user roles. However, the NIST model does not address the *exact extent* towards which such education/training should be conducted. It only provides *vague guidance* in terms of the education/training being at "beginner, intermediate or advanced level".

The following sections will briefly look at the need for more pedagogical theory in information security education and will then demonstrate how the use of a learning taxonomy could alleviate the above mentioned shortcoming of the NIST model.

6.4 The need for Pedagogics in Information Security

According to The American Heritage Dictionary of the English Language (2000) *pedagogics* can be defined as *the art of teaching.* A study of pedagogics is essentially a study of formal educational theory. Many current information security educational programs are constructed by information security specialists who do not necessarily have a strong educational background. Puhakainen (2006, pp. 33-56) reviews 59 current approaches to security awareness, most of which are **not based on pedagogical theories**. The qualitative content analysis in chapter 4 showed that only 22.7% of all approaches reviewed had **any** form of formal or pedagogical basis (section

4.3). Puhakainen (2006, p. 56) also argues that there is a need for theory-based information security education approaches. These approaches should not be only theoretical, but should also be practically effective. The nature of information security educational or awareness issues is often not understood, which could lead to programs and guidelines that are ineffective in practice (Siponen, 2000). A formally trained educationalist might, for example, raise the question whether or not **knowledge** is in fact enough. In Bloom's taxonomy, which is a well known and widely accepted pedagogical taxonomy, knowledge only comprises the very first, and lowest, level of education (Sousa, 2006, pp. 248-255). One could argue that this level of comprehension is in fact not adequate for most humans who play a role in the information security process. It is probable that security practitioners refer to **knowledge** as an all encompassing term which includes abilities at other levels of the cognitive domain. However, from an educational perspective, it would make sense to be precise in terms of exactly what level of cognition is required from users in an information security context. Especially for the purposes of designing educational content for information security campaigns. Similarly, the traditional approach of classifying the requisite information security educational needs as a continuum consisting of either awareness, training or education, might also be too simplistic.

In the current information society, educational or awareness issues affect almost all organizations. Despite this fact the nature of these programs is still not well understood and this often leads to ineffective security guidelines or programs (Siponen, 2000). Many organizations have some form of *awareness* program but often do not augment these with supporting training and/or education programs. The terms *awareness* and *education* are also often used interchangeably. It is not uncommon to hear security specialists talk about "awareness campaigns", when the campaigns actually focus on the training or education levels of the continuum. As mentioned earlier, the term knowledge only describes the lowest level of Bloom's taxonomy of the cognitive domain. From an educational viewpoint one could thus argue that *the terminology used lacks rigor*. This lack of rigor could contribute to the fact that the nature of awareness and educational issues is often misunderstood. One model that could possibly provide such rigor is Bloom's taxonomy.

Many formal learning theories that could contribute at various levels in the creation of information security educational programs exist. However, ”learning is such a complex matter that it might be impossible to conceive of a single theory broad enough to encompass all important aspects of learning and yet specific enough to be useful for instruction” (Driscoll, 2000, p. 299). Each learning theory can usually provide only one part of the overall perspective needed to ensure learning. Each of such part emphasizes specific aspects of learning, but might lack in other areas (Driscoll, 2000, p. 299). Attempting to address all the possible theories which could conceivably contribute to improving the design of information security educational content falls outside the scope of this thesis.

Instead this thesis will focus only on the use of a learning taxonomy to provide a more pedagogically sound interpretation of the educational needs of humans involved in information security processes. Bloom's taxonomy is arguably the most widely used, and best known, learning taxonomy. The rest of this chapter will thus focus exclusively on demonstrating how Bloom's revised taxonomy, as discussed in Anderson et al. (2001), could be incorporated into the design of information security educational material as a pedagogical framework.

6.5 Bloom's taxonomy of the cognitive domain

Bloom's taxonomy is the best known and most widely used learning taxonomy amongst educators today (Materna, 2007, p. 138). Bloom's model was originally developed in the 1950's and remained in use more or less unchanged until fairly recently (Sousa, 2006, p. 249). A revised version of the taxonomy was published in Anderson et al. (2001). This revised taxonomy has become accepted as more appropriate in terms of current educational thinking (Sousa, 2006, pp. 249-260). Both versions of Bloom's taxonomy consist of six levels which increases in complexity as the learner moves up through these levels. Figure 6.1 shows both versions of this taxonomy.

There are two main differences between the original and the revised versions of the taxonomy. Firstly, the revised version uses descriptive verbs for each level that more accurately describes the intended meaning of each level.

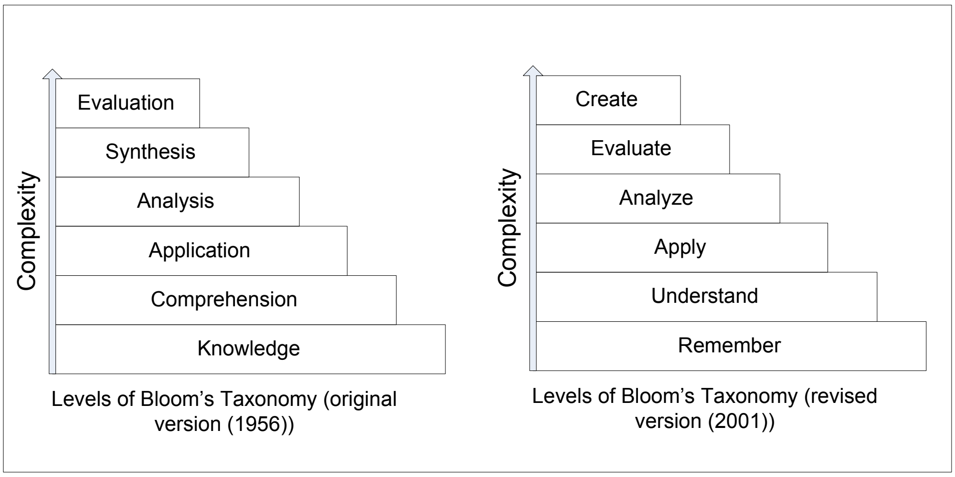


Figure 6.1: Blooms Taxonomy, Original and Revised (Adapted from Sousa (2006) pp. 249-250)

Secondly, the revised version has swapped the last two levels of the original version around. This was done because recent studies have suggested that generating, planning, and producing an original "product" demands more complex thinking than making judgements based on accepted criteria (Sousa, 2006, p. 250). The hierarchy of complexity in the revised taxonomy is also less rigid than in the original in that it recognizes that an individual may move among the levels during extended cognitive processes. This paper will focus on the revised version of the taxonomy. Wherever this paper mentions Bloom's taxonomy, it should be assumed that the revised version is intended, unless otherwise stated. The following is a brief explanation of each of the six levels of this revised taxonomy (Sousa, 2006, pp. 250-252):

- Remember: Remember refers to the rote recall and recognition of previously learned facts. This level represents the lowest level of learning in the cognitive domain because there is no presumption that the learner understands what is being recalled.

- Understand: This level describes the ability to "make sense" of the material. In this case the learning goes beyond rote recall. If a learner understands material it becomes available to that learner for future use in problem solving and decision making.

- Apply: The third level builds on the second one by adding the ability to use learned materials in *new* situations with a minimum of direction. This include the application of rules, concepts, methods and theories to solve problems within the given domain. This level combines the activation of procedural memory and convergent thinking to correctly select and apply knowledge to a completely new task. Practice is essential in order to achieve this level of learning.

- Analyze: This is the ability to break up complex concepts into simpler component parts in order to better understand its structure. Analysis skills includes the ability to recognize underlying parts of a complex system and examining the relationships between these parts and the whole. This stage is considered more complex than the third because the learner has to be aware of the thought process in use and must understand both the content and the structure of material.

- Evaluate: Evaluation deals with the ability to judge the value of something based on specified criteria and standards. These criteria and/or standards might be determined by the learner or might be given to the learner. This is a high level of cognition because it requires elements from several other levels to be used in conjunction with conscious judgement based on definite criteria. To attain this level learners need to consolidate their thinking and should also be more receptive to alternative points of view.

- Create: This is the highest level in the taxonomy and refers to the ability to put various parts together in order to formulate an idea or plan that is new to the learner. This level stresses creativity and the ability to form *new* patterns or structures by using divergent thinking processes.

In terms of recent studies on cognitive processing the lower three levels (remember, understand, and apply) describe a *convergent* thinking process. In such a process the learner will first recall information, then focus on what is known and understood in order to apply the knowledge to solve a problem (Sousa, 2006, p. 254). The upper three levels (analyze, evaluate, and create) describe a *divergent* thinking process. In such a process the learner's processing of the knowledge will result in *new insights*, or previously unknown information (Sousa, 2006, p. 254). It is important to remember that the levels of the taxonomy are fluid and overlapping (Sousa, 2006, p. 254).

In addition to these levels of the cognitive domain Anderson et al. (2001) also place major emphasis on the use of the following categorization of the knowledge dimension (Anderson et al., 2001, pp. 45-62):

- Factual Knowledge - The most basic elements the learner must know in order to be familiar with a discipline. I.e. terminology or specific details and elements.

- Conceptual Knowledge - The interrelationships among the basic elements of larger structures that enable these elements to function together. I.e. classification, categories, principles, theories, models, etc.

- Procedural Knowledge - How to do something, methods of inquiry, how to use skills, apply algorithms, techniques and methods. I.e. subject specific skills, algorithms, techniques, and methods as well as knowledge of criteria for determining when to use appropriate procedures.

- Meta-Cognitive Knowledge - An awareness and knowledge of one's own cognition. I.e. strategic knowledge, self-knowledge, knowledge about cognitive tasks, including contextual and conditional knowledge.

Activities at these six levels of the cognitive domain are usually combined with the one or more of the four types of knowledge in a collection of statements outlining the learning objectives of an educational program. Usually a *learning objective* statement will be used to create a set of *learning activities*. Learning activities are activities which help learners to attain the learning objectives. A Learning activity consist of a *verb* that relates to an activity at one of the levels of the cognitive domain, and a *noun* providing additional insight into the relationship of the specific learning objective to a category of knowledge (Anderson et al., 2001, pp. 93-109). The use of a taxonomy often assist educators in gaining better understanding of learning objectives, and activities. However, it is not always clear how this increased understanding can help the educators. Anderson et al. (2001, pp. 6-10) identify the following four "organizing questions" as the most important areas in which a taxonomy like Bloom's can assist educators:

- The Learning Question: What is the most important for learners to learn in the limited time available
- The Instruction Question: How does one plan and deliver instruction that will result in high levels of learning for large numbers of learners
- The Assessment Question: How does one select or design assessment instruments and procedures to provide accurate information about how well students are learning
- The Alignment Question: How does one ensure that objectives, instruction, and assessment are consistent with each other.

In most cases, the correct usage of a *taxonomy table* which combines elements from both the cognitive and knowledge dimensions, will allow educators to answer these question to some extent. An example of such a taxonomy table will be given later in this chapter in Table 6.5.

Educational taxonomies, such as Bloom's taxonomy, are useful tools in developing learning objectives and assessing learner attainment (Fuller et al., 2007). All well known educational taxonomies are generic. These taxonomies rely on the assumption that the hierarchy of learning outcomes applies to all disciplines (Fuller et al., 2007). Bloom's taxonomy would thus apply equally to a more traditional "subject", such as zoology, as to organizational information security education.

6.6 Bloom's Taxonomy for Information Security Education

Learning taxonomies assist the educationalist to describe and categorize the stages in cognitive, affective and other dimensions, in which an individual operates as part of the learning process. In simpler terms one could say that learning taxonomies help us to "understand about understanding" (Fuller et al., 2007). It is this level of meta-cognition that is often missing in information security education. According to Siponen (2000) awareness and educational campaigns can be broadly described by two categories, namely framework and content. The framework category contains issues that can be approached in a structural and quantitative manner. These issues constitute the more explicit knowledge. The second category, however, includes more tacit knowledge of an interdisciplinary nature. Shortcomings in this second area usually invalidate awareness frameworks (Siponen, 2000). How to really motivate users to adhere to security guidelines, for example, is an issue that would form part of this content category.

It has been shown that even in cases where users have "knowledge" of a specific security policy, they might still willfully ignore this policy because they do not understand *why* this policy is needed (Schlienger & Teufel, 2003). Answering the question "why" not only increase insight but also increases motivation (Siponen, 2000). Simply informing employees that "this is our policy", or "you just have to do it", which is often the traditional approach, is not likely to increase motivation or attitudes (Siponen, 2000). Learning is a willful, active, conscious, and constructive activity guided by intentions and reflections (Garde et al., 2007). According to most constructivist learning theories, learning should be learner-centered (Garde et al., 2007). In an organizational information security educational campaign, the learners **must** include each and every employee. It is also important to realize that the campaign has to be **successful for each and every learner** (Van Niekerk & Von Solms, 2004).

In order to ensure successful learning amongst all employees, it is extremely important to fully understand the educational needs of individual employees. According to Roper et al. (2005, pp. 27-36) managers often attempt to address the security education needs of employees without adequately studying and understanding the underlying factors that contribute to those needs. It has been argued before that educational material should ideally be tailored to the learning needs and learning styles of individual learners (Van Niekerk & Von Solms, 2004)(NIST 800-16, 1998, p. 19). One could also argue that awareness campaigns that have not been tailored to the **specific** needs of an individual, or the needs of a **specific target audience**, will be ineffective. It is in the understanding of these needs, that a learning taxonomy can play an important enabling role.

Information security specialists should use a taxonomy, like Bloom's taxonomy, before compiling the content category of the educational campaign. The use of such a taxonomy could help to understand the learning needs of the target audience better. It could also reduce the tendency to focus only on the framework category of these campaigns. For example, simply teaching an individual what a password is, would lie on the *remember*, and possibly *understand* level(s) of Bloom's taxonomy. However, the necessary information to understand *why* their own passwords are also important and why they should also be properly constructed and guarded, might lie as high as the *evaluate* level of the taxonomy. An information security specialist might think that teaching the users what a password is, is enough, but research has shown that understanding *why* is essential to obtaining buy-in from employees. It is this level of understanding that acts as a motivating factor and thus enables behavior change (Siponen, 2000)(Schlienger & Teufel, 2003)(Van Niekerk & Von Solms, 2004)(Roper et al., 2005, pp. 78-79).

The use of an educational taxonomy in the construction of information security educational programs requires that both the content and the assessment criteria for this program are evaluated against the taxonomy in order to ensure that learning takes place at the correct level of the cognitive domain. The reference point for any educational program should be a set of clearly articulated "performance objectives" that have been developed based on an assessment of the target audience's needs and requirements (Roper et al., 2005, p. 96). Correct usage of an educational taxonomy not only helps to articulate such performance objectives but, more importantly, helps the educator to correctly gauge the needs and requirements of the audience.

An example of how Bloom's revised taxonomy could be used in an information security context is supplied in Table 6.3. This example is not intended to be a definitive work, but rather to serve as an example or starting point for information security practitioners who want to use Bloom's taxonomy when constructing awareness and educational campaigns. It should however be clear that this taxonomy could easily be used to categorize most, if not all, information security educational needs effectively. Once categorized according to a taxonomy like Bloom's taxonomy, it should also be easier to find related information regarding pedagogical methods suitable to assist learners in attaining the desired level of cognitive understanding. The example in Table 6.3 demonstrates how the use of specific *terms* in the specification of a learning activity can help to ensure that the learning activity is in fact at the correct level of the cognitive domain. For example, if the activity is based purely on the learner's ability to *recognize* a specific threat, this

Level	Terms	Sample Activities
Create	imagine	Pretend you are an information security officer for a large firm. Write a report about a recent security incident.
	compose	Rewrite a given incident report as a news story.
	design	Write a new policy item to prevent users from putting sensitive information on mobile devices.
	infer	Formulate a theory to explain why employees still write down their passwords.
Evaluate	appraise	Which of the following policy items would be more appropriate. Why?
	assess	Is it fair for a company to insist that employees never use their work email for personal matters? Why or Why not?
	judge	Which of the security standards you have studied is more appropriate for use in the South African context? Defend your answer.
	critique	Criticize these two security products and explain why you would recommend one over the other to a customer.
Analyze	analyze	Which of the following security incidents are more likely?
	contrast	Compare and contrast the security needs of banking institutions to those of manufacturing concerns.
	distinguish	Sort these security controls according to the high level policies that they address.
	deduce	Which of these procedures could derive from the given policy.
Apply	practice	Use these mnemonic techniques to create and recall a secure password.
	calculate	Calculate how secure the following password is.
	apply	Think of three things that could go wrong should your password be compromised.
	execute	Use the given tool to encrypt the following message.
Understand	summarize	Summarize the given security policy in your own words
	discuss	Why should non alpha-numeric characters be used in a password?
	explain	Explain how symmetric encryption works.
	outline	Outline your own responsibilities with regards to the security of customer account information.
Remember	define	What is the definition of a security incident?
	label	Label each of the threats in the given picture.
	recall	What is social engineering?
	recognize	Which of the pictures shows someone ”shoulder surfing”?

Table 6.3: Bloom's Taxonomy for Information Security adapted from Sousa (2006, p. 251). (See also Anderson et al. (2001))

activity probably only involves cognitive skills at the remember level of the taxonomy. The next sub-section will further clarify how Bloom's taxonomy can be used in the construction of information security programs.

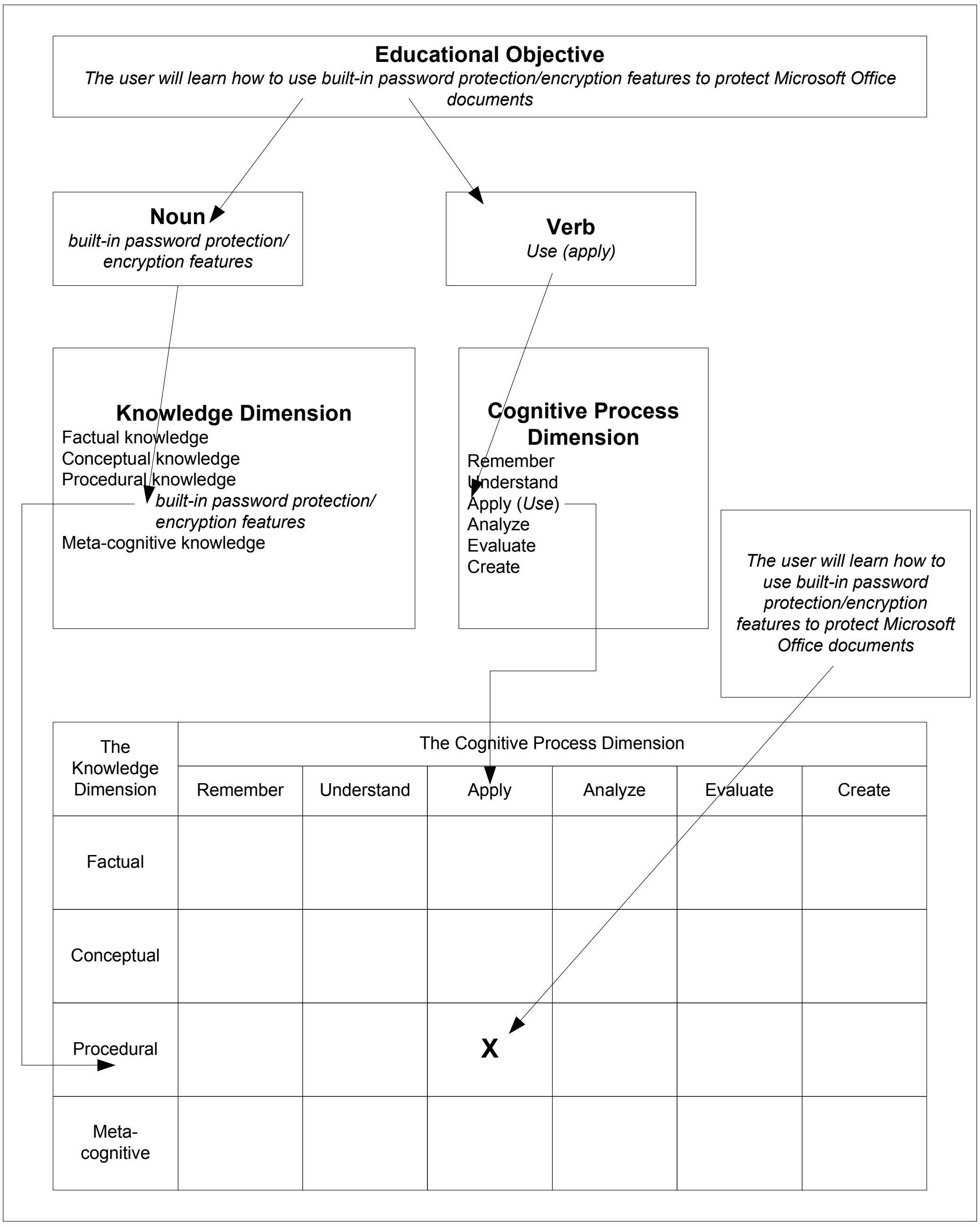
6.6.1 Using Bloom's taxonomy

When using Bloom's taxonomy to assist in the design of educational content, a simple list of activities like the one presented in 6.3 is of limited use. Usually such a list is used in combination with a *taxonomy table*. In order to clarify the use of such a taxonomy table, an abbreviated and more focused example of how the taxonomy could be used for a specific learning objective **(LO1)** will be used. This learning objective can be briefly expressed as: "Learners should be able to understand, construct and use passwords in the correct context".

Level	**Verb**	**Sample Activities**
Create	design	Write a new policy item to govern the use of passwords on company ABC's Information Systems. **(A6)**
Evaluate	critique	Critique these two passwords and explain why you would recommend one over the other in terms of the security it provides.**(A5)**
Analyze	analyze	Which of the following security incidents involving stolen passwords are more likely in our company?**(A4)**
Apply	execute	Use the appropriate application to change your password for the financial sub-system. **(A3)**
Understand	discuss	Why should non alpha-numeric characters be used in a password? **(A2)**
Remember	define	What is the definition of *access control*? **(A1)**

Table 6.4: Abbreviated and Focused Example of Password related Learning Activities based on Bloom's Taxonomy for Information Security, adapted from Anderson et al., 2001

Table 6.4 lists an abbreviated example of learning activities **(A1 to A6)**, based on this learning objective **(LO1)**. This abbreviated example, together with a taxonomy table, shown in Table 6.5, will be used to clarify the use of Bloom's taxonomy in an information security context. The use of a taxonomy table is central to the effective use of Bloom's taxonomy for the design of any educational material (Anderson et al., 2001, pp. 27-37). In order to fill such a taxonomy table the educator starts by examining each learning activity. The *noun* portion of the learning activity is used to determine which of the categories of the knowledge dimension would be the best match for the particular learning activity. A single learning activity could be classified into more than just one of the dimensions if necessary. The *verb* portion of the learning activity is used to determine at which level of the cognitive domain the activity would lie. Based on this, the particular learning activity is then mapped to the appropriate cell of the taxonomy table. An illustrated example of this process is provided in Figure 6.2.


Educational Objective
The user will learn how to use built-in password protection/encryption features to protect Microsoft Office documents
Noun
built-in password protection/ encryption features
Verb
Use (apply)
Knowledge Dimension
Factual knowledge
Conceptual knowledge
Procedural knowledge
built-in password protection/ encryption features
Meta-cognitive knowledge
Cognitive Process Dimension
Remember
Understand
Apply (Use)
Analyze
Evaluate
Create
The user will learn how to use built-in password protection/encryption features to protect Microsoft Office documents

The Knowledge Dimension	The Cognitive Process Dimension					
	Remember	Understand	Apply	Analyze	Evaluate	Create
Factual						
Conceptual						
Procedural			X			
Meta-cognitive						

Figure 6.2: How to fill the taxonomy table. Adapted from Anderson et al. (2001, p. 32)

A similar process to the one used to place learning activities into the taxonomy table is also used for the main learning objective of a learning program, and for the various assessments associated with these learning activities/learning objectives. Table 6.5 represents a completed taxonomy table for the learning objective (**LO1**) mentioned earlier, which is associated to the learning activities in Table 6.4.

The Knowledge Dimension	The Cognitive Process Dimension					
	Remember	Understand	Apply	Analyze	Evaluate	Create
Factual Knowledge	**A1**				**A6**	
Conceptual Knowledge		**Test1A** **A2**		**Test1B** **A4**	**A6**	
Procedural Knowledge			**LO1** **A3**		**A6**	
Meta-Cognitive Knowledge				**A5**		

Table 6.5: Example Taxonomy Table adapted from Anderson et al., 2001

Once such a taxonomy table has been completed, the educator can use it to identify any possible "gaps" in the intended learning program. This can be done by examining the four "organizing questions" as discussed in section 6.5. Answering the four "organizing questions" is one of the most difficult things for creators of educational matter to do. The following sub-section will briefly explain how the taxonomy table, Table 6.5, could be used to assist in answering these question for the learning activities, as shown in Table 6.3.

6.6.2 Answering the four "Organizing Questions"

Each learning activity in Table 6.3 consists of a *verb* that relates to one of the cognitive domain levels in Bloom's Taxonomy (Anderson et al., 2001, pp 67-68). Each activity also has a *noun* relating to knowledge that could be categorized as one of the four categories of knowledge. By marking the appropriate spaces in the taxonomy table for each activity, the educator can derive a lot of useful information about the "coverage" provided by the activities. As an example, the activity marked **A1** lies at the remember level of the cognitive domain and since it deals with basic subject terminology it deals with the "factual" category of knowledge. This is reflected by its positioning in Table 6.5. Each of the other activities, **A2** to **A6**, as shown in Table 6.3 has also been appropriately placed in Table 6.5. A complete information security educational program will obviously include many more activities, which would result in many more entries in the taxonomy table. Such a table does not always have to deal with an entire program, but could, like the given example, focus on a single learning objective, or even on a few related objectives.

By examining the taxonomy table the educator can easily identify areas of knowledge, or levels of the cognitive domain, that have not been covered by the learning activities. Similarly, areas where multiple activities covers the same levels of cognition and categories of knowledge can be identified. This can assist in answering the so-called ”learning question”, i.e. ”are most important activities receiving the larger share of the available resources?”. In order to design activities that will result in maximum learning, thus answering the ”learning question”, one can look for activities that involves more than just one type of knowledge. For example, in order to create a new policy item (Activity **A6**), the learner will need to know; basic terminology (factual knowledge), how items relate to each other (conceptual knowledge), and which steps to follow to create a policy (procedural knowledge). To answer the ”assessment question” the educator could choose to focus on the learning objective itself, and thus, in the example given, only use assessment methods that require the learner to apply procedural knowledge. Or the assessor might decide to focus on one or more learning activities and thus have a wider range of assessment coverage. By noting assessment activities on the same taxonomy table, the educator can ensure that the chosen assessments correspond directly to what he/she intends to assess. For example, that learners must *understand* the concept of a password (**Test1A**) and must be able to *analyze* the relative strength of a given password (**Test1B**). The table will also, at a glance, show which areas are not being assessed. Finally, given a complete taxonomy table, the ”alignment question” should be relatively easy to answer. In the given example, a clear ”disconnect” between the assessment and the learning objective itself exists. Instead of focusing on the **application, or use,** of passwords the assessments focus on the concept of what a password is, and how to determine its relative strength. Similarly, other ”miss-alignments” can be identified with the help of this taxonomy table.

As mentioned earlier, this example is not intended to be a definitive work, but rather to serve as an example or starting point for information security practitioners who want to use Bloom's taxonomy when constructing awareness and educational campaigns. It should however be clear that this taxonomy could easily be used to categorize most, if not all, information security educational needs effectively. Once categorized according to a taxonomy like Bloom's taxonomy, it should also be easier to find related information regarding pedagogical methods suitable to assist learners in attaining the desired level of cognitive understanding.

6.7 Conclusion

This chapter examined the widely used information security awareness, training and education continuum as defined in NIST 800-16 (1998). It was argued that this continuum, though useful, is not precise enough to meet all the requirements for the design of information security educational programs. Most information security professionals do not necessarily have a background in educational theory and thus require more precise guidance in the design of educational programs. This chapter suggested that information security educational programs would be more effective if they adhered more strictly to pedagogical principles. It was specifically suggested that the common categorization of security educational needs into the broad categories of awareness, training, and education, is not ideal. Instead an educational taxonomy, like Bloom's taxonomy, should be used to accurately define the security education needs of organizational users. Through the use of such a taxonomy certain common weaknesses in current security awareness and educational programs might be addressed.

An example of how Bloom's taxonomy might be applied to information security concepts was provided. This example was based on an information security specific learning objective. Specific examples of learning activities relating to this learning objective were given for each level of Bloom's taxonomy of the cognitive domain. The chapter used this brief example, to show how a taxonomy table based on this example, could assist educators in addressing the four "organizing questions" faced by educators. The use of a learning taxonomy, as discussed in this chapter, could be of assistance to information security practitioners who want to determine **what** to include in an information security related educational campaign. The related question:

"**How** should the users be taught?" will be discussed in the next chapter.

Chapter 7

EDUCATIONAL DELIVERY

This chapter discusses issues that should be considered in choosing a delivery medium for organizational information security education. The chapter firstly discusses the requirements of organizational information security educational programs. The chapter then discusses what e-learning is and examines the components of e-learning systems. Next the benefits offered by e-learning to various stakeholders in organizational information security educational programs are discussed. The chapter also briefly examines the benefits of e-learning from a strictly pedagogical viewpoint. Finally an argument is presented to show that e-learning is an ideal medium for the delivery of organizational information security education.

7.1 Introduction

Information security educational material must be designed according to the specific learning needs of the intended target audience (NIST 800-16, 1998, p. 19). The learning approach most effective for a particular individual will depend on several factors. These could include his/her preferred learning style, current level of education, and/or prior experience relating to the subject matter (NIST 800-16, 1998, p. 19). The designers of information security educational content thus need to focus on more questions than just "**what** information security related knowledge is required?" and "**by whom** is this knowledge required?". It is also very important to address the question; "**how** should the knowledge be communicated to the intended target audience?".

Every individual can learn in one or more different ways, but usually has a preferred or primary learning style. Some students might learn better through self-paced reading, others through watching instructional videos. How well the given instruction matches an individual's learning style preferences can affect the learner's performance in either a positive or a negative way (NIST 800-16, 1998, p. 19). If an information security education campaign is to be successful, it is vital to try to accommodate as many of the learning preferences of the intended target audience as possible.

The previous chapter discussed the use of the learning matrix from NIST 800-16 (1998) to identify **what** should be taught to **whom**. It also discussed the use of a learning taxonomy to correctly determine the scope and/or depth of learning needed in each of the identified topics. The previous chapter thus addressed the second objective of this thesis, namely; to *demonstrate how the use of a learning taxonomy can be used to add pedagogical rigor to information security educational programs.* This chapter will address **how** information security educational material should be delivered in an organizational context. The aim of this chapter is to address the third objective of this thesis as defined in section 1.7. Namely, to *demonstrate the suitability of e-learning as a delivery medium for organizational information security educational programs.*

7.2 Research Methodology and Process

This chapter argues in favor of e-learning as the ideal delivery medium for organizational information security educational content. The work in this chapter is primarily based on a *qualitative content analysis* of *literature*, as described by (Krippendorff, 2004, pp 87-88) and argumentative techniques, as described by (Mason, 1996, pp. 171-204). Arguments are primarily presented *evidentially* (by showing relevant evidence gathered from literature) and *narratively* (by showing the validity of interpretation through a meaningful/reasonable narrative) (Mason, 1996, p. 176). Through qualitative content analysis techniques, the presented arguments are interwoven with quotes from analyzed texts and literature to support the arguments and/or conclusions (Krippendorff, 2004, pp. 87-88). The presented requirements for organization information security education were initially verified through publication as Van Niekerk and Von Solms (2004) as part of the author's work prior to this thesis. An initial argument in favor of using e-learning, and specifically adaptive e-learning for information security education was presented as Van Niekerk and Von Solms (2006a). A related paper, which evaluates the appropriateness of using the Cisco networking academy's learning model as an e-learning framework for information security educational content planned according to Bloom's taxonomy, has been accepted for publication as (Van Niekerk & Thomson, 2010).

7.3 Requirements for Organizational Information Security Education

The user education programs needed for information security purposes differ from traditional educational programs. Unlike traditional educational programs, organizational information security education programs will primarily be aimed at teaching *adults*. Adults have well established, not formative, values, beliefs, and opinions (NIST 800-16, 1998, p. 20). Adults also have well established learning preferences. The educational approach 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. Information security education is not *just* about the transfer of knowledge to learners. The aim of organizational information security education should be to foster a culture of information security within the organization (B. Von Solms, 2000). Attention to behavioral theories is thus vital in the construction of organizational information security educational programs. In the rest of this section, this thesis will suggest and motivate some of the criteria that should typically be considered when selecting a medium for the *delivery* and *creation* of an information security education program. Most of the listed criteria have been previously published by the author in Van Niekerk and Von Solms (2004). The discussion below reiterates the arguments presented in Van Niekerk and Von Solms (2004) and also presents some additional arguments based on research subsequent to the original publication. The requirements below should be considered when choosing an educational approach for an organizational information security educational program.

7.3.1 Everyone should be able to "pass" the course

In an organizational information security program, it is essential that each and every "learner" **successfully** completes 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, do not 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. The delivery mechanism chosen for such a program should thus provide learners with multiple opportunities to acquire the requisite knowledge. Allowing learners multiple opportunities to learn is also vital from a purely educational viewpoint. Learning **requires** sufficient opportunities for practice (Smilkstein, 2003, p. 128). How much practice and/or repetition is needed before someone *learns* a specific concept will vary from one individual to another based on various factors (Smilkstein, 2003, p. 128).

7.3.2 Current values, beliefs, and opinions must be addressed

In Van Niekerk and Von Solms (2004) this requirement was previously expressed as "employees must know **why**" information security is important and why a specific policy or control is in place. 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 (NIST 800-16, 1998, pp. 16-17)(Schlienger & Teufel, 2003). A feature of the educational level is that the user must understand why information security is important (NIST 800-16, 1998, pp. 16-17)(Schlienger & Teufel, 2003). However, as shown in chapter 4, this clear distinction between awareness, training and education is **not** universal amongst current approaches. In terms of the NIST learning continuum, understanding **why** a specific control is needed refers to education as opposed to awareness. NIST 800-16 (1998) reserves this level of education for the information security specialist. It is not the contention of this thesis that all users should receive the same level of education as information security professionals. It should 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, due to the need to sometimes "convince" users about the relevance of a specific control, in information security, if a user asks *why*, it should always be explained (Tripathi, 2000). To a large extent, the need to explain to users why a specific control is needed, is based on the fact that the learners are adults and could thus already have values, beliefs, and/or opinions that are contrary to the taught material. Education aimed at younger learners is normally *formative* in nature. Because these younger learners do not yet have well established values, beliefs, and opinions, it is *easier* to convince them to conform to certain desired norms and/or behavior patterns. Adult learners, on the other hand, already have well established values, beliefs, and opinions. These values, beliefs, and opinions might *clash* with the desired values, beliefs, and opinions the organization would like to foster. In some cases explaining **why** a specific control is needed would be sufficient to address the differences between a user's current values, beliefs, and opinions, and the desired values, beliefs, and opinions. In other cases it might be necessary to address these existing values, beliefs, and opinions more comprehensively. In information security education *rationality may not necessarily be enough* to convince an employee to behave in a desired fashion

(Kabay, 2002, p. 35.2). ”People can get very angry about what they perceive as interference with their way of getting the work done” (Kabay, 2002, p. 35.2). The delivery medium chosen for an information security educational program should thus be capable of facilitating approaches that could be used to address these current values, beliefs, and opinions.

7.3.3 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 (M. 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). ISO/IEC 27002 (2005) 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 27002, 2005, 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 (content) and how it should be taught (delivery), will depend on both the user’s preferred learning style, and the specific role which that user plays within the organization. The educational approach used should thus, as far as possible, allow for the customization of both the program content and the specific delivery methods.

7.3.4 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, as well as the availability of training facilities. 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. Adults learners will "explore a variety of learning modalities" if they are empowered to use their own learning strengths (Materna, 2007, p. xii). Users should be provided with learning via a delivery mechanism that allows them to explore the learning in their own way. It is however, important to note that this does not mean learners should simply be provided with material and then ignored. Motivational factors, brain compatible learning strategies, current education levels, past experience, and other possible factors which could influence learning should still be addressed. "How a person *feels* about a learning situation determines the amount of attention devoted to it" (Sousa, 2006, p. 44). Allowing adult learners to gain more understanding of, and autonomy over, their own learning, leads to the learners becoming "more invested in their learning, rising to the challenge with new energy, enthusiasm, and commitment (Materna, 2007, p. xii).

7.3.5 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 27002, 2005, 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, 2009, pp. 89-90). 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, 2009, pp. 89-90). 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. This requirement also leads logically from the combination of the requirement that everyone must "pass" the course, and that users should be responsible for their own learning. If the organization allows users to have the responsibility over their own learning, but still requires everyone to successfully complete the learning, it would have to hold users accountable for their own learning to ensure that the users are trying to acquire the necessary knowledge. Research has shown that learners who are held accountable for the learning will spend more time attempting to process the same information (Sousa, 2006, p. 66).

7.3.6 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). *Prompt*, *specific*, and *corrective* feedback increases the likelihood of a learner continuing the learning process until successful completion (Sousa, 2006, p. 66). 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. Such a metric could also be used as a key performance indicator to assist in holding users accountable for their studies.

It is not the contention of this thesis that the above requirements constitute a definitive list of *all* requirements that should be met by an educational approach to organizational information security education. They do however represent factors that in the author's opinion should specifically be considered when choosing a *medium* for the creation and delivery of educational material for information security programs. Other psychological factors, such as aspects relating to motivating employees to both *learn* the required security knowledge and skills, and then *apply* this knowledge and skills when and where necessary, would still need to be addressed. These motivational aspects do not necessarily *directly* impact the choice of educational delivery approach and will thus be dealt with in the next chapter when the integration of the various contributions made by this thesis is discussed. As mentioned above, web-based-, or e-learning can be one of the most cost-effective approaches to the education of organizational users. However, such approaches do not necessarily have to completely exclude other forms of education. Classroom education, instructional videos, printed media, etc could still play a significant role in organizational information security education. Many recent studies have started to use the term *blended learning* to refer to an approach that mixes technological and other forms of education into a more holistic approach. The following sections will firstly clarify exactly what blended- and/or e-learning is. The benefits that such technology-integrated/blended approaches could offer will be examined, and finally a critical comparison of such approaches against the above identified criteria for organizational information security education will be performed.

7.4 What is Blended and/or E-learning?

Many different terms are commonly used to refer to educational approaches that utilize computer based technology in the delivery of learning material. It is important to understand the differences between the most commonly used terminology. Commonly used terminology includes e-learning, blended learning, online learning, web-based learning, and computer aided instruction. For the purposes of this thesis the term e-learning will be used to refer to **any** instructional approaches that include computer based delivery mechanisms. Online-, and web-based, learning will be used to refer to e-learning that specifically make use of web-based technologies to deliver instruction. Finally the term blended learning (sometimes called "hybrid" learning) refers to learning/teaching approaches where online and/or e-learning components are combined with more traditional approaches, such as face-to-face instruction, to provide an enhanced learning experience (DOE, 2009, p. 9).

Despite the fairly "broad" nature of the above definitions, it would be a mistake to simply view *any* learning content in an electronic form as e-learning. It is also important to not simply devolve the development of an e-learning system into a purely technical exercise (Ismail, 2002). This might result in an expensive software implementation that does not deliver much learning value. Instead, designers of e-learning programs should focus on understanding the basic components that constitute an e-learning environment (Ismail, 2002). Such environments could, for example, be based on a framework like the widely accepted Learning Technologies Systems Architecture (LTSA) as presented in the international standard IEEE 1484.1 (2003). A simplified overview of components common to such e-learning environments is provided by Ismail (2002). This simplified overview is graphically depicted in Figure 7.1.

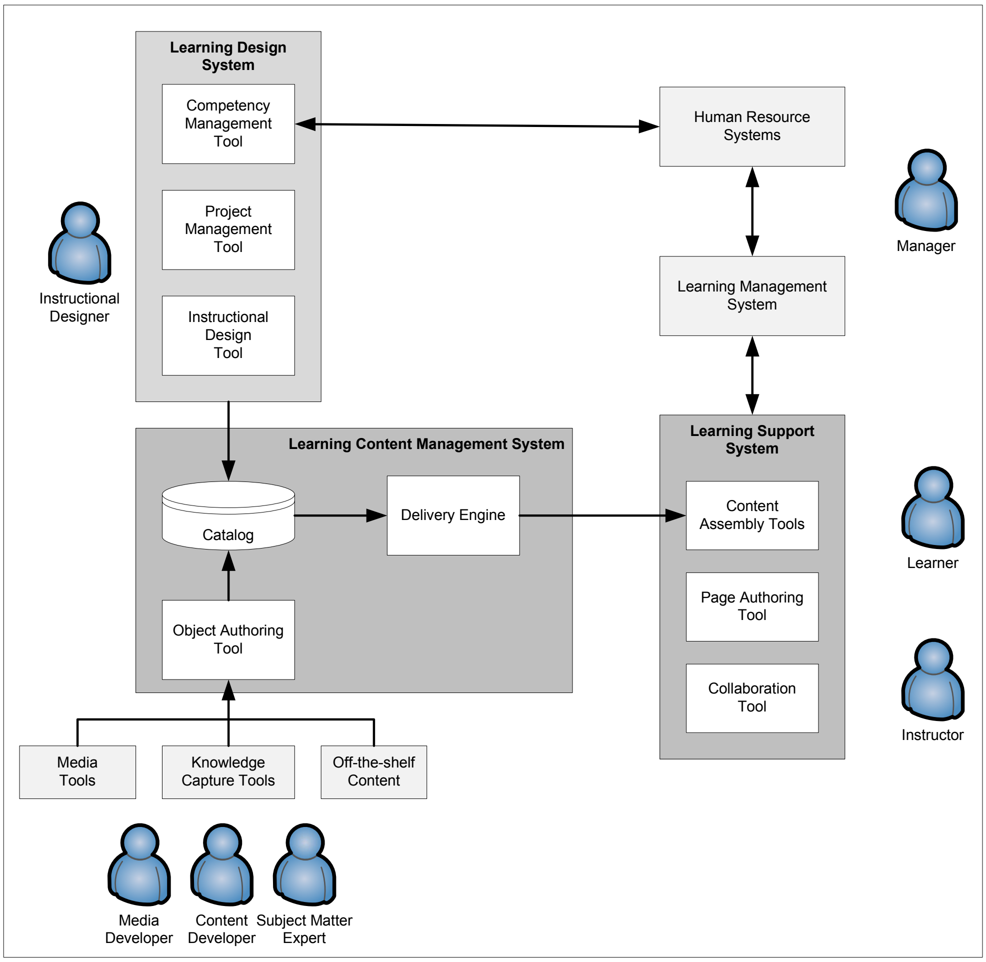


Figure 7.1: E-learning Application Environment. Adapted from (Ismail, 2002)

7.4.1 Components of an E-learning Environment

The first component of the e-learning environment shown in Figure 7.1 is a *Learning Design System* (LDS). A *learning design system* allows the design and analysis of instructionally sound learning programs (Ismail, 2002). A *learning design system* also provides the capability to manage the overall instructional design project. In a ”good” *learning design system* this would allow the incorporation of an instructional design methodology of choice (Ismail, 2002). Being able to incorporate an instructional design methodology of choice into the overall management of a learning program project allows the use of content developers who are not trained in instructional design principles to still develop content which adheres to such principles

(Ismail, 2002). In an e-learning environment, the *learning design system* is used to manage the creation of learning projects based on learning needs identified in the human resource management system of the organization (or possibly some other sub-system used to identify the educational needs for specific target employee groups).

The *learning design system* manages the overall creation of content in the *Learning Content Management System* (LCMS). The *learning content management system* provides a collaborative environment for the creation, and maintenance, of learning content. This system is usually supported by various forms of content creation tools and is used by subject matter experts, media-, and content developers (Ismail, 2002). The *learning content management system* also allows the storage of instructional content, and the delivery of this content to the learning support system.

A *learning support system* is an environment, often web-based, for the support of actual teaching and learning activities (Ismail, 2002). For an instructor, this component enables him/her to select various learning objects from the *learning content management system* and incorporate them into a blended learning approach. The instructor could plan the delivery of specific parts of a syllabus using this *learning support system.* For learners, this is their main point of entry into the available e-learning material. In a non-blended approach the *learning support system* could also be used directly by learners to plan and conduct their own learning activities. Such a *learning support system* commonly also contains entry points into automated assessment and feedback modules. Some modern systems would also support adaptive technologies (see discussion below). Ensuring that employees do in fact participate in the learning activities is achieved via the use of a learning management system.

Many early e-learning ”solutions” consisted of only a *Learning Management System* (LMS) (Ismail, 2002). Some current approaches still use the term *learning management system* to refer to an entire e-learning environment, and not only to the specific sub-component (Lonn & Teasley, 2009). The term *learning management system*, as used in this thesis, refers to the component of an e-learning environment that allows for the administration, documentation, tracking and reporting of learning activities. With the help of a *learning management system*, an organization’s human resource department can keep track of employees' learning. The *learning management system* can report on who learned, what content/subject matter was studied, when it took place, and even how much time was spent on learning. As depicted in Figure 7.1, the *learning management system* is usually connected to both the organization's human resource database, and to a *Learning Support System* (LSS).

The above components (sometimes described using different names and/or terminology) form part of the most common e-learning environments. Popular open-/community source e-learning platforms, such as Moodle (http://moodle.org) and Sakai (http://sakaiproject.org), are also based, at a conceptual level, on the component framework as described above. Some e-learning systems also have more advanced components. Of particular importance, for the purposes of this thesis, are the so-called *adaptive* e-learning systems which personalize the learner's access to educational material.

7.4.2 Adaptive E-learning

The need for *personalized* access to information has become a well established feature of many application areas in ICT (Brusilovsky & Henze, 2007). Areas such as e-commerce, news access, and many others already successfully make use of a variety of adaptive features. However, despite the fact that education, as a field, has one of the biggest needs for personalized access, adaptive technologies have not yet become widely used in education (Brusilovsky & Henze, 2007). This is primarily due to the fact that most of the "adaptation techniques that focus on user interests and work successfully in other fields have a limited applicability in the educational context" (Brusilovsky & Henze, 2007). In education users do not only differ in terms of interests, but also requires adaptation based on current knowledge levels, goals, skills, and personal learning styles (Brusilovsky & Henze, 2007). These adaptations form the basis of adaptive e-learning technologies.

Adaptive e-learning systems, as well as *intelligent tutoring systems*, are categories of e-learning solutions that make use of advances from the field of *artificial intelligence* (AI) to better support learning. The primary purpose of adaptive e-learning systems is to automatically adapt presented learning content to the learner. Artificial intelligence can be seen as the key to this automation of e-learning (Hentea, Shea, & Pennington, 2003). However, for the purposes of this thesis, the exact "form(s)" of artificial intelligence used need not be examined. Instead, the underlying architectural structure that enables the adaptation of content in current adaptive systems will be briefly examined.

Current adaptive e-learning systems make use of a *user model* and a *domain model* to provide adaptive features. "The user model is a representation of information about an individual user that is essential for an adaptive system to provide the adaptation effect, i.e., to behave differently for different users" (Brusilovsky & Millán, 2007). The adaptive system collects knowledge about the user from various sources. These sources could include both implicit observation of the user's behavior and/or explicitly *asking* the user for inputs (Brusilovsky & Millán, 2007). The type of information represented in a system's user model, as well as how much information is stored, will depend on the specific kind of adaptation effect that the system has to deliver (Brusilovsky & Millán, 2007). Adaptation of educational resources is done in order to increase the usefulness of the educational resource to the learner.

How useful a specific resource is to a learner depends on many factors. For example, "some resources may require additional knowledge that the learner does not yet have (in accordance to his/her user model), while others may teach the subject without sufficient in-depth information and are thus too easy for this learner" (Brusilovsky & Henze, 2007). The learner's current progress, personal learning style preferences, learning goals, and many other factors could thus all form part of the user model in a specific adaptive e-learning system. It should be clear that the user model will be continuously updated and adapted as the learner progresses through an e-learning course.

The user model is used in combination with an expert-, or *domain model.* The domain model is also sometimes referred to as the "ideal student model" (Brusilovsky & Millán, 2007). This *domain model* is constructed by subject experts and reflects the knowledge an "ideal" learner should have after successfully completing the desired educational module. The *domain model* will also contain a large amount of meta-knowledge regarding the pre-requisite knowledge that a learner would need before being able to attempt a specific learning task, and other relationships between various units of knowledge. Before choosing specific content to present to a learner, an adaptive system performs a comparison, with the help of artificial intelligence based techniques, between the *user model* and the *domain model.* Some systems perform this comparison with the assistance of an *overlay model.* An *overlay model* represents an individual user's knowledge as a subset of the domain model. "For each fragment of domain knowledge, an overlay model stores some estimation of the users knowledge level of this fragment" (Brusilovsky & Millán, 2007). Through the use of these user-, domain, and sometimes overlay-, models, an adaptive system can determine how to adapt the actual *content* of a learning module to be more applicable for a specific learner. However, the use of these models is not restricted to only the adaptation based on current knowledge.

User models can also be used to contain information specifically focused on user *interest.* In many current adaptive systems modeling user *interest* is seen as more important than modeling user *knowledge* (Brusilovsky & Millán, 2007). In an information security context, this might not necessarily be the case. Even if a user is not really interested in learning about information security it would still be necessary for the organization to ensure the user is educated. However, the same techniques that are used to model *interest* could probably be applied to model the *applicability* of specific knowledge based on a user's security roles and responsibilities. Brusilovsky and Millán (2007) also discusses the use of user models to model *goals and tasks.* This form of adaptation depends on the current context within which the user operates and would be used to present information that could fill the users immediate information needs. As an example, due to such a contextual adaptation, a user actively engaged in a task where encryption techniques could be of importance, might be presented with knowledge specifically relating to the use of encryption techniques. Additionally, user models can be used to model user *background* (previous experience outside the core knowledge domain), *individual traits* (including *cognitive styles* and *learning styles*), and *work context* (location, systems/platform(s) used, etc) (Brusilovsky & Millán, 2007). Adaptation of e-learning materials based on such extended *user models* would obviously require corresponding changes in the supporting *domain models.* As a field of study, adaptive e-learning is constantly evolving and improving.

According to Brusilovsky and Henze (2007) current adaptive techniques can already be used

- ”to support the learner in finding the most appropriate learning resource;
- for providing awareness about the learning process (e.g., by pointing out necessary pre-knowledge that this learner might otherwise miss);
- for providing guidance (e.g., by providing an individually tailored sequence of learning resources which teach the topics s/he is interested in while incorporating all required prerequisite knowledge);
- for providing orientation (e.g., by pointing out the next learning steps to take, or the existence of different schools-of-thought);
- for considering individual learning styles” (Brusilovsky & Henze, 2007)

Adaptive technologies already play an important role in e-learning and will probably start to play a progressively more important role in future e-learning solutions. It is the opinion of the author of this thesis that these technologies can play an especially important role in the use of e-learning for organizational information security education. This possible use will be discussed later in this chapter.

This section established **what** e-learning and blended learning are. It also explored the components that commonly form part of such systems, and the role(s) these components play in such a system. Finally the field of adaptive e-learning was briefly introduced and discussed. The next section will specifically focus on the benefits e-learning, and/or blended learning can offer to organizations.

7.5 Benefits of Blended and/or E-learning

Providing learning to organizational employees in an e-learning, or blended learning, format holds many advantages for all the stakeholders involved in these learning programs. These advantages can be loosely categorized according to the specific stakeholders who benefit as follows:

Firstly, e-learning approaches hold advantages for the learners themselves. These include:

- material can be used as self-study, with or without tutor support, or in blended environment (Nisar, 2002)
- learning material often has a hyper-linked nature which allows learners to explore related topics of interest
- learning can be enhanced and be more flexible (for example through adaptive features) (Nisar, 2002)
- time spent on training is significantly reduced (Nisar, 2002)
- travel away from home is not required (Nisar, 2002)
- training material is of a consistent quality (Nisar, 2002)
- individuals can work at their own pace (Nisar, 2002)
- student support systems are better (Nisar, 2002)
- learning environment is anonymous and there is less pressure to perform well in front of peers (Bell, 2007)
- anonymous learning environments also allow the exploration of more personal issues (Bell, 2007)
- adaptive features support preferred learning styles, allow for learners past experience, individual traits, specific learning needs, etc (Brusilovsky & Millán, 2007)
- training is available when and where required at a time and place convenient to both learner and employer (Bell, 2007)

The second major stakeholder in organizational information security education would be the organization itself. From the organization's viewpoint, e-learning also offers many advantages:

- huge cost savings including less time away from job, cheap premises, no travel and subsistence costs, and little or no course fees (Nisar, 2002)(Unneberg, 2007)

- E-learning based training solutions are inexpensive to distribute organization wide and can easily be administrated from a centralized point. This also means that it would be very easy to maintain, manage and update training materials.
- employees spend less time away from work
- participation in learning programs can easily be checked and monitored (Nisar, 2002). This is especially important from a legislatory compliance point of view (Bell, 2007). This includes detailed reports on when and where training took place, how much time was spent, how the employee performed in the assessments, etc
- learning management systems can also be used to audit which employees must go on additional or refresher training. This can help organizations to meet legal requirements (Bell, 2007)
- e-learning improves employees' abilities to interpret information, make decisions, and solve problems which in turn enable greater exploration of new technologies
- training can be ”targeted” to enhance the ability to interpret information relating to a *specific* task
- training can be delivered just in time. A learning management system could even be used to support customer relationship management through streamlining certain tasks (Deeny, 2003)
- course materials can be constantly updated which can ensure that the course is current, relevant and *in line with new legislation* (Bell, 2007)(Young, 2002)
- training can complement existing knowledge management processes (Young, 2002)
- e-learning can lead to a reduction in staff turnover (Deeny, 2003)
- material can be globalized, i.e. translated into many languages. This allows the reuse of existing material and once again leads to cost savings (Pollitt, 2008)(Bell, 2007)

- anonymous training environments can allow the exploration of issues relating to ethics, or other sensitive/personal matters. This could be of use in fostering a specific organizational culture
- e-learning activities often have a positive impact, in terms of both cost and efficiency, on critical business processes (Young, 2002)

Thirdly, the design and implementation of any instructional program requires a significant investment in time from course and/or content creators. E-learning also offers many benefits to the course/content creators involved in such a program:

- Electronic and/or web-based media are very *rich.* This means that educational material developed in these types of 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.
- E-learning training materials can include programmatic components, which could allow virtually limitless customization.
- wikis, blogs, podcast, e-portfolios, etc allow instructors a variety of tools. Furthermore, new technologies are constantly emerging. This gives course designers a lot of creative freedom (Clark, 2007)
- learning design systems allow the use of content creators who are not familiar with a specific pedagogical approach (Ismail, 2002)
- existing material can be re-used or even re-purposed to meet new training needs.
- the ability to rapidly distribute new material also allows more time spent on the actual *creation* of content, and less on administrative tasks

It can be argued that many, if not most, of the above mentioned benefits are logical and "expected". However, blended and e-learning also has some less obvious benefits. These relate specifically to improvements in learning from a strictly pedagogical point of view. From a purely educational point of view, it is these pedagogical benefits that should carry the most weight in a decision to make use of blended and/or e-learning.

7.5.1 Pedagogical benefits of Blended and/or E-learning

Since the first computer aided instruction systems appeared, many researchers have conducted studies to compare the effectiveness of these ”new” approaches to more traditional classroom based instruction approaches. Such research papers would thus be the most appropriate sources to evaluate in order to determine whether or not blended and/or e-learning approaches offer a pedagogical advantage over traditional instruction approaches. The United States Department of Education recently published a report based on a meta-analysis of the results of more than 1000 such empirical studies that were published from 1996 through July 2008 (DOE, 2009). The report focuses predominantly on publications after 2004 which compares the effectiveness of various forms of e-learning and blended learning to face-to-face education (DOE, 2009, p. xiii). This report would thus be an ideal source to provide insight into the effectiveness of blended and/or e-learning approaches. However, one might argue that many of these studies might not be applicable to information security education which focuses predominantly on *adult* education.

The report examined 51 identified study effects, of which 44 were drawn from research focusing on older (adult) learners. This focus on older learners is thus of particular importance to educators, focusing on organizational information security end-user education, who work exclusively with adult learners. Adults already 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 therefore vital to ensure that learning approaches followed are suitable for adult learners. The fact that 44 of the 51 study effects analyzed in the meta-analysis focus on adult learners makes the results of this analysis very relevant for the purposes of this thesis.

The following key-findings are of specific importance for the purposes of this thesis (DOE, 2009, p. xiv-xvi):

- ”Students who took all or part of their class online performed better, on average, than those taking the same course through traditional face-to-face instruction”

- ”Instruction combining online and face-to-face elements had a larger advantage relative to purely face-to-face instruction than did purely online instruction"

- "The effectiveness of online learning approaches appears quite broad across different content and learner types."
- "Most of the variations in the way in which different studies implemented online learning did not affect student learning outcomes significantly."
- "Effect sizes were larger for studies in which the online and face-to-face conditions varied in terms of curriculum materials and aspects of instructional approach in addition to the medium of instruction."
- "Online learning can be enhanced by giving learners control of their interactions with media and prompting learner reflection."
- "Providing guidance for learning for groups of students appears less successful than does using such mechanisms with individual learners."

From a purely pedagogical viewpoint the findings in DOE (2009) are very important. Firstly, the findings show that a **blended approach**, where e-learning and face-to-face instruction are combined, is the most effective educational approach. However, if such a blended approach is not possible, a purely e-learning based approach would in fact be better than classroom instruction. Secondly, the findings show that approaches incorporating e-learning are effective irrespective of the specific e-learning approach taken, the learner type, or the specific field of study. Finally, the findings showed that learners in e-learning based programs should be given control of their own learning, and should, if possible, be given individualized guidance.

The benefits discussed above should make it clear that an e-learning based approach would definitely be the best pedagogical approach towards educational delivery for organizational information security education **if** it also matches the general requirements for information security education identified in section 7.3. The next section will compare the features of an e-learning to the identified requirements for information security education.

7.6 E-learning for Information Security Education

Section 7.3 identified certain requirements that should be met by educational approaches used for information security education. These requirements have also been published before as part of Van Niekerk and Von Solms (2004). This section will compare these requirements against the features of e-learning approaches to determine how well e-learning as an educational delivery channel matches the needs of organizational information security education.

- The first identified requirement is the need for all employees to (eventually) "pass" the course. Information security depends on each and every person involved in the security process to have the necessary security related knowledge and/or skills to perform his/her job in a secure manner. It is thus necessary to ensure that the educational approach taken allows users who "fail" the assessments relating to a specific knowledge element, and/or skill that is needed, the opportunity for additional learning and, afterwards, to be re-assessed. E-learning approaches are arguably better suited to address this need than any other possible approach. Because e-learning can be done at a time and place that suits both the employee and the organization, there are little or no additional impact on a learner's normal job functions should he/she need to repeat on of the learning modules. There is also no additional cost involved in having an employee who repeats a specific learning module. The facilities provided by a learning management system will also enable the organization to keep track of each and every individual employee's learning/progress.

- The second identified requirement is the need to address current values, beliefs, and opinions of employees. This is especially important if the overall goal of the program is to foster an organizational culture of information security. However, employees can come from many different educational and/or cultural backgrounds. These different backgrounds, and many other factors could influence the current values, beliefs, and/or attitudes of employees towards information security. These values, beliefs, and attitudes can thus vary significantly amongst an organization's employees. In some cases, individuals might even consider their own values, beliefs, and attitudes to be *personal/private* and would thus not like to openly discuss/share these. E-learning systems provide an excellent medium to assist in the addressing of current employees' values, beliefs, and attitudes. Firstly, the user models / domain models in current adaptive e-learning systems can already accommodate the modeling of various user backgrounds and other individual traits. These and similar features could, to a certain extent, also be used to determine a difference between the desired values, beliefs, and attitudes (as modeled in the domain model) and the specific user's (as modeled in the user model). The content can then be adapted to the specific user's needs in order to allow the user to explore (if preferable, anonymously) the reasons/reasoning for the inclusion of specific information security controls. In addition to this, e-learning solutions offer the ability to use a multitude of approaches. Course designers could thus address specific "contentious" issues in wiki's, blogs, videos, or even via interactive discussion forums. According to Kabay (2002, p. 35.9) the use of simulations, videos, and role-laying exercises could assist in changing user beliefs/attitudes during a culture change program by helping users bridge the gap between intellect and emotion (what they are taught is logical, but it conflicts with how they *feel* about the topic). The use of interactive discussion forums could allow users to not only explore the reasons/reasoning for a specific control, but to also provide their own opinions on specific issues.

- Thirdly, information security education requires that learning materials are customized to the needs of specific target users and/or groups. Such customization is one of the central features of e-learning. The entire field of adaptive e-learning systems specifically aims at the implementation and improvement of such learner specific customization. As discussed earlier, these systems can customize content based on the individual user's learning preferences, learning needs, current activities (work context), background, location, systems and/or platforms used, individual traits, cognitive styles, goals and tasks. E-learning approaches are arguably more accommodating of such customization needs than any other educational delivery medium.

- The fourth requirement for information security education that was identified is that users should be *responsible* for their own learning. This requirement was motivated in Van Niekerk and Von Solms (2004) specifically based on the cost implications of education in terms of both time and financial resources. It is also important in terms of the first requirement identified, namely that everyone should ”pass” the course. From a time and cost perspective, users could only be allowed multiple opportunities to learn, if such additional opportunities do not require them to spend additional time away from their job responsibilities. E-learning systems allow users to learn when and where they choose to. It also allows users to learn at their own pace, according to their own learning needs, and to explore topics according to their own interests. E-learning enables users to participate in group discussions, or not to, should they so choose. With the help of the learning support systems in modern e-learning solutions, learners are empowered to take control of their own learning. E-learning systems thus allow organizations to pass the responsibility for their learning to the users themselves. However, in order to ensure that the user takes this responsibility seriously, organizations need to hold the users accountable for their learning.

- Holding users accountable for their own learning was the fifth requirement identified for information security educational approaches. This requirement goes hand-in-hand with making users responsible for their own learning. Through the use of learning management systems organizations can not only hold users accountable for their own learning, but can also keep extensive records of learning. E-learning systems allow organizations to monitor user learning progress, in terms of training completed, time spent on specific modules, performance in assessments, etc. With the extensive learner monitoring and tracking capabilities of current e-learning solutions organizations can also identify learners who need remedial or additional training in order to remain compliant with legislatury changes.

- The final identified requirement for information security education is the need to provide learners with feedback. Feedback is a central feature of any successful educational approach. Providing learners with prompt, specific, and corrective feedback increases the likelihood that the learners will persist in their learning activities until they are successful (Sousa, 2006, p. 66). The ability of computers (e-learning) to provide immediate and objective feedback is considered to be a motivating factor towards continued learning because learners can understand their own level of competence and can evaluate their own progress (Sousa, 2006, p. 66). E-learning systems can be used to provide continuous formative assessments and feedback to enhance the learners own learning process, or to administer summative assessments for use by the organization in order to determine whether or not a specific learning module has been completed successfully.

E-learning systems thus meet all the identified requirements for information security education. It can be argued that e-learning is in fact *the* most appropriate delivery channel for information security education available to modern organizations. Additionally, e-learning components can also be included in more traditional educational approaches to form a blended learning environment. Research discussed earlier in this chapter has shown that such blended approaches are highly effective from a pedagogical point of view.

7.7 Conclusion

This chapter examined the requirements of organizational information security education. It was argued that information security is dependant on each and every human involved in the security process. Organizations thus cannot afford to have any of the users in an information security educational program *fail* the course. It was also argued that the existing values, beliefs, and attitudes of users must be addressed by these educational programs. This is especially important if the organization wishes to foster a culture of information security. Thirdly, the learners in organizational information security educational programs are adults, who have well established learning preferences, educational backgrounds, and levels of technological competency. These adult learners also have very specific, and varied, roles and responsibilities towards information security. There is thus a need to customize learning material in organizational information security educational programs in order to accommodate the variety of needs and background amongst the target learners. The fourth, fifth, and sixth identified requirements were all based on the fact that few organizations can afford to send **all** their staff for extensive classroom training. Organizations should thus be able to make the users responsible for their own learning. However, if users are responsible for their own learning, organizations would have to hold them accountable for this learning in order to ensure compliance with possible legislatory requirements, and in order to ensure that organizational information resources are in fact secure. Finally, learning *requires* feedback. If users are to be responsible for their own learning, the educational approach would have to accommodate this need for feedback. Based on the identified requirements, e-learning was suggested as the preferred educational delivery medium for organizational information security education. The chapter examined the components of such e-learning systems, as well as the role(s) each of these components play(s) in an e-learning environment. In addition to the "normal" components, the features of adaptive e-learning systems were briefly examined. The chapter examined the benefits that e-learning, and blended learning approaches that incorporate e-learning components, can offer to various organizational stakeholders. The specific benefits offered by these approaches from a purely pedagogical viewpoint were also discussed. Finally the chapter compared the requirements of organizational information security education to the features provided by e-learning systems. It is the conclusion of this chapter that e-learning would be a medium that is ideally suited for the delivery of organizational information security education. Furthermore, the possibilities provided by adaptive e-learning technologies can potentially add a lot of value to information security educational programs. Through the use of e-learning environments, organizations can not only create appropriate information security educational material, but can also effectively administer and manage such programs. This chapter has thus addressed the third research objective of this thesis, namely to "*demonstrate the suitability of e-learning as a delivery medium for organizational information security educational programs*". The next chapter will show how e-learning can be used as part of a pedagogically sound process in order to address the final research objective identified in section 1.7, namely to demonstrate "*how the various elements contributed by this thesis integrate into existing transfor-*

mative change management processes for the fostering of an organizational information security culture".

Chapter 8

INTEGRATING THEORY AND TECHNOLOGY

This chapter integrates the theoretical and technological concepts discussed in the previous three chapters. The chapter discusses the typical design of an e-learning based information security educational program, using Bloom's taxonomy to plan the educational activities, in order to address specific needs relevant to the fostering of an organizational information security culture.

8.1 Introduction

The previous three chapters each discussed a specific element with regards to dealing with the human factor in information security, but did not clearly describe or demonstrate the integration between these elements. Chapter 5 discussed the concept of an information security culture and proposed a conceptual model to aid in understanding the interaction(s) between the various dimensions of such a culture. The fostering of an information security culture is seen as fundamental to effectively addressing the human factors in information security. Through the establishment of an organizational information security culture, secure behavior can be made a "normal" part of the organization's employees' day-to-day behavior.

Chapter 5 also identified the vital role played by knowledge in the fostering of such an organizational culture of information security. The role of knowledge was argued to be critically important in an information security culture. For this reason it warranted the extension of the classical model used to define a ”normal” organizational culture, as presented by Schein (1999a), to include knowledge as an additional dimension in the model used to define an information security culture. Knowledge is also one of the dimensions of the human factor in information security.

The human factor in information security consists of two closely interrelated dimensions, namely knowledge and behavior. These two dimensions are mutually dependant. Without adequate information security related knowledge it is not possible for organizational end-users to behave correctly. This would be true even if a user has the desired attitude towards his/her information security role(s) and responsibilities, and is properly motivated to adhere to the information security related policies and procedures relevant to his/her daily tasks. A lack of the requisite knowledge could potentially prevent users from behaving securely. Similarly, having the requisite information security related knowledge still does not guarantee the desired behavior. A user who has the requisite knowledge but who views security as a hindrance to performing his/her job, or as not being very important, might still behave in an insecure manner. Any attempt to address the human factors in information security should thus address both these dimensions holistically. Both of these dimensions form part of an organizational information security culture, as discussed in chapter 5, and to a large extent both of these dimensions to the human factor can be addressed via information security educational programs.

Due to the important role information security educational programs play in the establishment of an organizational information security culture, it is vital that these educational programs are pedagogically sound. Chapter 6 examined the design of educational content for information security educational programs from a pedagogical point of view. Chapter 6 also suggested the use of Bloom’s taxonomy, a major learning taxonomy, to accurately define the security education needs of organizational users. Once the specific information security related educational requirements of a target user/user group have been identified, the appropriate educational content needs to be developed and delivered.

Chapter 7 identified e-learning as an ideal medium for the development and delivery of organizational information security educational programs. This chapter will discuss the integration of the work done in the previous three chapters. The aim of this chapter is to integrate the concepts discussed in the previous three chapters in order to address the fourth research objective of this thesis listed in section 1.7, namely *to provide a detailed overview of how educational content should be delivered in a corporate information security educational program, with specific emphasis on the role(s) technology can play as a media channel.* In order to address this objective, it is important to remember that the overall aim of addressing the human factors in information security is to foster an organizational information security culture. This should be accomplished through a culture change process. The following section will firstly provide a brief overview of a "generic" culture change process. This overview will then be followed by an adapted culture change process which incorporates the work done in this thesis in order to make it specific to changing an information security culture.

8.2 Organizational Culture Change Process

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 impossible, to change the underlying beliefs, values and principles of employees, to a "level" that matches the organization's espoused values.The management, and/or change of, organizational culture is a problem that has been extensively studied in the management sciences. The process presented in this section has been "borrowed" from the management sciences. An adapted version of this process, which incorporates the contributions made by this thesis, will be presented in the next section. This process is depicted in Figure 8.1.

8.2.1 Top Management Commitment

Any culture change process has to start with top management commitment to the process. 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*

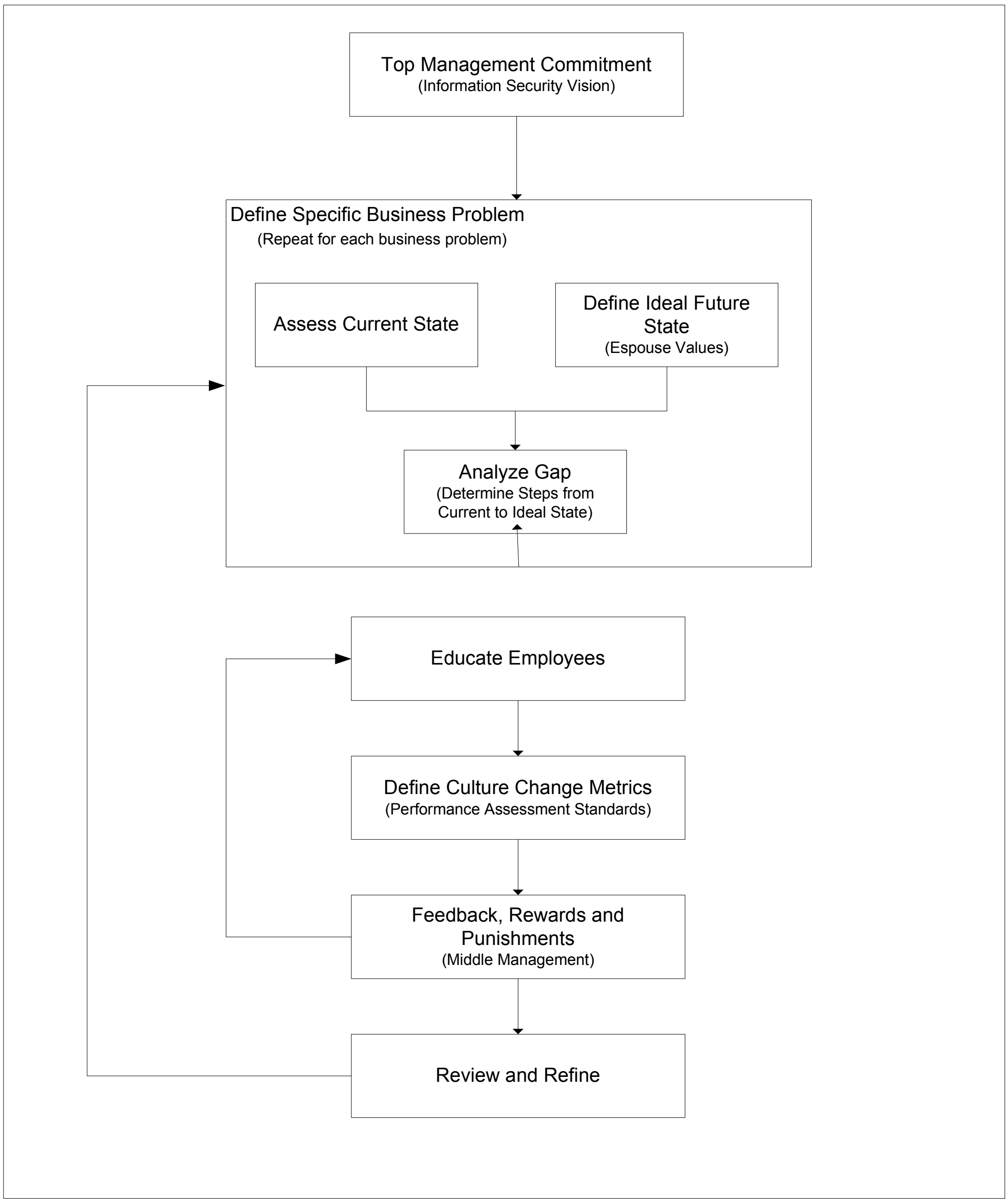

Top Management Commitment
(Information Security Vision)
Define Specific Business Problem
(Repeat for each business problem)
Assess Current State
Define Ideal Future State
(Espouse Values)
Analyze Gap
(Determine Steps from Current to Ideal State)
Educate Employees
Define Culture Change Metrics
(Performance Assessment Standards)
Feedback, Rewards and Punishments
(Middle Management)
Review and Refine

Figure 8.1: Organizational Culture Change Process

exceptional customer service" (or any other value the organization wishes to espouse). Top management also has to visibly support the desired culture through its own behavior (Wallace, Hunt, & Richards, 1999). 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 levels of sub-policies and/or operational procedures, each dealing with specific aspects of the desired culture.

8.2.2 Define Change Needed in Business Context

According to Schein (1999a, pp. 86-87), culture change should always be done in a specific business context. Culture itself is too vast to accurately assess. The impact of culture on a specific goal can, however, be assessed meaningfully. Organizational culture affects all aspects of the day-to-day business of an organization. Changing such a culture could thus have a far reaching impact. As such, it is very important to understand the *current* culture in an organization, *before* trying to change it. 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. Before it is possible to decide *what should change*, one first needs to know what the current *state* of the culture is, in terms of the specific business context being examined.

Assess Current State

In order to determine the desired future *state* of an organizational culture for a specific business context, each of the underlying dimensions of the culture needs to be examined, in terms of the specific business context. 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). For an information security culture, whether or not the employees currently have the underlying **knowledge** required to act securely in the specific business context, would also need to be assessed. Assessing the current state of an *information security culture* will be dealt with in more depth in the next section. Once the current *state* of the culture has been determined, the desired future state (the ideal culture) needs to be defined.

Define *Ideal* Future 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 in the case of information security). The first step in this definition is to create "new" **espoused values**. Existing policies, sub-policies, and operational procedures need to be updated in order to reflect the new desired culture. The actual desired way in which employees should behave (**artifacts**) must also be clearly defined. Such a definition should be specific and in terms of measurable outcomes. Finally the organization needs to define the desired beliefs, attitudes, and values employees should have in order to support this new culture (as well as the requisite knowledge they would need in the case of an information security culture). Once the *ideal* future state has been defined, the "gap" between the current state and the desired ideal state needs to be analyzed for the specific business problem being addressed.

Analyze Gap

The extent of the "gap" between the current state of the culture and the desired ideal state will determine the amount of *work* needed to attain the new culture. 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.

Determining exactly how much work needs to be done in order to affect change for a specific business context can be seen as the high level planning phase of a culture change process. During this phase the primary aim should be to clearly define the steps needed to get from the current state to the desired future state. In some cases it might be necessary to go through several intermediate "states" to eventually attain the desired *ideal* state. Once this high level planning is complete, the actual change is affected via a transformative change management process (Schein, 1999a, pp. 116-139).

8.2.3 Transformative Change Management

Culture is extremely stable and any attempt to change it will thus have to start with a disconfirmation process. 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). To large extent this process is realized by means of awareness and education activities. In an information security context it would be essential to include formal, pedagogically sound, educational programs to impart the needed information security knowledge to employees. The process in a transformative change program thus consists of three basic steps (Schein, 1999a, pp. 116-126):

1. **Unfreezing: creating the motivation to change**. 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.

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*, as well as a continuous *motivational process* to encourage employees to change. Despite the fact that these educational and motivational programs will be discussed separately below, these programs are usually part of the above *learning cycle* and cannot, at implementation level, be dealt with in isolation.

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* (Schein, 1999a, p. 19). 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 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.

Motivate Employees

Employee motivation plays a vital role in culture change management. Without proper motivation, employees will only comply with behavioral guidelines that are in line with their own tacit assumptions. Employees *could* be coerced into behaving in a specific way, but such a behavior change will be superficial and unstable (Schein, 1999a, p. 115). It is thus essential to provide incentives for employees to *want to* behave in the desired way. One of the most widely accepted theories to explain motivation is Vroom’s *expectancy theory* (Robbins, Odendaal, & Roodt, 2003, pp. 140-141)(Huczynski & Buchanan, 2007, pp. 251-254). ”*Expectancy theory argues that the strength of a tendency* *to act in a certain way depends on the strength of the expectation that the act will be followed by a given outcome and on the attractiveness of that outcome to the individual*" (Robbins et al., 2003, p. 140). Essentially this means that an employee will be motivated to behave in a certain way if he/she believes this will lead to some positive outcome like a financial reward, good performance appraisal, peer recognition, promotion, etc. It is also important to note that the expected positive outcome must be in line with the employee's personal goals (Robbins et al., 2003, pp. 140-141). Robbins et al. (2003, pp. 140-141) provide the following three "questions" that need to be answered affirmatively from the employee's point of view if the employee is to be motivated:

- "First, if I give maximum effort, will it be recognized in my performance appraisal?"
- "Second, if I get a good performance appraisal, will it lead to organizational rewards?"
- "Finally, if I'm rewarded, are the rewards ones that I find personally attractive?" (Robbins et al., 2003, pp. 140-141)

These three questions help to clarify the underlying processes that should be in place in order to effectively motivate employees to adhere to the desired behavior patterns. Firstly, it is necessary to *measure* employee adherence to desired behavior in an impartial way. Secondly, it is necessary to provide *feedback* to employees regarding the appropriateness of their behavior. Finally, desirable behavior should be positively reinforced by being *rewarded*, conversely undesirable behavior should be discouraged/punished. A feedback and/or reward system plays a very important role in such a motivational process. Management buy-in is essential for such a system to work. Organizational 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. In order to have the desired motivational effect, the link between *performance* and *rewards* must be clear and visible (Huczynski & Buchanan, 2007, p. 254). Management *must* show their commitment to cultural change through **rewarding** employees who behave correctly (Brubakk & Wilkinson, 1996)(Huczynski & Buchanan, 2007, pp. 253-254). Organizations should be careful to not only "punish" those who break the rules. Most studies on behavioral change have shown that reward works better than punishment to modify behavior (Kabay, 2002, p. 35.10). 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.

This transformative change management process forms 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).

8.2.4 Review and Refine Culture

It is also necessary to review and refine the entire culture management process periodically. The modern business environment is a dynamic environment with constantly changing needs. In addition to this, new employees could join the organization and/or existing employees could leave/move. Various aspects of the culture might be affected by these changes. It is therefor essential to continuously manage the organization's culture to ensure that it continues to meet the organization's needs.

As mentioned earlier, the culture change process outlined in this section is not specific to information security. The next section will incorporate the contributions made by this thesis into the generic culture change process in order to demonstrate how an information security culture change process could work.

8.3 Information Security Culture Change

This section will integrate the use of the conceptual model for information security culture (introduced in chapter 5), the use of Bloom's taxonomy (as discussed in chapter 6), and the use of e-learning as an educational design and delivery medium (as discussed in chapter 7), into the organizational culture change process that was discussed in the previous section. The aim of this section is not to provide a definitive information security culture change process, but rather to demonstrate **how** the various contributions made in this thesis *could* be used to assist in addressing the human factor in information security. In order to aid understanding, the process will be discussed within the specific context of *user authentication*. Specifically the need for *secure password usage* and the fostering of a supporting *secure password culture* will be used as a continuous example throughout the remainder of this chapter. This example will be presented within the same culture change process outlined in the previous section. In terms of this process, the first step towards the changing/fostering of an information security culture would thus be to get top management to commit to the culture change process.

8.3.1 Top Management Commitment

In the case of information security top management would have to visibly support an *information security* culture. In this case an awareness campaign might, for example, use a poster, signed by the CEO, that is posted throughout the organization stating: *"At ABC we are committed to the integrity, availability and confidentiality of all our information"*. Top management also needs to commit to the information security culture by setting an example through their own behavior, 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). The information security vision statements should be followed by an organizational information security policy, which in turn would have to be supported by various levels of sub-policies and/or operational procedures. These policies and/or procedures will form the espoused values dimension of the information security culture and will thus be examined in more depth in the next subsection.

8.3.2 Define Change Needed in Business Context

As mentioned earlier, culture change is only meaningful if applied in a specific business context. It would thus be necessary to identify each area of information security for which the information security culture would have to be managed individually. The information security specific business context of the current example is the need for *user authentication* or the fostering of a *secure password culture*. Any of the various operational controls specified by the organization's information security policy/sub-policies could be viewed as a specific business context for the purposes of managing the organization's information security culture. Once a specific information security area has been identified, the current state of the underlying culture must be assessed.

Assess Current State

In order to assess the current state of an organizational information security culture in the context of a specific information security control/area of concern, one has to examine the underlying dimensions of the culture. For an information security culture it would thus be necessary to asses each of the four dimensions of such a culture. For the given *secure password usage* example, such an assessment could include:

- **Espoused values**: Are the espoused values supportive of the desired secure password culture? Does the information security policy state that users must be authenticated appropriately? Are there adequate procedural guidelines to prescribe the structure/minimum length of secure passwords?

- **Artifacts**: Are the visible artifacts desirable? Do employees change their passwords on a regular basis? Do employees keep their passwords a "secret"? Are the passwords that are used "strong"? Are there any violations of current policies/procedures governing the use of passwords?

- **Shared Tacit Assumptions**: Do the employees have the desired beliefs, values, and/or attitudes (shared tacit assumptions) regarding the usage of passwords? Does every employee believe his/her own password is also important? Would employees "share" their passwords with their colleagues?

- **Knowledge**: Do all employees have adequate knowledge to enable them to use passwords correctly? Does every employee know how to construct a "strong" password. Do employees know how to use mnemonic techniques to remember their passwords? Do employees know how to change their own passwords on the organization's information systems?

The above example is by no means complete, however, it should serve to demonstrate the kinds of questions that should be asked/answered during an assessment of the current information security culture. It is important to realize that not all aspects of the current culture will necessarily be easy, or even possible, to directly measure. 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 are understood, it is easy to predict the artifacts. One of the keys 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).

Define *Ideal* Future State

Once the current state of the information security culture has been assessed for the specific business context, the *ideal*/desired future state of the culture, in terms of the specific business context, must be determined. For an information security culture this ideal state could also be expressed in terms of the various dimensions of such a culture. For the given *secure password usage* example, describing the ideal future state could include:

- **Espoused values**: The espoused values should directly support the desired secure password culture. At a policy level the need for user authentication must be stated. At a sub-policy and/or procedural level specific guidance should be given, for example, for password usage these procedures could include:
  - All users must use passwords that are 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**: The description of the ideal state should also include the desired artifacts in terms of *measurable* "goals". For the password example, these could include:
  - All passwords should withstand a standard brute force attack performed with *tool x*.
  - 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 that would be required by individual employees in order to behave in the desired *ideal* way should be clearly defined. This should ideally be done in terms of the specific assessment outcomes for the related employee educational program. For the password example these specific assessment 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 the organizational information security culture the gap between the current state and the desired state must be analyzed for the specific business problem being addressed.

Analyze Gap

The gap between the current and the desired future state, will determine the amount of *work* that needs to be done to attain the future state. During this phase 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. The gap should also be analyzed in terms of each of the underlying dimensions of the information security culture. The difficulty/complexity of analyzing the gap, and determining the steps needed to get from the current culture to the desired culture, will not be equal across all of the various underlying dimensions of the information security culture. For example, determining, and addressing, the gap between the current and desired future *espoused values* should be straightforward. However, determining the gap between the current and desired future shared tacit assumptions will be much more difficult, and in some cases might even be impossible to accurately measure. This is one area where the conceptual model presented in section 5.6 of this thesis could be of assistance. The possible role(s) this model could play in the entire process from analyzing the current culture, to assessing the gap between the current and desired culture will be discussed in the next subsection.

The Role of the Conceptual Model

When analyzing the organization's current information security culture, and the gap between this culture and the desired future culture, one should be careful not to underestimate the complexity of such a culture. It could be tempting to assume that examining each of the underlying dimensions of the current information security culture in isolation, would be sufficient. However, according to Schein (1999a, p. 25) the biggest risk when working with culture is to oversimplify it. ”Culture is a complex concept that must be analyzed at every level before it can be understood” (Schein, 1999a, p. 25). In an information security culture, the behavior of employees (artifacts) occur as a result of interactions between the other dimensions of the culture. In order to determine the steps needed to change current behavior patterns (artifacts) into the desired *ideal* behavior, the interactions between the various underlying dimensions of the culture should also be viewed holistically. The conceptual model of information security culture presented in chapter 5 can to a certain extent assist in such a holistic understanding of the information security culture. Firstly, an *ideal* information security culture would be one where all the underlying dimensions of the culture are aligned **and** are at least equal to, or more secure, than the acceptable minimum baseline level of security. Figure 8.2 represents such an ideal culture in terms of the conceptual model presented in chapter 5.

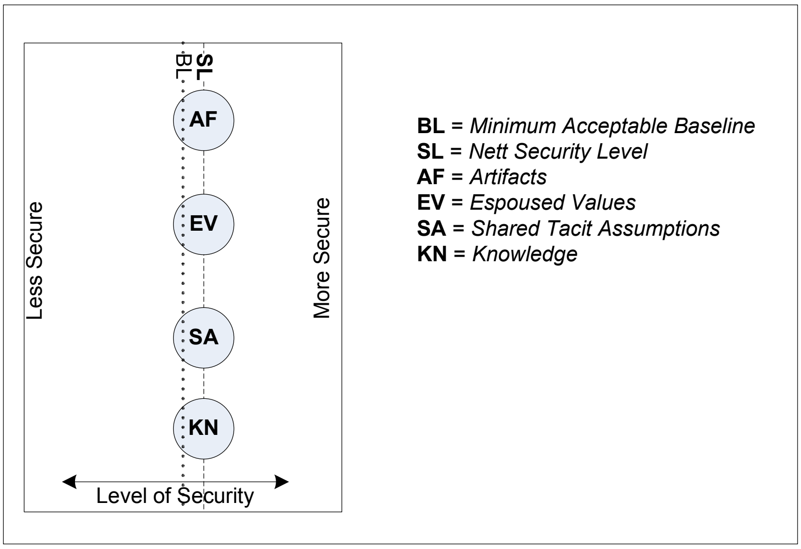


Figure 8.2: *Ideal* future culture

Assuming that the organization's goal is to attain such an *ideal* for the specific information security *area* being analyzed, the following *scenarios* will outline various areas where the conceptual model could contribute towards better understanding of the culture as a whole.

- When analyzing the current information security culture in order to determine the work that needs to be done to attain the ideal culture the relative "strength" of the underlying espoused values should not be analyzed in isolation. In an information security culture the minimum acceptable *baseline* serves as a useful guide to the determination of the relative "strength" of the espoused values. In comparison with the baseline, the espoused values could either be less secure than the baseline, equal to the baseline, or more secure than the baseline. This is represented in Figure 8.3. Should either the current, or the future espoused values be less secure than a minimum acceptable baseline, it would be necessary to adjust these values. However, if the espoused values are equal to, or slightly more secure, than the minimum acceptable baseline, these values would not need to be adjusted further. It is also possible that the espoused values are significantly more secure than a minimum acceptable baseline. In such a case it might be necessary to ascertain whether or not such ”strong” espoused values are really required. If espoused values are *too* strong, it might also have undesirable effects. For example, should the policy governing the usage of passwords require the use of passwords that are extremely complex and long, and this requirement is furthermore enforced at a technical and/or procedural level, it might result in more employees writing their password down due to the increased difficulty of remembering such a password. It would thus be more sensible to have a requirement that is less ”severe” but still equal to or stronger than a certain minimum baseline.

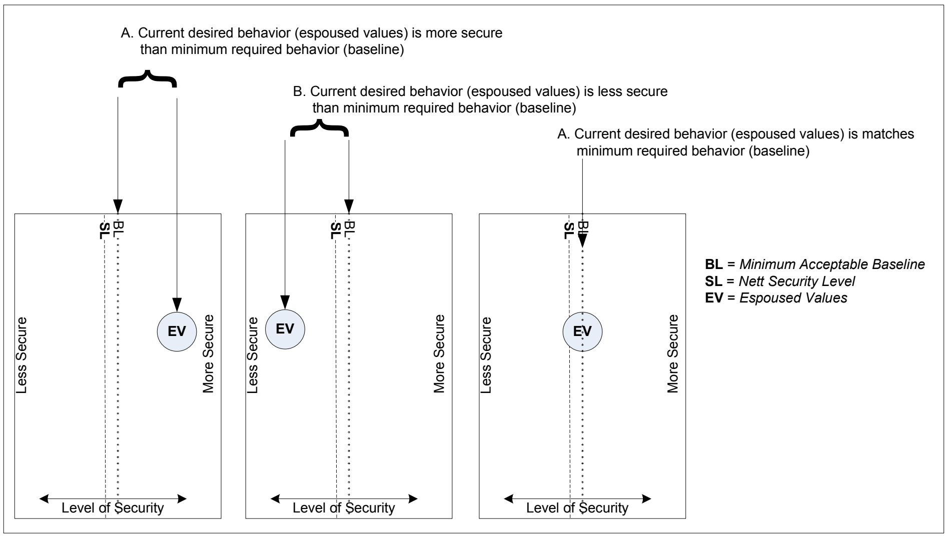

A. Current desired behavior (espoused values) is more secure than minimum required behavior (baseline)
B. Current desired behavior (espoused values) is less secure than minimum required behavior (baseline)
A. Current desired behavior (espoused values) is matches minimum required behavior (baseline)
BL
SL
EV
Less Secure
More Secure
Level of Security
BL = Minimum Acceptable Baseline
SL = Nett Security Level
EV = Espoused Values

Figure 8.3: Assessing the Gap: *Espoused Values* vs. *Baseline*

- Secondly, for each specific information security context, the observable behavior (artifacts) should be compared to the stipulated policy items (espoused values). For example, the regularity with which employees currently change their passwords should be compared to the operational guidelines that prescribe how often such passwords should be changed. It is possible for the observable artifacts to be more secure than the espoused values, less secure than the espoused values, or in line with the requirements stipulated in the espoused values. Figure 8.4 illustrates these possibilities (assuming the espoused values are at the *ideal* level).

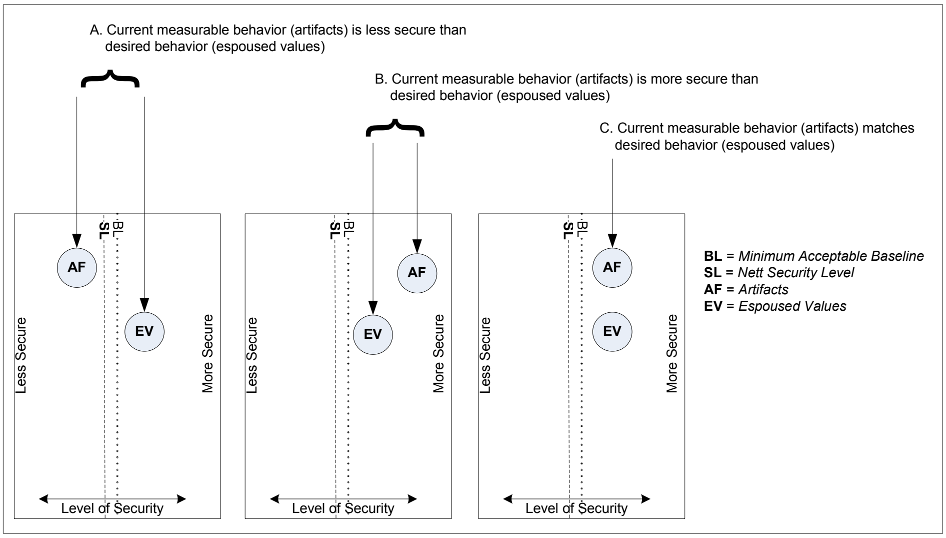

A. Current measurable behavior (artifacts) is less secure than desired behavior (espoused values)
B. Current measurable behavior (artifacts) is more secure than desired behavior (espoused values)
C. Current measurable behavior (artifacts) matches desired behavior (espoused values)
SL
BL
AF
EV
Less Secure
More Secure
Level of Security
BL = *Minimum Acceptable Baseline*
SL = *Nett Security Level*
AF = *Artifacts*
EV = *Espoused Values*

Figure 8.4: Assessing the Gap: *Espoused Values* vs. *Artifacts*

If the current artifacts are in line with the desirable espoused values, there is a chance that the underlying *shared tacit assumptions* and/or *knowledge* dimensions of the culture are also already in line with the espoused values. In such a case the culture would already be *ideal* for the specific information security context being examined. However, if the current artifacts are either more secure, or less secure, than the espoused values, it is an indication that either the underlying *shared tacit assumptions* dimension, and/or the *knowledge* dimension, are not aligned with the espoused values. In the case where the current artifacts are more secure than the espoused values, the misalignment of the underlying cultural dimensions would cause the culture to be less predictable. However, the overall culture could probably still be considered secure. Conversely, in the case where the artifacts are less secure than the desired espoused values, the underlying knowledge and/or shared tacit assumptions dimension would need to be improved in order to ensure secure behavior. The next *scenario* listed will explore this situation in more depth.

- If the current behavior of employees (artifacts) is less secure than the desired level of behavior (espoused values), one would have to determine the *cause* of this misalignment in order to address the misalignment. If one assumes the espoused values are both adequate and reasonable, the only remaining cause for such a misalignment would be that either the shared tacit assumptions, and/or the knowledge are not at the requisite level of security. The shared tacit assumptions of employees should ideally be assessed by means of individual and group interviews Schein (1999a, p. 86). Such a process could be difficult, expensive, and time-consuming. However, assessing whether or not the employees have the requisite knowledge *should* be easier. Such an assessment could, for example, be done by means of automated assessment modules in an e-learning environment. If the employees are found to have an adequate level of knowledge to enable them to behave according to the requirements as stated in the espoused values, one could assume that the underlying shared tacit assumptions of the employees *must* be the cause for the undesirable behavior. This would **not** provide any insight into the exact nature of the underlying beliefs, values, and/or attitudes that are negatively affecting the culture, but it would indicate that such undesirable shared tacit assumptions exist and need to be addressed. Figure 8.5 illustrates such a scenario.

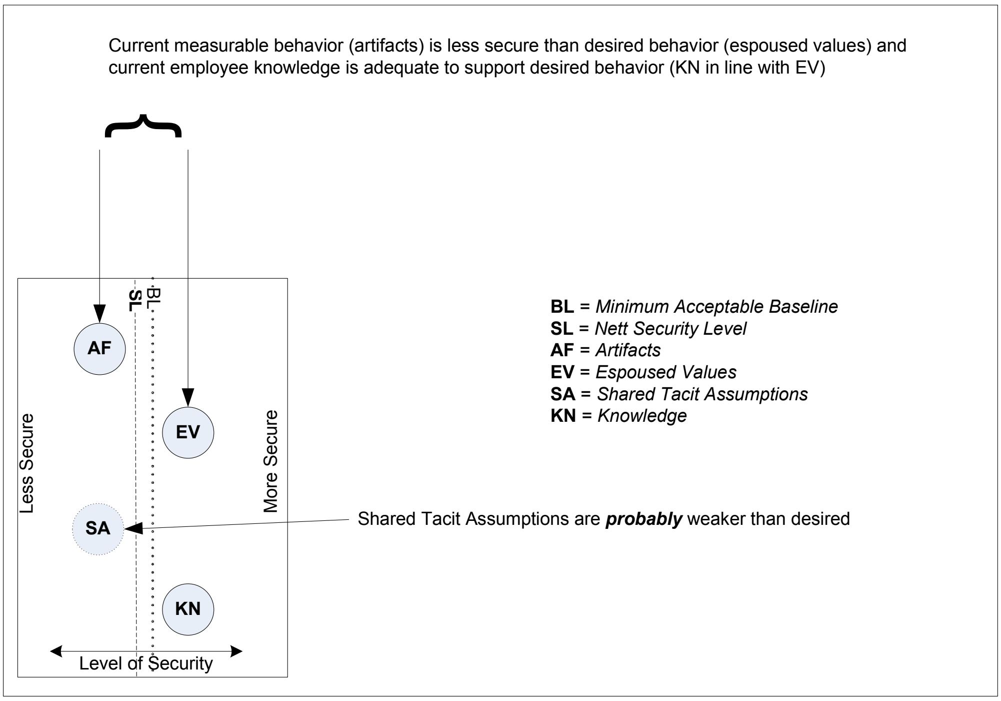

Current measurable behavior (artifacts) is less secure than desired behavior (espoused values) and current employee knowledge is adequate to support desired behavior (KN in line with EV)
BL
SL
AF
EV
SA
KN
Less Secure
More Secure
Level of Security
Shared Tacit Assumptions are ***probably*** weaker than desired
BL = *Minimum Acceptable Baseline*
SL = *Nett Security Level*
AF = *Artifacts*
EV = *Espoused Values*
SA = *Shared Tacit Assumptions*
KN = *Knowledge*

Figure 8.5: Assessing the Gap: *Adequate Knowledge* vs. *Shared Tacit Assumptions*

Alternatively, should the employees be found to have inadequate knowledge, this lack of knowledge will act as an "anchor" and will cause an infinite degree of elasticity between the various dimensions of the culture. Such a scenario is illustrated in Figure 8.6. The employees will **never** be able to act in the desired way because they do not have the necessary knowledge and/or skills to enable them to act securely. In such a case one cannot infer anything about the shared tacit assumptions. It would thus make sense to first address the *known* lack of knowledge before re-assessing the underlying culture.

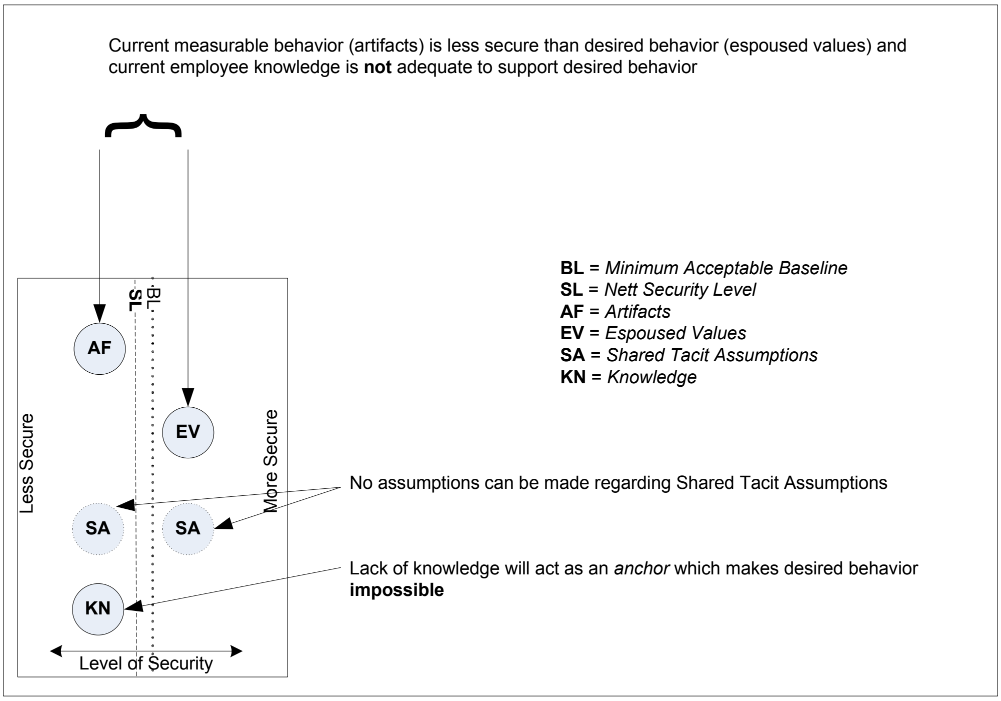

Current measurable behavior (artifacts) is less secure than desired behavior (espoused values) and current employee knowledge is **not** adequate to support desired behavior
SL
BL
AF
EV
Less Secure
More Secure
SA
SA
KN
Level of Security
BL = *Minimum Acceptable Baseline*
SL = *Nett Security Level*
AF = *Artifacts*
EV = *Espoused Values*
SA = *Shared Tacit Assumptions*
KN = *Knowledge*
No assumptions can be made regarding Shared Tacit Assumptions
Lack of knowledge will act as an *anchor* which makes desired behavior **impossible**

Figure 8.6: Assessing the Gap: *Inadequate Knowledge* vs. *Shared Tacit Assumptions*

The purpose of the various scenarios discussed in this subsection was not to provide complete *coverage* of all possible combinations of the various cultural dimensions. Instead, the scenarios serve to illustrate that an understanding of the interaction between the underlying dimensions of an information security culture *could* enable the person(s) responsible for managing the fostering of an information security culture to better understand the underlying cause(s) of undesirable employee behavior (artifacts). Such

an improved understanding could lead to a more optimal allocation of available resources during the culture change process. The conceptual model presented in section 5.6 of this thesis could *aid* in gaining such an improved understanding of the interaction between the underlying levels of an information security culture. In cases where a lack of more concrete information exists, the conceptual model could also in some cases aid in predicting the areas that need to be addressed. However, if the available resources allow it, it would be better to *measure* the actual underlying shared tacit assumptions and/or knowledge levels of employees in order to determine the gap.
Once the gap between the current and the desired future information security culture has been determined, the actual culture change should be initiated through a transformative change management process.

8.3.3 Transformative Change Management

Culture is extremely stable and, as discussed in section 8.2.3, any attempt to change it will thus have to start with a disconfirmation process. 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” create 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 and/or motivational programs to impart the needed information security knowledge to employees. For the password example used in this chapter 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.

It is important to realize that, firstly, 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.

Secondly, the above steps of the transformative change management process would not be implemented as discrete processes. To a large extent, the three steps will be dealt with as part of an internal information security awareness, training, and education program. This program will consist of both educational and motivational elements in order to address both the underlying need for information security *knowledge*, as well as the need to encourage new employee *behavior* through changing existing *beliefs, values, and attitudes* (shared tacit assumptions).

Thirdly, it should be noted that the aim of the *educational* programs is not exclusively to address the need for underlying information security *knowledge*. Education **can** to a large extent also address the underlying shared tacit assumption dimension of the organization's information security culture. Both *beliefs* and *attitudes* can be influenced by education. In psychological terms, *beliefs* are not the same as *attitudes* (Kabay, 2002, p. 35.10). A *belief* is cognitive information that does not necessarily have an emotional component, whilst an *attitude* is primarily an *emotional response* (Kabay, 2002, p. 35.10). Beliefs can change when contradictory information is presented. However this change might take time and requires the opportunity to reflect on current beliefs before change can take place (Kabay, 2002, p. 35.10). An *attitude* on the other hand is a "learned evaluative response, directed as specific objects, which is relatively enduring and influences behavior in a generally motivating way" (Kabay, 2002, p. 35.10). Attitudes can, to a certain extent, be addressed by motivational programs. However, "studies of *how attitudes are learned* consistently show that rewards and punishments are important motivators of behavior" (Kabay, 2002, p. 35.10). Ensuring employees have the desired attitudes will thus require more than just education.

Finally, all of the discussed elements, including the educational and motivational components, the punishment and rewards system, as well as top management commitment and support, form part of the overall transformative change management learning cycle discussed above. These processes should form an integrated "whole". The remainder of this section will discuss the "steps" that would form part of the design and delivery of specifically the underlying educational and motivational programs. It is important to note that, as discussed in section 1.5, the in-depth examination of the motivational components for this process falls outside the scope of the current thesis. Such motivational aspects will thus only be dealt with in sufficient depth to demonstrate the integrated nature of the educational and motivational campaigns.

Step 1: Define Learning Objectives

The formal educational components of the transformative change management process will consist of both an instructional design phase and an ongoing instructional delivery phase. During the instructional design phase, the use of Bloom's taxonomy, as discussed in chapter 6, can assist in determining exactly **what**, should be taught to **whom**. As discussed in chapter 6, the creation of a relevant taxonomy table would start with the expression of one or more **learning objectives**. The following examples might be applicable to the given password example:

- Learning Objective 1 (**LO1**): "Learners should be able to understand, construct and use passwords in the correct context"
- Learning Objective 2 (**LO2**): "Learners should be able to change their own passwords on the organization's financial information system"
- Learning Objective 3 (**LO3**): "Learners should be able to memorize and recall passwords of appropriate strength with the help of mnemonic techniques"

These learning objectives can be "general" in nature, like **LO1** listed above, or could be more specific, like **LO2**. The degree of specificity of learning objectives will to a large extent depend on the difficulty of the underlying subject matter and/or the specific intended target audience.

Step 2: Determine Target Audience

In order to plan learning activities that are suitable for the intended target audience, everyone who needs to be educated has to be identified. As discussed in section 7.3.3, learning activities and/or material should be customized according to the both current technical capabilities of the intended target audience, the type of user (end-user, IT, etc), and/or individual learning preferences. The need for specific information security related education should also be recorded in the human resources system. The human resources system can then, in conjunction with a learning management system, be used to ensure that each and every employee attains the requisite level of information security knowledge. For the password example it would be sensible to provide educational material suitable for the average organizational end-user. **All** users of information systems in the organization should complete this educational program.

Step 3: Plan Learning Activities

Once the relevant target audience for a specific learning objective has been established, various learning activities can be defined to address the learning objective. Examples of such learning activities were demonstrated in Table 6.4 of chapter 6. The activities listed in Table 6.4 of chapter 6 included learning at all of the six levels of the cognitive domain identified by Bloom's taxonomy. However, for an information security educational campaign focussing on culture change amongst organizational end-users, activities at the higher levels of the cognitive domain would not always be relevant. Specifically, for the *secure password culture* example, it would make more sense to have additional learning activities at the ***apply*** level of the cognitive domain, rather than having activities at the ***create*** level. Table 8.1 contains example learning activities for learning objective 1 (**LO1**) for an intended target audience of organizational end-users.

Level	**Verb**	**Sample Activities**
Evaluate	critique	Critique these two passwords and explain why you would recommend one over the other in terms of the security it provides.**(LA5)**
Analyze	analyze	Which of the following security incidents involving stolen passwords are more likely in our company?**(LA4)**
Apply	execute	Use the appropriate application to change your password for the financial sub-system. **(LA3-2)**
	practice	Practice using these mnemonic techniques to create and recall a **secure** password **(LA3-1)**
Understand	discuss	Why non alpha-numeric characters should be used in a password? **(LA2-3)**
	explain	Explain why your password should not be shared with **anyone**, not even your direct superior **(LA2-2)**
	outline	Outline responses you could use should someone from IT ask you to disclose your password over the phone **(LA2-1)**
Remember	define	What is the definition of *access control*? **(LA1)**

Table 8.1: Learning Activities relating to Learning Objective 1 (LO1), adapted from Anderson et al., 2001

Usually learning activities are not pre-categorized according to the levels of the Bloom's taxonomy directly. Instead, learning activities are planned according to the instructional designers perception of what would be needed to attain the learning objective. Once the preliminary set of learning activities has been planned, each of these learning activities is categorized appropriately according to both the categories of the knowledge dimension, and the levels of the cognitive domain, and then placed in a *taxonomy table.* As discussed in section 6.6.1, this taxonomy table can then be used to identify possible gaps in the curriculum. Identified gaps can be addressed by the addition of extra learning activities to the curriculum. The learning activities are placed in the appropriate cell of the taxonomy table by firstly examining the *noun* portion of the learning activity. This is used to determine which of the categories of the knowledge dimension would be the best match for the particular learning activity. For the learning activity **LA3-1** in Table 8.1, the *noun* portion would be the concept of *mnemonic techniques*, which can be classified as a form of procedural knowledge. A single learning activity could be classified into more than just one of the dimensions if necessary. The *verb* portion of the learning activity is used to determine at which level of the cognitive domain the activity would lie. For the learning activity **LA3-1** in Table 8.1, the *verb* is *practice*, which belongs at the **apply** level of the cognitive domain. Based on this, the particular learning activity is then mapped to the appropriate cell of the taxonomy table. This process will be repeated for all learning activities linked to the learning objective.

Step 4: Plan Assessments

Once the learning activities relating to the specific learning objective have been created, assessments for the various learning activities have to be designed. The reference point for any educational program should be a set of clearly articulated ”performance objectives” that have been developed based on an assessment of the target audience’s needs and requirements (Roper et al., 2005, p. 96). The role of assessments in an educational program is to ensure that these ”performance objectives” can be met by the successful learner. Assessments can be either formative or summative. Formative assessment provides feedback on learning progress to the learner him/her self. Summative assessments evaluate the overall success of the learner and in order to determine whether or not the learner has successfully completed the ”course”.

For **LO1** in the example listed above, the following summative assessment might be appropriate for some of the listed learning activities:

- Assessment 1 **(AS-1)**: The learner must be able to create a strong password and change his/her own password on the organization's network to this new strong password without assistance.

The above assessment (**AS-1**) serves only as an example. A complete curriculum would normally include a wide range of assessments. A similar process to the one used to place learning activities into the taxonomy table is also used for the main learning objective itself, **and** for the various assessments associated with these learning activities/learning objectives. Table 8.2 represents a completed taxonomy table for the learning objective (**LO1**) mentioned earlier, which is associated to the learning activities in Table 8.1 and the above assessment. It is important to note that a single activity, assessment or learning objective **can** be placed in more than one cell in the taxonomy table. In Table 8.2 the assessment **AS-1** has been placed in multiple cells since it tests both conceptual and procedural knowledge.

The Knowledge Dimension	The Cognitive Process Dimension					
	Remember	Understand	Apply	Analyze	Evaluate	Create
Factual Knowledge	**LA1**	**LA2-1** **LA2-3**			**A6**	
Conceptual Knowledge		**LA2-2**	**AS-1**	**LA4**	**A6**	
Procedural Knowledge			**LO1** **LA3-1** **LA3-2** **AS-1**		**A6**	
Meta-Cognitive Knowledge				**LA5**		

Table 8.2: Example Taxonomy Table adapted from Anderson et al., 2001

Step 5: Review and Revise Topic Coverage

As discussed in section 6.5, the curriculum designer can use a taxonomy table, like Table 8.2, to answer the four ”organizing questions”. By examining the taxonomy table the educator can easily identify areas of knowledge, or levels of the cognitive domain, that have not been covered by the learning activities. Similarly, areas where multiple activities cover the same levels of cognition and categories of knowledge can be identified.

In the example given in Table 8.2, the assessment and the primary learning objective clearly overlap. This means that the assessment is at the correct dimension of the cognitive domain **and** that it also tests the right kind of knowledge in order to properly evaluate the learner's mastery of the stated learning objective, thus answering the **"assessment question"**. Should it be necessary, due to lack of resources, to choose specific learning activities to prioritize, the taxonomy table can help to answer the **"learning question"** by determining which of the learning activities provide the best "coverage". One activity could, for example, "cover" more than just one type of knowledge. This also helps to answer the **"instruction question"** by helping educators plan learning activities in such a way that all necessary types of knowledge and levels of the cognitive domain are addressed for the specific target audience's needs. Finally, the **"alignment question"** can be addressed by ensuring that there exists no miss-alignments between learning objectives, learning activities, and assessments. If the learning activities **LA3-1** and **LA3-2** were omitted from the given example in Table 8.2, there would have been such a disconnect because the learning object and assessment both require the ability to **apply** knowledge, but none of the other learning activities would have addressed this need. Through the use of Bloom's taxonomy, information security educational program designers can ensure the pedagogical soundness of the planned curriculum. It would also be sensible at this stage to ensure that motivational aspects will be adequately addressed.

If an appropriate e-learning platform was chosen as delivery channel for the informational security educational and motivational programs, steps 1 to 5 listed above could have been performed with the assistance of the platform's *learning design system* (LDS). As discussed in section 7.4.1, a "good" *learning design system* allows the incorporation of an instructional design methodology of choice (Ismail, 2002). Once the appropriate content for a specific target user group has been determined, the next step would be to develop the instructional material.

Step 6: Develop Learning Content

Learning content for each of the learning activities identified has to be developed using the tools provided by the e-learning platform's *learning content management system* (LCMS). Various learning objects will be created by a combination of content developers, subject matter experts, and media developers. These learning objects are added to the learning object catalog and are linked to specific learning activities and automated assessments. Learning objects are also indexed according to meta-data tags. This allows the easy re-use and/or re-purposing of these learning objects in future learning programs. In the case of adaptive e-learning systems an explicit model of the knowledge domain to be taught also has to be created. This model then has to be linked to the specific elements in the adaptive educational material in order to let the adaptive system "know" what the specific page, or page fragment, presents. Knowledge behind pages is "the secret of adaptivity in all adaptive hypermedia systems" (Brusilovsky, 2003). Learning objects can thus include all forms of media and/or adative/programmatic content. These objects can thus cover the full range of awareness, training, and/or education requirements of the information security educational program. For the password example used in this section, learning objects related to some of the learning activities listed in Table 8.1 could, for example, include the following:

- A web page discussing the concept of access control and providing a formal definition (addresses learning activity **LA1**)
- An interactive "role playing game" where learners get to choose the appropriate responses from lists of possible answers in response to social engineering attempts (addresses learning activity **LA2-1**)
- A company wide competitive "memory game" where participants have limited time to memorize and recall various "passwords". The game is supported by web-pages explaining mnemonic techniques. Rewards are given for the best overall score, and for the "mnemonic rhymes" voted most entertaining by other staff members (addresses learning activity **LA3-1**)
- An awareness video listing various employee roles in the company and

explaining how each of these could lead to specific vulnerabilities should a person in such a role allows his/her password to be compromised (addresses learning activity **LA4**)

The above descriptions of learning objects serve only as example. It should however be clear that the scope of *what* such learning objects could comprise of is limited only by the availability of resources. Learning objects could be combined to create more complex learning objects. Once created, these learning objects must be deployed.

Step 7: Link to Learning Management System and Learning Support System

The completed learning objects are deployed to the *learning support system* (LSS) and simultaneously linked to the specific learning activities in the *learning management system* (LMS). The learning management system allows for the administration, documentation, tracking and reporting of learning activities, whilst the learning support system acts as a portal that provides learning access to the learners. The learning management system can be linked to the human resource system in order to ensure that each and every employee receive the requisite level of information security education. Data regarding assessments completed, etc, could in turn feed back into the human resource system if it is to serve as a job related performance indicator. The learning support system could also be used to encourage collaborative learning, and the discussion of contentious topics via forums. Such discussion could aid in fostering the eventual change of beliefs since it would allow employees to articulate and evaluate their own beliefs (Kabay, 2002, p. 35.10). Allowing interaction and collaboration is a very important feature of the learning support system. Student dissatisfaction rises dramatically when the social aspects of the classroom are missing (Ismail, 2002). Collaborative/interactive features in the learning support system can thus also increase the motivation to learn.

The above steps outline the overall transformative change management process and the roles that the use of Bloom's taxonomy and an e-learning platform could play in such a process. It is however **vital** to remember that both the disconfirmation and the internalization stages of such a process require top-management support. Top management must commit in terms of resources to enable rewards for desirable behavior, and in terms of authority to allow the punishment of 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). Education can **help** to change behavior, but must also be supported through the proper positive and/or negative incentives, as well as strong leadership.

8.3.4 Review and Refine Culture

The above "steps" will form part of a continuous cycle which will be executed for each underlying information security "business context" for which the culture needs to be fostered/changed. Due to the dynamic nature of both modern business and the field of information technology, it would also be sensible to review the "strength" of the culture needed. For example, if technological advances were to make all forms of memorized passwords obsolete, the need for a "secure password culture" would also become obsolete. It is therefor necessary to continuously review and refine the *ideal* state for each "business context" of the organization's information security culture. If necessary, the culture would need to be adjusted through the re-iteration of the above steps. The review process should also examine all underlying elements, such as the effectiveness of the educational programs, the need for additional motivation, etc, to ensure that the culture change process has the desired effect.

8.4 Conclusion

This chapter has shown how the various elements towards dealing with the human factor in information security, as discussed in chapters 5, 6, and 7, integrate with, and relate to, each other. In order to comprehensively address the human factor in information security, organizations must ensure that their employees have both the requisite knowledge, which enables them to perform the day-to-day function in a secure manner, as well as the desired attitude, which ensures that they *want to* behave securely. It has become widely accepted amongst the information security research fraternity that the ideal way to address both the dimension of the human factor in information security would be to **foster an information security culture** within the organization. Chapter 5 has discussed the concept of such a culture and has adapted the "generic" model used to define an organizational culture, to a specific model which can be used to define an information security culture. This chapter has demonstrated how this model can be used to enhance the understanding of the work needed to be done during a formal process to foster an information security culture within an organization. Part of such a formal transformative change management process to foster an information security culture, is a formal **information security educational program**. Chapter 6 has discussed the use of Bloom's taxonomy as a pedagogically sound way to determine the information security educational needs of employees. This chapter has shown, by means of example, how the use of Bloom's taxonomy can be integrated into the transformative change management process during the fostering of an information security culture. Once the educational needs of employees has been determined, the actual learning program(s) needs to be developed and "delivered". Chapter 7 has shown that e-learning environments would be very well suited to the needs of information security educational programs. As a final element, this chapter also showed how the use of such an e-learning platform could be incorporated into the overall process of fostering an information security culture. The process outlined in this chapter has thus demonstrated how the various theoretical and technological elements from this thesis form part of an integrated, holistic, process towards dealing with the human factors in information security. The next chapter will conclude this thesis.

Chapter 9

CONCLUSION

This chapter concludes this dissertation

9.1 Introduction

Organizational information security **depends** on the behavior of humans involved in the processes that secure organizational information resources. Humans are the weakest link in information security. In today's information society is is thus vital for organizations to ensure that the humans involved in their information security processes are a security asset and not a liability. This *human factor* in information security consists of two dimensions, namely *knowledge*, and *behavior*. These two dimensions are closely interrelated. Firstly, all humans involved in information security processes need to know **what** their security role(s) and responsibilities are, and also **how** these role(s) and responsibilities should be executed. However, even if organizational users do have the requisite knowledge, they might still choose not to behave in the desirable, secure manner. It is therefor also necessary to ensure the users behave in the correct way by instilling the underlying beliefs, values, and attitudes which would lead to such desirable behavior. Conversely, should a user want to behave in the desirable way, but lacks the requisite knowledge, such a user would still be unable to perform his/her security role(s) and responsibilities. It is thus necessary to address both these dimensions of the human factor in information security holistically. One way of addressing this human factor is through the fostering of an organizational information security culture. This thesis showed that, to a certain extent, existing research focussing on the establishment of such an information security culture, and/or on the underlying information security educational programs that support the fostering of such a culture, lacks a theoretical basis. The aim of this thesis was to address this lack by demonstrating how existing theory from the managerial- and the educational sciences could be adapted and/or used in order to improve the processes addressing the human factor in information security.

9.2 Summary of Results

The primary objective of the thesis, as presented in section 1.7, was to *demonstrate* ***how*** *existing theory can be modified and/or used when addressing the human factor in information security.* In order to achieve this objective, several sub-objectives had to be achieved.

The first sub-objective was to *adapt the* generic *model which defines organizational culture, as presented by Schein (1999a, pp. 15-16) to be specific to the needs of information security.* Chapter 5 modified Schein's model of organizational culture to be specific to the needs on information security. Chapter 5 also "borrowed" the concept of elasticity from the economical sciences in order to assist in understanding the interaction of the underlying dimensions of such an information security culture. This adapted model to define information security culture was extensively peer-reviewed and finally published as Van Niekerk and Von Solms (2010). This achieved the first sub-objective and thus answered the first research question from section 1.6, namely *"how can the* generic *definition of organizational culture be* ***adapted*** to be specific *to the needs of information security?"*.

The second sub-objective was to "*demonstrate how the use of a learning taxonomy can be used to add pedagogical rigor to information security educational programs*". This objective was addressed in chapter 6. Chapter 6 introduced Bloom's taxonomy of the cognitive domain, the most widely used learning taxonomy in education, as a possible tool to ensure that the content of information security educational programs is at the correct level required for the information security related learning needs of the intended target audience. The chapter also demonstrated how Bloom's taxonomy could be used in order to design learning objectives, learning activities, and assessments for information security educational programs. Through the use of this taxonomy, chapter 6 showed how information security practitioners can ensure the pedagogical integrity of information security learning programs. This answered the second research question of this thesis, namely *"how can a learning taxonomy be used to plan the contents of an information security educational program?"*.

The third sub-objective was to *"demonstrate the suitability of e-learning as a delivery medium for organizational information security educational programs."* This sub-objective was met in chapter 7. Chapter 7 outlined the requirements that should be met by any educational approach in order for it to meet the needs of organizational information security education. These requirements were previously published in Van Niekerk and Von Solms (2004). The features offered by e-learning were then matched to the listed requirements. E-learning was shown to not only meet the listed requirements of information security education, but to also be pedagogically more suitable than other approaches. This answered the third research question of this thesis, namely *"how should information security educational activities be delivered to organizational learners?"*.

The final sub-objective of this thesis was to *"provide a detailed overview demonstrating how the various elements contributed by this thesis integrates into existing transformative change management processes for the fostering of an organizational information security culture"*. This objective was met in chapter 8. Chapter 8 firstly integrated the use of the conceptual model presented in chapter 5 into an existing transformative change management for the fostering of an organizational information security culture. The thesis demonstrated how the conceptual model can assist during the analysis of the work that should be done in order to move from the current state of the organizational culture, to the desired future state. Secondly, the use of Bloom's taxonomy was integrated into the underlying educational processes which support the transformative change management process. The thesis demonstrated, by means of example, how this taxonomy could be used during the fostering of an information security culture. Finally, the thesis showed, by means of the same example, how the use of an e-learning environment could be integrated as a development and delivery platform for educational material during the overall transformative change management process. Collectively, this addressed the fourth sub-objective of the thesis and thus answered the fourth research question, namely, *"how can the various theoretical and technical elements be integrated into transformative change management processes in order to foster an organizational information security culture?"*.

Through meeting the four sub-objectives of the thesis, the primary objective, to *demonstrate **how** existing theory can be modified and/or used when addressing the human factor in information security*, was achieved. This answered the primary research question of this thesis, namely, "*how can existing theory be adapted and/or used to address the human factors in information security?*".

9.3 Summary of Contributions

The work in this thesis led to two primary contributions towards the body of knowledge in the field of information security. The following is a brief summary of these contributions:

- The first research contribution of this thesis was the adaptation of Schein's model of organizational culture to the specific needs of information security. Most current approaches to the human factor in information security recognize the need for the fostering of an organizational culture of information security. However, only a very small percentage of these approaches adapts the generic definition(s) for such a culture which has been "borrowed" from the management sciences to the specific needs of information security. None of the approaches that **do** adapt the generic model(s) to be more specific to the needs of information security focused specifically on the underlying need to information security related knowledge in an information security culture, or on the interaction between the various underlying dimensions of such a culture and the elastic effects of these underlying dimensions on the resulting employee behavior (artifacts). This thesis thus made a unique contribution which could improve the understanding of information security culture amongst information security practitioners.

- The second contribution was to show how the use of Bloom's taxonomy of the cognitive domain could be used to improve the pedagogical rigor of information security educational program design. Less than a quarter of current approaches towards dealing with the human factor in information security uses and/or proposes the use of a formal pedagogically sound approach towards information security education. None of these approaches that do propose the use of a formal approach towards information security education *uses* a learning taxonomy. The use of learning taxonomies is very widespread in education. The use of such taxonomies during the design of educational programs improves the overall pedagogical rigor of such programs. Bloom's taxonomy is the best known, and most widely used, of such learning taxonomies. By demonstrating how the use of Bloom's taxonomy could increase the pedagogical rigor of information security educational programs, this thesis has thus made an important contribution. The use of Bloom's taxonomy *per se* is not unique, however, the use of this taxonomy for the purposes of improving information security education has, as far as could be determined, never been proposed before.

9.4 Publications Stemming from this Research

The following publications stemmed directly from the work in this thesis:

- Van Niekerk, J., & Von Solms, R. (2006). The roles of e-learning in corporate information security. E-Learn, Waikiki Beach, Honolulu, Hawaii, Oct. 13-17, 2006 .

- Van Niekerk, J., & Von Solms, R. (2006b). Understanding information security culture: A conceptual framework. Information Security South Africa (ISSA), Johannesburg, South Africa, 5-7 July 2006.

- Van Niekerk, J., & Von Solms, R. (2008). Bloom's taxonomy for information security education. Information Security South Africa (ISSA), Johannesburg, South Africa, 7-9 July 2008.

- Van Niekerk, J., & Von Solms, R. (2009b). Using bloom's taxonomy for information security education. Education and Technology for a Better World. 9th IFIP TC 3 World Conference on Computers in Education, WCCE 2009, Bento Goncalves, Brazil, July 2009.

- Van Niekerk, J., & Von Solms, R. (2010). Information security culture: A management perspective. Computers & Security, 29 (4), 476 - 486.

The following publications stemmed from work closely related to the work in this thesis:

- Van Niekerk and Van Greunen (2006): Van Niekerk, J., & Van Greunen, D. (2006). Is user education the answer to online security problems? Proceedings of the Conference on Information Technology in Tertiary Education, Pretoria, South Africa, 18 -20 September 2006.
- Monk, Van Niekerk, and Von Solms (2010): Monk, T., Van Niekerk, J., & Von Solms, R. (2010). Sweetening the medicine: Educating users about Information Security by means of game play. South African Institute for Computer Scientists and Information Technologists (SAICSIT) 2010, October 11-13, 2010, Bela Bela, South Africa.
- Van Niekerk and Thomson (2010): Van Niekerk, J., & Thomson, K. (2010). Evaluating the Cisco Networking Academy Program's Instructional Model against Bloom's Taxonomy for the purpose of Information Security Education for Organizational End-users. Key Competencies in the Knowledge Society (KCKS 2010), World Computer Congress (WCC) 2010, Brisbane, Australia, 20-23 September 2010 .

9.5 Suggestions for Further Research

It is important to realize that the establishment of an organizational 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. The conceptual model proposed by this thesis can aid in the understanding of such a culture and could help the person(s) responsible for the fostering of such an information security culture within an organization to understand ”where” additional change is required in order to foster the culture. However, as it currently stands, the utility of this conceptual model is limited to improving *conceptual* understanding, and is not directly usable. Should methods become available to directly measure and normalize the strength(s) of the underlying dimensions represented by this model, the impact of the model would become much higher. Such metrics would enable organizations to directly manage specific aspects of an information security culture. Future research should focus on the development of such metrics.

References

Acs, Z. J., & Gerlowski, D. A. (1996). *Managerial economics and organization.* Prentice Hall.

Albrechtsen, E., & Hovden, J. (2009). The information security digital divide between information security managers and users. *Computers & Security*, *28*, 476-490.

Alnatheer, M., & Nelson, K. (2009). A proposed framework for understanding information security culture and practices in the saudi context. *7th Australian Information Security Management Conference, 1-3 December 2009, Kings Perth Hotel, Perth.*

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

Alvesson, M., & Sköldberg, K. (2000). *Reflexive methodology: New vistas for qualitative research.* SAGE Publications.

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

Amis, J. M., & Silk, M. L. (2008, July). The philosophy and politics of quality in qualitative organizational research. *Organizational Research Methods*, *11*(3), 456-480.

Anderson, L., Krathwohl, D., Airasian, P., Cruikshank, K., Mayer, R., Pintrich, P., et al. (2001). *A taxonomy for learning, teaching, and assessing: A revision of bloom's taxonomy of educational objectives, complete edition* (L. Anderson & D. Krathwohl, Eds.). Longman.

Ashenden, D. (2008). Information security management: A human challenge? *Information Security Technical Report*, *13*, 195-201.

Atkinson, S., Furnell, S., & Phippen, A. (2009, July). Securing the next generation: enhancing e-safety awareness among young people. *Computer*

Fraud & Security, 13-19.

Aytes, K., & Connolly, T. (2003). A research model for investigating human behavior related to computer security. *Proceedings of the Ninth Americas Conference on Information Systems.*, 2027-2031.

Banerjee, D., Cronan, T., & Jones, T. (1998). Modeling it ethics: A study in situational ethics. *MIS Quarterly*, *22*(1), 31-60.

Bell, J. (2007). E-learning: your flexible development friend? *Development and Learning in Organizations*, *21*(6), 7-9.

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.

Brusilovsky, P. (2003). Authoring tools for advanced technology learning environment. In T. Murray, S. Blessing, & S. Ainsworth (Eds.), (p. 377-409). Kluwer Academic Publishers.

Brusilovsky, P., & Henze, N. (2007). The adaptive web: Methods and strategies of web personalization. lecture notes in computer science. In P. Brusilovsky, A. Kobsa, & W. Neidl (Eds.), (Vol. 4321, p. 671-696). Berlin Heidelberg New York: Springer-Verlag.

Brusilovsky, P., & Millán, E. (2007). The adaptive web: Methods and strategies of web personalization. lecture notes in computer science. In P. Brusilovsky, A. Kobsa, & W. Neidl (Eds.), (Vol. 4321, p. 3-53). Berlin Heidelberg New York: Springer-Verlag.

Bryce, J., & Klang, M. (2009). Young people, disclosure of personal information and online privacy: Control, choice and consequences. *Information Security Technical Report*, *14*, 160-166.

Cameron, K. S., & Quinn, R. E. (1999). *Diagnosing and changing organizational culture: Based on the competing values framework.* Addison-Wesley.

Carr, N. G. (2003). IT Doesn't Matter. *Harvard Business Review*, 41–49.

Chang, S. E., & Lin, C. (2007). Exploring organizational culture for information security management. *Industrial Management & Data Systems*, *107*(3), 438-458.

Chen, C. C., Medlin, B. D., & Shaw, R. S. (2008). A cross-cultural investigation of situational information security awareness programs. *Information Management & Computer Security*, *16*(4), 360-376.

Choi, N., Kim, D., Goo, J., & Whitmore, A. (2008). Knowing is doing an empirical validation of the relationship between managerial information security awareness and action. *Information Management & Computer Security*, *16*(5), 484-501.

Clark, A. (2007, March). The future of e-learning. *Adults learning*, 14-15.

Cohen, F. (1999, June). Managing network security: The limits of awareness. *Network Security*, 8-10.

Collingridge, D. S., & Gantt, E. E. (2008). The quality of qualitative research. *American Journal of Medical Quality*, *23*, 389-395.

Collis, J., & Hussey, R. (2003). *Business research. a practical guide for undergraduate and postgraduate students.* (2nd ed.). Palgrave Macmillan.

Cone, B. D., Irvine, C. E., Thompson, M. F., & Nguyen, T. D. (2007). A video game for cyber security training and awareness. *Computers & Security*, *26*, 63-72.

Creswell, J. W. (1998). *Qualitative inquiry and research design: Choosing among five traditions. thousand oaks, ca: Sage, 1998.* Thousand Oaks, CA: SAGE.

Creswell, J. W. (2007). *Qualitative inquiry and research design: Choosing among five approaches.* (2nd ed.). SAGE Publications.

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

Da Veiga, A., & Eloff, J. H. P. (2009). A framework and assessment instrument for information security culture. *Computers & Security*, 1-12.

Da Veiga, A., Martins, N., & Eloff, J. H. P. (2007). Information security culture validation of an assessment instrument. *Southern African Business Review*, *11*(1), 146-166.

Deeny, E. (2003). Calculating the real value of e-learning. *Industrial and Commercial Training*, *35*(2), 70-72.

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

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

Dhillon, G. (2007). *Principles of information systems security.* John Wiley & Sons.

Dodge, R. C., Carver, C., & Ferguson, A. J. (2007). Phishing for user security awareness. *Computers & Security*, *26*, 73-80.

Drevin, L., Kruger, H. A., & Steyn, T. (2007). Value-focused assessment of ict security awareness in an academic environment. *Computers & Security*, *26*, 36-43.

Driscoll, M. P. (2000). *Psychology of learning for instruction.* Allyn and Bacon, Needham Heights.

Du, W., Shang, M., & Xu, H. (2006). A novel approach for computer security education using minix instructional operating system. *Computers & Security*, *25*, 190-200.

Easterby-Smith, M., Golden-Biddle, K., & Locke, K. (2008, April). Working with pluralism: Determining quality in qualitative research. *Organizational Research Methods*, *11*(3), 419-429.

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.

Endsley, M. (1995). Measurement of situation awareness in dynamic systems. *Human Factors*, *37*(1), 65-84.

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

Finne, T. (1996). The information security chain in a company. *Computers & Security*, *15*, 297-316.

Fuller, U., Johnson, C. G., Ahoniemi, T., Cukierman, D., Hernán-Losada, I., Jackova, J., et al. (2007). Developing a computer science-specific learning taxonomy. *SIGCSE Bull.*, *39*(4), 152–170.

Furnell, S. (2008, April). End-user security culture: A lesson that will never be learnt? *Computer Fraud & Security*, 6-9.

Furnell, S., Gennatou, M., & Dowland, P. (2001). Promoting security awareness and training within small organizations. *2nd AISM Workshop, Perth, Western Australia, November, 2001*.

Furnell, S., Gennatou, M., & Dowland, P. (2002). A prototype tool for is security awareness and training. *International Journal of Logistics Information Management*, *15*(5), 352-357.

Furnell, S., & Thomson, K. (2009a, February). From culture to disobedience: Recognizing the varying user acceptance of it security. *Computer Fraud*

& Security, 5-10.

Furnell, S., & Thomson, K. (2009b, November). Recognizing and addressing 'security fatigue'. *Computer Fraud & Security*, 7-11.

Garde, S., Heid, J., Haag, M., Bauch, M., Weires, T., & Leven, F. J. (2007). Can design principles of traditional learning theories be fullfilled by computer-based training systems in medicine: The example of campus. *International Journal of Medical Informatics*, *76*, 124–129.

Gaunt, N. (1998). Installing an appropriate is security policy. *International Journal of Medical Informatics*, *49*(1), 131-134.

Gaunt, N. (2000). Practical approaches to creating a security culture. *International Journal of Medical Informatics*, *60*(2), 151-157.

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*.

Goucher, W. (2008, April). Getting the most from training sessions: the art of raising security awareness without curing insomnia. *Computer Fraud & Security*, 15.

Grimson, J., Grimson, W., Flahive, M., Foley, C., OMoore, R., Nolan, J., et al. (2000). A multimedia approach to raising awareness of information and communications technology amongst healthcare professionals. *International Journal of Medical Informatics*, *58-59*, 297-305.

Guenther, M. (2001). Social engineering security awareness series. *[WWW document]. URL http://www.iwar.org.uk/comsec/resources/security-awareness/social-engineering-generic.pdf. Cited 15 December 2009*.

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

Hagen, J. M., & Albrechtsen, E. (2009). Effects on employees information security abilities by e-learning. *Information Management & Computer Security*, *17*(5), 388-407.

Hall, E. T. (1959). *The silent language* (2nd ed.). Anchor Books.

Hentea, M. (2005). A perspective on achieving information security awareness. *Proceedings of InSITE2005: Informing Science + Information Technology Education, Flagstaff, Arizona, USA, 16-19 June 2005*.

Hentea, M., Shea, M. J., & Pennington, L. (2003). A perspective on fulfilling the expectations of distance education. *CITC4 03: Proceeding of the*

4th conference on Information technology curriculum, 160167.

Herold, R. (2005). *Managing an information security and privacy awareness and training program.* Auerbach Publications.

Hevner, A. R., March, S. T., Park, J., & Ram, S. (2004, March). Design science in information systems research. *MIS Quarterly*, *28*(1), 75-105.

Hofstede, G. (1991). *Cultures and organizations: Software of the mind.* McGraw-Hill, London.

Hofstee, E. (2006). *Constructing a good dissertation.* EPE.

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

Hu, J., & Meinel, C. (2004). Tele-lab it-security on cd: portable, reliable and safe it security training. *Computers & Security*, *23*, 282-289.

Huczynski, A. A., & Buchanan, D. A. (2007). *Organizational behaviour.* (6th ed.). Prentice Hall.

IEEE 1484 Learning Technology Standards Committee. (2003). *IEEE Standard for Learning Technology-Learning Technology Systems Architecture (LTSA).*

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

International Standards Organization. (2004). *ISO/IEC TR 13335-1:2004 Information technology Security techniques Management of information and communications technology security Part 1: Concepts and models for information and communications technology security management. ISO/IEC, JTC 1, SC27, WG 1.*

International Standards Organization. (2005). *ISO/IEC 27002: Code of Practice for Information Security Management.*

Ismail, J. (2002). The design of an e-learning system: Beyond the hype. *The Internet and Higher Education*, *4*, 329-336.

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.

Johnson, E. C. (2006, February). Security awareness: switch to a better programme. *Network Security*, 15-18.

Kabay, M. E. (2002). Computer security handbook. In S. Bosworth & M. E. Kabay (Eds.), (4th ed., p. 35.1-35.18). John Wiley & Sons.

Katsikas, S. (2000). Health care management and information system security: awareness, training or education? *International Journal of Medical Informatics*, *60*(2), 129-135.

Klein, H. K., & Myers, D. M. (1999, March). A set of principles for conducting and evaluating interpretive field studies in information systems. *MIS Quarterly*, *23*(1), 67-94.

Knapp, K. J., Marshall, T. E., Rainer, R. K., & Ford, F. N. (2006). Information security: managements effect on culture and policy. *Information Management & Computer Security*, *14*(1), 24-36.

Kraemer, S., Carayon, P., & Clem, J. (2009). Human and organizational factors in computer and information security: Pathways to vulnerabilities. *Computers & Security*, *28*, 509-520.

Krippendorff, K. (2004). *Content analysis: An introduction to its methodology (second edition).* SAGE Publications.

Kritzinger, E., & Smith, E. (2008). Information security management: An information security retrieval and awareness model for industry. *Computers & Security*, *27*, 224-231.

Kruger, H. A., & Kearney, W. D. (2006). A prototype for assessing information security awareness. *Computers & Security*, *25*, 289-296.

Kruger, H. A., & Kearney, W. D. (2008). Consensus ranking an ict security awareness case study. *Computers & Security*, *27*, 254-259.

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

Layton, T. (2005). *Information security awareness: The psychology behind the technology.* AuthorHouse.

Leach, J. (2003). Improving user security behaviour. *Computers & Security*, *22*(8), 685-692.

Lonn, S., & Teasley, S. (2009). Saving time or innovating practice: Investigating perceptions and uses of learning management systems. *Computers & Education*, *53*, 686694.

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

Mason, J. (1996). *Qualitative researching.* SAGE Publications.

Materna, L. (2007). *Jump start the adult learner. how to engage and motivate* *adults using brain-compatible strategies.* Corwin Press.

May, C. (2008, September). Approaches to user education. *Network Security*, 15-17.

Mays, N., & Pope, C. (2000, January). Qualitative research in healthcare. assessing quality in qualitative research. *BMJ*, *320*, 50-52.

Meyrick, J. (2006). What is good qualitative research? a first step towards a comprehensive approach to judging rigour/quality. *Journal of Health Psychology*, *11*(5), 799-808.

Mitchell, R., Marcella, R., & Baxter, G. (1999). Corporate information security management. *New Library World*, *100*(1150), 213-227.

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

Mitnick, K., & Simon, W. (2006). *The art of intrusion: The real stories behind the exploits of hackers, intruders & deceivers.* Wiley Publishing.

Monk, T., Van Niekerk, J., & Von Solms, R. (2010). Sweetening the medicine: Educating users about Information Security by means of game play. *South African Institute for Computer Scientists and Information Technologists (SAICSIT) 2010, October 11-13, 2010, Bela Bela, South Africa.*

National Institute of Standards and Technology. (1998). *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.*

National Institute of Standards and Technology. (2003). *NIST 800-50: Building an Information Technology Security Awareness and Training Program. NIST Special Publication 800-50, National Institute of Standards and Technology.*

Nisar, T. (2002). Organizational determinants of e-learning. *Industrial and Commercial Training*, *34*(7), 256-262.

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* (4th ed.). Irwin/McGraw-Hill.

Organization for Economic Co-operation and Development. (2002). *OECD guidelines for the security of information systems and networks: Towards a culture of security.*

Pollitt, D. (2008). Whitbread gets the right blend for training: E-learning combined with classroom teaching benefits company and employees. *HUMAN RESOURCE MANAGEMENT INTERNATIONAL DIGEST*, *16*(7), 18-20.

Power, R., & Forte, D. (2006a, May). Case study: a bold new approach to awareness and education, and how it met an ignoble fate. *Computer Fraud & Security*, 7-10.

Power, R., & Forte, D. (2006b, October). Social engineering: attacks have evolved, but countermeasures have not. *Computer Fraud & Security*, 17-20.

Puhakainen, P. (2006). *A design theory for information security awareness.* Unpublished doctoral dissertation, Acta Universitatis Ouluensis A 463, The University of Oulu.

Rezgui, Y., & Marks, A. (2008). Information security awareness in higher education: An exploratory study. *Computers & Security*, *27*, 241-253.

Rheea, H., Kimb, C., & Ryuc, Y. U. (2009). Self-efficacy in information security: Its influence on end users information security practice behavior. *Computers & Security*, *28*, 816-826.

Ritchie, J., & Lewis, J. (2003). *Qualitative research practice: A guide for social science students and researchers.* SAGE Publications.

Robbins, S., Odendaal, A., & Roodt, G. (2003). *Organizational behaviour. global and southern african perspectives.* Pearson Education.

Roper, C., Grau, J., & Fischer, L. (2005). *Security Education, Awareness and Training: From Theory to Practice.* Elsevier Butterworth Heinemann.

Rudolf, K., Warshawsky, G., & Numkin, L. (2002). Computer security handbook. In S. Bosworth & M. E. Kabay (Eds.), (4th ed., p. 29.1-29.19). John Wiley & Sons.

Ruighaver, A., Maynard, S., & Chang, S. (2007). Organisational security culture: Extending the end-user perspective. *Computers & Security*, *26*, 56-62.

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

Saunders, M., Thornhill, A., & Lewis, P. (2007). *Research methods for business students.* (4th ed.). Financial Times Press.

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. *South African Computer Journal*, *31*, 46-52.

Schultz, E. (2004). Security training and awarenessdfitting a square peg in a round hole. *Computers & Security*, *23*, 1-2.

Sharma, S., & Sefchek, J. (2007). Teaching information systems security courses: A hands-on approach. *Computers & Security*, *26*, 290-299.

Shaw, R., Chen, C., Harris, A., & Huang, H. (2009). Information security awareness in higher education: An exploratory study. *Computers & Education*, *52*, 92-100.

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

Siponen, M. (2000). A conceptual foundation for organizational information security awareness. *Information Management & Computer Security*, *8*(1), 31-41.

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

Smilkstein, R. (2003). *We're born to learn. using the brain's natural learning process to create today's curriculum.* Corwin Press.

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

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

Sousa, D. A. (2006). *How the brain learns* (3rd ed.). Corwin Press.

South African Bureau of Standards - Recommended Practice: Glossary of IT Security Terminology ARP 057 (1st ed.). (2002).

Straub, D., & Welke, R. (1998). Coping with systems risks: security planning models for management decision making. *Management Information Systems Quarterly*, *22*(4), 441-469.

Theoharidou, M., Kokolakis, S., Karyda, M., & Kiountouzis, E. (2005). The insider threat to information systems and the effectiveness of iso17799. *Computers & Security*, *24*, 472-484.

Thomson, K., & Von Solms, R. (2005). Information security obedience: a definition. *Computers & Security*, *24*, 69-75.

Thomson, K., & Von Solms, R. (2006, May). Towards an information security competence maturity model. *Computer Fraud & Security*, 11-15.

Thomson, K., Von Solms, R., & Louw, L. (2006, October). Cultivating an organizational information security culture. *Computer Fraud & Security*, 7-11.

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

Unneberg, L. (2007). Grand designs for e-learning can e-learning make the grade for our biggest corporates? *INDUSTRIAL AND COMMERCIAL TRAINING*, *39*(4), 201-207.

U.S. Department of Education: Office of Planning, Evaluation, and Policy Development Policy and Program Studies Service. (2009). *Evaluation of Evidence-Based Practices in Online Learning: A Meta-Analysis and Review of Online Learning Studies.*

Valentine, J. A. (2006, June). Enhancing the employee security awareness model. *Computer Fraud & Security*, 17-19.

Van Niekerk, J., & Thomson, K. (2010). Evaluating the Cisco Networking Academy Program's Instructional Model against Bloom's Taxonomy for the purpose of Information Security Education for Organizational End-users. *Key Competencies in the Knowledge Society (KCKS 2010), World Computer Congress (WCC) 2010, Brisbane, Australia, 20-23 September 2010*.

Van Niekerk, J., & Van Greunen, D. (2006). Is user education the answer to online security problems? *Proceedings of the Conference on Information Technology in Tertiary Education, Pretoria, South Africa, 18 - 20 September 2006*.

Van Niekerk, J., & Von Solms, R. (2004). 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.

Van Niekerk, J., & Von Solms, R. (2006a). The roles of e-learning in corporate information security. *E-Learn, Waikiki Beach, Honolulu, Hawaii, Oct. 13-17, 2006.*

Van Niekerk, J., & Von Solms, R. (2006b). Understanding information security culture: A conceptual framework. *Information Security South Africa (ISSA), Johannesburg, South Africa, 5-7 July 2006.*

Van Niekerk, J., & Von Solms, R. (2008). Bloom's taxonomy for information security education. *Information Security South Africa (ISSA), Johannesburg, South Africa, 7-9 July 2008.*

Van Niekerk, J., & Von Solms, R. (2009). Using bloom's taxonomy for information security education. *Education and Technology for a Better World. 9th IFIP TC 3 World Conference on Computers in Education, WCCE 2009, Bento Goncalves, Brazil, July 2009.*

Van Niekerk, J., & Von Solms, R. (2010). Information security culture: A management perspective. *Computers & Security*, *29*(4), 476 - 486.

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

Von Solms, B. (2006). Information security - the fourth wave. *Computers & Security*, *25*, 165-168.

Von Solms, R., & Von Solms, B. (2004). From policies to culture. *Computers & Security*, *23*, 275-279.

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.

Vroom, C., & Von Solms, R. (2004). Towards information security behavioural compliance. *Computers & Security*, *23*, 191-198.

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.

Werlinger, R., Hawkey, K., & Beznosov, K. (2008). An integrated view of human, organizational, and technological challenges of it security management. *Information Management & Computer Security*, *17*(1), 4-19.

White House. (2003a). The National Strategy to Secure Cyberspace, Appendix: Actions and Recommendations (A/R) Summary. *[WWW document]. URL http://www.iwar.org.uk/cip/resources/pcipb/appendix.pdf. Cited 15 December 2009*.

White House. (2003b). The National Strategy to Secure Cyberspace, Priority III: A National Cyberspace Security Awareness and Training Program. *[WWW document]. URL http://www.iwar.org.uk/cip/resources/pcipb/priority_3.pdf. Cited 15 December 2009*.

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

Whitman, M. E., & Mattord, H. J. (2009). *Principles of information security* (3rd ed.). Thompson Course Technology.

Williams, P. (2008). When trust defies common security sense. *Health Informatics Journal*, *14*(3), 211-221.

Wood, C. C. (1997, December). 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.

Wylder, J. (2004). *Strategic information security.* Auerbach Publications.

Young, K. (2002). Is e-learning delivering roi? *Industrial and Commercial Training*, *34*(2), 54-61.

Appendices

During the research conducted towards this thesis, four peer-reviewed conference papers, and one journal publication stemmed directly from the work in this thesis. These publications are:

1. **Journal Publications**

   - **Appendix A** - Van Niekerk, J., & Von Solms, R. (2010). Information security culture: A management perspective. Computers & Security, 29 (4), 476 - 486.

2. **Conference Papers**

   - **Appendix B** - Van Niekerk, J., & Von Solms, R. (2006). The roles of e-learning in corporate information security. E-Learn, Waikiki Beach, Honolulu, Hawaii, Oct. 13-17, 2006 .
   - **Appendix C** - Van Niekerk, J., & Von Solms, R. (2006b). Understanding information security culture: A conceptual framework. Information Security South Africa (ISSA), Johannesburg, South Africa, 5-7 July 2006.
   - **Appendix D** - Van Niekerk, J., & Von Solms, R. (2008). Bloom's taxonomy for information security education. Information Security South Africa (ISSA), Johannesburg, South Africa, 7-9 July 2008.
   - **Appendix E** - Van Niekerk, J., & Von Solms, R. (2009b). Using Bloom's taxonomy for information security education. Education and Technology for a Better World. 9th IFIP TC 3 World Conference on Computers in Education, WCCE 2009, Bento Goncalves, Brazil, July 2009.

available at www.sciencedirect.com

ScienceDirect

journal homepage: www.elsevier.com/locate/cose

ELSEVIER

Computers & Security

Information security culture: A management perspective

J.F. Van Niekerk*, R. Von Solms

Institute for Information and Communication Technology Advancement, Nelson Mandela Metropolitan University, South Africa

ARTICLE INFO

Article history:
Received 30 October 2008
Received in revised form
19 October 2009
Accepted 20 October 2009

Keywords:
Information security
Information security culture
Corporate culture
Organizational learning
Schein's model

ABSTRACT

Information technology has become an integral part of modern life. Today, the use of information permeates every aspect of both business and private lives. Most organizations need information systems to survive and prosper and thus need to be serious about protecting their information assets. Many of the processes needed to protect these information assets are, to a large extent, dependent on human cooperated behavior. Employees, whether intentionally or through negligence, often due to a lack of knowledge, are the *greatest threat* to information security. It has become widely accepted that the establishment of an organizational sub-culture of information security is *key* to managing the human factors involved in information security. This paper briefly examines the *generic* concept of corporate culture and then borrows from the management and economical sciences to present a conceptual model of information security culture. The presented model incorporates the concept of *elasticity* from the economical sciences in order to show how various variables in an information security culture influence each other. The purpose of the presented model is to facilitate conceptual thinking and argumentation about information security culture.

1. Introduction

Today information can be seen as a basic commodity, similar to electricity, without which many businesses simply **cannot** operate (Carr, 2003). Unfortunately, in the interconnected world we live in, information is a lot more vulnerable than other basic commodities. It is highly unlikely that the actions of a discontent teenager on another continent can affect a company's electricity supply. The same cannot necessarily be said about the availability of information resources. It is thus vital for organizations to ensure their continued access to this commodity by protecting their information assets.

Many organizations will be unable to do business without access to their information resources. However, protecting these information resources often has no direct return on investment. Securing information resources does not as a rule generate income for an organization. Business people are therefore rarely interested in how their information resources are protected. From a business perspective, any solution would be adequate as long as it is cost-effective and takes into account issues such as productivity and ease of use (Wylder, 2004, p. 6). It can thus be argued that the goal of securing information is, to a certain extent, in conflict with the normal business goals of maximizing productivity and minimizing cost. Security is often seen as detrimental to business goals because it makes systems less usable. According to Wood (2005, p. 224) the only absolutely secure system is an unusable one.

This conflict between business and security objectives has become so well recognized, that the ability to resolve such conflicts should be seen as a key performance indicator for information security officers (Wood, 2005, p. 224). It can also be argued that the problem of managing information security, to a certain extent, is nothing more than the management of

* *Corresponding author*. School of ICT, PO Box 77000, Port Elizabeth 6031, South Africa. Tel.: +27 41 5043048; fax: +27 41 5043313.
E-mail addresses: johanvn@nmmu.ac.za (J.F. Van Niekerk), rossouw@nmmu.ac.za (R. Von Solms).

0167-4048/$ – see front matter © 2009 Elsevier Ltd. All rights reserved.
doi:10.1016/j.cose.2009.10.005

many similar conflicts. These ''conflicts of interests'' are of special importance once one starts dealing with the role(s) humans play in the information security process. Information security consists of many processes. Some of these processes are, to a large extent, dependent on human cooperated behavior. Employees, whether intentionally or through negligence, often due to a lack of knowledge, are the *greatest threat* to information security (Mitnick and Simon, 2002, p. 3). Without an adequate level of user **cooperation** 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). An organization's information security strategy should thus comprehensively address this ''human factor''.

Many recent studies have shown that the establishment of an **information security culture** in the organization is **necessary** for effective information security (Eloff and Von Solms, 2000; Von Solms, 2000). Through the establishment of such a culture, the employees can become a security asset, instead of being a risk (Von Solms, 2000). However, even with such a culture in place there still exist certain ''trade offs'' and ''conflicts of interests'' that should be managed. This paper aims to provide a conceptual framework to assist readers in understanding the interactions at various levels of such an information security culture. It is hoped that this framework, which incorporates elements of both managerial and economical science, will promote better understanding of information security culture amongst readers from a managerial background.

2. Research paradigm and rationale

The work in this paper is based on qualitative, or phenomenological-, research methods, as described in Creswell (1998). This paper should thus be seen as ''an inquiry process of understanding based on distinct methodological traditions of inquiry that explore a social or human problem'' (Creswell, 1998, p. 15). The research presented here does not attempt to define *new* knowledge, but rather to provide a more in-depth understanding of the phenomenon described as ''information security culture''. The work presented in this paper is a continuation, an expansion, of work previously published by the authors (Van Niekerk and Von Solms, 2006). As far as could be determined, the specific conceptual model, as well as the underlying interactions between the various levels of information security culture, as presented in this paper, has never been published before. It is the authors' belief that the use of this conceptual model could improve the understanding of the concept of information security culture. Since the concept of organizational culture has been largely ''borrowed'' by information security researchers from the humanities, it was deemed fitting to also ''borrow'' the research paradigm, used in this paper from the humanities.

The model for corporate culture as presented in Schein (1999) has become widely accepted amongst information security researchers (Schlienger and Teufel, 2003). However, this model describes corporate culture in *general*, and not information security culture *specifically*. In order to ensure a rigorous research approach, even concepts with a seemingly obvious meaning will be revisited in this paper. The description of these concepts in the presented information security framework is deemed necessary because there might exist differences between the ontologies commonly adhered to by information security specialists and researchers from the management sciences.

The aim of this paper is thus to present a holistic, conceptual model of information security culture, for information security practitioners and students. This model aims to clarify, at a conceptual level, the interactions between various elements comprising such an information security culture. The model also attempts to clearly define, in an information security context, concepts such as the strength and the stability (or predictability) of an information security culture. The model presented in this paper is intended to clarify, and improve, the understanding of existing concepts. It is hoped that this model will be of use to other information security researchers when examining the human factors in information security. Before the specific concept of an information security culture is examined, this paper will first explore the existing definition of corporate culture.

3. Corporate culture

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

A better way to think about culture is to examine the different ''levels'' at which culture exists (Schein, 1999, p. 15). This way of thinking about corporate culture is already widely accepted in information security (Schlienger and Teufel, 2003). In order to clarify these levels of culture, each of the levels will be briefly examined:

- **Level One: Artifacts**. Artifacts are what can be observed, seen, heard, and felt, in an organization (Schein, 1999, 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, 1999, p. 16). Observing the artifacts alone, however, does not explain **why** the members of the organization behave as they do (Schein, 1999, 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, 1999, 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, 1999, 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 consists 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, 1999, p. 17). However, it is possible for two organizations to have very different observable artifacts and yet share very similar espoused values (Schein, 1999, pp. 18–19). This is because there is an even deeper level of thought and perception that drives the overt, or observable, behavior (Schein, 1999, 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-day running of the organization depend on the shared tacit assumptions between the employees of that organization.

- **Level Three: Shared Tacit 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, 1999, 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, 1999, 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 and 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 *espoused 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. These three levels of corporate culture could be seen to correspond closely to the behavioral aspects of the ''human factor'' in information security. As mentioned earlier, this ''human factor'' in information security consists of two dimensions, namely knowledge and behavior, which are very inter-related. Due to the co-dependency between these two dimensions it is not possible to ignore the impact a lack of information security related knowledge would have on an organizational sub-culture of information security.

4. Information security culture

In ''normal'' definitions of organizational culture, the relevant job-related knowledge is generally ignored, because it can be assumed that the average employee would have the required 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. It **cannot be assumed** that the average employee has the necessary knowledge to perform his/her job in a secure manner. 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** normal activity in a secure manner. Information security knowledge, or a lack thereof, could therefore be seen s a fourth level to an information security culture that will affect each of the other three layers. For example:

4.1. *Artifacts*

Artifacts are *what actually happens* in the organization. Without the necessary skills and proficiencies, it would be impossible to perform information related tasks securely. Thus, for the day-to-day task to happen in a secure way, the users would have to have sufficient knowledge of **how** to perform their tasks securely.

4.2. *Espoused values*

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 in order to adequately address the organization's security needs.

4.3. *Shared tacit assumptions*

This layer consists of the beliefs and values of employees. If such a belief should conflict with one of the espoused values, knowing **why** a specific control is needed, might play a vital role in ensuring compliance (Schlienger and Teufel, 2003).

It should be clear that in an information security culture, knowledge **underpins** and **supports** all three the ''normal'' levels of corporate culture. Without adequate knowledge, information security cannot be ensured. The co-dependency between the three ''normal'' levels of an organization's information security culture, and knowledge, the ''fourth level'', implies that each of these four levels will have an impact on how ''secure'', or desirable, the overall information security culture will be. The first part of the model presented in this paper is thus an adaptation of Schein's model. This adaptation incorporates the underlying need for information security related knowledge into Schein's model. Knowledge is added as a fourth level of culture that is specific to an information security culture. This adaptation is necessary because in an information security culture the requisite knowledge **cannot be assumed to be present**. Fig. 1, provides a graphical exposition of this adaptation. In this presented conceptual model, knowledge is dealt with as an additional level to culture, as opposed to viewing knowledge as a sub-component of each of the original three levels. This is done solely because modeling knowledge as an additional level makes it easier to clearly show the effect that knowledge, or a lack thereof, would have on the overall information security culture.

In order to ensure an adequate level of information security knowledge, international standards such as ISO/IEC 27002 (International Standards Organization, 2005) recommends the use of an organizational information security awareness campaign. Awareness campaigns address the problems that a lack of knowledge could lead to. These campaigns help to create a culture of information security, by instilling the aspects of information security in every employee as a natural way of performing his or her daily job (Von Solms, 2000). Awareness campaign is **the** key element in ensuring that the knowledge level of an information security culture is of adequate ‘‘strength’’.

Before the interactions between the above levels of an information security culture can be examined in more depth, a final ‘‘tool’’ is needed. The model presented later in this paper also needs to borrow the concept of *elasticity* from the economical sciences.

5. Elasticity in information security culture

Elasticity is a general economic concept that measures the *change in one variable caused by changes in other, related variables* (Acs and Gerlowski, 1996, p. 49). In other words, elasticity measures how *sensitive* a variable is *to change* in another variable. In the presented model, the concept of elasticity will be borrowed, but instead of attempting to **measure** the change the concept will simply be used to explain the fact that change will be inherent in any such system and that the speed at which such change takes place depends on the *degree of elasticity* in the system. In order to provide more clarity of exactly what is meant by elasticity, another basic idea will first be borrowed from the economical sciences. Fig. 2 shows a basic supply and a basic demand curve. According to economic theory (Acs and Gerlowski, 1996, p. 45) the market will be in *equilibrium* if the quantity of goods or services demanded in the market is matched perfectly by the quantity of goods or services supplied in this market. In such a system, assuming all other variables are fixed, the price that could be asked for the goods or services would be perfectly static **and predictable**.

If, however, one of the variables in such a market were to change, for example if an increase in the quantity of goods or services demanded was to occur, the equilibrium would be disturbed. In such a case the other variable, the quantity of goods or services supplied would have to increase to match the increase in demand in order to bring the system back into equilibrium. While this situation of *disequilibrium*, exists, the price that could be asked for the goods or services supplied, would be more dynamic and **difficult to predict**. In Fig. 3, the price could fall anywhere in the shaded area, due to the increase in demand.

The term **elasticity** is used in economics to describe the relationship, shown in the above system, whereby increased demand would **cause** an increase in supply to eventually bring the system back into equilibrium. However, not all systems would have the same inherent *degree of elasticity*. Elasticity could in fact range from systems that are *infinitely elastic* to systems that are completely *inelastic*. In an infinitely elastic system, shown in Fig. 4, an increase in supply would have no effect on either the demand or the price people would be willing to pay. Fig. 4 thus does not even show the supply curve since its position in such a perfectly elastic system is irrelevant in determining the price. On the other hand, in a completely inelastic system, shown in Fig. 5, the variables would be ‘‘locked together’’. The supply and demand would thus always stay in equilibrium (Acs and Gerlowski, 1996, p. x). An example of such an inelastic system would be certain types of life saving medicines. People who need such medicines would be willing to pay **any** price for such medicines. For the purposes of this paper it is also important to note that in such an inelastic system consumers would be willing to pay any

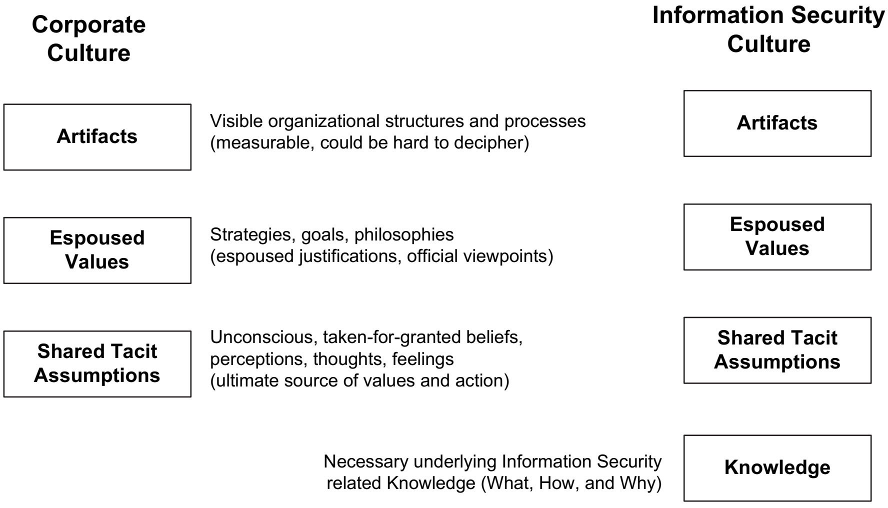

Corporate Culture
Information Security Culture
Artifacts
Visible organizational structures and processes (measurable, could be hard to decipher)
Artifacts
Espoused Values
Strategies, goals, philosophies (espoused justifications, official viewpoints)
Espoused Values
Shared Tacit Assumptions
Unconscious, taken-for-granted beliefs, perceptions, thoughts, feelings (ultimate source of values and action)
Shared Tacit Assumptions
Necessary underlying Information Security related Knowledge (What, How, and Why)
Knowledge

Fig. 1 – Levels of culture. Adapted from Schein (1999, p. 16).

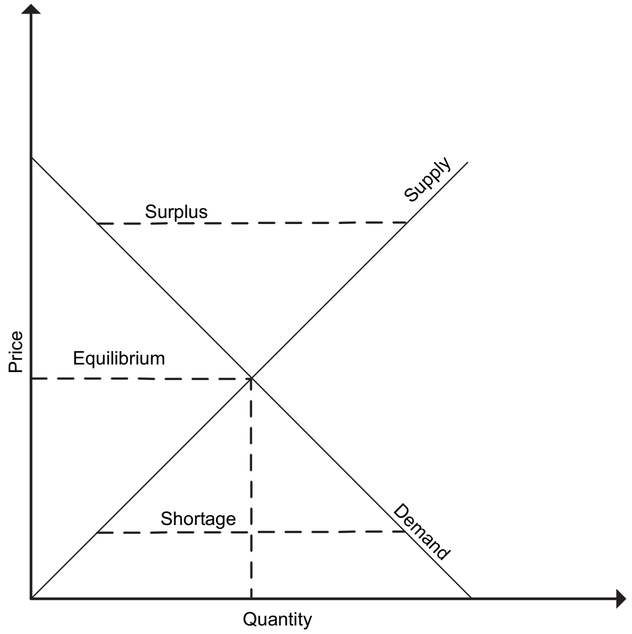


Fig. 2 – Market equilibrium (Acs and Gerlowski, 1996, p. 47).

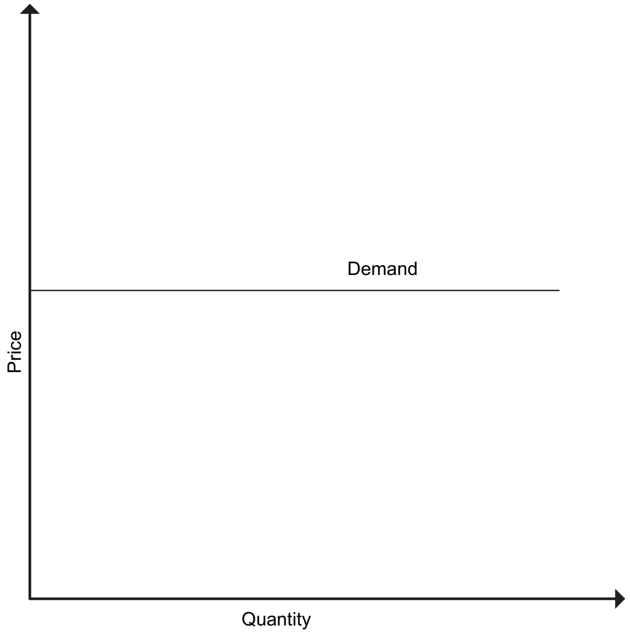


Fig. 4 – Perfectly elastic demand curve (Acs and Gerlowski, 1996, p. 52).

price but can only do so *if they have the necessary means*. Without the necessary means even consumers who are willing to pay any price would still be unable to do so.

A very **similar** situation to the one demonstrated above also exists when one looks at the human factors in an organization's information security environment. As discussed earlier, two of the basic "levels" of an information security culture would be the company's espoused values and the employees' shared tacit assumptions. To a certain extent, it can be argued that the policies and procedures comprising the espoused values in an information security culture are an indication of how much security management is "demanding" from employees. Similarly, the shared tacit assumptions can be seen as a reflection of how much "compliance" employees are willing to "supply". If one were to model these two "supply" and "demand" curves, the intersection of these curves would be an indication of the actual amount of effort employees are willing to give. In other words, the "price" in this case would be the measurable

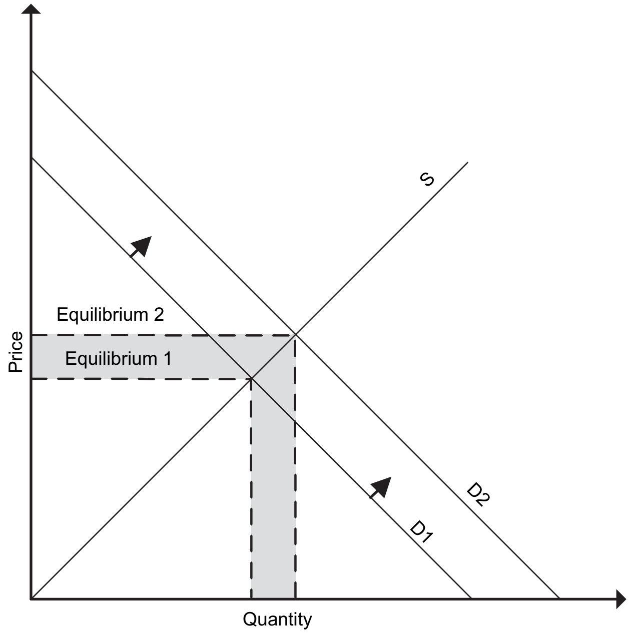


Fig. 3 – Change in equilibrium caused by increased demand. Adapted from Acs and Gerlowski (1996, p. 48).

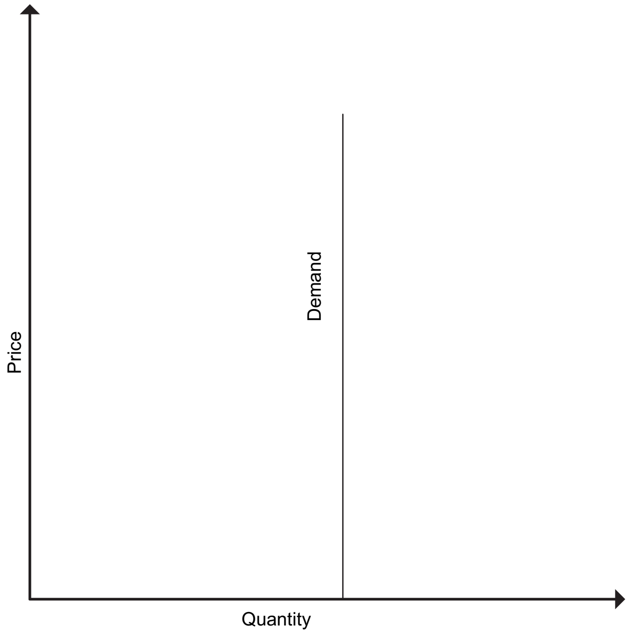


Fig. 5 – Perfectly inelastic demand curve (Acs and Gerlowski, 1996, p. 52).

employee participation in the organization's security efforts. Similarly, having the requisite knowledge to be able to participate in these security efforts is analogous to having the means to pay the required price. Such a system is modeled in Fig. 6. If the management expectations are in perfect equilibrium with the employees' shared tacit assumptions, the resulting effort employees expended on behalf of the organization's information security would be perfectly predictable (Fig. 6). Should management expect more than employees are willing to provide, it would be less easy to predict the actual amount of effort employees would expend towards the overall security goals (Fig. 7). It should also be clear that employees who are in fact willing to perform their security related roles would only be able to do so if they have the requisite knowledge.

In an information security culture there exists a causal relationship between the artifact level and the other three levels. In other words: the visible artifacts or, ''how the employees *actually* behave towards information security'', is caused by the combined effects of the espoused values, the shared tacit assumptions and the underlying information security knowledge. In Fig. 6 the artifact level is represented by the intersection of the lines. In Fig. 7 the artifact level is represented by the shaded area between the two possible intersection points. This reflects the fact that it would be difficult to predict how employees will actually behave (artifacts) in a scenario where management demands (espoused values) and the effort employees are willing (shared tacit assumptions), or able (knowledge), to supply are not in equilibrium. In such a causal relationship elasticity plays an important role. More ''demanding'' espoused values will have an elastic effect on the artifacts, and will require a matching increase in the shared tacit assumptions and/or the knowledge level(s). Thus, if an organization's management increases the ''strength'' of the organization's security related policies and procedures, the ''demand'' (security needed) will increase in Figs. 6 and 7. Such an increase will in turn require an increase in how much ''security effort'' employees are willing to give, or an increase in the security related knowledge of employees, or an increase in both. Without such matching increases in the other levels of the security culture, the culture will not be in equilibrium and it would thus become more difficult to predict the resulting employee behavior (artifacts).

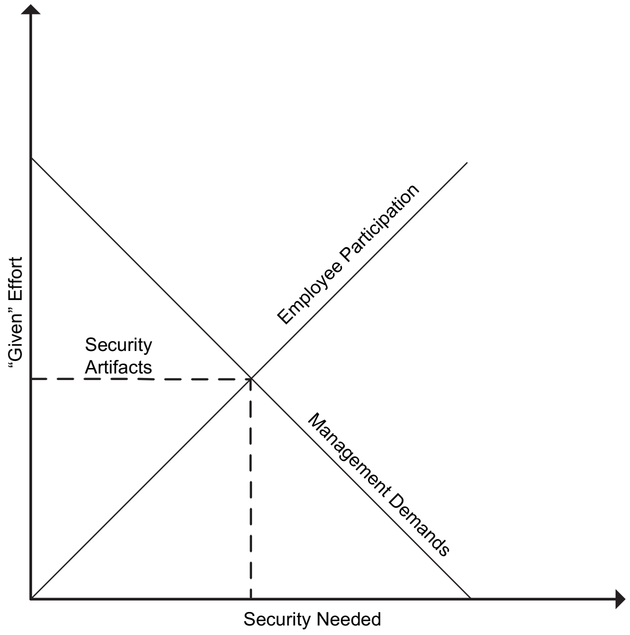


Fig. 6 – Management expectations in equilibrium with employee's security contribution. Adapted from Acs and Gerlowski (1996, p. 47).

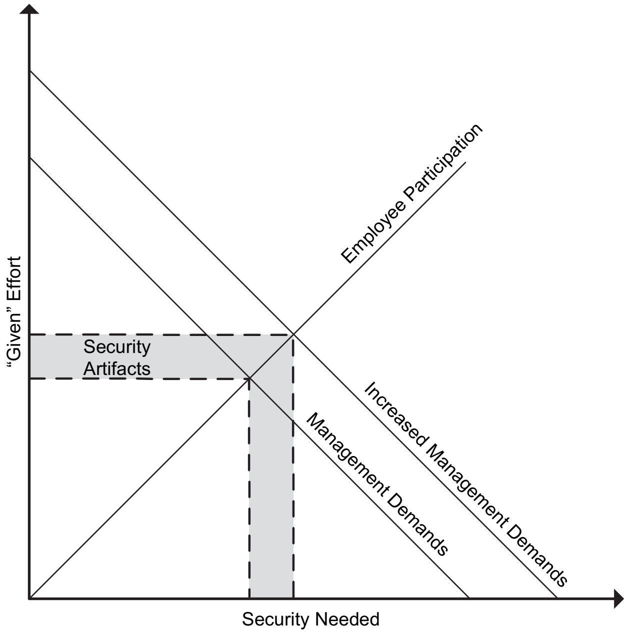


Fig. 7 – Increased management expectations require increased employee participation. Adapted from Acs and Gerlowski (1996, p. 48).

In order to simplify the representation of the elasticity concept, it should be noted that the dynamic system represented in Figs. 6 and 7 currently does not explicitly show the knowledge level. The knowledge level should, however, be assumed present in all cases. As mentioned above, this level can be seen as representing the ability to ''pay'' the demanded ''price'', and as such will have an equally important effect on the resulting employee behavior (artifacts) as the other two levels. The conceptual framework presented in the rest of this paper will attempt to clarify this causal relationship between the artifact level and the other three levels of an information security culture.

6. Information security culture: a conceptual framework

The overall effect of an organization's information security culture can be seen as an accumulation of the effects of each of the culture's underlying levels. Each of these levels can either positively or negatively influence the information security culture. In order to clearly demonstrate the interactions between these four levels, and their effects on the overall security efforts, it is necessary to first provide a basic reference framework.

6.1. *Basic elements and terminology of the conceptual framework*

The basic elements of this framework are depicted in Fig. 8. The representation in this and subsequent figures was chosen over the basic curves used in Figs. 2 and 3, because it is easier to model all the interactions in this way, rather than adding an additional dimension to the model used to examine the concept of elasticity. The elements in Fig. 8 can be described as follows:

- BL: Minimum Acceptable Baseline – This line indicates what would be an acceptable minimum security baseline; in other words, a culture whose net effect would meet the minimum requirements for some industry standard.
- SL: Nett Security Level – This line indicates the actual nett effect of the culture on the overall security effort. This line can be seen as the cumulative effect of the four underlying levels of the culture. The nett security level (SL) can either be more secure (to the right), less secure (to the left), or just as secure (overlapping) as the minimum acceptable baseline (BL).
- AF: Artifacts – This node represents the relative *strength* of the artifact level (AF) of the culture. If this node is to the left of the minimum acceptable baseline (BL), it indicates that the measurable artifacts are not as secure as they should be. A node to the right of the baseline (BL) would indicate artifacts that are even more secure than the acceptable minimum. A node exactly on the baseline (BL) would indicate artifacts that are just as secure as required by this baseline.
- EV: Espoused Values – This node represents the relative *strength* of the organization's espoused value level (EV). The various policies and procedures comprising this level could be more, less, or just as comprehensive than those recommended as the minimum acceptable baseline.
- SA: Shared Tacit Assumptions – This node represents the relative *strength* of the organization's shared tacit assumption level (SA). The underlying beliefs or values of the employees could be either more, less, or just as in favor of good secure practices as required by the minimum acceptable baseline.
- KN: Knowledge – This node represents how much knowledge the organization's employees have regarding information security. Employees can be more knowledgeable than a certain minimum level needed to perform their jobs securely, they could be less knowledgeable, or they could have exactly the minimum requisite level of knowledge.

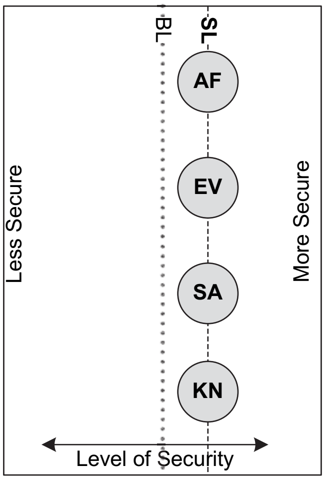


Fig. 8 – Basic elements of the conceptual framework. (BL = minimum acceptable baseline, SL = nett security level, AF = artifacts, EV = espoused values, SA = shared tacit assumptions, KN = knowledge.)

As mentioned above, the horizontal alignment of the nodes representing the various cultural levels, AF, EV, SA and KN, in comparison to the minimum acceptable baseline, should be interpreted as an indication of the relative *strength* of each level. In a similar fashion, the horizontal alignment of the nodes in comparison to the same horizontal alignment of the other levels should be interpreted as an indication of how *stable*, or predictable, the culture is. The nett security level line (SL) is an indication of the average strength of the culture, or the nett combined effect of all four the levels. The culture depicted in Fig. 8 should thus, firstly, be interpreted as a *strong*, or secure culture. All four levels in Fig. 8 have a strength greater than the baseline, which also results in a nett security level that is positive, or greater than the baseline. Secondly, all four levels are perfectly aligned with each other. This results in a culture that should be completely *stable*, or predictable. One could also say that this would be perfect cultural *equilibrium*. The culture depicted in Fig. 8 could thus be said to be the *ideal* culture in terms of information security since it is both *strong* and *stable*.

The terms *strong*, and *stable*, as used above, should not be confused as being indicative of how pervasive or resistent to change the culture might be. According to Schein (1999, pp. 25–26), corporate culture is always strong in the sense of affecting every single aspect of daily life in an organization at a more than superficial level. Culture is also always stable, in the sense that it resists attempts at changing it. In that sense, culture is one of the most stable facets in an organization (Schein, 1999, p. 26). When referring to an **information security culture**, the term *strong*, as used in this paper, should be interpreted as a **desirable** culture that is conducive to information security. The term *stable*, as used in the same context, should be interpreted as an indication of how **predictable** the resulting artifacts, or nett security level of the culture would be for any specific scenario.

All of the factors mentioned above would contribute to the overall desirability of an information security culture. How *strong* and *stable* an organization's information security culture is, would depend on the interaction between the various levels of culture.

6.2. *Interpreting the conceptual framework*

Each of the underlying cultural levels will contribute towards the overall strength and stability of such a culture. For example, if an organization has espoused values that are in line with recommended best practices for security, this would make the overall security better. Conversely, should the espoused values fail to address all relevant security related issues, the overall security would be weaker.

The combination of the espoused values, and the ''elasticity effect'', of the shared tacit assumptions and the user knowledge on these espoused values, results in the visible, and measurable *artifacts*. From a security viewpoint, the artifact level is a very good indication of the overall security of the organization's information, since this level reflects what *actually happens* in the day-to-day operations. In cases where the various levels are not in equilibrium this artifact level becomes more difficult to predict. In such cases the degree of elasticity in the specific system would determine how long it would take before the system ''settles'' into equilibrium. In infinitely elastic systems this equilibrium might never be attained, whilst completely inelastic systems would always be in equilibrium. In terms of the degree of elasticity in a security culture, the knowledge level also plays a very specific role in that it can act as an ''inhibitor'' of the elastic effect. A lack of knowledge can prevent employees who want to act securely from doing so. For the specific areas where the necessary security knowledge is lacking, this lack results in an infinite degree of elasticity in the security culture. The visible behavior (artifact level) cannot move towards equilibrium because the employees lack the means to provide the desired behavior.

Figs. 9–13 show a few possible effects interactions between the various levels of culture could have on the overall state of the organization's information security.

The examples in Figs. 9–13 assume that the desirability of the various levels can be quantified and normalized to the same scale. In other words, it is assumed that, for example, the desirability of the relevant espoused values can be measured and expressed as a value that indicates the contribution of this level towards the overall security. It is also assumed that the other levels can be expressed in the same way, and that the scale of such measurements can be normalized in such a way that these values will indicate the relative desirability of that level when compared to the other levels. The line marked **SL**(*Security Level*) represents the nett effect of the interactions between various levels of the culture. The five examples can be interpreted as follows:

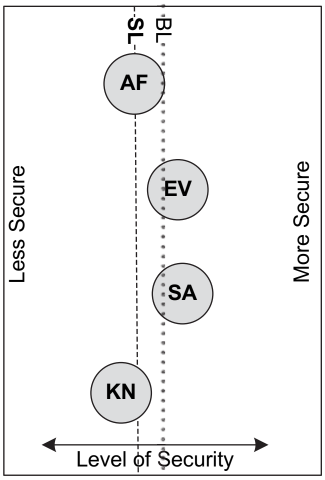


Fig. 10 – Insecure and ''Mostly Stable'' Culture. (BL = minimum acceptable baseline, SL = nett security level, AF = artifacts, EV = espoused values, SA = shared tacit assumptions, KN = knowledge.)

''Neutral'' and Stable (Fig. 9). The desirability of the various levels of culture is ''neutral'', or average. In other words the *strength* of each level neither exceeds, nor falls short, of the minimum acceptable baseline standards. The Nett Security Level (SL) perfectly overlaps the Baseline (BL). Since all the levels have the same level of desirability, the various levels will neither negate nor reinforce the effects of other levels on the overall security. The effects of such a culture would thus be predictable and stable.

Insecure and ''Mostly Stable'' (Fig. 10). Both the espoused values and the shared tacit assumptions in this culture are of sufficient *strength* to meet the minimum acceptable baseline standard. However, in this culture, the employees do not have the requisite level of information security related knowledge. It is thus possible for the measurable artifacts to fall short of the minimum acceptable baseline. For example, either the

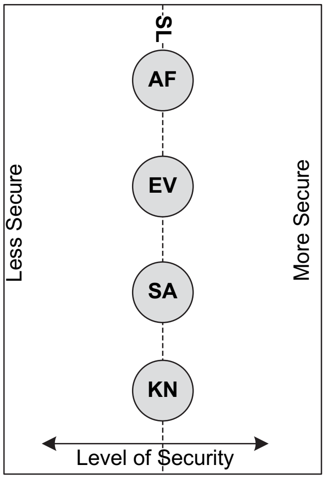


Fig. 9 – ''Neutral'' and stable culture. (BL = minimum acceptable baseline, SL = nett security level, AF = artifacts, EV = espoused values, SA = shared tacit assumptions, KN = knowledge.)

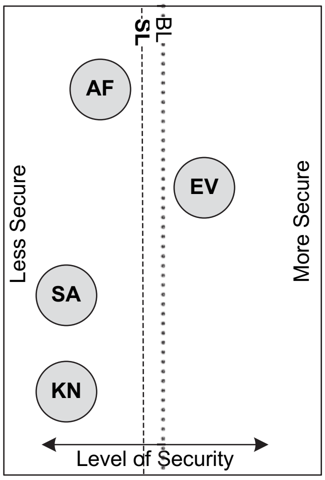


Fig. 11 – Insecure and unstable culture. (BL = minimum acceptable baseline, SL = nett security level, AF = artifacts, EV = espoused values, SA = shared tacit assumptions, KN = knowledge.)

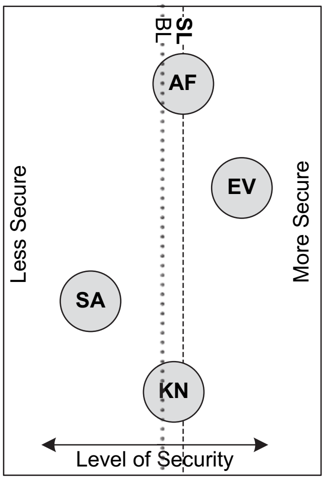


Fig. 12 – Secure and unstable culture. (BL = minimum acceptable baseline, SL = nett security level, AF = artifacts, EV = espoused values, SA = shared tacit assumptions, KN = knowledge.)

policy dealing with a specific control might be lacking because the person(s) responsible for creating the policy lacks the necessary knowledge, or the knowledge needed to implement this control in day-to-day operations might be lacking amongst the responsible employees. In both such cases, the resulting artifacts *might* be weaker than expected. This misalignment between the various levels also means that it would be difficult to predict the exact relative strength of the overall security level. In this case one could probably assume that the culture will be mostly predictable, hence stable, because the lack of knowledge would probably not apply equally to all controls. This culture would also have an almost infinite degree of elasticity and the artifacts would thus never perfectly align with the espoused values and shared tacit assumptions. This is due to the lack of supporting information security knowledge. The lack of knowledge acts as an "anchor" and prevents the artifacts from aligning with the other layers. By addressing the lack of knowledge the degree of elasticity inherent in this culture could be reduced. This would increase the rate at which a more desirable state is reached where the artifacts align with the shared tacit assumptions and espoused values.

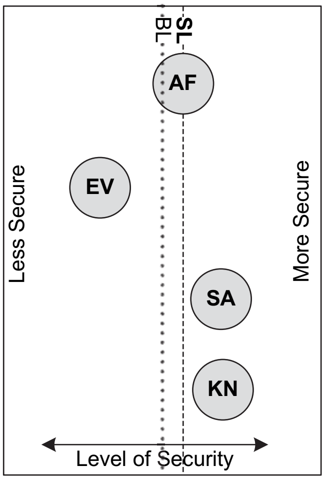


Fig. 13 – Secure and unstable culture. (BL = minimum acceptable baseline, SL = nett security level, AF = artifacts, EV = espoused values, SA = shared tacit assumptions, KN = knowledge.)

Insecure and Unstable (Fig. 11). The various levels contributing to the culture are not aligned. This would mean that the nett effects of the culture might be unpredictable, due to the opposing forces at play in this culture. The espoused values are very desirable, but the users lack the requisite knowledge and do not have the desired beliefs and values, resulting in a measurable artifact level that is not secure. For any specific security control, a user may, or may not, have the requisite knowledge to fulfill his/her role in the implementation of that specific control. That same user could also agree with the relevant espoused value, or could have beliefs that are contrary to that espoused value. It would thus be very difficult to predict the nett security level of this culture. Such a culture would not be a desirable culture. In order to make this culture more desirable it would be necessary to address both the lack of knowledge and the underlying shared tacit assumptions of the employees. Once these aspects have been addressed the various levels of the culture will re-align to become more "stable". The rate at which this re-alignment will take place would be dependent on the degree of elasticity present in the system.

Secure and Unstable (Fig. 12). The various levels contributing to the culture are not aligned. The espoused values are desirable, and the users have adequate knowledge. The high level of user knowledge in this case somewhat negates the fact that the users do not have the desired beliefs and values, resulting in an overall culture that is more secure than the minimum acceptable baseline. However, this culture should be considered not desirable, because its effects cannot always be predicted. It might be possible for the users to behave insecurely with regards to a specific security control because the specific control conflicts with their beliefs (Schlienger and Teufel, 2003). In this culture the knowledge level is already sufficient to enable employees to behave securely. However, there is still a gap between the knowledge level and the espoused values. This gap will have to be addressed before the culture could possibly align with the espoused values. The degree of elasticity in this culture could be reduced by addressing the shared tacit assumptions of employees. If employees can be convinced of the importance of their respective roles and responsibilities towards the organization's information security the culture *should* start to align itself.

Secure and Unstable (Fig. 13). As in Fig. 12 the various levels contributing to the culture are not aligned. In this case the figure models the scenario where the organization is small and all staff are skilled IT professionals who have both the requisite knowledge levels and the personal belief systems that enable secure behavior. In such a case it is quite likely to have a secure artifact level **despite** the fact that there are little or no espoused values. This is still not a desirable culture. Without adequate security policies (espoused values) in place, there can be no guarantees of desirable behavior. The appointment of additional staff members who might lack the underlying security knowledge can easily move the observable artifacts in this model back towards the less secure side. Unless the organization actively addresses the lack of espoused values this culture will have an infinite degree of elasticity. The espoused values will never align themselves without active intervention.

The above examples only reflect a few possible scenarios. It should, however, be clear that the nett effect of any information security culture can be influenced, either positively, or negatively, by how "secure" the underlying levels of such a culture is. In such a model it might also be possible to deduce the relative state of one or more of the cultural levels. For example, if the organization has *good* espoused values, but the measurable artifacts indicate *bad* security, it might be inferred that the employees lack either the required knowledge or the desired attitude. In the cultures represented by Figs. 12 and 13 the culture can probably be "improved" by involving employees in the process of creating the espoused values. In both these cultures involving the employees in a "negotiation" process when creating espoused values could reduce the "gap" between the espoused values and shared tacit assumption layers. In both cases this would make the culture more predictable, and thus more desirable. In all cases insight into the degree of elasticity inherent in the culture can help guide decisions as to what course would be most appropriate to help manage the culture. If a system has infinite elasticity it will never align itself unless the underlying cause for this infinite elasticity is addressed. If management wants to see faster changes at the artifacts layer, i.e. how people behave on a day-to-day basis, steps should be taken to decrease the degree of elasticity. From a management perspective, the "perfect security culture" would be one that is completely inelastic. Such a culture will always instantly reflect changes in the espoused values of the organization.

7. Conclusion

This paper suggested that, for an effective information security culture, the requisite information security knowledge amongst an organization's users could be seen as a fourth layer to Schein's (1999) model for corporate culture. The various interactions between the layers of such an information security culture were then presented conceptually.

The conceptual model presented showed that the nett overall effect that an information security culture would have on the organization's information security efforts would depend on the relative desirability, or *strength*, of each underlying level in such a culture. Furthermore, the alignment of the strengths of the individual underlying culture levels relative to the other levels, would to a large extent determine how predictable, hence *stable*, the effects of such a culture would be. The ideal culture would thus be one where all four underlying levels are stronger than the minimum acceptable baseline, and are also perfectly aligned relative to each other. The example in Fig. 8 would be such an *ideal* culture.

The model also attempted to show that management demands and employees' participation are strongly interrelated. In an information security culture the visible artifacts are thus dependent on both the supporting knowledge as well as this relationship between espoused values (management demands) and shared tacit assumptions (employees' underlying beliefs and values). In any information security culture a certain degree of elasticity will be present. This elasticity will determine whether or not the shared tacit assumptions will over time align itself to the espoused values of the organization. It will also determine how fast changes will occur if the system is not infinitely elastic. The lower the degree of elasticity in the system, the faster it would take for a possible re-alignment to happen. From a management perspective it would thus be highly desirable to reduce the degree of elasticity in such a culture as much as possible.

In its current form, the model's primary contribution is at a *conceptual* level where it aids in the understanding of information security culture. The current model has limited "hands-on" use. In a scenario where an organization's measurable artifacts are undesirable, a manager who is sure that the organization's espoused values is of adequate strength and who is also certain his/her staff members have adequate knowledge, might infer that the employees' beliefs and values are not in line with the espoused values. Based on the presented model, such a manager will also be able to deduce that he/she can make the artifacts easier to predict by addressing the shared tacit assumptions, for example by trying to convince the employees to buy into the espoused values. Through campaigns aimed at improving the employees' attitude towards security management can reduce the degree of elasticity inherent in the culture and thus speed up the pace at which the measurable artifacts become more in line with the espoused values. Alternatively the espoused values could be "relaxed" to be more in line with the shared tacit assumptions, similar to the idea of adjusting the governing variables in a double-loop learning system (Smith, 2001). This might result in a culture that is slightly less secure but more predictable.

In either of the above mentioned approaches, use of the current model would only provide very vague guidance to someone wanting to manage an information security culture. In order for this model to become useful as a "hands-on" cultural management tool additional research would be required. If one could accurately quantify and normalize the various levels at play in this conceptual model it should be possible to use the model to manage specific aspects of an information security culture more precisely. The assumption made when presenting the example, namely that the desirability of the various levels can in fact be quantified and normalized to the same scale, should by no means be taken as an assertion made by this paper. The aim of the paper was not to present such metrics and normalization processes but rather to show, at a certain level of abstraction, how this conceptual model could be used to reason about information security culture. It should, however, be possible to quantify and normalize the various factors for certain subsets of controls. For example, it might be possible to turn the presented conceptual model into a working model for a smaller sub-problem such as mapping the relationships between the four levels for password usage. If the required processes and metrics are developed, the conceptual framework might also play a valuable role in the management of an information security culture. For example; a metric that quantifies the actual degree of elasticity in an information security culture would be a very useful tool to have. This type of usage for the presented model could possibly be addressed by future research efforts. For the present, the contention of this paper is simply that the conceptual model presented, could assist in improving the understanding of an information security culture. The work in this paper should thus be seen as an attempt to lay a solid foundation on which future research could be built.

Appendix. Supplementary data

Supplementary data associated with this article can be found in the online version at doi:10.1016/j.cose.2009.10.005.

REFERENCES

Acs ZJ, Gerlowski DA. Manegerial economics and organization. Prentice Hall; 1996.

Carr NG. It doesn't matter. Harvard Business Review 2003:41–9.

Creswell JW. Qualitative inquiry and research design: choosing among five traditions. Thousand Oaks, CA: Sage; 1998.

Eloff MM, Von Solms SH. Information security management: an approach to combine process certification and product evaluation. Computers & Security 2000;19(8):698–709.

International Standards Organization. ISO/IEC 27002: code of practice for information security management; 2005.

Mitnick KD, Simon WL. The art of deception: controlling the human element of security. Wiley Publishing; 2002.

Schein EH. The corporate culture survival guide. Jossey-Bass Inc.; 1999.

Schlienger T, Teufel S. Information security culture – from analysis to change. Johannesburg, South Africa: Information Security South Africa (ISSA); 2003.

Siponen MT. Five dimensions of information security awareness. Computers and Society 2001:24–9.

Smith MK. Chris Argyris: theories of action, double-loop learning and organizational learning [WWW document]. URL, http://www.infed.org/thinkers/argyris.htm; 2001. Sited 4 March 2004.

Smit PJ, Cronjé GJde J. Management principles: a contemporary South African edition. JUTA; 1992.

Van Niekerk J, Von Solms R. Understanding information security culture: a conceptual framework. Johannesburg, South Africa: Information Security South Africa (ISSA); 2006.

Von Solms B. Information security – the third wave? Computers & Security 2000;19(7):615–20.

Wood CC. Information security roles & responsibilities made easy. Information Shield. 2nd ed.; 2005.

Wylder J. Strategic information security. CRC Press; 2004.

Johan van Niekerk is a senior lecturer in the Department of Information Systems at the Nelson Mandela Metropolitan University. He has been in the employ of the NMMU for the past 13 years and has been a full-time academic for the past 9 years. He is currently working towards a PhD as part of the research efforts at the Institute for Information and Communication Technology Advancement. His research focuses on the human factors in information security.

Prof. Rossouw von Solms is a well know researcher in information security. He has had many previous publications in this field and is employed as a full-time researcher in the Institute for Information and Communication Technology Advancement at the Nelson Mandela Metropolitan University.

The Role of E-Learning in Corporate Information Security

Johan Van Niekerk , Rossouw Von Solms
Centre for Information Security Studies, Nelson Mandela Metropolitan University
South Africa
{johanvn,rossouw}@nmmu.ac.za

Abstract: Modern humans live in a society that is dependant on information. Information and its uses permeate all aspects of modern life. For many organizations, information has become one of its most valuable assets. It is thus imperative for organizations to protect their information resources. The protection of information, also known as information security, is to a large extent dependant on the active involvement of humans in the information security process. Each and every user in an organization is supposed to have enough knowledge regarding his/her role(s) in the information security processes. Unfortunately this is rarely the case. Employees, whether intentionally or through negligence, often due to a lack of knowledge, are the greatest threat to information security. This paper forms part of an ongoing research project which attempts to address this lack of knowledge. This paper presents the rationale and motivation of current work which investigates the possible use of e-learning systems, as well as the use of artificial intelligence in such e-learning systems to address the needs of corporate information security education. The purpose of this paper is to acquire feedback and input from researchers and practitioners in the e-learning field of study.

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]. Modern businesses operate in an emerging global information society. The current global economy is increasingly dependent on the creation, management, and distribution of information resources. Today, many organizations need information systems to survive and prosper. It is therefore imperative for modern organizations to take the protection of their information resources seriously. Information security is typically implemented in the form of various security controls [Barnard and Von Solms, 2000, Van Niekerk and Von Solms, 2003]. These controls are typically selected from an internationally accepted standard. There exist several such standards and codes of practice. Some of the better known examples would include the ISO/IEC 17799 [ISO/IEC 17799, 2005] and 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]. 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 [ISO/IEC 17799, 2005, ISO/IEC TR 13335-1, 2004]. 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 forms part of an ongoing research project at the Nelson Mandela Metropolitan University in South Africa. The aim of the project is to address the some of the human factors in information security. This paper introduces the educational needs of corporate information security programs, as well as the rationale for attempting to use e-learning, and specifically adaptive e-learning, to address these educational needs. It is the author's hope that the background and rationale presented in this paper will form a basis for acquiring feedback and input from researchers who specialize in the field of e-learning. 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 [Siponen, 2001]. Both the authors of this paper have in the past worked in the field of information security as their primary research focus area. This paper should thus be seen as an attempt to gain additional input from e-learning researchers, regarding future research directions, and should not be seen as an attempt to present completed, or significantly new, work.

2. The Human Factors in Information Security

Information security controls can generally be sub-divided into three categories: Physical controls, Technical controls and Operational controls [Van Niekerk and Von Solms, 2004]. Physical controls deal with the physical aspects of security, for examp le; 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 [Mitnick and 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 contro ls, alone, offer true security is settling for the illusion of security [Mitnick and Simon, 2002, p. 4].

Siponen 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 [Siponen, 2001]. 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 800-16, 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, increasing awareness of security issues is the most cost-effective control that an organization can implement [Dhillon, 1999]. 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 [Van Niekerk and Von Solms, 2004].

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 and 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. The establishment of such a culture has been discussed in many recent papers [Van Niekerk and Von Solms, 2003, Van Niekerk and Von Solms, 2005, Schlienger and Teufel, 2003].

3. 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. Van Niekerk and Von Solms [Van Niekerk and Von Solms, 2004] identified these requirements and discussed the pedagogical implications of these requirements in depth. The following is a brief summary of the identified requirements

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

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 [Siponen, 2001]. Instead of ”re-inventing the wheel” when designing user education programs, information security practitioners should thus ”borrow” methodologies from the educational sciences. Researchers who wish to solve information security education problems should thus be basing their work on sound pedagogical models.

Van Niekerk and Von Solms [Van Niekerk and Von Solms, 2004] showed that the same elements required for effective information security education, are present in outcomes based education (OBE), an existing, and pedagogical sound, methodology. Subsequently, it has been shown how OBE could be effectively incorporated into the transformative change processes required to actively manage the introduction of a corporate information security sub-culture [Van Niekerk and Von Solms, 2005]. However, even though OBE has been shown to be pedagogically adequate to the requirements of information security education, in practice the cost-implications of some of the identified requirements might be prohibitive.

The need to customize learning materials for individual learners can been shown to be central to both the requirements of an information security education program, and an outcomes based educational program [Killen, 2000, Van Niekerk and Von Solms, 2004, NIST 800-16, 1998, p. 43]. However, customizing learning material to individual learners would be both time-consuming and expensive. Most organizations only spend a very small portion of their total IT budget on information security, and only a small portion of this is usually allocated to information security education [Ernest & Young, 2004]. It has been found that most organizations can significantly improve its information protection with cost-effective awareness and training initiatives [Ernest & Young, 2004]. Affordability would thus have to be a major deciding factor in determining the suitability of an information security educational program. In most cases, this would mean that an alternative to classroom training would be needed.

4. E-learning for Information Security

Probably the most cost-effective substitute for traditional classroom training is to provide employees with intranet based instruction, hence e-learning. Web-based training material has been used to great effect in many other areas and has proven to be an extremely cost-effect delivery mechanism for such programs. For example, AT&T was able to cut classroom time in half for 4500 customer service reps 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. This also means that it would be very easy to maintain, manage and update web-based training materials.
- 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.
- Web-based training materials can include programmatic components.

The fact that web-based training materials can include programmatic components has several important implications for its possible use in information security education [Van Niekerk and Von Solms, 2002]. Firstly, it would make it feasible to add automated assessment modules to such training materials, which means that learners can receive continuous feedback on their progress. Automated feedback, in combination with the fact that web-based material would be available at all times, means that learners could be made responsible for their own learning. This satisfies the fourth requirement for information security education listed above. Automated assessment would also enable organizations to hold learners accountable for their own learning, which satisfies the fifth requirement for information security education. Finally, the inclusion of programmatic components in a web-based educational environment could make it possible to develop content to automatically adapt to the individual preferences of learners.

According to Hentea [Hentea et al., 2003] the key to automation of web-based education lies in the effective application of the computer science field artificial intelligence (AI). Automated feedback in the form of hyperlinked documents are already available, however, more advanced forms of personalization will require both knowledge of educational theory and design, and technical (artificial intelligence) expertise [Hentea et al., 2003]. In order to automatically customize learning experiences to individual learners, such an intelligent learning environment would have to determine the learner's intent and detect learner misconceptions [Lester et al., 1997]. This diagnosis must be performed as non-invasively as possible [Lester et al., 1997]. This problem, and several other issues regarding the creation of automatically adaptive web-learning material, form part of the relatively new field of study know as adaptive e-learning.

As a field of study, adaptive e-learning can already demonstrate some impressive results [Brusilovsky, 2004]. However, very few of these systems are actually being used currently to teach real courses [Brusilovsky, 2004]. The problem with current systems is not their performance, but their architecture [Brusilovsky, 2004]. In addition to this, as far as could be determined, little or no current knowledge exists regarding the suitability of these technologies for use in information security education in an organizational environment.

Conclusion

This paper briefly introduced the educational needs of corporate information security programs. Modern organizations must protect their information resources. This protection, known as information security, depends on the organization's employees. Employees must be educated regarding their roles and responsibilities in the information security process. They should also be taught the necessary skills they need in order to effectively apply this knowledge. In order to be effective, information security educational programs should meet certain basic requirements, and should be based on a sound pedagogical model. One of these requirements is the need to customize learning material to the needs of individual learners. Web-based information security educational programs can contain programmatic components. These components might be used to automatically adapt the learning content to the needs of individual learners. Several techniques from the field of artificial intelligence could contribute to the creation of such automatically adapting learning material. However, little or no knowledge exist regarding the use of such components *specifically for information security education*. This paper thus proposes a new research project that will attempt to answer the question: *How can artificial intelligence be used to create adaptable learning material for information security education*? It is hoped that the presentation of this paper will lead to valuable feedback and inputs into this proposed research direction, from e-learning researchers.

References

Arroyo, I., Schapira, A., and B.P., W. (2001). Authoring and sharing word problems with AWE. Proceedings of the Tenth International Conference on Artificial Intelligence in Education, pages 527–529.

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

Brusilovsky, P. (2004). Knowledgetree: A distributed architecture for adaptive e-learning. In WWW Alt. '04: Proceedingsof the 13th international World Wide Web conference on Alternate track papers & posters, pages 104–113, New York, NY, USA. ACM Press.

Brusilovsky, P. and Rizzo, R. (2002). Map-based horizontal navigation in educational hypertext. In HYPERTEXT '02: Proceedings of the thirteenth ACM conference on Hypertext and hypermedia, pages 1–10, New York, NY, USA. ACM Press.

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

Ernest & Young (2004). Global Information Security Survey - 2004.

Hentea, M., Shea, M. J., and Pennington, L. (2003). A perspective on fulfilling the expectations of distance education. In CITC4 '03: Proceeding of the 4th conference on Information technology curriculum, pages 160–167, New York, NY, USA. ACM Press.

ISO/IEC 17799 (2005). ISO/IEC 17799: Code of Practice for Information Security Management.

ISO/IEC TR 13335-1 (2004). 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.

Jerinic, L. and Devedric, V. (1999). A Survey of Components for Intelligent Tutoring Pedagogical Aspects of GETBITS Model. SIGCUE Outlook, 27(1):3–24.

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.

Lester, J. C., Fitzgerald, P. J., and Stone, B. A. (1997). The pedagogical design studio: exploiting artifact-based task models for constructivist learning. In IUI '97: Proceedings of the 2nd international conference on Intelligent user interfaces, pages 155–162, New York, NY, USA. ACM Press.

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

NIST 800-16 (1998). 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.

Nodenot, T., Marquesuzaa, C., Laforcade, P., and Sallaberry, C. (2004). Model based engineering of learning situations for adaptive web based educational systems. In WWW Alt. '04: Proceedings of the 13th international World Wide Web conference on Alternate track papers & posters, pages 94–103, New York, NY, USA. ACM Press.

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. Irwin/McGraw-Hill, 4 edition.

Schlienger, T. and 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, pages 183–196.

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

Turban, E., Mclean, E., and Wetherbe, J. (2002). Information Technology for Management: Transforming Business in the Digital Economy. John Wiley and Sons.

Van Niekerk, J. and Von Solms, R. (2002). A web-based portal for information security education. Information Security South Africa (ISSA), Johannesburg, South Africa.

Van Niekerk, J. and Von Solms, R. (2003). Establishing an information security culture in organisations: An outcomes based education approach. Information Security South Africa (ISSA), Johannesburg, South Africa.

Van Niekerk, J. and Von Solms, R. (2004). 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.

Van Niekerk, J. and Von Solms, R. (2005). An holistic framework for the fostering of an information security subculture in organizations. Information Security South Africa (ISSA), Johannesburg, South Africa.

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

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

UNDERSTANDING INFORMATION SECURITY CULTURE: A CONCEPTUAL FRAMEWORK

Johan van Niekerk[1], Rossouw von Solms[2]

[1,2]Centre for Information Security Studies, Nelson Mandela Metropolitan University, South Africa

[1]johanvn@nmmu.ac.za, +27 41 5043048, PO Box 77000, Port Elizabeth, 6000
[2]rossouw@nmmu.ac.za, +27 41 5043669, PO Box 77000, Port Elizabeth, 6000

ABSTRACT

The importance of establishing an information security culture in an organization has become a well established idea. The aim of such a culture is to address the various human factors that can affect an organization's overall information security efforts. However, *understanding* both the various elements of an information security culture, as well as the relationships between these elements, can still be problematic. Schein's definition of a *corporate* culture is often used to aid understanding of an information security culture. This paper briefly introduces Schein's model. It then incorporates the important role knowledge plays in information security into this definition. Finally, a conceptual framework to aid understanding of the interactions between the various elements of such a culture, is presented. This framework is explained by means of illustrative examples, and it is suggested that this conceptual framework can be a useful aid to understanding information security culture.

KEYWORDS

Information Security, Information Security Culture, Corporate Culture, Organizational Learning, Schein's Model.

UNDERSTANDING INFORMATION SECURITY CULTURE: A CONCEPTUAL FRAMEWORK

1 INTRODUCTION

Today, most organizations need information systems to survive and prosper. Information has become a valuable asset to modern organizations. It is therefore imperative for modern organizations to take the protection of their information resources seriously. This protection of information resources, also known as information security, consist of many processes. Some of these processes are, to a large extent, dependent on human co-operated behavior. Employees, whether intentionally or through negligence, often due to a lack of knowledge, are the *greatest threat* to information security (Mitnick & Simon, 2002, p. 3). Without an adequate level of user **cooperation** 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). An organization's information security strategy should thus comprehensively address this ”human factor”. It is important to note that there are two dimensions to this ”human factor” in information security, namely *knowledge*, and cooperation, or *behavior*. These dimensions are to a large extend interrelated to each other.

Organizations cannot protect the integrity, confidentiality, and availability of information in today's highly networked systems environment without ensuring that each person involved shares the security vision of the organization, understands his/her roles and responsibilities, and is adequately trained to perform them (ISO/IEC TR 13335-1, 2004, p. 14). In order to assist in ensuring information security, individual users thus needs **knowledge** regarding their specific role in the security process. This knowledge can be provided via education, training and awareness campaigns.

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 the desired **behavior**, towards information security. In order to ensure the desired user behavior, it is necessary to cultivate an organizational sub-culture of information security (Von Solms, 2000; Schlienger & Teufel, 2003). 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). 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 a security asset, instead of being a risk (Von Solms, 2000).

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). However, such a culture **must** be supported by adequate knowledge regarding information security (Van Niekerk & Von Solms, 2005). Without adequate knowledge, users who want to behave securely, might still apply a security control incorrectly. Conversely, a user who has adequate knowledge, but believes that secure behavior is unnecessary in his/her specific role, might still behave in an insecure way. Due to this co-dependence between the knowledge dimension of the human factor in information security, and the behavioral dimension, it would be beneficial to deal with both these dimensions holistically. It would thus make sense to have a single conceptual framework that can be used to reason about both the knowledge, and the behavioral aspects of this human factor in information security. This paper will briefly adapt the ”generic” definition of *corporate* culture to the specific needs of an *information security* culture. This adapted definition will then be used to provide a conceptual framework for examining the various aspects of the human factors in information security.

In examining this adapted definition, it is important to realize that knowledge, and the underlying educational programs needed to impart such knowledge, is often seen as part of corporate culture. It is not the intent of this paper to dispute this view. In fact, this paper supports the view that knowledge and education will always play a role towards ensuring specific behavior patterns. However, this paper does attempt to highlight the fact that the knowledge ”dimension” is of *particular* importance in an information security culture, and that security knowledge plays a very specific *enabling* role in information security. The additional knowledge ”dimension” this paper will present, represents the knowledge needed to effectively implement, or use, the security measures if the desired attitude can be assumed. The knowledge that form an underlying part of *any* corporate culture is *still* assumed to be present. In *that* respect, an information security culture is assumed to be the same as a ”normal” corporate culture.

2 RESEARCH PARADIGM AND RATIONALE

The work in this paper is based on qualitative, or phenomenological- , research methods, as described in Creswell (1998). This paper should thus be seen as ”an inquiry process of understanding based on distinct methodological traditions of inquiry that explore a social or human problem” (Creswell, 1998, p. 15). The research presented here does not attempt to define *new* knowledge, but rather to provide a more in-depth understanding of the phenomenon described as ”information security culture”. As far as could be determined, the specific conceptual model, as well as the underlying interactions between the various levels of information security culture, as presented in this paper, has never been published before. It is the authors’ belief that the use of this conceptual model could improve the understanding of the concept of information security culture. Since the concept of organizational culture has been largely ”borrowed” by information security researchers from the humanities, it was deemed fitting to also ”borrow” the research paradigm, used in this paper from the humanities.

The model for corporate culture as presented in Schein (1999) has become widely accepted amongst information security researchers (Schlienger & Teufel, 2003). However, this model describes corporate culture in *general*, and not information security culture *specifically*. In order to ensure a rigorous research approach, even concepts with a seemingly obvious meaning will be revisited in this paper. The description of these concepts in the presented information security framework is deemed necessary because there might exist differences between the ontologies commonly adhered to by information security specialists and researchers from the management sciences.

The aim of this paper is thus to present an holistic, conceptual model of information security culture, for information security practitioners and students. This model aims to clarify, at a conceptual level, the interactions between various elements comprising such an information security culture. The model also attempt to clearly define, in an information security context, concepts such as the strength and the stability (or predictability) of an information security culture. The model presented in this paper is intended to clarify, and improve, the understanding of exiting concepts. It is hoped that this model will be of use to other information security researchers when examining the human factors in information security. Before the specific concept of an information security culture is examined, this paper will first explore the existing definition of corporate culture.

3 CORPORATE CULTURE

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, 1999, 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, 1999, p. 15).

A better way to think about culture is to examine the different ”levels” at which culture exists (Schein, 1999, p. 15). 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 be briefly examined:

- **Level One: Artifacts.** Artifacts are what you can observe, see, hear, and feel, in an organization (Schein, 1999, 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, 1999, p. 16). Observing the artifacts alone, however, does not explain **why** the members of the organization behave as they do (Schein, 1999, 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, 1999, 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, 1999, 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, 1999, p. 17). However, it is possible for two organizations to have very different observable artifacts and yet share very similar espoused values (Schein, 1999, pp. 18-19). This is because there is an even deeper level of thought and perception that drives the overt, or observable, behavior (Schein, 1999, 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.** 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, 1999, 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, 1999, 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 *espoused 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. These three levels of corporate culture could be seen to correspond closely to the behavioral aspects of the ”human factor” in information security. As mentioned earlier, this ”human factor” in information security consist of two dimensions, namely knowledge and behavior, which are very inter-related. Due to the co-dependency between these two dimensions it is not possible to ignore the impact a lack of information security related knowledge would have on an organizational sub-culture of information security.

4 INFORMATION SECURITY CULTURE

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. It **can not be assumed** that the average employee has the necessary knowledge to perform his/her job in a secure manner. 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** normal activity in a secure manner. Information security knowledge, or a lack thereof, could therefor be seen as a fourth level to an information security culture that will affect each of the other three layers. For example:

Artifacts: Artifacts are *what actually happens* in the organization. Without the necessary skills and proficiencies, it would be impossible to perform security related tasks correctly. Thus, for the day-to-day task to happen in a secure way, the users would have to have sufficient knowledge of **how** to perform their tasks securely.

Espoused Values: 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 in order to adequately address the organization’s security needs.

Shared Tacit Assumptions: This layer consists of the beliefs and values of employees. If such a belief should conflict with one of the espoused values, knowing **why** a specific control is needed, might play a vital role in ensuring compliance (Schlienger & Teufel, 2003).

It should be clear that in an information security culture, knowledge **underpins** and **supports** all three the ”normal” levels of corporate culture. Without adequate knowledge, information security cannot be ensured. The co-dependency between the three ”normal” levels of an organization’s information security culture, and knowledge, the ”fourth level”, implies that each of these four levels will have an impact on how ”secure”, or desirable, the overall information security culture will be. The first part of the model presented in this paper is thus an adaptation of Schein’s model. This adaptation incorporates the underlying need for information security related knowledge into Schein’s model. Knowledge are added as a fourth level of culture that is specific to an information security culture. This adaptation is necessary because in an information security culture the requisite knowledge cannot be assumed to be present. Figure 1, provides a graphical exposition of this adaptation. In this presented conceptual model, knowledge is dealt with as an additional level to culture, as opposed to viewing knowledge as a sub-component of each of the original three levels. This is done solely because modeling knowledge as an additional level makes it easier to clearly show the effect knowledge, or a lack thereof, would have on the overall information security culture.

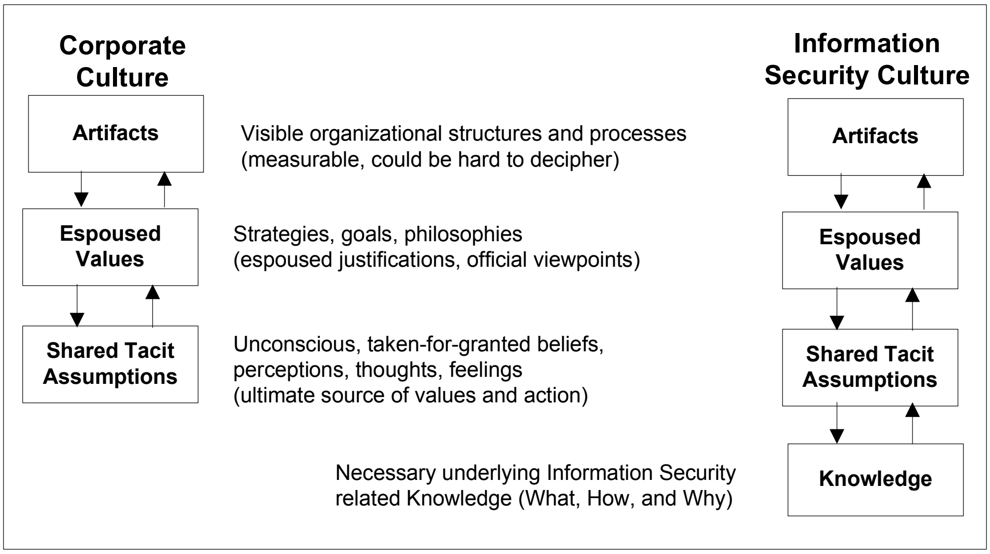

Corporate Culture
Information Security Culture
Artifacts
Visible organizational structures and processes (measurable, could be hard to decipher)
Artifacts
Espoused Values
Strategies, goals, philosophies (espoused justifications, official viewpoints)
Espoused Values
Shared Tacit Assumptions
Unconscious, taken-for-granted beliefs, perceptions, thoughts, feelings (ultimate source of values and action)
Shared Tacit Assumptions
Necessary underlying Information Security related Knowledge (What, How, and Why)
Knowledge

Figure 1: Levels of Culture (adapted from Schein, 1999, p. 16)

5 INFORMATION SECURITY CULTURE: A CONCEPTUAL FRAMEWORK

The overall effect of an organization's information security culture can be seen as an accumulation of the effects of each of the culture's underlying levels. Each of these levels can either positively or negatively influence the overall information security culture. In order to clearly demonstrate the interactions between these four levels, and their effects on the overall security efforts, it is necessary to first provide a basic reference framework.

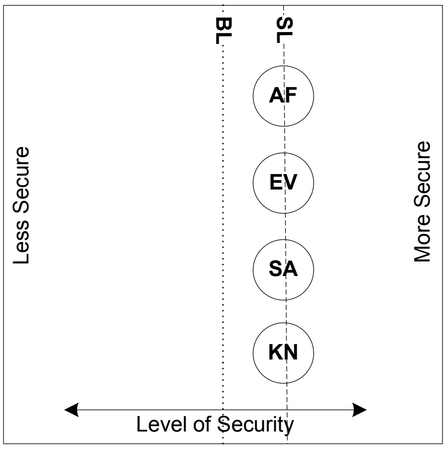


Figure 2: Basic Elements of the Conceptual Framework. *(BL = Minimum Acceptable Baseline, SL = Nett Security Level, AF= Artifacts, EV = Espoused Values, SA= Shared Tacit Assumptions, KN= Knowledge)*

5.1 Basic Elements and Terminology of the Conceptual Framework

The basic elements of this framework are depicted in Figure 2. The elements in Figure 2 can be described as follows:

- BL: Minimum Acceptable Base Line - This line indicates what would be an acceptable minimum security baseline. In other words, a culture whose net effect would meet the minimum requirements for some industry standard.

- SL: Nett Security Level - This line indicates the actual nett effect of the culture on the overall security effort. This line can be seen as the cumulative effect of the four underlying levels of the culture. The nett security level (SL) can either be more secure (to the right), less secure (to the left), or just as secure (overlapping) as the minimum acceptable baseline (BL).

- AF: Artifacts - This node represents the relative *strength* of the artifact level (AF) of the culture. If this node is to the left of the minimum acceptable baseline (BL), it indicates that the measurable artifacts are not as secure as they should be. A node to the right of the baseline (BL) would indicate artifacts that are even more secure than the acceptable minimum. A node exactly on the baseline (BL) would indicate artifacts that are just as secure as required by this baseline.

- EV: Espoused Values - This node represents the relative *strength* of the organization's espoused value level (EV). The various policies and procedures comprising this level could be more, less, or just as comprehensive than those recommended as the minimum acceptable baseline.

- SA: Shared Tacit Assumptions - This node represents the relative *strength* of the organization's shared tacit assumption level (SA). The underlying beliefs or values of the employees could be either more, less, or just as in favor of good secure practices as required by the minimum acceptable baseline.

- KN: Knowledge - This node represents how much knowledge the organization's employees have regarding information security. Employees can be more knowledgeable than a certain minimum level needed to perform their jobs securely, they could be less knowledgeable, or they could have exactly the minimum requisite level of knowledge.

As mentioned above, the horizontal alignment of the nodes representing the various cultural levels, AF, EV, SA and KN, in comparison to the minimum acceptable baseline, should be interpreted as an indication of the relative *strength* of each level. In a similar fashion, the horizontal alignment of the nodes in comparison to the same horizontal alignment of the **other** levels should be interpreted as an indication of how *stable*, or predictable, the culture is. The nett security level line (SL) is an indication of the average strength of the culture, or the nett combined effect of all four the levels. The culture depicted in Figure 2 should thus, firstly, be interpreted as a *strong*, or secure culture. All four levels in Figure 2 has a strength greater than the baseline, which also results in a nett security level that is positive, or greater than the baseline. Secondly, all four levels are perfectly aligned with each other. This results in a culture that should be completely *stable*, or predictable. The culture depicted in Figure 2 could thus be said to be the *ideal* culture in terms of information security since it is both *strong* and *stable*.

The terms *strong*, and *stable*, as used above, should not be confused as being indicative of how pervasive or resistent to change the culture might be. According to Schein (1999, pp. 25-26), corporate culture is always strong in the sense of affecting every single aspect of daily life in an organization at a more than superficial level. Culture is also always stable, in the sense that it resists attempts at changing it. In that sense, culture is one of the most stable facets in an organization (Schein, 1999, p. 26). When referring to an **information security culture**, the term *strong*, as used in this paper, should be interpreted as a **desirable** culture that is conductive to information security. The term *stable*, as used in the same context, should be interpreted as an indication of how **predictable** the resulting artifacts, or nett security level of the culture would be for any specific scenario.

All of the factors mentioned above would contribute to the overall desirability of an information security culture. How *strong*, and *stable* an organization's information security culture is, would depend on the interaction between the various levels of culture.

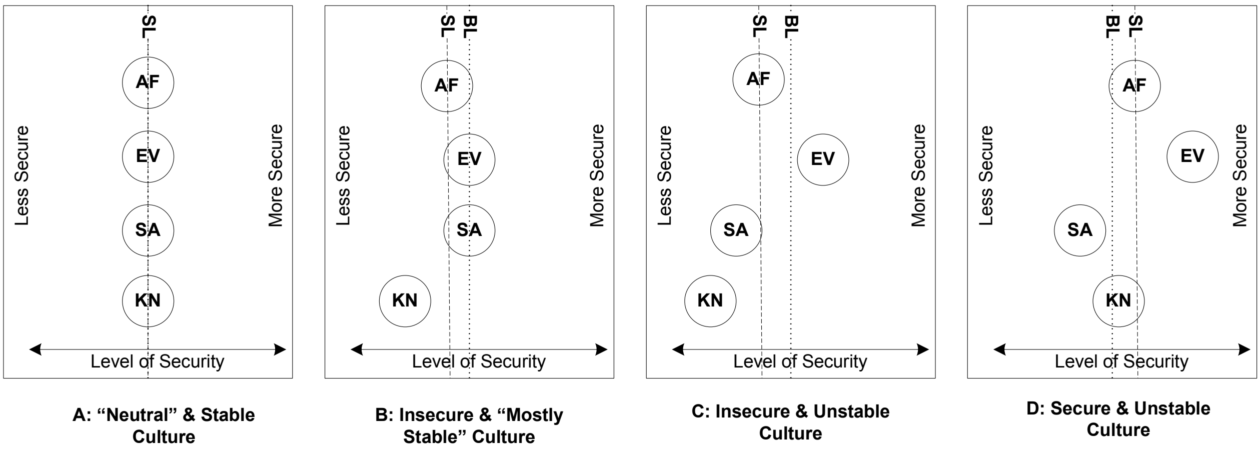

SL
BL
AF
EV
SA
KN
Less Secure
More Secure
Level of Security
A: "Neutral" & Stable Culture
B: Insecure & "Mostly Stable" Culture
C: Insecure & Unstable Culture
D: Secure & Unstable Culture

Figure 3: Possible interactions between the various levels of an Information Security Culture. *(BL = Minimum Acceptable Baseline, SL = Nett Security Level, AF= Artifacts, EV = Espoused Values, SA= Shared Tacit Assumptions, KN= Knowledge)*

5.2 Interpreting the Conceptual Framework

Each of the underlying cultural levels will contribute towards the overall strength and stability of such a culture. For example, if an organization has espoused values that are in line with recommended best practices for security, this would make the overall security better. Conversely, should the espoused values fail to address all relevant security related issues, the overall security would be weaker.

The combination of the espoused values, and the ”filtering effect” of the shared tacit assumptions and the user knowledge, on these espoused values, results in the visible, and measurable *artifacts*. From a security viewpoint, the artifact level is a very good indication of the overall security of the organization’s information, since this level reflects what *actually happens* in the day to day operations. Fig. 3 shows a few possible effects interactions between the various levels of culture could have on the overall state of the organization’s information security.

The examples in Fig. 3 assumes that the desirability of the various levels can be quantified and normalized to the same scale. In other words, it is assumed that, for example, the desirability of the relevant espoused values can be measured and expressed as a value that indicates the contribution of this level towards the overall security. It is also assumed that the other levels can be expressed in the same way, and that the scale of such measurements can be normalized in such a way that these values will indicate the relative desirability of that level when compared to the other levels. The line marked **SL**(*Security Level*) represents the nett effect of the interactions between various levels of the culture. The four examples in Fig. 3 can be interpreted as follows:

- **A:”Neutral” and Stable**. The desirability of the various levels of culture are ”neutral”, or average. In other words the *strength* of each level neither exceeds, nor falls short, of the minimum acceptable baseline standards. Since all the levels have the same level of desirability, the various levels will neither negate nor reinforce the effects of other levels on the overall security. The effects of such a culture would thus be predictable and stable.

- **B:Insecure and ”Mostly Stable”**. Both the espoused values and the shared tacit assumptions in this culture are of sufficient *strength* to meet the minimum acceptable baseline standard. However, in this culture, the employees do not have the requisite level of information security related knowledge. It is thus possible for the measurable artifacts to fall short of the minimum acceptable baseline. For example, either the policy dealing with a specific control might be lacking because the person(s) responsible for creating the policy lack the necessary knowledge, or the knowledge needed to implement this control in day-to-day operations might be lacking amongst the responsible employees. In both such cases, the resulting artifacts *might* be weaker than expected. This misalignment between the various levels also means that it would be difficult to predict the exact relative strength of the overall security level. In this case one could probably assume the culture will be mostly predictable, hence stable, because the lack of knowledge would probably not apply equally to all controls.

- **C:Insecure and Unstable**. The various levels contributing to the culture are not aligned. This would mean that the nett effects of the culture might be unpredictable, due to the opposing forces at play in this culture. The espoused values are very desirable, but the users lack the requisite knowledge and do not have the desired beliefs and values, resulting in a measurable artifact level that is not secure. For any specific security control, a user may, or may not, have the requisite knowledge to fulfill his/her role in the implementation of that specific control. That same user could also agree with the relevant espoused value, or could have beliefs that are contrary to that espoused value. It would thus be very difficult to predict the nett security level of this culture. Such a culture would not be a desirable culture.

- **D:Secure and Unstable**. The various levels contributing to the culture are not aligned. The espoused values are desirable, and the users have adequate knowledge. The high level of user knowledge in this case somewhat negates the fact that the users do not have the desired beliefs and values, resulting in an overall culture that is more secure than the minimum acceptable baseline. However, this culture should be considered not desirable, because its effects cannot always be predicted. It might be possible for the users to behave insecurely with regards to a specific security control because the specific control conflicts with their beliefs (Schlienger & Teufel, 2003).

The above examples only reflect a few possible scenarios. It should however be clear that the nett effect of any information security culture can be influenced, either positively, or negatively, by how ”secure” the underlying levels of such a culture is. In such a model it might also be possible to deduce the relative state of one or more of the cultural levels. For example, if the organization has *good* espoused values, but the measurable artifacts indicate *bad* security, it might be inferred that the employees lack either the required knowledge or the desired attitude.

6 CONCLUSION

This paper suggested that, for an effective information security culture, the requisite information security knowledge amongst an organization’s users could be seen as a fourth layer to Schein’s (Schein, 1999) model for corporate culture. The various interactions between the layers of such an information security culture were then presented conceptually.

The conceptual model presented showed that the nett overall effect that an information security culture would have on the organization’s information security efforts would depend on the relative desirability, or *strength*, of each underlying level in such a culture. Furthermore, the alignment of the strengths of the individual underlying culture levels relative to the other levels, would to a large extend determine how predictable, hence *stable*, the effects of such a culture would be. The ideal culture would thus be one where all four underlying levels are stronger than the minimum acceptable baseline, and are also perfectly aligned relative to each other. The example in Figure 2 would be such an *ideal* culture.

The assumption made when presenting the example, namely that the desirability of the various levels can be quantified and normalized to the same scale, should by no means be taken as an assertion made by this paper. The aim of the paper was not to present such metrics and normalization processes but rather to show, at a certain level of abstraction, how this conceptual model could be used to reason about information security culture. It should, however, be possible to quantify and normalize the various factors for certain subsets of controls. For example, it might be possible to turn the presented conceptual model into a working model for a smaller sub-problem such as mapping the relationships between the four levels for password usage. If the required processes and metrics are developed, the conceptual framework might also play a valuable role in the management of an information security culture. This type of usage for the presented model could possible be included in future research efforts. For the present, the contention of this paper is simply that the conceptual model presented, could assist in improving the understanding of an information security culture. The work in this paper should thus be seen as an attempt to lay a solid foundation on which future research could be built.

7 REFERENCES

Creswell, J. W. (1998). *Qualitative inquiry and research design: Choosing among five traditions. thousand oaks, ca: Sage, 1998*. Thousand Oaks, CA: Sage.

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.

International Standards Organization. (2004). *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.*

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

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

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

Schlienger, T., & Teufel, S. (2003). Information security culture - from analysis to change. *Information Security South Africa (ISSA), Johannesburg, South Africa*.

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.

Van Niekerk, J., & Von Solms, R. (2005). An holistic framework for the fostering of an information security sub-culture in organizations. *Information Security South Africa (ISSA), Johannesburg, South Africa*.

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

8 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.

BLOOM'S TAXONOMY FOR INFORMATION SECURITY EDUCATION

Johan van Niekerk[1], Rossouw von Solms[2]

[1]Nelson Mandela Metropolitan University
South Africa
[2]Nelson Mandela Metropolitan University
South Africa

[1]johan.vanniekerk@nmmu.ac.za, [2]rossouw.vonsolms@nmmu.ac.za

ABSTRACT

The importance of educating organizational end users about their roles and responsibilities towards information security is widely acknowledged. However, many current user education programs have been created by security professionals who do not necessarily have an educational background. The nature of such programs is thus not always properly understood. This lack of understanding could result in the ineffectiveness of security guidelines or programs in practice. This paper attempts to provide additional understanding of these programs through an examination of the revised version of Bloom's taxonomy. The paper show how this taxonomy could be applied to information security education.

KEY WORDS

Information Security, Information Security Education, Awareness, Bloom's Taxonomy

BLOOM'S TAXONOMY FOR INFORMATION SECURITY EDUCATION

1 INTRODUCTION

In recent years information technology has become such an intrinsic part of modern business that some authors no longer see the use of information technology as a strategic benefit. Instead, it can be argued that information technology is a basic commodity, similar to electricity, and that the lack of this commodity makes it **impossible** to conduct business (Carr, 2003). It is therefor vital for organizations to ensure that they have continuous access to this valuable commodity. The process of ensuring this continuous access is known as information security.

Humans, at various levels in the organization, play a vital role in the processes that secures organizational information resources. Many of the problems experienced in information security can be directly contributed to the humans involved in the process. Employees, either intentionally or through negligence, often due to a lack of knowledge, can be seen as the greatest threat to information security (Mitnick & Simon, 2002, p. 3). It is thus imperative for organizations that are serious about the protection of its information resources to be serious about the education of its employees. The aim of corporate information security education should be to ensure that each and every employee in the organization knows his/her responsibility towards information security.

This need to educate organizational users about their roles and responsibilities towards information security is in fact a well established idea. Most major information security standards address this need in some form. For example, the ISO/IEC standard 13335-1 states that organizations cannot protect the integrity, confidentiality, and availability of information in today's highly networked systems environment without ensuring that each person involved shares the security vision of the organization, understands his/her roles and responsibilities, and is adequately trained to perform them (ISO/IEC TR 13335-1, 2004, p. 14). In order to assist in ensuring information security, individual users thus needs **knowledge** regarding their specific role in the security process. This knowledge can be provided via education, training and awareness campaigns.

Most current information security educational programs are constructed by information security specialists who do not necessarily have a strong educational background. Puhakainen (2006, pp. 33-56) reviews 59 current approaches to security awareness, most of which are not based on pedagogical theories. Puhakainen (2006, p. 56) also argues that there is a need for theory-based security approaches. These approaches should also be practically effective. The nature of security educational or awareness issues are often not understood, which could lead to programs and guidelines that are ineffective in practice (Siponen, 2000). A formally trained educationalist might, for example, raise the question whether or not **knowledge** is in fact enough. In Bloom's taxonomy, which is a well know and widely accepted pedagogical taxonomy, knowledge only comprises the very first, and lowest, level of education (Sousa, 2006, pp. 248-255). One could argue that this level of comprehension is in fact not adequate for most humans who play a role in the information security process. Similarly, the traditional approach of classifying the requisite information security educational needs as a continuum consisting of either awareness, training or education, might also be too simplistic.

This paper will attempt to provide a more pedagogically sound interpretation of the educational needs of humans involved in information security processes, based on their respective roles and responsibilities towards security, through the incorporation of Bloom's revised taxonomy (Anderson et al., 2001) as a pedagogical framework.

2 RESEARCH PARADIGM AND RATIONALE

The work in this paper is based on qualitative, or phenomenological-, research methods, as described in Creswell (1998). This paper should thus be seen as "an inquiry process of understanding based on distinct methodological traditions of inquiry that explore a social or human problem" (Creswell, 1998, p. 15). The research presented here does not attempt to define *new* knowledge, but rather to provide a more formalized understanding of information security *awareness*, *training* and *education*. As far as could be determined, the application of Bloom's Taxonomy, both the original and the revised versions, specifically to *information security* education has never been published before. It is the authors' belief that the use of this taxonomy could improve the understanding of the pedagogical issues that **should** be considered in any educational program, amongst information security specialists.

Since education, as a field of study, is normally seen as a ""human science" it was deemed fitting to also "borrow" the research paradigm used in this paper from the humanities. Most current work dealing with information security education see this education as a continuum consisting of three main levels, namely; awareness, training and education (Schlienger & Teufel, 2003),(Van Niekerk & Von Solms, 2004),(NIST 800-16, 1998, pp. 15-17). This continuum is used by many information security specialists when constructing information security educational campaigns. These specialists may not necessarily be educationalists. In order to ensure a rigorous research approach, this paper will thus revisit even concepts with a seemingly obvious meaning. The description and discussion of these concepts is deemed necessary because there might exist differences between the ontologies commonly adhered to by information security specialists and researchers from the educational sciences. The primary purpose of this paper is to encourage information security specialists to "borrow" from the humanities when engaged in activities that deals with humans. It can be argued that for most security education programs more knowledge of the underlying theoretical background can help both practitioners and scholars to understand why a particular information security awareness approach is expected to have the desired impact on users security behavior (Puhakainen, 2006, p. 139). It is believed that adherence to sound pedagogical principles when constructing information security educational campaigns, could improve the efficiency of such campaigns.

3 AWARENESS, TRAINING AND EDUCATION

As mentioned earlier, most current work dealing with information security education see this education as a learning continuum that "starts with awareness, builds to training, and evolves into education" (NIST 800-50, 2003, p. 7). NIST 800-16 (1998, pp. 15-17) provides more detail on the various levels of this continuum and describes these levels as follow:

- Awareness: The main purpose of awareness campaigns is to make employees "*aware*" of information security. In other words, these campaigns focus attention on security. This is normally done using techniques that can reach broad audiences. Awareness campaigns are generally aimed at **all** employees in the organization and aims to equip employees with enough knowledge to enable them to recognize potential security threats. Awareness is not training.

- Training: Training is more formal than awareness and have the goal of building employee knowledge and skills to facilitate the *secure* performance of the employee's normal tasks. Training strives to produce security skills and competencies that are relevant to the specific employee and needed in the performance of the employee's duties. "The most significant difference between training and awareness is that training seeks to teach skills that allow a person to perform a specific function, while awareness seeks to focus an individuals attention on an issue or set of issues."

- Education: "The Education level integrates all of the security skills and competencies of the various functional specialties into a common body of knowledge, adds a multi-disciplinary study of concepts, issues, and principles (technological and social), and strives to produce IT security specialists and professionals capable of vision and pro-active response."

In the current information society, educational or awareness issues affect almost all organizations. Despite this fact the nature of these programs are still not well understood and this often leads to ineffective security guidelines or programs (Siponen, 2000). Many organizations have some form of *awareness* program but often do not augment these with supporting training and/or education programs. The terms *awareness* and *education* are also often used interchangeably. It is not uncommon to hear security specialists talk about "awareness campaigns", when the campaigns actually focus on the training or education levels of the continuum. The purpose of these campaigns is often listed as instilling security **knowledge**, or fostering a **culture** of information security amongst organizational end-users (Van Niekerk & Von Solms, 2006). As mentioned earlier, the term knowledge only describe the lowest level of Bloom's taxonomy of the cognitive domain. From an educational viewpoint one could thus argue that the terminology used lacks rigor. This lack of rigor could contribute to the fact that the nature of awareness and educational issues is often misunderstood. One model that could possibly provide such rigor is Bloom's taxonomy.

4 BLOOM'S TAXONOMY OF THE COGNITIVE DOMAIN

Bloom's taxonomy is possibly one of the best known and most widely used models of human cognitive processes. Bloom's model was originally developed in the 1950's and remained in use more or less unchanged until fairly recently (Sousa, 2006, p. 249). A revised version of the taxonomy was published in Anderson et al. (2001). This revised taxonomy has become accepted as more appropriate in terms of current educational thinking (Sousa, 2006, pp. 249-260). Both versions of Bloom's taxonomy consist of six levels which increases in complexity as the learner moves up through these levels. Figure 1 shows both versions of this taxonomy.

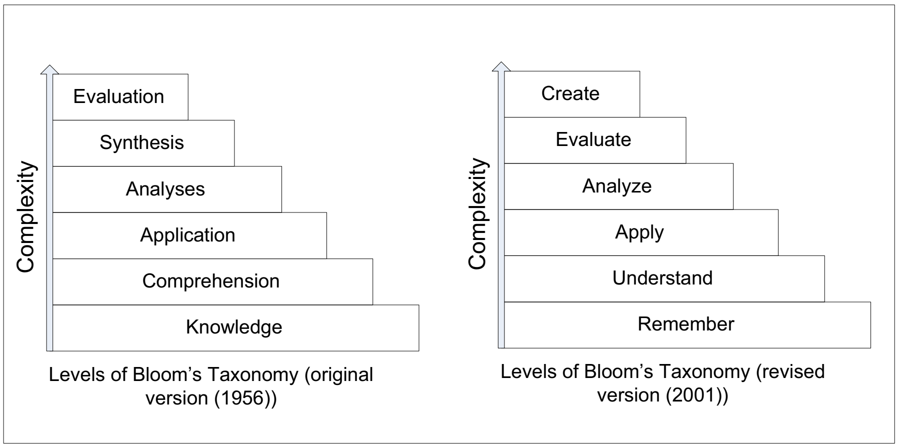


Figure 1: Blooms Taxonomy, Original and Revised (Adapted from Sousa (2006) pp. 249-250)

There are two main differences between the original and the revised versions of the taxonomy. Firstly, the revised version uses descriptive verbs for each level that more accurately describes the intended meaning of each level. Secondly, the revised version has swapped the last two levels of the original version around. This was done because recent studies have suggested that generating, planning, and producing an original "product" demands more complex thinking than making judgements based on accepted criteria (Sousa, 2006, p. 250). The hierarchy of complexity in the revised taxonomy is also less rigid than in the original in that it recognizes that an individual may move among the levels during extended cognitive processes. This paper will focus on the revised version of the taxonomy. Wherever this paper mentions Bloom’s taxonomy, it should be assumed that the revised version is intended, unless otherwise stated. The following is a brief explanation of each of the six levels of this revised taxonomy (Sousa, 2006, pp. 250-252):

- Remember: Remember refers to the rote recall and recognition of previously learned facts. This level represents the lowest level of learning in the cognitive domain because there is no presumption that the learner understands what is being recalled.

- Understand: This level describes the ability to ”make sense” of the material. In this case the learning goes beyond rote recall. If a learner understands material it becomes available to that learner for future use in problem solving and decision making.

- Apply: The third level builds on the second one by adding the ability to use learned materials in *new* situations with a minimum of direction. This includes the application of rules, concepts, methods and theories to solve problems within the given domain. This level combines the activation of procedural memory and convergent thinking to correctly select and apply knowledge to a completely new task. Practice is essential in order to achieve this level of learning.

- Analyze: This is the ability to break up complex concepts into simpler component parts in order to better understand its structure. Analysis skills includes the ability to recognize underlying parts of a complex system and examining the relationships between these parts and the whole. This stage is considered more complex than the third because the learner has to be aware of the thought process in use and must understand both the content and the structure of material.

- Evaluate: Evaluation deals with the ability to judge the value of something based on specified criteria and standards. These criteria and/or standards might be determined by the learner or might be given to the learner. This is a high level of cognition because it requires elements from several other levels to be used in conjunction with conscious judgement based on definite criteria. To attain this level a learner needs to consolidate their thinking and should also be more receptive to alternative points of view.

- Create: This is the highest level in the taxonomy and refers to the ability to put various parts together in order to formulate an idea or plan that is new to the learner. This level stresses creativity and the ability to form *new* patterns or structures by using divergent thinking processes.

Educational taxonomies, such as Bloom's taxonomy, are useful tools in developing learning objectives and assessing learner attainment (Fuller et al., 2007). All well known educational taxonomies are generic. These taxonomies rely on the assumption that the hierarchy of learning outcomes apply to all disciplines (Fuller et al., 2007). Bloom's taxonomy would thus apply equally to a more traditional "subject", such as zoology, as to organizational information security education.

5 BLOOM'S TAXONOMY FOR INFORMATION SECURITY EDUCATION

Learning taxonomies assist the educationalist to describe and categorize the stages in cognitive, affective and other dimensions, in which an individual operates as part of the learning process. In simpler terms one could say that learning taxonomies help us to "understand about understanding" (Fuller et al., 2007). It is this level of meta-cognition that is often missing in information security education. According to Siponen (2000) awareness and educational campaigns can be broadly described by two categories, namely framework and content. The framework category contains issues that can be approached in a structural and quantitative manner. These issues constitute the more explicit knowledge. The second category, however, includes more tacit knowledge of an interdisciplinary nature. Shortcomings in this second area usually invalidate awareness frameworks (Siponen, 2000). How to really motivate users to adhere to security guidelines, for example, is an issue that would form part of this content category.

It has been shown that even in cases where users have "knowledge" of a specific security policy, they might still willfully ignore this policy because they do not understand *why* this policy is needed (Schlienger & Teufel, 2003). Answering the question "why" not only increase insight but also increases motivation (Siponen, 2000). Simply informing employees that "this is our policy", or "you just have to do it", which is often the traditional approach, is not likely to increase motivation or attitudes (Siponen, 2000). Learning is a willful, active, conscious, and constructive activity guided by intentions and reflections (Garde et al., 2007). According to most constructivist learning theories, learning should be learner-centered (Garde et al., 2007). In an organizational information security educational campaign, the learners **must** include each and every employee. It is also important to realize that the campaign has to be **successful for each and every learner** (Van Niekerk & Von Solms, 2004).

In order to ensure successful learning amongst all employees, it is extremely important to fully understand the educational needs of individual employees. According to Roper, Grau, and Fischer (2005, pp. 27-36) managers often attempt to address the security education needs of employees without adequately studying and understanding the underlying factors that contribute to those needs. It has been argued before that educational material should ideally be tailored to the learning needs and learning styles of individual learners (Van Niekerk & Von Solms, 2004)(NIST 800-16, 1998, p. 19). One could also argue that awareness campaigns that have not been tailored to the **specific** needs of an individual, or the needs of a **specific target audience**, will be ineffective. It is in the understanding of these needs, that a learning taxonomy can play an important enabling role.

Information security specialists should use a taxonomy, like Bloom's taxonomy, before compiling the content category of the educational campaign. The use of such a taxonomy could help to understand the learning needs of the target audience better. It could also reduce the tendency to focus only on the framework category of these campaigns. For example, simply teaching an individual what a password is, would lie on the *remember*, and possibly *understand* level(s) of Bloom's taxonomy. However, the necessary information to understand *why* their own passwords is also important and should also be properly constructed and guarded might lie as high as the *evaluate* level of the taxonomy. An information security specialist might think that teaching the users what a password is, is enough, but research have shown that understanding *why* is essential to obtaining buy-in from employees. It is this level of understanding that acts as a motivating factor and thus enables behaviour change (Siponen, 2000)(Schlienger & Teufel, 2003)(Van Niekerk & Von Solms, 2004)(Roper et al., 2005, pp. 78-79).

The use of an educational taxonomy in the construction of information security educational programs requires that both the content and the assessment criteria for this program is evaluated against the taxonomy in order to ensure that learning takes place at the correct level of the cognitive do-

Level	**Terms**	**Sample Activities**
Create	imagine	Pretend you are an information security officer for a large firm. Write a report about a recent security incident.
	compose	Rewrite a given incident report as a news story.
	design	Write a new policy item to prevent users from putting sensitive information on mobile devices.
	infer	Formulate a theory to explain why employees still write down their passwords.
Evaluate	appraise	Which of the following policy items would be more appropriate. Why?
	assess	Is it fair for a company to insist that employees never use their work email for personal matters? Why or Why not?
	judge	Which of the security standards you have studied is more appropriate for use in the South African context? Defend your answer.
	critique	Critique these two security products and explain why you would recommend one over the other to a customer.
Analyze	analyze	Which of the following security incidents are more likely?
	contrast	Compare and contrast the security needs of banking institutions to those of manufacturing concerns.
	distinguish	Sort these security controls according to the high level policies that they address.
	deduce	Which of these procedures could derive from the given policy.
Apply	practice	Use these mnemonic techniques to create and recall a secure password.
	calculate	Calculate how secure the following password is.
	apply	Think of three things that could go wrong should your password be compromised.
	execute	Use the given tool to encrypt the following message.
Understand	summarize	Summarize the given security policy in your own words
	discuss	Why should non alpha-numeric characters be used in a password?
	explain	Explain how symmetric encryption works.
	outline	Outline your own responsibilities with regards to the security of customer account information.
Remember	define	What is the definition of a security incident?
	label	Label each of the threats in the given picture.
	recall	What is social engineering?
	recognize	Which of the pictures shows someone ”shoulder surfing”?

Table 1: Bloom’s Taxonomy for Information Security adapted from Anderson et al., 2001

main. The reference point for any educational program should be a set of clearly articulated ”performance objectives” that have been developed based on an assessment of the target audience’s needs and requirements (Roper et al., 2005, p. 96). Correct usage of an educational taxonomy not only helps to articulate such performance objectives but, more importantly, helps the educator to correctly gauge the needs and requirements of the audience. An example of how Bloom’s revised taxonomy could be used in an information security context is supplied in Table 1. This example is not intended to be a definitive work, but rather to serve as an example or starting point for information security practitioners who want to use Bloom’s taxonomy when constructing awareness and educational campaigns. It should however be clear that this taxonomy could easily be used to categorize most, if not all, information security educational needs effectively. Once categorized according to a taxonomy like Bloom’s taxonomy, it should also be easier to find related information regarding pedagogical methods suitable to assist learners in attaining the desired level of cognitive understanding.

6 CONCLUSION

This paper suggested that information security educational programs would be more effective if they adhered to pedagogical principles. It was specifically suggested that the common categorization of security educational needs into the broad categories of awareness, training, and education, is not ideal. Instead an educational taxonomy, like Bloom’s taxonomy should be used to accurately define the security education needs of organizational users. Through the use of such a taxonomy certain common weaknesses in current security awareness and educational programs might be addressed.

An example of how Bloom’s taxonomy might be applied to information security concepts was provided. The primary weakness of this paper is the lack of empirical evidence to support the suggested use of Bloom’s taxonomy. Future research in this regard should therefor focus on addressing this weakness. It has been argued before that security practitioners who engage in research or activities that relate to the human sciences should not re-invent the wheel, but should rather ”borrow” from the humanities when appropriate. This paper is one such an attempt, to ”borrow” from the humanities.

References

Anderson, L., Krathwohl, D., Airasian, P., Cruikshank, K., Mayer, R., Pintrich, P., et al. (2001). *A taxonomy for learning, teaching, and assessing: A revision of bloom's taxonomy of educational objectives, complete edition* (L. Anderson & D. Krathwohl, Eds.). Longman.

Carr, N. G. (2003). IT Doesn't Matter. *Harvard Business Review*, 41–49.

Creswell, J. W. (1998). *Qualitative inquiry and research design: Choosing among five traditions. thousand oaks, ca: Sage, 1998.* Thousand Oaks, CA: Sage.

Fuller, U., Johnson, C. G., Ahoniemi, T., Cukierman, D., Hernán-Losada, I., Jackova, J., et al. (2007). Developing a computer science-specific learning taxonomy. *SIGCSE Bull.*, *39*(4), 152–170.

Garde, S., Heid, J., Haag, M., Bauch, M., Weires, T., & Leven, F. J. (2007). Can design principles of traditional learning theories be fullfilled by computer-based training systems in medicine: The example of campus. *International Journal of Medical Informatics*, *76*, 124–129.

International Standards Organization. (2004). *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.*

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

National Institute of Standards and Technology. (1998). *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.*

National Institute of Standards and Technology. (2003). *NIST 800-50: Building an Information Technology Security Awareness and Training Program. NIST Special Publication 800-50, National Institute of Standards and Technology.*

Puhakainen, P. (2006). *A design theory for information security awareness.* Unpublished doctoral dissertation, Acta Universitatis Ouluensis A 463, The University of Oulu.

Roper, C., Grau, J., & Fischer, L. (2005). *Security Education, Awareness and Training: From Theory to Practice.* Elsevier Butterworth Heinemann.

Schlienger, T., & Teufel, S. (2003). Information security culture - from analysis to change. *Information Security South Africa (ISSA), Johannesburg, South Africa.*

Siponen, M. (2000). A conceptual foundation for organizational information security awareness. *Information Management & Computer Security, 8*(1), 31-41.

Sousa, D. A. (2006). *How the brain learns* (3rd ed.). Corwin Press.

Van Niekerk, J., & Von Solms, R. (2004). 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.*

Van Niekerk, J., & Von Solms, R. (2006). Understanding information security culture: A conceptual framework. *Information Security South Africa (ISSA), Johannesburg, South Africa.*

7 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.

Using Bloom's Taxonomy for Information Security Education

Johan Van Niekerk[1] and Rossouw Von Solms[2]

Institute for ICT Advancement, Nelson Mandela Metropolitan University
johan.vanniekerk@nmmu.ac.za, rossouw.vonsolms@nmmu.ac.za

Abstract. The importance of educating organizational end users about their roles and responsibilities towards information security is widely acknowledged. However, many current user education programs have been created by security professionals who do not necessarily have an educational background. This paper show how the use of learning taxonomies, specifically Bloom's taxonomy, can improve such educational programs. It is the authors belief that proper use of this taxonomy will assist in ensuring the level of education is correct for the intended target audience.

1 Introduction

The primary aim of corporate information security education is to ensure that each and every employee is instilled with the requisite **knowledge** and/or skills to perform his or her function in a secure way [1]. Most current information security educational programs are constructed by information security specialists who do not necessarily have a strong educational background. Studies have shown that the vast majority of current awareness approaches lacks theoretical grounding [2, pp. 33-56]. The nature of security educational or awareness issues are often not understood, which could lead to programs and guidelines that are ineffective in practice [3]. This paper shows how the use of Bloom's revised taxonomy [4], as a pedagogical framework, can assist the creators of information security educational programs in defining more pedagogically sound learning objectives for the humans involved in information security processes.

The work in this paper is based on qualitative research methods. This paper should thus be seen as "an inquiry process of understanding based on distinct methodological traditions of inquiry that explore a social or human problem" [5, p. 15]. Since education, as a field of study, is normally seen as a "human science" it was deemed fitting to also "borrow" the research paradigm used in this paper from the humanities. The research presented here does not attempt to define *new* knowledge, but rather to show how an existing taxonomy, Bloom's taxonomy, could be used to improve information security *educational* programs. This paper is an expansion on ideas previously published by the authors in [6]. It is the authors' belief that the use of Bloom's taxonomy could improve the understanding of the pedagogical, or learning, objectives that **should** be considered in any educational program, amongst information security specialists.

The rest of this paper will briefly examine this taxonomy, before discussing its possible use in information security education.

2 Bloom's taxonomy of the cognitive domain

Bloom's taxonomy is possibly one of the best known and most widely used models of human cognitive processes. Bloom's model was originally developed in the 1950's and remained in use more or less unchanged until fairly recently [7, p. 249]. A revised version of the taxonomy was published in 2001 [4]. This revised taxonomy has become accepted as more appropriate in terms of current educational thinking [7, pp. 249-260]. Both versions of Bloom's taxonomy consist of six levels which increases in complexity as the learner moves up through these levels. Figure 1 shows both versions of this taxonomy.

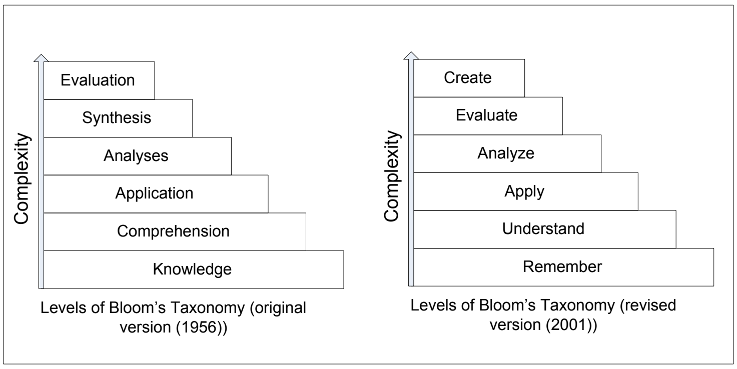


Fig. 1. Blooms Taxonomy, Original and Revised (Adapted from Sousa (2006) pp. 249-250)

There are two main differences between the original and the revised versions of the taxonomy. Firstly, the revised version uses descriptive verbs for each level that more accurately describes the intended meaning of each level. Secondly, the revised version has swapped the last two levels of the original version around. This was done because recent studies have suggested that generating, planning, and producing an original "product" demands more complex thinking than making judgements based on accepted criteria [7, p. 250]. The hierarchy of complexity in the revised taxonomy is also less rigid than in the original in that it recognizes that an individual may move among the levels during extended cognitive processes. This paper will focus on the revised version of the taxonomy. Wherever this paper mentions Bloom's taxonomy, it should be assumed that the revised version is intended, unless otherwise stated. The following is a brief explanation of each of the six levels of this revised taxonomy [7, pp. 250-252]:

- Remember: Remember refers to the rote recall and recognition of previously learned facts. This level represents the lowest level of learning in the cognitive domain because there is no presumption that the learner understands what is being recalled.
- Understand: This level describes the ability to "make sense" of the material. In this case the learning goes beyond rote recall. If a learner understands material it becomes available to that learner for future use in problem solving and decision making.
- Apply: The third level builds on the second one by adding the ability to use learned materials in *new* situations with a minimum of direction. This includes the application of rules, concepts, methods and theories to solve problems within the given domain. This level combines the activation of procedural memory and convergent thinking to correctly select and apply knowledge to a completely new task. Practice is essential in order to achieve this level of learning.
- Analyze: This is the ability to break up complex concepts into simpler component parts in order to better understand its structure. Analysis skills includes the ability to recognize underlying parts of a complex system and examining the relationships between these parts and the whole. This stage is considered more complex than the third because the learner has to be aware of the thought process in use and must understand both the content and the structure of material.
- Evaluate: Evaluation deals with the ability to judge the value of something based on specified criteria and standards. These criteria and/or standards might be determined by the learner or might be given to the learner. This is a high level of cognition because it requires elements from several other levels to be used in conjunction with conscious judgement based on definite criteria. To attain this level a learner needs to consolidate their thinking and should also be more receptive to alternative points of view.
- Create: This is the highest level in the taxonomy and refers to the ability to put various parts together in order to formulate an idea or plan that is new to the learner. This level stresses creativity and the ability to form *new* patterns or structures by using divergent thinking processes.

In addition to these levels of the cognitive domain [4] also places major emphasis on the use of the following categorization of the knowledge dimension [4, pp. 45-62]:

- Factual Knowledge - The most basic elements the learner must know in order to be familiar with a discipline. I.e. Terminology or specific details and elements.
- Conceptual Knowledge - The interrelationships among the basic elements of larger structures that enable these elements to function together. I.e. Classification, categories, principles, theories, models, etc.
- Procedural Knowledge - How to do something, methods of inquiry, how to use skills, apply algorithms, techniques and methods. I.e. Subject specific

skills, algorithms, techniques, and methods as well as knowledge of criteria for determining when to use appropriate procedures.
- Meta-Cognitive Knowledge - An awareness and knowledge of one's own cognition. I.e. Strategic knowledge, Self-knowledge, knowledge about cognitive tasks, including contextual and conditional knowledge.

Activities at these six levels of the cognitive domain are usually combined with the one or more of the four types of knowledge in a collection of statements outlining the learning objectives of an educational program. Usually a *learning objective* statement will be used to create a set of *learning activities*. Learning activities are activities which help learners to attain the learning objectives. A Learning activity consist of a *verb* that relates to an activity at one of the levels of the cognitive domain, and a *noun* providing additional insight into the relationship of the specific learning objective to a category of knowledge [4, pp. 93-109]. The use of a taxonomy often assist educators in gaining better understanding of learning objectives, and activities. However, it is not always clear how this increased understanding can help the educators. [4, pp. 6-10] identifies the following four "organizing questions" as the most important areas in which a taxonomy like Bloom's can assist educators:

- The Learning Question: What is the most important for learners to learn in the limited time available
- The Instruction Question: How does one plan and deliver instruction that will result in high levels of learning for large numbers of learners
- The Assessment Question: How does one select or design assessment instruments and procedures to provide accurate information about how well students are learning
- The Alignment Question: How does one ensure that objectives, instruction, and assessment are consistent with each other.

In most cases, the correct usage of a *taxonomy table*, like the one given in Table 2, which combines elements from both the cognitive and knowledge dimensions, will allow educators to answer these question to some extent.

3 Bloom's Taxonomy for Information Security Education

Learning taxonomies assist the educationalist to describe and categorize the stages in cognitive, affective and other dimensions, in which an individual operates as part of the learning process. In simpler terms one could say that learning taxonomies help us to "understand about understanding" [8]. It is this level of meta-cognition that is often missing in information security education. According to Siponen awareness and educational campaigns can be broadly described by two categories, namely framework and content [3]. The framework category contains issues that can be approached in a structural and quantitative manner. These issues constitute the more explicit knowledge. The second category, however, includes more tacit knowledge of an interdisciplinary nature. Shortcomings in this second area usually invalidate awareness frameworks [3]. How to really motivate users to adhere to security guidelines, for example, is an issue that would form part of this content category.

Level	**Verb**	**Sample Activities**
Create	design	Write a new policy item to prevent users from putting sensitive information on mobile devices. **(A6)**
Evaluate	critique	Critique these two passwords and explain why you would recommend one over the other in terms of the security it provides.**(A5)**
Analyze	analyze	Which of the following security incidents involving stolen passwords are more likely in our company?**(A4)**
Apply	execute	Use the appropriate application to change your password for the financial sub-system. **(A3)**
Understand	discuss	Why should non alpha-numeric characters be used in a password? **(A2)**
Remember	define	What is the definition of *access control*? **(A1)**

Table 1. Abbreviated example of Learning Activities based on Bloom's Taxonomy for Information Security, adapted from Anderson et al., 2001

In order to ensure successful learning amongst all employees, it is extremely important to fully understand the educational needs of individual employees. Managers often attempt to address the security education needs of employees without adequately studying and understanding the underlying factors that contribute to those needs [9, pp. 27-36]. It has been argued before that educational material should ideally be tailored to the learning needs and learning styles of individual learners [10][11, p. 19]. One could also argue that awareness campaigns that have not been tailored to the **specific** needs of an individual, or the needs of a **specific target audience**, will be ineffective. It is in the understanding of these needs, that a learning taxonomy can play an important enabling role.

Information security specialists should use a taxonomy, like Bloom's taxonomy, before compiling the content category of the educational campaign. The use of such a taxonomy could help to understand the learning needs of the target audience better. It could also reduce the tendency to focus only on the framework category of these campaigns. For example, simply teaching an individual what a password is, would lie on the *remember*, and possibly *understand* level(s) of Bloom's taxonomy. However, the necessary information to understand *why* their own passwords is also important and should also be properly constructed and guarded might lie as high as the *evaluate* level of the taxonomy. An information security specialist might think that teaching the users what a password is, is enough, but research have shown that understanding *why* is essential to obtaining buy-in from employees. It is this level of understanding that acts as a motivating factor and thus enables behaviour change [3][10][9, pp. 78-79].

The use of an educational taxonomy in the construction of information security educational programs requires that both the content and the assessment criteria for this program is evaluated against the taxonomy in order to ensure that learning takes place at the correct level of the cognitive domain. The reference point for any educational program should be a set of clearly articulated "performance objectives" that have been developed based on an assessment of the target audience's needs and requirements [9, p. 96]. Correct usage of an educational taxonomy not only helps to articulate such performance objectives but, more importantly, helps the educator to correctly gauge the needs and requirements of the audience.

An example of how Bloom's revised taxonomy could be used in an information security context is supplied in Table 1. This example contains learning activities for a learning objective **(LO1)** that can be briefly expressed as: "Learners should be able to understand, construct and use passwords in the correct context". This example is not intended to be a definitive work, but rather to serve, with taxonomy table Table 2, towards clarifying the use of Bloom's taxonomy in an information security context.

The Knowledge Dimension	**The Cognitive Process Dimension**					
	Remember	**Understand**	**Apply**	**Analyze**	**Evaluate**	**Create**
Factual Knowledge	**A1**				**A6**	
Conceptual Knowledge		**Test1A** **A2**		**Test1B** **A4**	**A6**	
Procedural Knowledge			**LO1** **A3**		**A6**	
Meta-Cognitive Knowledge				**A5**		

Table 2. Example Taxonomy Table adapted from Anderson et al., 2001

It was mentioned earlier that answering the four "organizing questions" is one of the most difficult things for creators of educational matter to do. The following sub-section will briefly explain how the taxonomy table, Table 2 could be used to assist in answering these question for the learning activities, as shown in Table 1.

3.1 Answering the four "Organizing Questions"

Each learning activity in Table 1 consist of a *verb* that relates to one of the cognitive domain levels in Bloom's Taxonomy [4, pp 67-68]. Each activity also has a *noun* relating to knowledge that could be categorized as one of the four categories of knowledge. By marking the appropriate spaces in the taxonomy table for each activity, the educator can derive a lot of useful information about the "coverage" provided by the activities. As an example, the activity marked **A1** Lies at the remember level of the cognitive domain and since it deals with basic subject terminology it deals with the "factual" category of knowledge. This is reflected by its positioning in Table 2. Each of the other activities, **A2** to **A6**, as shown in Table 1 has also been appropriately placed in Table 2. A complete information security educational program will obviously include many more activities, which would result in many more entries in the taxonomy table. Such a table do not always have to deal with an entire program, but could, like the given example, focus on a single learning objective, or even on a few related objectives.

By examining the taxonomy table the educator can easily identify areas of knowledge, or levels of the cognitive domain, that has not been covered by the learning activities. Similarly, areas where multiple activities covers the same levels of cognition and categories of knowledge can be identified. This can assist in answering the so-called "learning question", i.e. "are most important activities receiving the larger share of the available resources?". In order to design activities that will result in maximum learning, thus answering the "learning question", one can look for activities that involves more than just one type of knowledge. For example, in order to create a new policy item (Activity **A6**), the learner will need to know; basic terminology (factual knowledge), how items relate to each other (conceptual knowledge), and which steps to follow to create a policy (procedural knowledge). To answer the "assessment question" the educator could choose to focus on the learning objective itself, and thus, in the example given, only use assessment methods that require the learner to apply procedural knowledge. Or the assessor might decide to focus on one or more learning activities and thus have a wider range of assessment coverage. By noting assessment activities on the same taxonomy table, the educator can ensure that the chosen assessments correspond directly to what he/she intends to assess. For example, that learners must *understand* the concept of a password (**Test1A**) and must be able to *analyze* the relative strength of a given password (**Test1B**). The table will also, at a glance, show which areas are not being assessed. Finally, given a complete taxonomy table, the "alignment question" should be relatively easy to answer. In the given example, a clear "disconnect" between the assessment and the learning objective itself exist. Instead of focusing on the **application, or use,** of passwords the assessments focus on the concept of what a password is, and how to determine its relative strength. Similarly, other "miss-alignments" can be identified with the help of this taxonomy table.

4 Conclusion

This paper suggested that information security educational programs would be more effective if they adhered to pedagogical principles. It was specifically suggested that an educational taxonomy, like Bloom's taxonomy should be used to accurately define the security education needs of organizational users. Through the use of such a taxonomy certain common weaknesses in current security awareness and educational programs might be addressed.

An example of how Bloom's taxonomy might be applied to a learning objective in an information security educational program was provided. The paper used this brief example, to show how a taxonomy table based on this example, could assist educators in addressing the four "organizing questions" faced by educators. The primary weakness of this paper is the lack of empirical evidence to support the suggested use of Bloom's taxonomy. Due to space limitations, the examples are also by necessity, very brief. Future research in this regard should focus on addressing the lack of empirical evidence, and on expanding the examples to be more comprehensive. It has been argued before that security practitioners who engage in research or activities that relate to the human sciences should not re-invent the wheel, but should rather "borrow" from the humanities when appropriate. This paper is one such an attempt, to "borrow" from the humanities.

References

[1] Van Niekerk, J., Von Solms, R.: An holistic framework for the fostering of an information security sub-culture in organizations. Information Security South Africa (ISSA), Johannesburg, South Africa (2005)

[2] Puhakainen, P.: A design theory for information security awareness. PhD thesis, Acta Universitatis Ouluensis A 463, The University of Oulu (2006)

[3] Siponen, M.: A conceptual foundation for organizational information security awareness. Information Management & Computer Security **8**(1) (2000) 31–41

[4] Anderson, L., Krathwohl, D., Airasian, P., Cruikshank, K., Mayer, R., Pintrich, P., Raths, J., Wittrock, M.: A Taxonomy for Learning, Teaching, and Assessing: A Revision of Bloom's Taxonomy of Educational Objectives, Complete Edition. Longman (2001)

[5] Creswell, J.W.: Qualitative Inquiry and Research Design: Choosing among Five Traditions. Thousand Oaks, CA: Sage, 1998. Thousand Oaks, CA: Sage (1998)

[6] Van Niekerk, J., Von Solms, R.: Bloom's taxonomy for information security education. Information Security South Africa (ISSA), Johannesburg, South Africa (2008)

[7] Sousa, D.A.: How the brain learns. 3rd edn. Corwin Press (2006)

[8] Fuller, U., Johnson, C.G., Ahoniemi, T., Cukierman, D., Hernán-Losada, I., Jackova, J., Lahtinen, E., Lewis, T.L., Thompson, D.M., Riedesel, C., Thompson, E.: Developing a computer science-specific learning taxonomy. SIGCSE Bull. **39**(4) (2007) 152–170

[9] Roper, C., Grau, J., Fischer, L.: Security Education, Awareness and Training: From Theory to Practice. Elsevier Butterworth Heinemann (2005)

[10] Van Niekerk, J., Von Solms, R.: 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)

[11] National Institute of Standards and Technology: 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)