Creating a Security Culture Development Plan and a Case Study

O. Olivos

Inca Garcilaso University, Lima, Peru
e-mail: olivosomar@gmail.com

Abstract

When developing training and awareness programs, information security specialists usually fail to consider the human element as an important component of the program (Kruger et al, 2006). They tend to focus on security policies and technical aspects leaving aside the human aspect of information security. We argue that it is necessary that the characteristics of the employees (roles and learning styles), the compliance with the current policies, the state of the security culture and the mission, vision and strategic planning of the organization be considered when setting up a security culture development plan. This paper describes the steps that should be followed to develop a Security Culture and reports a case study in an organisation where the development plan was applied.

Keywords

Social Engineering, Training, Awareness, Security Culture

1 Introduction

Organizations that are in the process of developing training and awareness programs need to take into account the audience. They need to provide information and case studies that the audience can relate to, not a one size fits all training program (Deloitte, 2007). The human resources need to be evaluated so that we get a better understanding of the different learning styles and needs of each individual. The security policies in place and the perception of security within the organization need to be evaluated too. The strategic business plan must also be considered for the goals of the program are to be aligned with the business goals. With all this information the organization is ready to design and implement its Security Culture Development Plan (see Figure 1) to fight Social Engineering attacks. The processes have been devised with social engineering in mind; however, they could be used in a wider scope.

Security is not a technology problem-it's a people and management problem. As developers continuously invent better security technologies, making it increasingly difficult to exploit technical vulnerabilities, attackers will turn more and more to exploiting the human element (Nolan and Levesque, 2005). Social engineering is defined as the social/psychological process, by which an individual, the social engineer, can gain information from an individual about a targeted organization (Thornburgh, 2004). Therefore physical and technical controls are not enough to protect the confidentiality, integrity and availability of the information. The human

dimension is usually considered the weakest link in the overall ICT security chain (Tarimo et al, 2006). This paper describes the steps (see Figure 1) that should be followed to develop a security culture which will help the organization mitigate the risks of social engineering attacks.

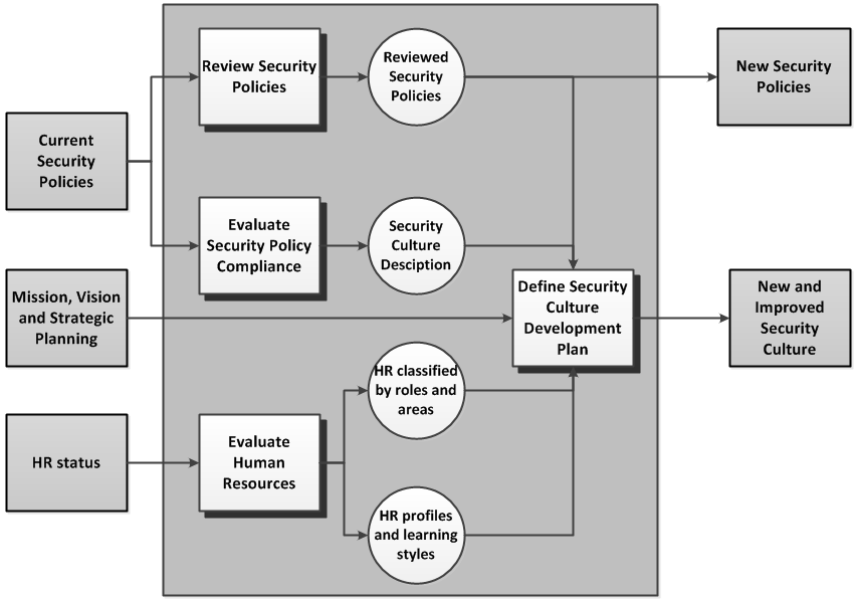

Figure 1: Security Culture Development Plan

The security culture development plan introduced in this paper is based on the conceptual model of information security culture described by Van Niekerk and Von Solms (2006, 2010). Their work is an extension of the model for corporate culture presented by Schein (1999). This model has become widely accepted amongst information security researchers (Schlienger & Teufel, 2003).

The adaptation of Schein's model is composed of 4 layers: Artifacts, Espoused Values, Shared Tacit Assumptions and Knowledge (Van Niekerk and Von Solms, 2006, 2010).

According to Schein and Van Niekerk and Von Solms, artifacts are what actually happen in the organization. Espoused values can be seen as the visible contributions of the organization's management towards the organization's culture. The mission, vision and policies form part of the espoused values. The shared and tacit assumptions layer consists of the beliefs and values of employees. Having adequate knowledge regarding information security is a prerequisite to perform any normal activity in a secure manner. Without adequate knowledge, information security cannot be ensured (Van Niekerk and Von Solms, 2006, 2010).

The artifacts layer will be evaluated by the Evaluate Security Policy Compliance process. The espoused values are assessed and standardized in the Review Security Policies process. They are also included in the Define Security Culture Development Plan process in the form of the mission, vision and strategic planning. The knowledge is instilled as part of the training and culturization process (Lower order thinking skills). The shared tacit assumptions will be dealt with in the training and culturization process when the instructor helps the employees develop their higher order thinking skills.

The remainder of the paper is organized as follows. Section 2 explains how to evaluate the organization's security policies. Section 3 gives details on the steps followed to determine what is the organization's perception and attitude towards security. Section 4 deals with the aspects that should be taken into account when evaluating the human resources of the organization. Section 5 explains in detail how the security culture development plan works and Section 6 how to measure its results. A case study is reported in Section 7. Finally, Section 8 concludes the paper with some general comments.

2 Review Security Policies

The security policy is basically a plan, outlining what the company's critical assets are, and how they must be protected. Its main purpose is to provide employees with a brief overview of the acceptable use of any of the Information Assets, as well as to explain what is deemed as allowable and what is not, thus engaging them in securing the company's critical systems (Danchev 2003).

Danchev (2003) also mentions that the main reasons behind the creation of a security policy is to set a company's information security foundations, to explain to employees how they are responsible for the protection of the information assets, and emphasize the importance of having secured communications while doing business online. Policies also have to address issues such as threats and possible countermeasures as well as defining roles and responsibilities (Mlangeni and Biremann, 2005).

Management should set a clear policy direction in line with business objectives and demonstrate support for, and commitment to, information security through the issue and maintenance of an information security policy across the organization (ISO 17799, 2005). Policies should reflect the overall attitude of top management about security controls and its importance to the organization (Dhillon, 2001).

Since information security culture emerges where specific behaviour is encouraged such as complying with a well-established standard (Martins and Eloff, 2002), we suggest that the current organization's security policies be compared with an international standard such as ISO/IEC 27002.

In this section of the paper we consider three aspects of security: Physical, Technical and Administrative. Since we focus on the human aspect of security and ISO 27002

does not specifically address social engineering we have taken into account only those elements or controls that are related to the human component of security. A checklist for each of the three aspects of security is provided so that the current security policies can be assessed. As a result of this process, an improved ISO 27002-compliant set of policies are suggested to the organization to provide better protection against social engineering attacks.

3 Evaluate Security Policy Compliance

In this process we evaluate the compliance with the security policies. This will help us understand the employee's perception and attitude towards security. This is important because inconsistent application of policies may lead to frustration by employees and thus undermine the effectiveness of policies (Stephanou and Dagada, 2008). Our goal is to develop an information security culture and to achieve this we need to provide knowledge, promote a positive attitude towards security and modify the behaviour because it's not what people know, or feel, or are aware of that is the final determinant of the quality of security — it's what they do (Roper et al, 2006 p7).

Good security practice goes beyond technical IT solutions. It is driven by a business strategy with associated security policies and procedures implemented in a culture of Security. These practices are supported by IT and Financial Resources dedicated to Security (Ang et al, 2006). As suggested by some authors, one way of measuring the level of an organization's information security culture is to use an information security culture assessment instrument (e.g. questionnaires or surveys) (Da Veiga et al, 2007) so a survey is applied to members of the organization and they are asked to rate a series of statements about their perception of security, specifically: The current state of that security issue within their organization and the importance of that security issue for their organization.

4 Evaluate Human Resources

In order to develop a successful security culture development plan the human component needs to be taken into account. In this step we suggest that the human resources be evaluated in two aspects:

4.1 Roles

An inventory of the roles that the employees have within the organization is required. These roles grant them access to different information systems and provide them with the appropriate level of information. Employees with different roles perform different tasks and also have different needs which make them vulnerable to different kinds of social engineering attacks. Due to the nature of their job, phone operators will benefit more from training on pretexting, mobile users will require more training on shoulder surfing and receptionists and guards on impersonation to name a few. Other topics like phishing among others will apply to all employees.

4.2 Learning Styles

Students learn in many different ways –by seeing and hearing; reflecting and acting; reasoning logically and intuitively; memorizing and visualizing and drawing analogies and building mathematical models; steadily and in fits and starts. How much a given student learns in a class is governed in part by the student's native ability and prior preparation but also by the compatibility of his or her learning style and the instructor's teaching style (Felder and Silverman, 1988). A learning style model classifies students according to where they fit on a number of scales pertaining to the ways they receive and process information (Felder and Silverman, 1988).

Adults have previous knowledge, experiences, relationships, believes that influence the way they behave and how they learn (Lowy and Hood, 2004 p 267). We should make use of this background when creating the groups and also when preparing the training and culturization sessions. Kolb's learning theory sets out four distinct learning styles (Figure 2), which are based on a four-stage learning cycle. Knowing a person's learning style enables learning to be orientated according to the preferred method (Kolb and Kolb, 2005).

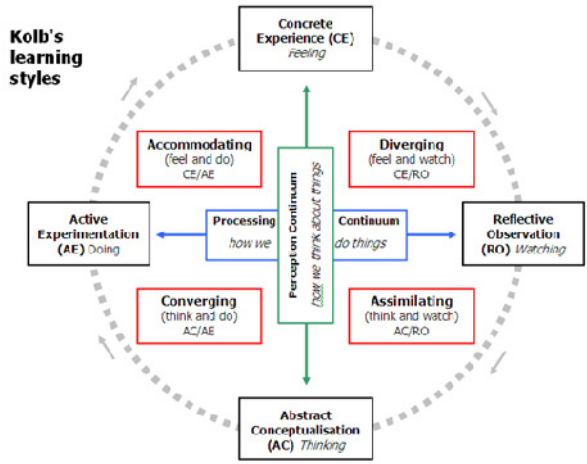

Figure 2: Kolb's Learning Styles (Chapman, 2005)

A learning style is a preference, not an absolute. All learners, regardless of preference, can function in all four styles when needed (Sharp, 1998). Assessing an individual's learning style is vital to the teaching and learning process (Hein and Budny, 2000). There is vast collection of learning models amongst which Kolb Learning Style Inventory (KLSI) remained one of the most influential and widely distributed instruments used to measure individual learning preferences (Kayes, 2005). The original KLSI encountered serious attacks because of his low test-retest reliability and limited construct validity. In 1985, the inventory was reorganized and redeveloped in light of the psychometric criticism it received. The KLSI was redesigned with the aim of experimentally evaluating skills of individuals in learning

process. The inventory was further redeveloped in 1996 (Lu et al, 2007; Yildirim, 2010). Researchers have examined and found support for the revised KLSI and found increased stability (Lu et at, 2007).

As shown in Figure 2, Kolb's model works on two levels - a four-stage cycle:
* Concrete Experience - (CE)
* Reflective Observation - (RO)
* Abstract Conceptualization - (AC)
* Active Experimentation - (AE)

And a four-type definition of learning styles, each representing the combination of two preferred styles:
* Diverging (CE/RO)
* Assimilating (AC/RO)
* Converging (AC/AE)
* Accommodating (CE/AE)

Each individual learning style should be taken into account by the Security Culture Development Plan team when setting out the groups and also by the instructor when preparing the lessons and activities that will be used in the culturization sessions.

5 Security Culture Development Plan (SCDP)

This is the most important process because here we will provide the necessary knowledge and will establish the foundations for the shared tacit assumptions. Without adequate knowledge, information security cannot be ensured (Van Niekerk and Von Solms, 2010). The shared tacit assumptions consist of the beliefs and values of employees. If such 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).

The main goal of the SCDP is to set the foundations to develop a new security culture that takes into account the needs and learning styles of each individual, their security perception, the security policies of the organization and its business goals.

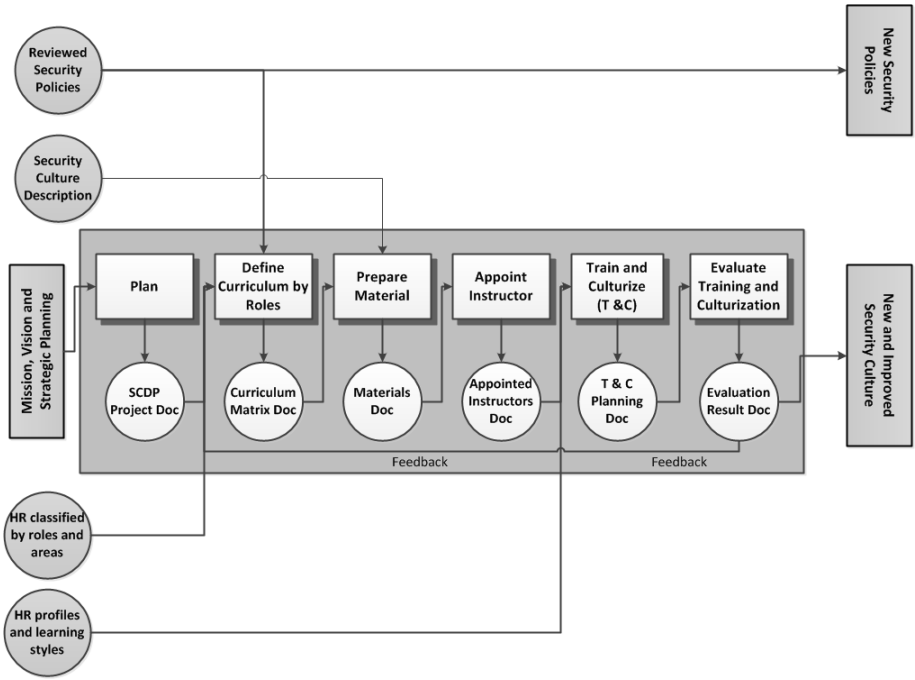

Figure 3: Define a Security Culture Development Plan

This process is composed of 6 sub processes and each of these processes produces a document that is used as the input for the following step. In Figure 3, we can observe the main and first feedback loop. The result of the evaluation of the training and culturization process provides the SCDP Team with the necessary feedback to reorganize and redefine the curriculum, prepare and acquire better material or appoint another instructor that fulfils the requirements.

5.1 Plan

It is a very important part of the process but is often overlooked. Just like in any other project the goals of the SCDP must be clearly stated and must be aligned with the organization's goals. The SCDP Team needs to make sure that the security program adapts to the changing business environment, requirements and technology (Tyukala et al, 2006). The necessary resources (people, money, time, etc.) must be allocated to the project and the support from the higher levels of the organization must be obtained. It is composed of four steps:

a) **Define Goals.** Goals must be in line with the organization's goals and must support the business needs of the organization and be relevant to the organization's culture and IT architecture (NIST 800-50, 2003, p.22).

b) **Appoint a champion**. It is the person that will lead the project and be the link with the stakeholders. This individual will provide leadership and should have

overall responsibility for the preparation and implementation of the program (Baybutt, 2003). Since support and commitment from the top management is vital, it is suggested that the champion be a member of the senior management (Höne, 2004).

c) **Form the SCDP Team**. Since it is not just a training program but a project to develop a security culture, personnel from different areas will be required to participate. Members of the following business areas should be included: IT, HR, Marketing, Legal Department and Security. Representatives from other areas could and should participate depending on the size and needs of the organization.

d) **Allocate resources and budget**. A special budget must be allocated, it cannot be the same budget assigned to IT or physical security. This is a different project and as such it needs its own resources. The Security Culture Development Plan should not be seen as a spending cost but as an investment (Soon Lim et al, 2009).

5.2 Define curriculum by roles.

The first job of the SCDP Team is to prepare a list of relevant security topics that need to be addressed during the training and culturization process. Since not all areas have the same needs, these topics must be carefully mapped to the different business areas in the organization. The receptionist and assistants may need more training on pretexting and attacks over the phone while laptop users may need training on how to prevent shoulder surfing for instance. It is important to distinguish between job-specific and overall security training and practices (Kraemer and Carayon, 2005). The topics chosen must reflect the weaknesses identified during the revision of the security policies. Members of the IT department and the CIO/CISO play an important role in adding items to this list as they are aware of new threats and techniques used by social engineers.

5.3 Prepare material

This process receives the Security Culture Description document as an input from the Evaluate Security Policy Compliance process. This document will help the SCDP Team prioritize the topics that need urgent attention and that should be dealt with first.

The next step is to acquire or produce the marketing material necessary to spread the new ideas and information about training possibilities, security tips, etc. The marketing area of the organization will play an important role in this process. It is suggested that the direct marketing approach be used to spread the new ideas. Unlike mass marketing, direct marketing takes into account the characteristics of each individual such as the age, sex, role in the organization, experience and others (Stewart, 2009). Once the marketing material is acquired, it is recorded in the

inventory and then using the Marketing Material Matrix the SCDP Team matches the marketing material with the topics listed in the Define Curriculum by Roles process.

Then SCDP Team needs to obtain training material (videos, books, presentations, CBT, WBT, etc.) that will be used during the training and culturization process. Ideas on how to develop and deliver awareness and training material can be found on NIST 800-50 (2003).

5.4 Appoint instructor.

Usually it is a member of the IT department who delivers the classes. We consider that it is extremely important that the instructor have teaching experience and knowledge of teaching techniques. We believe that one of the main reasons why training programs fail to achieve a change in attitude is because they only work on the lower order thinking skills (LOTS). Lower order thinking skills are related to remembering and understanding knowledge while higher order thinking skills (HOTS) are related to evaluating, judging, creating and formulating ideas. (Van Niekerk & Von Solms, 2008)

5.5 Train and culturise.

This is the most important process and it is the main contribution of this paper. Most training programs work only on LOTS and therefore accomplish neither a change in attitude nor a change in behaviour.

Users may know and understand their roles in the organization correctly but still don't adhere to a security policy because it conflicts with their beliefs and values (Schlienger & Teufel, 2003). It is therefore important to also ensure that the users have the correct attitude, and thus the desired behaviour, towards information security (Van Niekerk & Von Solms, 2006; Kruger et al, 2006). In order to ensure the desired user behaviour, it is necessary to cultivate an organizational culture of information security (Von Solms, 2000; Schlienger & Teufel, 2003; Tarimo et al, 2006).The Training and Culturization process is composed of five steps (see Figure 4)

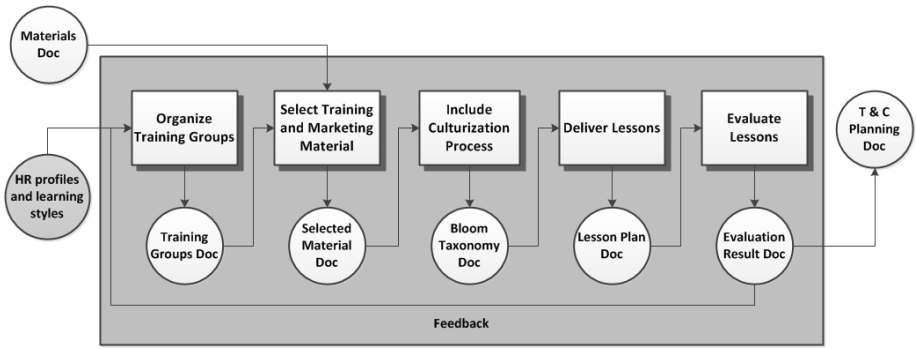

Figure 4: Training and Culturization process

a) **Organize Training Groups.** Employees are divided into groups based on the roles they play in the organizations, the tasks they perform, their learning styles and their availability. It is important to record the criterion that was used to form the groups so that the instructor is aware of it.

b) **Select Training and Marketing Material.** The material relevant to the topics listed in the Define Curriculum process and the groups formed is chosen from the available material acquired in the Prepare Material process.

c) **Include Culturization Process.** During the preparation of the training and culturization sessions the appointed instructor must take into account the different learning styles identified in the Evaluating Human Resources process. The activities that will be used in the training and culturization sessions should correspond to each of the Bloom's levels in order to make the participants reach the highest level of the taxonomy hence promoting a change in the attitude and behaviour. An information security specialist might think that teaching the users what a password is (or lecturing users on the organization's security policies), is enough, but research has shown that understanding why is essential to obtaining buy-in from employees (Van Niekerk & Von Solms, 2008). Table 1 shows examples of activities that can be used in each level during the training and culturization sessions on Password Management. Based on these examples, the instructor should create activities that will help users (considering their different learning styles) move from a passive role (remembering and understanding) to a more active role (evaluating and creating).

d) **Deliver Lessons.** The instructor will work on the activities designed in the previous step, see Table 1 for suggested activities. The lessons must be delivered using a variety of techniques that accommodate participants with different learning styles. We believe that the instructor must have some teaching experience as the goal is not just to make sure that the employees acquire knowledge but that they change their attitude towards security and behave in a secure manner.

Level	Activities
Create	Formulate a theory to explain why employees still write down their passwords and what the risks of doing so are. Propose solutions to this problem (Van Niekerk & Von Solms, 2006).
Evaluate	Judge and evaluate organization's security policies about passwords and suggest changes and improvements
Analyse	Compare the level of protection provided by passwords and other mechanisms (biometrics, smartcards, etc).
Apply	Use mnemonic techniques to create and recall a secure password.
Understand	Explain why the organization requires that the password includes non-alphanumeric characters and a minimum of 8 characters.
Remember	Describe the characteristics of a strong password as stated in the organization's security policies.

Table 1: Suggested Activities based on Bloom's taxonomy

5.6 Evaluate Lesson

It is extremely important to evaluate each and every training and culturization session or lesson delivered. It will provide feedback to make the necessary amendments to the lessons. Since our goal is to develop a security culture within each of the participants we believe that each session should be assessed. First, it should assessed by each employee who participated in the session using a form provided. Second, by the instructor to check if the goals set were achieved. And in some cases by the SCDP team. In a large organization it would impossible for the SCDP team to evaluate every session but it should definitely assess some. This process provides the inner feedback loop. This feedback allows the instructor to make the necessary amendments.

6 Evaluate Training and Culturization

Without effective measurement and evaluation, there is no real evidence from which to conclude that training and culturization have been effective - not just that awareness of information security issues has been raised, but also and more importantly that positive behavioural change towards information security has actually been effected (Davis, 2008).

Without this measurement, it is impossible to establish whether or not an appropriate return on the investment has been realized. Measurement also plays an important part in allowing organizations to adopt a risk-based approach to information security, as it allows a business to identify where there is a need for greater investment in training as well as where it may be possible to spend less without impacting the security risk profile adversely (Davis, 2008).

Once the Training and Culturization process has been completed it is necessary to evaluate its success. In the previous step, Evaluate Lesson, we assessed the success/failure of an individual lesson, in this process we look at the whole process that means the effect that it has had on the knowledge, attitude and behaviour of the individuals (Kruger and Kearney, 2005). It provides the outer and main feedback loop which allows the SCDP Team to make the necessary amendments and also to justify future investments in the program (Schlienger & Teufel, 2003).

To evaluate knowledge we suggest that multiple choice, True/False, fill in the blanks and matching definitions tests be used. They are all easy to administer and can be done through a virtual learning environment. Surveys, interviews and focus groups are the most effective methods to evaluate the change in attitude. Surveys, interviews and focus groups can also be used to evaluate the change in behaviour. Although they are time-consuming activities they are very effective.

Other methods such as the following can also be used:

* Internal and External Audits.
* Participation in coaching programs.
* Participation as security champions for their section or department.
* Posting in blogs and/or wikis about security.

One of the main focuses of this work is to make sure that the learning styles of each member of the organization be taken into account. Therefore it is important to keep a record of each individual. Social engineers will always look for the weakest link in the security chain so it is necessary that the organization keeps track of the development of each employee in terms of knowledge, attitude and behaviour towards security.

7 Case Study

The proposed Security Culture Development Plan was applied in an organization with over 20 years of experience in manufacturing and trading high-quality canned, fresh and frozen products. The organization has 40 employees in its main office and 8 admin employees in its two branches plus a large number of workers on the fields.

The first step was to review the security policies. We requested all the documents that the organization had related to information security (policies, procedures, guidelines and others). We also interviewed two of the managers, the head of the IT section and 5 employees from different sections. We found that the security policies were spread over several documents many of which are not known by the employees. No specific roles or responsibilities are defined in the documents. Some of the rules are not applicable in the organisation anymore. For example, one of the documents states that employees are responsible for backing up all their critical information stored in their computers and that they are to contact the IT department if they require any assistance with the process. In our interview with the Head of IT he mentioned that all backup was centralised and that the IT department was responsible

for the backup and restore processes. In other cases, the employees are asked to perform certain tasks but are not explained how and are not provided with more information. For example, employees must change their password every three months but are not told what the password requirements are (length, use of symbols, etc). However, this information appears in a PowerPoint presentation available in a folder in the public network drive. None of the 5 employees interviewed had ever received copies of all these documents.

After this assessment, an improved ISO 27002-compliant set of policies were suggested to the organization. Management and the IT department made some changes and finally the new policies were approved.

The second step was to evaluate the Security Policy compliance so we applied a questionnaire to 3 of the managers, the 3 members of the IT department and 21 employees from different sections.

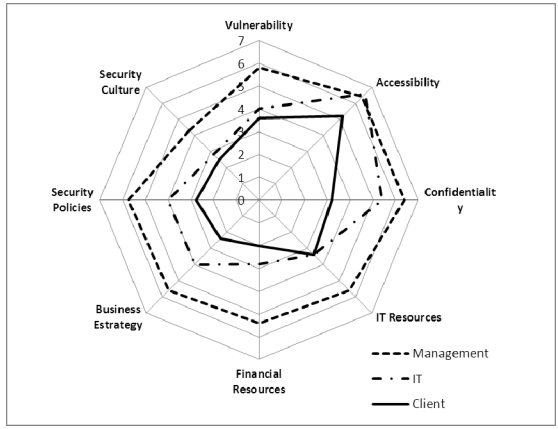

Figure 5: Security Assessment Results

The results (see Figure 5) show that the managers feel that the main weakness in information security in the organisation lies on people. They also feel that they are providing enough financial and IT resources for security purposes and that business strategies and security policies are well aligned. The three members of the IT department agree on the fact that security culture is an issue but think that they are not provided with enough resources to fulfil their roles in terms of information security. Finally the 21 employees who participated had a more pessimistic perception of security in the organization and assessed it very low in almost all the aspects of the questionnaire. As had been discovered earlier most employees are not aware of the existing security policies and do not feel that the organization management supports information security adequately.

Role/ Area	Employees
Manager / supervisor	6
Administration	15
Commercial	9
Reception/Secretary	3
IT	3

Learning Style	Employees
Diverging	10
Assimilating	7
Converging	7
Accommodating	6
Total	**30**

Table 2: HR classification by roles and learning styles

Members of the organisation were also classified according to the roles they have, the areas they belong and their learning styles (Table 2). Only 36 out of the 40 employees were considered as one employee was away on parental leave and 1 had a contract that was due in the next couple of weeks and would not be renewed. One was on holidays and another had been sent to one of the branches to replace the branch supervisor who was away on vacations. Out of the 36 only 30 completed properly and on time the learning style questionnaire.

The Chief of Admin and Finance was designated SCDP Champion and the SCDP Team was formed by 2 members of the IT department, 1 member from the commercial section and the human resources supervisor. One of their first tasks was to put together a list of security topics that need to be addressed during the training and culturization process. These topics included: Social Engineering, shoulder surfing, password management, dumpster diving, phishing, information classification, laptop/mobile security, internal threats, influence techniques and impersonation.

The next step was to map these topics to the clients based on their roles in the organisations (see Table 3). Some topics are specific to some clients, for example since laptops are only issued to managers and supervisors, the receptionist would not need special training on this area.

The SCDP Team then prioritized the suggested topics based on the needs of the organization. Password management, laptop security, phishing and information classification were considered the topics with the highest priority. Flyers related to the topics were downloaded from the European Network and Information Security Agency (ENISA) website and posted on the walls in different parts of the building. Some comic strips (taken from Dilbert's website) about password management and other security related topics were found by the SCDP Team. An employee volunteered to translate them into Spanish and emailed them to his colleagues. There was very positive feedback on this.

Due to budget constrains no books or videos were bought at this time. All material used during the Training and Culturization sessions was prepared in house. Since we

have a teaching background, experience in information security and knowledge of the proposed methodology we became the instructor.

	Managers / Supervisor	Admin	Commercial	Secretary / Reception	IT
Social Engineering	√	√	√	√	√
Shoulder Surfing	√	√	√	√	
Password Management	√	√	√	√	
Dumpster diving		√	√	√	√
Phishing	√	√	√	√	√
Information classification	√	√	√	√	√
Laptop Security	√				
Internal threats		√	√	√	√
Impersonation			√	√	
Influence techniques			√	√	√

Table 3: Security topics by roles

The training groups were formed based on time availability, role in the organization and learning styles. Time availability became the main restriction. The first group was composed of 10 employees. Since all 4 learning styles were present in the group the activities were planned to accommodate all learning styles.

The activities presented in Table 1 were used during the training and culturization sessions. All sessions were planned using the provided lesson plan format. The lesson plan contained the topic, objectives, activities, material needed and assessment opportunities for each session (Figure 6).

Lesson Plan format

Lesson Plan Title		Topic
Safe Passwords in the Organisation		**Password Management I**
Instructor	**Time**	**Sub Topics**
Omar Olivos	**1h 15m**	• **Mnemotechnic rules** • **Attack techniques**
Main Objectives		**Secondary Objectives**
• Describe the Organisation security policies regarding the use of passwords • Apply Mnemotechnic rules to create and remember strong passwords		• Name common techniques used by social engineers to obtain passwords • Name god and bad habits on password management

Activities	Materials	Assessment Strategies
• Explain Objectives • First Assessment (Pre Test) • Presentation ○ Organisation Security Policies ○ Social Engineer techniques. ○ Mnemotechnic rules (Group discussion) ○ Group presentation– Feedback • Final Assessment (Post Test)	• Laptop • Projector • PowerPoint Presentation (ppt) • Memory Stick USB • Whiteboard / Markers / Large pieces of paper • Organisation Policies– hard copies • Paper / pens • Internet Access. The password meter	Pre Test - Multiple Option Post Test - Multiple Option Group Work • Discussion • Presentation - Feedback

Notes
Final Assessment (Post Test) can be handed in at the beginning of the following session if there is not enough time left at the end of Session I.

Figure 6: Lesson Plan - Session I on Password Management

At the beginning of the session the First Assessment (Pre-Test) was distributed to all and out of the 10 participants:

Only 5	Knew what was the minimum password length as stated in the organization's policies
Only 2	Were able to identified a password that fulfilled all the requirements as stated in the policy documents
Only 2	Knew how often they needed to change their password
Only 3	Would not provide their password to another person under any circumstances

In this session we only worked on the lower order thinking skills (LOTS): remember, understand and apply.

At the end of the session the Post-Test was distributed to all and out of the 10 participants

All	Remembered what was the minimum password length as stated in the organization's policies
All	Identified the password that fulfilled all the requirements as stated in the policy documents
9	Knew how often they needed to change their password
All	Would not provide their password to another person

In a later session, we continued working on Password Management but with an emphasis on higher order thinking skills (HOTS): analyse, evaluate and create. Our

goal is to promote a positive attitude towards information security and a change in the behaviour. During this session participants identified bad security practices in the organisation and provided solutions to these problems. A common problem was that managers shared their passwords with their assistants so that they could check and update their calendars. It was suggested that the calendars be shared and permissions be granted to the assistants so that they could access their bosses' calendars without knowing their passwords. Participants also came up with new techniques to create strong password that were easy to remember (like using two words in different languages and adding numbers and symbols to make it more complex).

Knowledge acquired was assessed with the Post-Tests in each session. Attitude was assessed during the group activities and also through their feedback and comments. Change in behaviour was assessed in later interviews with participants. Some participants mentioned that they had requested that their computers be changed positions as some other employees could shoulder surf them while entering their passwords. The SCDP champion supported this request and the workstations were repositioned. Another participant mentioned that now she shuts the blinds when the cleaners are cleaning her office windows to avoid them from looking at her computer screen. IT support granted assistants access to manager's calendar as requested by them and approved by their bosses. Another participant was very proud because she was able to teach her teenage son some techniques to create strong password. Even though the son spent a great deal of time in the computer he did not have good security habits. All the participants interviewed had changed at least one of their passwords in the last 10 days and their work password was different from the other passwords they had.

All the responses we got showed that all participants had acquired the required knowledge, that they had a different attitude towards security and that they had a more positive and proactive behaviour towards security in the organisation and in their private lives. A new security culture was emerging.

8 Conclusions

In this paper we presented a holistic approach on how to create a security culture development plan in an organization based on the conceptual model of information security culture described by Van Niekerk and Von Solms (2006). This approach considers the human component as one of the most important ones. Employees play different roles within the organization, they have different learning styles and have different backgrounds that need to be considered when creating groups, planning activities and delivering lessons. The training and culturization sessions cannot be just traditional lectures, it is important that different activities are used to reach all learning styles. The activities must also be carefully planned based on the different levels of Bloom's taxonomy. The instructor must have some teaching experience or pedagogical background as the main goal is not just to provide knowledge but to change the attitude and the behaviour which will later develop a security culture in the organization. Assessment of knowledge, attitude and behaviour is also necessary and the SCDP Team must keep track of the progress of members of the organization.

Policies are also very important and must reflect the organization's business strategy. Since support from the top management is necessary for the project to be successful, it is suggested that the SCDP champion be a member of the senior management.

Information security is not just the responsibility of the computer department but of every single member of the organization. Therefore we need to make sure that all business areas are part of the security culture development plan. Finally after applying the suggested methodology a change in behaviour was observed in all the employees that participated in the Training and Culturisation sessions.

9 References

Ang, W.H., Lee, Y., Madnick, S., Mistree, D., Siegel, M., Strong, D. and Wang, R. (2006), "Designing the house of security: Stakeholder perceptions of security assessment and importance", *MIT Sloan Working Paper* 4623-06, Proceedings of the Twelfth Americas Conference on Information Systems.

Baybutt, P. (2003), "Process security management systems: Protecting plans against threats". *Chemical Engineering*, Vol 110, No 1, pps 48-55.

Chapman, A. (2005), "The Kolb Learning Styles", www.businessballs.com/kolblearningstyles.htm (Accessed 10 June 2010) .

Da Veiga, A., Martins, N., Eloff, J. (2007), "Information security culture - validation of an assessment instrument". *Southern African Business Review*, vol. 11, no. 1, pp. 147-166.

Danchev, D. (2003), "Building and Implementing a Successful Information Security Policy", *Windows Security*.

Dhillon, G. (2001), "Violation of safeguards by trusted personnel and understanding related information security concerns". Computers & Security, Volume 20, pp 165-172.

Felder, R.M., Silverman, L.K. (1988), "Learning and teaching styles in engineering education", *Engineering Education*, 78(7), pp. 674–681.

Hein, T.L., Budny, D.D. (2000), " Styles and types in science and engineering education", *International Conference on Engineering and Computer Education (ICECE)*, Sao Paulo, Brazil. Article published in the ICECE proceedings.

Höne, K. (2004), "The information security policy - an important information security management control". *Faculty of economic and management science*, Rand Afrikaans University.

ISO. (2005), "Information technology. Security techniques. Code of practice for information security management", ISO/IEC 17799 (BS 7799–1: 2005).

Kayes, D.C. (2005), "Internal validity and realiability of Kolb's Learning Style Inventory version 3 (1999)". *Journal of Business and Psychology*, 20 (2), 249-257.

Kolb, A., Kolb, D. (2005), "The Kolb Learning Style Inventory, Version 3.1", Boston, Hay Group.

Kraemer, S., Carayon, P., (2005), "Computer and information security culture: Findings from two studies". *Proceedings of the Human Factors and Ergonomics Society 49th Annual Meeting*.

Kruger HA., Drevin, L., Steyn, T. (2006), "A framework for evaluating ICT security awareness". *Proceedings of the 2006 Information Security South Africa Conference*, Sandton, South Africa.

Kruger, HA., Kearney, WD. (2005), "Measuring information security awareness: A West Africa gold mining environment case study". *Proceedings of the 2005 Information Security South Africa Conference*, Sandton, South Africa.

Lowy, A., Hood, P. (2004), "The Power of the 2x2 matrix" Jossey-Bass, New York.

Lu, H., Jia, L., Gong, S.H. and Clark, B. (2007), "The relationship of Kolb learning styles, online learning behaviors and Learning outcomes". *Educational Technology & Society*, 10(4), 187-196.

Martins, A., Eloff, J. (2002), "Information Security Culture". Security in the information society, pp 203-214. *IFIP/SEC2002*. Boston, MA: Kluwer Academic Publishers.

Mlangeni, SA., Biermann, E. (2005), "An assessment of Information Security Policies within the Polokwane area: A case study". *Proceedings of the 2005 Information Security South Africa Conference*, Sandton, South Africa.

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.

Nolan, J. and Levesque, M. (2005). "Hacking human: data-archaeology and surveillance in social networks", ACM SIGGROUP Bulletin, vol. 25, no. 2, pp33-37.

Roper, C., Grau, J. and Fischer, L. (2005), "Security education, awareness and training: From theory to practice". Elsevier Butterworth Heinemann.

Schein, EH. (1999), "The corporate culture survival guide". Jossey-Bass Inc.

Schlienger, T., Teufel, S. (2003), Information Security Culture – from Analysis to Change, *Proceedings of the 3rd Annual Information Security South Africa Conference*, Sandton, South Africa.

Sharp, J., (1998) , "Learning Styles And Technical Communication: Improving Communication And Teamwork Skills". Proceedings, 1998 Frontiers in Education Conference.

Soon Lim, J., Chang, S., Maynard, S., Ahmad, A., (2009), "Exploring the relationship between organizational culture and information security culture". *7th Australian Information Security Management Conference* pp 88-95. AISM2009. Perth, Western Australia.

Stephanou, AT., Dagada R. (2008), "The impact of information security awareness training on information security behaviour: The case for further research", Information Security South Africa (ISSA), Johannesburg, South Africa.

Stewart, G,. (2009), "Maximising the effectiveness of information security awareness using marketing and psychological principles". *Technical Report*, RHUL –MA-2009-02. Royal Halloway, University of London.

Tarimo, C., Kuwe, J., Yngström, L., Kowalski, S. (2006), "A social-technical view of ICT security issues, trends, and challenges: Towards a culture of ICT security – The case of Tanzania". *Proceedings of the 2006 Information Security South Africa Conference*, Sandton, South Africa.

Thornburgh, T. (2004), "Social Engineering: The dark art". *InfoSecCD Conference'04*, Kennesaw State University.

Tyukala, M., Pottas, D., Van de Haar, H., Von Solms, R. (2006), "The organisational information security profile – a tool to assist the board". *Proceedings of the 2006 Information Security South Africa Conference*, Sandton, South Africa.

Van Niekerk, J., Von Solms, R. (2006), "Understanding information security culture: A conceptual framework". *Information Security South Africa (ISSA)*, Johannesburg, South Africa.

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

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

Workman, M. (2007), "Gaining access with social engineering: An empirical study of the threat". *Information Security Journal*: A global perspective 16:6, 315-331, Florida USA.

Yildirim, N. (2010), "Increasing effectiveness of strategic planning seminars through learning style" . *Australian Journal of Teacher Education*, Vol 35, 4, July 2010.

Zakaria, O. (2004), "Understanding challenges of information security culture: a methodological issue". *2nd Australian Information Security Management Conference* pp 83-93. AISM2004. Perth, Western Australia.