Information Security Service Management

- a service management approach to Information Security Management

Rahul Rastogi

Information Security Service Management

- a service management approach to Information Security Management

Rahul Rastogi

Thesis

submitted in fulfilment of the requirement 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**

January 2011

“Har haqeeqat majaaz ho jaaye …”

(Let all established truths be questioned …)

- Faiz Ahmed Faiz

ABSTRACT

In today's world, information and the associated Information Technology are critical assets for many organizations. Any information security breach, or compromise of these assets, can lead to serious implications for organizations that are heavily dependent on these assets. For such organizations, information security becomes vital.

Organizations deploy an information security infrastructure for protecting their information assets. This infrastructure consists of policies and controls. Organizations also create an information security management system for managing information security in the organization. While some of the policies and controls are of a purely technical nature, many depend upon the actions of end-users. However, end-users are known to exhibit both compliant and non-compliant behaviours in respect of these information security policies and controls in the organization. Non-compliant information security behaviours of end-users have the potential to lead to information security breaches. Non-compliance thus needs to be controlled.

The discipline of information security and its management have evolved over the years. However, the discipline has retained the technology-driven nature of its origin. In this context, the discipline has failed to adequately appreciate the role played by the end-users and the complexities of their behaviour, as it relates to information security policies and controls. The pervasive information security management philosophy is that of treating end-users as the enemy. Compliance is sought to be achieved through awareness programs, rewards, punishments and evermore strict policies and controls. This has led to a bureaucratic information security management approach.

The philosophy of treating end-users as the enemy has had an adverse impact on information security in the organization. It can be said that rather than curbing non-compliance by end-users, the present-day bureaucratic approach to information security management has contributed to non-compliance. This thesis calls this the end-user crisis. This research aims at resolving this crisis by identifying an improved approach to information security management in the organization.

This research has applied the service management approach to information security management. The resultant Information Security Service Management (ISSM) views end-users as assets and resources, and not as enemies. The central idea of ISSM is that the end-user is to be treated as a customer, whose needs are to be satisfied. This research presents ISSM. This research also presents the various components of ISSM to aid in its implementation in an organization.

DECLARATION

I **RAHUL RASTOGI** , 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 fulfilment of the requirements for an equivalent or higher qualification at any other recognized educational institution.

_____

My sincerest gratitude to the following people,
without whom this thesis would never have been:

My promoter Prof. Rossouw von Solms,
for his kindness, understanding and guidance.

My wife,
for holding the fort for me,
and my children,
for the time I took from them and which was rightfully theirs.

My parents and extended family,
for always believing that I could do it and for letting me be.

My seniors at Engineers India Limited,
for extending to me the opportunity to undertake this study.

The Internet,
without which this study would have been unthinkable.

The numerous other researchers in Information Security,
on whose shoulders I stand.

All the people at NMMU,
who were ever so helpful that I never felt a stranger in their midst.

My friends and colleagues,
they were always there for relieving the stress.

And countless, nameless, faceless others,
who helped me carry on with my life, work and study.

Table of Contents

List of Figures

List of Tables

CHAPTER 1

Introduction

“One thing is sure. We have to do something. We have to do the best we know how at the moment... If it doesn't turn out right, we can modify it as we go along.”

- Franklin D. Roosevelt

1.1 Background

This thesis does not attempt to make a case for the importance of information, information technology (IT) and information security in today’s organizations. It treats this issue as being axiomatic for many of today’s organizations; and hence, does not provide references to substantiate the claim. Organizations, for which the axiom holds, are the target of this thesis. The subject of this thesis is the management of information security in such organizations.

Organizations implement information security through a plethora of information security policies and controls. These policies and controls constitute the information security infrastructure in the organization. Organizations also create an organizational structure to provide information security management (ISM) to ensure the *“supervision and making of decisions necessary to achieve business objectives through the protection of the organization's information assets”* (ISO/IEC 27000, 2009). This organizational structure is the information security management system (ISMS) which, according to ISO/IEC 27000:2009 (ISO/IEC 27000, 2009), provides a *"model for establishing, implementing, operating, monitoring, reviewing, maintaining and improving"* information security in the organization (for the purpose of this thesis, ISM and ISMS are synonymous). The ongoing effectiveness of information security policies and controls becomes an issue of critical importance. Any weaknesses in this regard have the potential to lead to significant losses for the organization. In this scenario, as stated in ISO/IEC 27000:2009 (ISO/IEC 27000, 2009), one of the critical success factors for ISM in the organization is the

behaviour of users of information and related information technology, commonly known as end-users. ISM operates in the organization by formulating information security policies and controls and mandating specific or 'expected' end-user behaviours and obligations. The end-users are expected to comply with their 'information security obligations' (ISO/IEC 27000, 2009) arising from these policies and controls. This coupling between end-user behaviour and information security management has an important bearing on the success of information security in the organization. It is thus an interesting issue to investigate.

1.2 Identification of the problem area

There is an implicit coupling between the end-user behaviour and the success of ISM in the organization. As end-users undertake their day-to-day work in the organization, they interact with information security policies and controls. However, the compliance of end-users with these policies and controls cannot be taken for granted. During these interactions, end-users are confronted by issues of knowledge, skills and attitudes towards information security. These issues ensure that end-users depict a variety of information security behaviours – sometimes they may comply, sometimes they may not comply (Furnell, 2010). In this scenario of inconsistent levels of compliance, the coupling between end-user behaviour and the success of ISM reveals its dark side. While compliance is commendable and leads to successful ISM in the organization, non-compliance takes end-users into a zone of deviation from the mandated or expected behaviours and leads to the failure of ISM in the organization.

The coupling between end-user behaviour and ISM is shown graphically in Figure 1.1 below. In the figure, the level of compliance or non-compliance is reflected by the amount of convergence or divergence between the expected and the actual end-user behaviour. The divergence between expected and actual end-user behaviour is shown along the horizontal axis. The level of success of ISM in the organization is shown along the vertical axis. The variation in the level of convergence or divergence (and hence variation in the level of compliance or non-compliance) relates directly to the success or failure of ISM in the organization. As the amount of divergence varies, so does the level of success or failure of ISM – decreasing divergence leads to more successful ISM, while increasing divergence leads to unsuccessful ISM.

As stated in the previous section, according to ISO/IEC 27000:2009 (ISO/IEC 27000, 2009) the compliance of end-users with information security policies and controls in the organization is a critical success factor for information security management. In view of the preceding discussion, this critical success factor can be restated more explicitly. Thus, in terms of the actual, observable end-user behaviours, the aforementioned critical success factor for information security management can now be restated as the minimization of the divergence between the

expected and the actual end-user behaviours in regard to information security policies and controls in the organization.

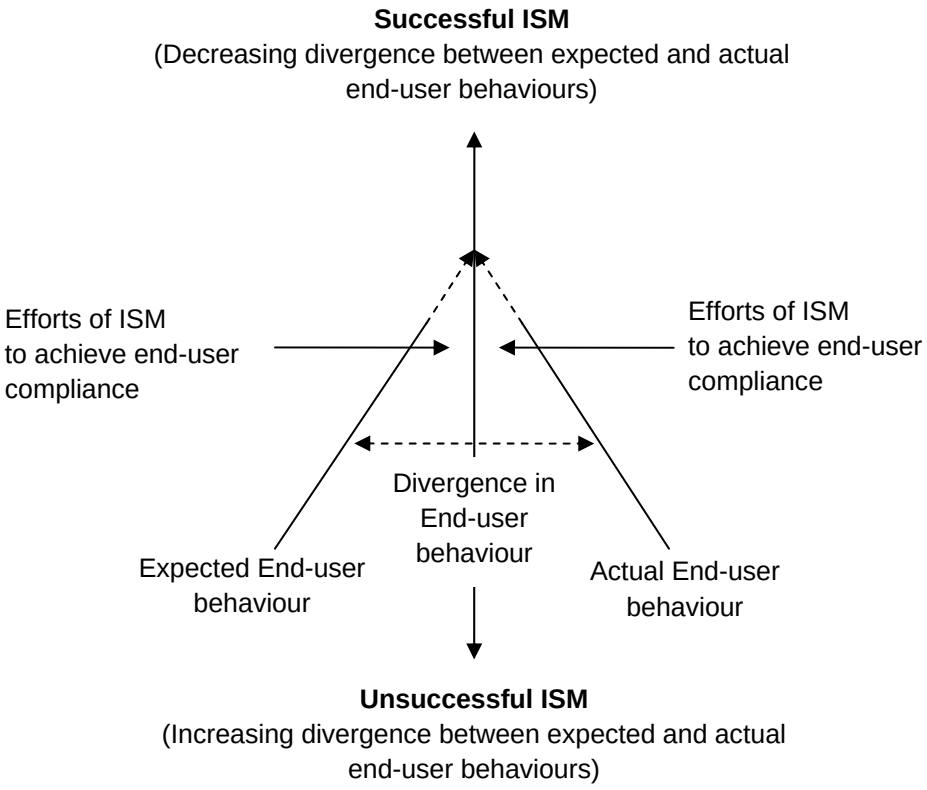


Figure 1.1: The coupling between end-user behaviour and information security management

Figure 1.1 shows another aspect of the coupling between end-user behaviour and ISM. It illustrates that ISM can make efforts to improve end-user behaviour, and thereby contribute to its own success in the organization. ISO/IEC 27002:2005 (ISO/IEC 27002, 2005) provides guidance regarding these end-user centric efforts by ISM in an organization. According to ISO/IEC 27002:2005 (ISO/IEC 27002, 2005), ISM can reduce the divergence between the expected and the actual end-user behaviours by providing *"an adequate level of awareness, education, and training in security procedures and the correct use of information processing facilities"* to the end-users. This program is to be further complemented by *"a formal disciplinary process for handling security breaches"* (ISO/IEC 27002, 2005).

The present-day approach to ISM, comprising the efforts stated above, however, has failed to yield good results. In spite of the efforts of ISM, end-users continue to exhibit significant levels of non-compliance with the information security policies and controls in the organization (Adams & Sasse, 1999; Dhillon, 2001b; Dourish, Grinter, Delgado de la Flor & Joseph, 2004; Furnell, 2010). Further, actions of ISM are leading to the creation of a 'digital divide' between information security managers and end-users (Albrechtsen & Hovden, 2009). Thus it can be said that rather than reducing the divergence between the expected and the actual information security behaviour of end-users, the actions of ISM are actually leading to increased divergence. This is the 'end-user crisis' of ISM which can be stated as follows:

Knowing the important role that end-users play in information security, ISM concerns itself with achieving end-user compliance with information security policies and controls; however, on the contrary, present-day ISM is leading to the creation of a digital divide between information security managers and end-users; this failure of ISM constitutes its end-user crisis.

1.3 Problem statement

The previous section has identified the end-user crisis as a problem area for ISM in organizations. For effective and successful information security in the organization, it is essential that this crisis be resolved. Present-day ISM, rather than resolving this crisis, is actually contributing to it; and the end-user crisis may be seen as self-inflicted. The problem facing ISM in the organization can be stated as follows:

There is a need to improve information security management in the organization, so that the digital divide between information security managers and end-users is bridged leading to improved compliance by end-users and improved effectiveness of information security in the organization.

1.4 Objectives

This thesis concerns itself with addressing the statement above, namely, that of identifying an improved approach to ISM, one that can resolve the end-user crisis. Taking this problem statement into account, the primary objective of this thesis is defined as:

To identify an improved approach to ISM that can assist in resolving the end-user crisis and lead to improved compliance of end-users with the information security policies and controls in the organization.

To achieve this primary objective, a number of secondary objectives need, initially, to be addressed. These secondary objectives provide a road-map for this research and are:

- To understand the information security behaviours of end-users and the reasons behind non-compliance.
- To understand the link between managerial styles and the behaviours of employees in the organization.
- To study the dominant managerial style inherent in present-day ISM and how it leads to the end-user crisis.
- To identify a management approach that has the potential to resolve the end-user crisis.
- To apply this identified approach to formulate an alternative approach to ISM and to identify the components of this approach so it can be applied in organizations for the management of information security.

The integration of the aspects addressed in the secondary objectives will help this thesis complete the resolution of the end-user crisis, which indeed is the primary objective. To meet its objectives and thereby to provide an improved approach to ISM in the organization, this thesis seeks to follow a research approach appropriate to the field of study. The next section discusses various research paradigms as they serve as the foundation of any research. The subsequent section identifies the research approach and methodology followed in this study.

1.5 Research philosophy and process

March and Smith (1995) stated that information gained through research is valuable as it helps in the formation of true beliefs about the subject under study, and then promotes the use of effective, goal-achieving action. This research project represents such a quest – to create new knowledge for resolving the end-user crisis of present-day information security management in the organization. Gioia and Pitre (1990) define theory as, *"any coherent description or explanation of observed or experienced phenomena"*. Corley and Gioia (2011) provide a similar definition: *"theory is a statement of concepts and their interrelationships that shows how and/or why a phenomenon occurs"*. In keeping with the objectives of this research project and the definitions of theory, it may be said that this research project leads to the creation of theory. The new knowledge or theory that is created is of two kinds. Firstly, there is a theory that links the managerial style of information security managers with the observed phenomena of end-user non-compliance with information security policies and controls in the organization. This theory

has a descriptive and explanatory nature (following Ven de Ven & Johnson, 2006) – it answers the 'what' and 'how' questions regarding the observed phenomena; it also establishes the managerial style of information security managers as the explanation behind the observed phenomena. Secondly, the research project leads to the creation of a theory that has a control purpose (following Ven de Ven & Johnson, 2006) – this latter theory seeks to provide an effective intervention or a solution to resolve the problems associated with the observed phenomena of end-user non-compliance. To create these theories, this research project has adopted a critical-interpretivist stance; it has followed the cycle of deductive-inductive theory building and has used argumentation to move from description to explanation to control of the observed phenomena. This section provides a brief overview of research paradigms, theory and theory building and argumentation. The next section describes the research process followed in this study.

1.5.1 Research paradigms

Saunders, Thornhill and Lewis (2003) concur with Guba and Lincoln (1994) that the research paradigm is of primary importance when embarking on any research. In the 'research onion' of Saunders et al. (2003), the 'research paradigm' or 'research philosophy' forms the outermost layer. In a similar manner, the importance of the 'research paradigm' is underscored by the 'research pyramid' of Jonker and Pennink (2010), wherein the research paradigm forms the top-most layer of the pyramid. Thus, either as part of the 'research onion' or the 'research pyramid', the first question that needs to be considered is that of the research paradigm. A researcher needs to make certain definite decisions regarding the choice of paradigm before formulating other aspects of the research process. The following sub-sections discuss the importance of the research paradigm in more detail and provide a brief overview of the various possible paradigms available.

1.5.1.1 The importance of the research paradigm

Various authors have provided definitions for the concept 'paradigm'. These definitions underline the importance of the choice of research paradigm. Burrell and Morgan (1979) defined paradigm as *"very basic meta-theoretical assumptions that underwrite the frame of reference, mode of theorizing and modus operandi"* of the researcher. Further, paradigm *"is intended to emphasize the commonality of perspective which binds the work of a group of theorists"* (Burrell & Morgan, 1979). Hirschheim and Klein (1989) defined a paradigm as, *"the most fundamental set of assumptions adopted by a professional community that allows its members to share similar perceptions and engage in commonly shared practices"*. Hirschheim and Klein (1989) follow

Burrell and Morgan (1979) and state that a paradigm *"consists of assumptions about knowledge and how to acquire it, and about the physical and social world"*. Guba and Lincoln (1994) defined the paradigm as *"the basic belief system and worldview that guides the investigator, not only in choices of method but in ontologically and epistemologically fundamental ways"*. Given (2008, pp. 591) defines a paradigm as *"a set of assumptions and perceptual orientations shared by members of a research community"*. Jonker and Pennink (2010) state that a paradigm may be considered as *"a coherent whole of assumptions, premises and self-evident facts as shared by a certain group of professionals"*. According to these definitions, a paradigm essentially consists of assumptions. These assumptions are meta-theoretical in nature. The assumptions also influence the choice of methods to be utilized in the research process at a later stage. Furthermore, the assumptions are shared by all the followers of the paradigm.

Apart from influencing the choice of methods, paradigms play an important role in setting the boundaries of the research process. Burrell and Morgan (1979) stated that the paradigm establishes the range of 'intellectual territory'. According to Chua (1986), the *"constellation of beliefs, values and techniques"* delimit the boundaries of 'worthwhile problems' and 'acceptable scientific evidence'. Likewise, Guba and Lincoln (1994) stated that the paradigm defines *"what falls within and outside the limits of legitimate inquiry"*. Chua (1986) stated that a paradigm consists of assumptions regarding the domains of knowledge, the empirical phenomena being studied and the relationship between knowledge and the phenomena – each of these assumptions could have different values under different paradigms – and given these values, the set of assumptions leads to a particular way of *"seeing and researching the world"*.

Rowan (1973) stated that research can unravel answers only to those questions that are asked (Orlikowski & Baroudi, 1991). The choice of research paradigm or philosophy is, therefore, extremely important. It not only establishes the space of methodological tools and techniques, but more importantly, it sets up the space of questions that can be asked and the answers that can be obtained through the research process. The following sub-section provides a brief overview of the various research paradigms.

1.5.1.2 A variety of research paradigms

Burrell and Morgan (1979) and Chua (1986) identified different research paradigms, based on a set of underlying, meta-theoretical assumptions. According to Burrell and Morgan (1979), the assumptions lie along the dimensions of: subjective-objective dimension (consisting of issues pertaining to ontology, epistemology, human nature and methodology) and the nature of society dimension (consisting of radical change and regulation). In the model of Chua (1986), the assumptions are classified along three dimensions. These three dimensions are: beliefs about knowledge (concerned with the epistemology of knowledge and methodological issues), beliefs

about physical and social reality (concerned with ontological issues, issues of human intention and rationality and societal order and conflict) and the relationship between theory and practice.

The assumptions underlying the paradigms of Burrell and Morgan (1979) and Chua (1986) are quite similar (Chua, 1986). These assumptions play an important role as changing the set of assumptions *"gives us a new purpose for theorizing, different problems to research, and an alternative standard to evaluate the validity of research evidence"* (Chua, 1986). Without going into the details of these assumptions, the discussion below provides a brief overview of the three main streams of research paradigms, namely, the functionalist or positivist, interpretivist and critical research paradigms, as identified by Burrell and Morgan (1979), Chua (1986) and Orlikowski and Baroudi (1991).

The functionalist or positivist paradigm. According to Burrell and Morgan (1979), the functionalist or positivist paradigm is characterized by a realist, positivist, determinist and nomothetic approach. The functionalist or positivist approach is a search for generalisable principles or universal laws leading to a close coupling between explanation, prediction and technical control. In this approach, people are considered as *"passive entities that may be passively described in objective ways"*, and not as *"makers of their social reality"* (Chua, 1986). People are seen though a 'deterministic' lens, as responding mechanically to situations in their environment (Burrell & Morgan, 1979). The functionalist or positivist approach is problem-oriented in nature and attempts to provide practical solutions to practical problems (Burrell & Morgan, 1979). Orlikowski and Baroudi (1991) stated that the relationship between theory and practice in the functionalist or positivist paradigm is of a technical nature. In spite of its strengths in the conduct of scientific research, the functionalist or positivist paradigm suffers from several weaknesses, particularly in its conception of people. This paradigm largely ignores the historical and contextual factors that influence the behaviour of people, and thus runs the hazard of revealing only an incomplete picture of the phenomena under study (Orlikowski & Baroudi, 1991). In the context of information systems research, Orlikowski and Baroudi (1991) rejected the functionalist or positivist paradigm as yielding useful results; in their assessment, this paradigm is suitable only for phenomena where the relationships underlying the phenomena are determinate and one-dimensionally causal. This is just not the case with the phenomena of interaction between people and information technology.

The interpretivist paradigm. According to Burrell and Morgan (1979), the interpretivist paradigm tends towards a nominalist, anti-positivist, voluntarist and ideographic approach. The focus of this paradigm is on understanding the *"world as it is"* and the *"fundamental nature of the social world"* (Burrell & Morgan, 1979) – the interpretivist paradigm seeks to understand a specific context, unlike the functionalist or positivist paradigm, which tends towards providing a practical solution through generalisation and universal laws. According to Orlikowski and Baroudi (1991), following Gibbons (1987), the interpretivist paradigm seeks to *"explain why*

people act the way they do". Chua (1986) stated that interpretivist research has no technical application and it does not seek to control empirical phenomena; rather, the aim of interpretivist-oriented research is to enhance the understanding of the meanings of people's actions. Saunders et al. (2003) state that in the interpretive paradigm, the researcher takes an 'empathetic stance', and attempts to understand the phenomena from the perspective of the people involved. The focus is on people, unlike the functionalist or positivist paradigm where the focus is on objects (Saunders et al., 2003). The interpretive paradigm views people through the lens of 'voluntarism' which ascribes a much more active role to people *"where man is regarded as the creator of his environment, the controller as opposed to the controlled, the master rather than the marionette"* (Burrell & Morgan, 1979). As a research paradigm, Orlikowski and Baroudi (1991) state that interpretivism has advantages over functionalism or positivism in that this paradigm unravels greater understanding of the factors underlying the behaviours of people. Where the functionalist or positivist paradigm lead to *"artificial models of human action"* (Chua, 1986), the interpretivist paradigm leads to the creation of a more realistic understanding of people's behaviour. According to Orlikowski and Baroudi (1991), interpretivism is particularly suited to the study of phenomena involving people's behaviours and the meanings behind those behaviours.

The critical paradigm. The critical paradigm involves the study of social systems with the intention of unravelling their inherent contradictions and conflicts (Orlikowski & Baroudi, 1991). According to this paradigm, people exist in a state of 'unfulfilled potentiality' – everything is defined by what it is and also by what it is not (Chua, 1986). The aim of critical researchers is to provide a remedy by creating an awareness and an understanding of the various forms of economic, political, social and cultural domination – and thereby, enabling people to realize their potential (Orlikowski & Baroudi, 1991). According to Orlikowski and Baroudi (1991), conflict is inherent in any organization in which there is a separation between labour and capital – this conflict may be hidden through *"role segmentation, ideological formulations, segregation of participants"* etc. Conflict arises from the managerial desire to control and the attempts of labor to overthrow the mechanisms of control (Orlikowski & Baroudi, 1991). In the context of information systems in organizations, conflicts and domination are studied in the realms of the issues of power, gender, the digital divide, information systems failure etc. (Niehaves & Stahl, 2006). Critical researchers hope to expose these structures of domination and help people overcome these *"oppressive social relations"* (Orlikowski & Baroudi, 1991). Just like the interpretivist researchers, the critical researchers too need to understand people and their behaviours; however, critical researchers believe that this is not sufficient and so they go further in order to understand the sources of such contradictions and conflicts.

This section has discussed the importance of the research paradigm in the research project – the choice of paradigm determines the way the researcher sees and investigates the world and its phenomena. The section has also discussed the three major research paradigms, namely, the

functionalist or positivist, the interpretivist and the critical research paradigms. Each has its own set of underlying assumptions, strengths, weaknesses and, more importantly, its own best-fit phenomena. The next section will carry this discussion forward and identify the research paradigm to be followed in this study.

1.5.2 Theory building

Gioia and Pitre (1990) defined theory building as *"the process or cycle by which such representations are generated, tested and refined"*. Lynham (2000) defines theory building as *"the ongoing process of producing, confirming, applying and adapting theory"* (Lynham, 2002). The theory building process has certain attributes – it is cyclic (Lynham, 2002; Schneberger, Pollard & Watson, 2009) and it utilizes certain paradigmatic assumptions (Gioia & Pitre, 1990). These attributes of theory building are discussed below.

Cyclical nature of theory building. According to Lynham (2002), there are two major strategies for theory building – the theory-to-research strategy and the research-to-theory strategy. The theory-to-research strategy is deductive in nature. In this strategy, researchers begin with a theory or explanation and then attempt to validate this theory through further enquiry or observations. The research-to-theory is inductive in nature. In this strategy, *"theory follows the data"* (Saunders et al., 2003). This strategy involves generating a theory based on patterns in observations of the phenomena under study. Schneberger et al. (2009) state that these approaches are combined in a cycle of research, analysis and learning. Lynham (2002) has provided a conceptualization of applied theory building consisting of a cycle of five phases: conceptual development, operationalisation, application, confirmation or disconfirmation and continuous refinement and development of the theory.

Paradigms in theory building. Gioia and Pitre (1990) explained how theory building proceeds in each of the four paradigms of Burrell and Morgan (1979). The paradigms were discussed in the previous sub-section; their implications for theory building are discussed here. In the functionalist paradigm, the focus is usually on theory refinement, rather than on new theory generation; further, the approach is deductive in nature. In the interpretivist paradigm, theory building proceeds through induction. The goal of interpretivist theory building is to *"describe and explain in order to diagnose and understand"*. In the critical paradigm, theory building is similar to interpretivism, except that the goal also involves change. The goal of radical-humanist theory building is to *"describe and critique in order to change"*. The goal of radical-structuralist theory-building is to *"identify sources of domination and persuade in order to guide revolutionary practices"*. Gioia and Pitre (1990) further stated that theory building should proceed in a manner compatible with the paradigmatic assumptions of the topic under study.

Theory building leads to the creation of theory or new knowledge. The discussion so far in this section has highlighted two different aspects of theory building, namely, the choice of research paradigm and the process of theory building. The next sub-section discusses argumentation and its role in reasoning about the theory, or new knowledge, that has resulted from theory building.

1.5.3 Argument and Argumentation

Govier (2010) defines an argument as *"a set of claims in which one or more of them – the premises – are put forward so as to offer reasons for another claim, the conclusion"* and further states that *"an argument is a reasoned attempt to justify a claim on the basis of other claims"* (Govier, 2010). Thus, an argument can be said to consist of premise(s) and a conclusion; the premises being intended to lead to the conclusion (IEP, 2003). It is the objective of the researcher to argue and establish the validity and soundness of his/her argument. This is done by using the process of argumentation. Argumentation is defined as, *"the action or process of reasoning systematically in support of an idea, action, or theory"* (Oxford Dictionaries, 2010). There are three modes of argumentation or reasoning, namely, the abductive, the deductive and the inductive (Given, 2008). An abductive argument seeks to provide a plausible explanation based on the premises (Given, 2008; IEP, 2006). A deductive argument holds that the premises guarantee the truth of the conclusion while in an inductive argument, the premises support the probable truth of the conclusion (Given, 2008; IEP, 2006). An alternative definition of deduction and induction are also available. Deduction may be defined as, *"reasoning from the general to specific"*, while induction may be defined as, *"reasoning from the specific to the general"* (IEP, 2003; Saunders et al., 2003).

Stephen E. Toulmin has developed a model of argumentation (Toulmin, 1958). This discussion of Toulmin's model of argumentation is based on the information provided by the *"Toulmin Project Home Page"* hosted by the University of Nebraska-Lincoln (UNL, 1998) and *"Toulmin's argument model"* hosted at ChangingMinds (ChangingMinds, 2002). In his model, Toulmin identified the layout of an argument (Figure 1.2).

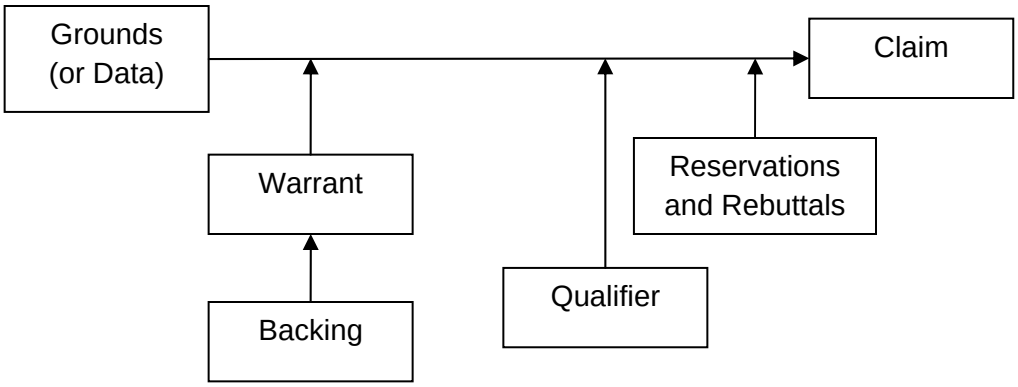


Figure 1.2: Toulmin's layout of argument (based on UNL, 1998)

In Toulmin's layout of an argument, the components making up an argument are 'claim', 'grounds' (or 'data'), 'warrant', 'backing', 'qualifier' and 'rebuttal' (or 'reservation'). The 'claim' is the conclusion that needs to be established based on the grounds (or data) that are the premises. The claim is the position advocated by the researcher and which the researcher wishes the audience to accept. The claim is the essence or the purpose behind the argument. The 'grounds' or data establish the 'truth' behind the claim. This consists of evidence, facts, data, information and the reasoning behind the claim (UNL, 1998; ChangingMinds, 2002). The grounds provide for a 'reasoned beginning' (UNL, 1998).

A 'warrant' serves the purpose of logically linking the grounds with the claim. Warrants answer the question, *"How did you arrive at the claim based on the grounds (or data) presented?"*; and represent the reasoning process that binds the grounds to the claim. Warrants may be based on logos, ethos or pathos – or values that are assumed to be shared with the listener (ChangingMinds, 2002). Warrants are supported by 'backing', which comprises the further data supporting the warrants. Backing enhances the credibility of the argument. A 'qualifier' indicates the strength of the argument – as discussed earlier, the strength varies from strong to weak, from 'guaranteed' (deductive), 'probable' (inductive) or 'plausible' (abductive). In Toulmin's layout, arguments are not universally true, and 'reservations' are the exceptions, limitations or counter-arguments to the claim; these reservations are countered through 'rebuttals'.

This section has provided a brief overview of the major components of the research process followed in this project, namely, the research paradigm, the theory building cycle and argumentation. The next section will discuss how these components have been combined in this research project.

1.6 Research approach and methodology

This research project seeks to identify a solution for a general problem faced by organizations, namely, how to improve present-day information security management so as to improve the effectiveness of information security in the organization through improved compliance of end-users. The research process of this project is as follows:

- Based upon the nature of the subject under study, namely, the end-users and information security management in the organization, the study adopts a critical-interpretivist stance as the paradigm choice.
- This study uses extant literature as the primary source of information and data for various aspects of the study.
- Theory building is achieved through the inductive-deductive cycle. Argumentation is used to establish the links and interconnections between the various concepts.
- The results of the research are validated through the presentation and publication of papers in various conferences and journals for peer review.

The research process will now be discussed further in greater detail.

1.6.1 The choice of paradigm

During the course of this study, the research has adopted a pragmatic approach, i.e. instead of being bound by a particular research paradigm, it has chosen whichever paradigm best suited the problem under study (Goles & Hirschheim, 2000; Saunders et al., 2003). There are essentially two entities being studied: end-users and information security management in the organization. For the study of end-users, the research sought to understand the varied reasons behind the non-compliance displayed by end-users. The research thus adopted an interpretivist stance towards the study of end-users as it sought to describe and explain in order to diagnose and understand the observed phenomena of end-user non-compliance. For the study of information security management, the research sought to understand the impact of information security management on the end-users. The research thus adopted a critical stance towards the study of information security management as it sought to identify the sources of domination and lead, thereby, to change in information security management practices. Thus, it may be said that this research adopts a critical-interpretivist approach (Niehaves & Stahl, 2006) by combining the elements of the interpretivist and critical research paradigms. Since research paradigms arise from a set of underlying assumptions, the assumptions necessitating the interpretivist and critical approach of this research are as follows:

- **The end-user of information security policies and controls.** This study takes an empathetic stance towards end-users. Typically, the end-user in information security is treated as the enemy, from whom the information is to be protected, and who is often the source of threats to the security of information. This study discards this approach. It sees the end-user, essentially, as a friend and not as a foe, as someone who does not desire to compromise information security in the organization, and as someone whose behaviour is determined by a host of competing circumstances in the organization. In this study, the end-user, if given a choice, would rather undertake the assigned information security behaviours; however, the end-user often fails to comply because of various factors not under his/her control. Consequently, the end-user is not someone who needs to be controlled, but rather someone who needs to be supported in his/her efforts to both work in the organization and comply with information security policies and controls in the organization. Under these assumptions, an interpretivist approach is necessitated for the study of end-users as only this approach can examine the full range of technical and social factors that influence the behaviour of end-users.
- **Information security management and policies and controls in the organization.** This study takes a critical stance towards information security management and policies and controls in the organization. It is the assumption of this study that information security management often creates conflict for end-users in the organization, and that this conflict is the source of end-user non-compliance. The information security policies and controls are often designed without any due consideration of the needs and characteristics of end-users. End-users are caught between a 'rock and a hard place' – between doing their work in the organization and being productive, on the one hand, and complying with information security policies and controls, on the other hand. This conflict creates non-compliance. Information security management approaches this conflict reactively through trainings, rewards and sanctions. This study believes that if information security management adopts a proactive approach and information security policies and controls are in tune with the needs and characteristics of end-users in the organization, non-compliance can be arrested. Under these assumptions, a critical approach is necessitated for the study of information security management. The central idea is 'change'. The critical stance rejects the question, *"why do end-users indulge in non-compliance?"* Instead, the critical stance seeks to answer the question, *"what is it in the organization that causes end-users to exhibit non-compliance and how do we need to change it?"* The critical stance is necessitated in order to critique and evaluate information security management.

1.6.2 The sources of data

This research project has primarily relied upon extant literature as its source of data for analysis and theory building. The works from diverse fields and from respected authorities have been considered:

- Literature related to the human aspect of information security and the information security behaviours of people, information security culture and information security awareness.
- Literature related to thinking under risk, human error, loyalty and commitment and the psychology of human behaviour.
- Literature related to general management and the influence of managerial style upon the behaviour of people in organizations.
- Literature related to information security management in organizations and its nature.
- Literature related to service management.
- Literature related to service branding, service encounters and service culture.

These sources represent a diversity of relevant disciplines and care was taken to consider both old and recent papers. Furthermore, care was taken to ensure that respected authorities in the various disciplines were considered.

1.6.3 Theory building and Argumentation

The research project began by first exploring and understanding the information security behaviours of end-users, i.e. the behaviours end-users demonstrate, as they interact with information security policies and controls in the organization. This phase was exploratory, as it sought to explore and gain an understanding of the diverse factors that influence human behaviour, in general, and the information security behaviours of end-users, in particular. This phase was based on an inductive approach and established some of the basic assumptions of this research regarding human nature and the management of people. Subsequently, the research project undertook a more focused approach that converged upon establishing managerial style as a determinant of the behaviour of people in organizations. This is a generalized result that was transferred to the domain of information security management. The research project then undertook a deductive approach to validate the link between the nature of information security management and its influence upon end-user non-compliance. This inductive-deductive cycle continued its iterations until it was firmly established that the present-day bureaucratic and technology-focused managerial style of information security managers is a primary cause of end-user non-compliance and that this non-compliance can be remediated through adopting an end-user centric approach to information security management. The research project then undertook a

focused literature study to identify such a managerial style from the domain of general management. This literature study culminated in identifying service management as the desired approach for managing information security in the organization. The research project subsequently undertook a detailed study of service management including service characteristics, service management principles, service branding, service encounters, service culture etc. in order to formulate Information Security Service Management (ISSM) as the service management approach to information security management in the organization.

Throughout the research process, argumentation has been used as the tool for reasoning and establishing the links between various concepts. The detailed argumentation is presented in section 6.3. For the purpose of this section, it suffices to say that two arguments were framed establishing the following two claims:

- C1: The present-day approach to information security management (ISM) alienates end-users and fails to achieve the commitment and loyalty of end-users to information security in the organization; it creates a digital divide between end-users and information security managers and, thereby, fails to obtain end-users' compliance to information security policies and controls in the organization;
- C2: Information Security Service Management (ISSM) will overcome the short-comings of the present-day approach to ISM and will lead to improved compliance of end-users with information security policies and controls in the organization.

The theory building process culminated with the validation of the above claims and the formulation of the principles behind ISSM and guidance for its implementation in organizations.

1.6.4 Validation of the results

This research project offers organizations an improved approach for information security management. This improved approach is Information Security Service Management (ISSM) which is based upon service management. The results of the research project are two-fold:

- Conceptual: the conceptual results consist of the CARE principles and the ISSM approach (Chapter 6).
- Applied: the applied results are in the form of guidance for the implementation of ISSM in organization and consists of the ISSMCube (Chapter 6) and the three components of ISSM, namely, Information Security Service Branding (Chapter 7), Information Security Service Support (Chapter 8) and Information Security Service Culture (Chapter 9).

This research project has adopted peer review as the method for the validation of its results. Multiple papers have been published or are in an advanced stage of acceptance and publication

covering the different aspects of ISSM. The papers cover both the conceptual and applied results of this research. The papers are as follows:

- Rastogi, R., & von Solms, R. (2005). Information Security Governance – a re-definition.
- Rastogi, R., & von Solms, R. (2009). A service-oriented approach to information security management.
- Three papers have been prepared and submitted at various conferences and journals. These are:
  - "Information Security Service Branding – beyond information security awareness". This paper has been accepted for presentation at the 9th International Conference on Education and Information Systems, Technologies and Applications: EISTA 2011, USA.
  - "Information Security Service Support – helping end-users cope with security". This paper has been accepted for publication by the Journal of Computer Technology and Application.
  - "Information Security Service Culture – information security for end-users". This paper has been submitted to the Human Aspects in Information Security and Assurance (HAISA 2011) conference.

This concludes the discussion on the research process to be followed for this project. The following section provides the chapter road map.

1.7 Chapter road map

This thesis consists of ten chapters. These chapters are divided into four broad sections, namely, the Introduction, the Literature Study, the Solution and the Conclusion. Section I, "Introduction" consists of Chapter 1. Chapter 1 includes the identification of the problem area, the problem statement and the research objectives that govern this thesis. Chapter 1 also includes an overview of the research approach and the methodology followed by the research.

Section II, "Literature Study" consists of Chapters 2 to 5 which respectively address the following secondary objectives:

- To understand the information security behaviours of end-users and the reasons behind non-compliance.
- To understand the link between managerial styles and the behaviours of employees in the organization.
- To study the dominant managerial style inherent in present-day ISM and how it leads to the end-user crisis.
- To identify a management approach that has the potential to resolve the end-user crisis.

Chapter 2 discusses the actual information security behaviours exhibited by end-users as they interact with information security policies and controls in the organization. The chapter also seeks to provide an insight into these behaviours in light of studies of human behaviour in such areas as thinking under risk, human error, loyalty and commitment and behavioural psychology. Chapter 3 discusses how the behaviour of employees in the organization is linked to the consequential managerial style followed in the organization. Since managerial style is determined by managerial assumptions on human nature, this chapter establishes the link that employee behaviour is determined, to a large extent, by the managerial style in the organization. Chapter 4 highlights the managerial assumptions of present-day ISM in the organization. It brings forth the bureaucratic nature of present-day ISM. Based on the results from Chapters 2 and 3, this chapter inductively establishes the link between the end-user crisis and present-day ISM. Chapter 5 presents an overview of the concept of service management. The chapter also discusses how this concept has been applied to internal services and IT management in organizations.

Section III, "Solution" consists of Chapters 6 to 9. These chapters address the following secondary objective:

- To apply this identified approach to formulate an alternative approach to ISM and to identify the components of this approach so it can be applied in organizations for the management of information security.

Chapter 6 provides an overview of Information Security Service Management (ISSM). ISSM is based on the concept of service management and is aimed at resolving the end-user crisis of present-day ISM. Chapter 6 also establishes the CARE principles for achieving end-user centric ISM.

Chapters 7, 8 and 9 provide further details on the components of ISSM, namely, Information Security Service Support (ISSS), Information Security Service Branding (ISSB) and Information Security Service Culture (ISSC). ISSS, ISSB and ISSC together allow ISSM to implement the CARE principles. The guidance provided in these chapters will be helpful for organizations in implementing ISSM.

Section IV, "Conclusion" comprises Chapter 10. Chapter 10 provides a cumulative conclusion to this thesis. It evaluates the research to determine whether the research objectives have been met. The chapter also includes a discussion for possible further research.

The chapter road map, as discussed above, is shown in Figure 1.2 and illustrates the logical order of the research in this thesis.

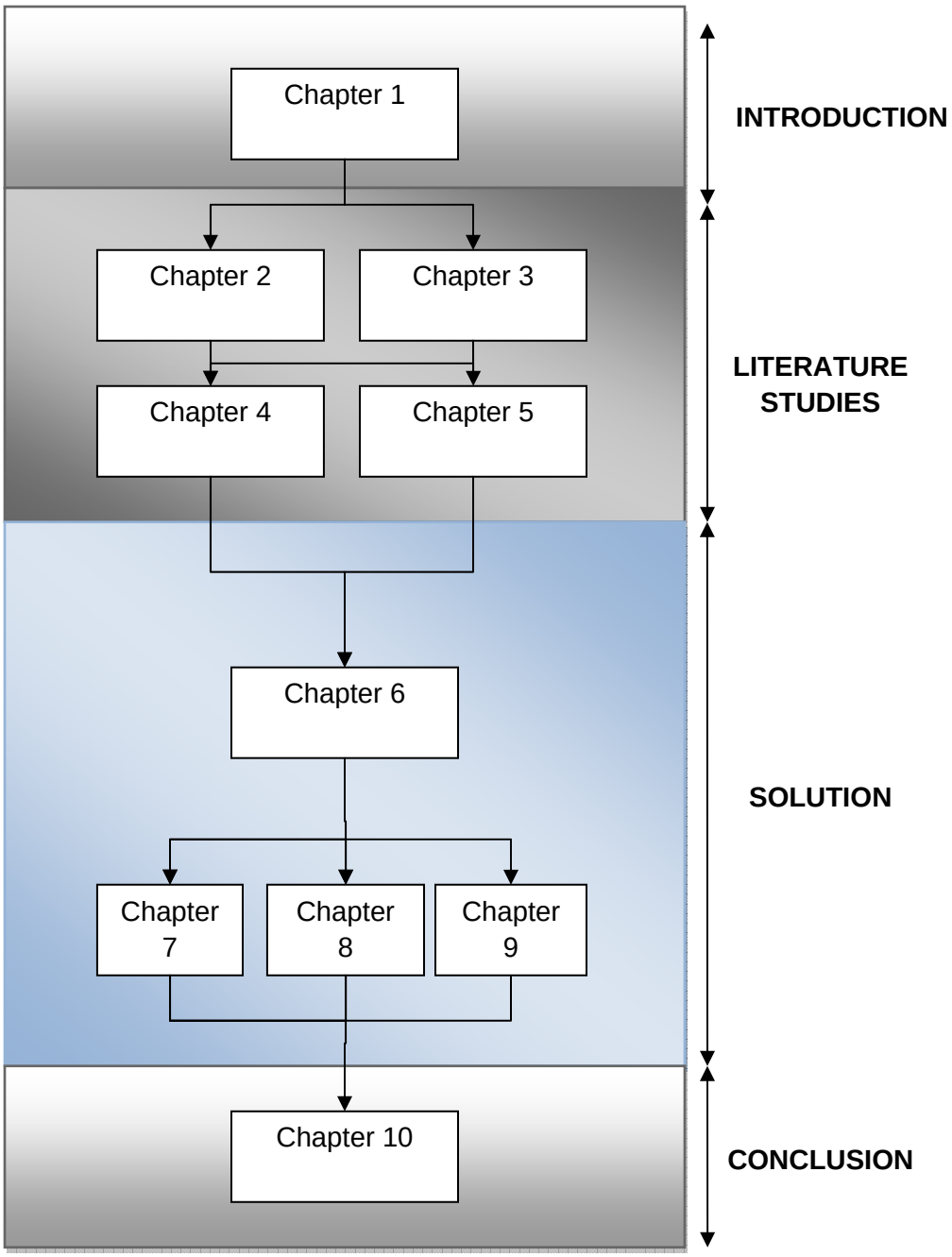
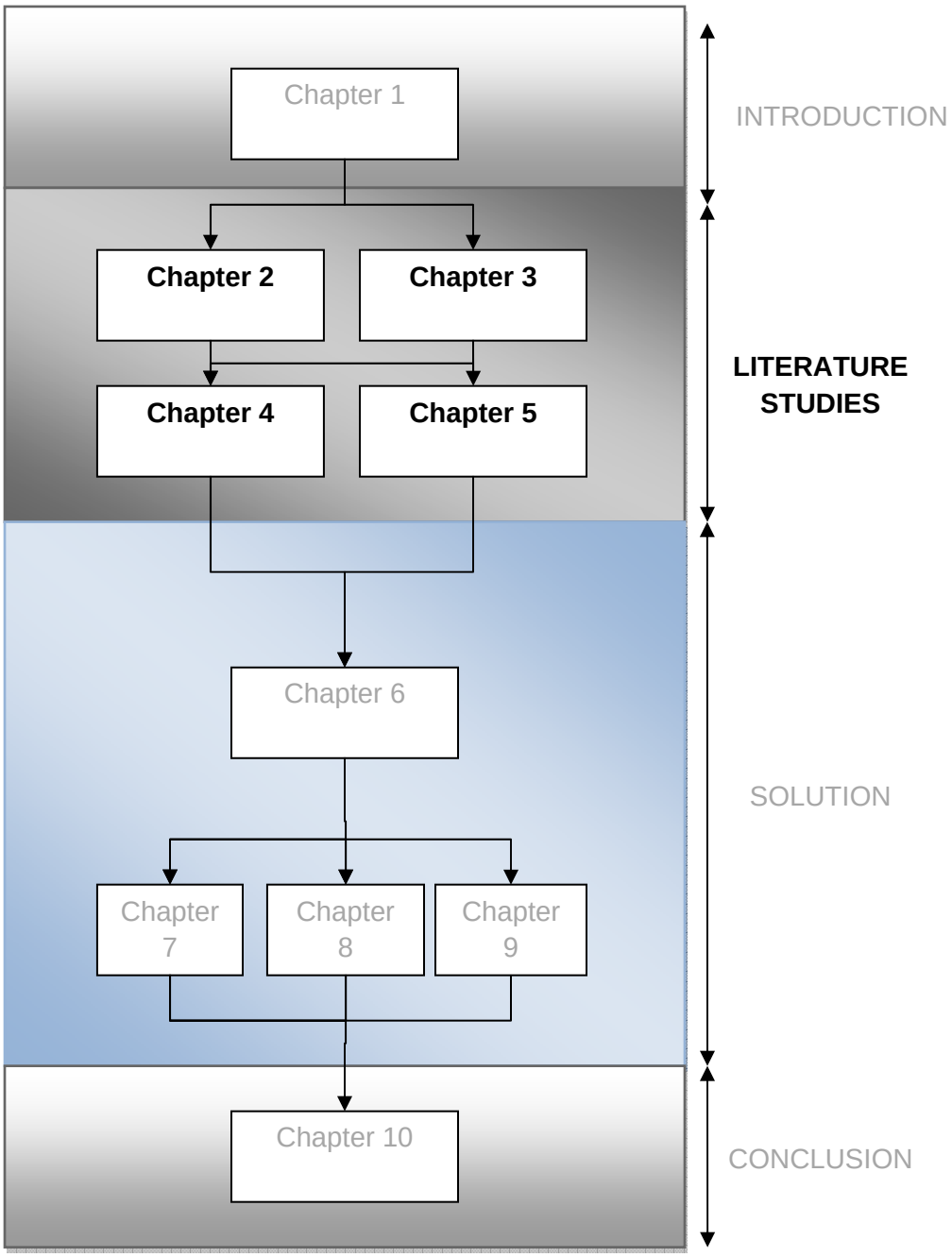


Figure 1.2: Chapter road map

SECTION II

LITERATURE STUDIES



CHAPTER 2

Understanding the information security behaviour of end-users

"… people's responses often deviate from the performance considered normative on many reasoning tasks. For example, people assess probabilities incorrectly, they display confirmation bias, they test hypotheses inefficiently, they violate the axioms of utility theory, they do not properly calibrate degrees of belief, they overproject their own opinions onto others, they display illogical framing effects, they uneconomically honour sunk costs, they allow prior knowledge to become implicated in deductive reasoning, and they display numerous other information processing biases".

- Stanovich and West (2003)

2.1 Introduction

Since long, the operations of most organizations have grown highly dependent on their information and associated information systems (Bakos & Treacy, 1986; Clemens & Row, 1991; Gurbaxani & Whang, 1991; Porter & Millar, 1985). These are assets without which the organizations may not succeed, and indeed, may fail to survive (Peppard, 2003). Hence, organizations deploy considerable resources in establishing an information security infrastructure for the protection of their information assets. This infrastructure normally consists of policies, controls, technologies, administrative rules, processes and structures.

An organization operates through the actions of its people (Mintzberg, 1980). These people are authorized to actively use the information and associated information systems in the organization. Consequently, they also have to interact with the information security infrastructure in the organization. These people are the end-users of the information, information systems and information security infrastructure. As end-users use the information and information systems, they interact with the information security infrastructure. The information security infrastructure is built on the assumption that end-users will be able to understand,

interpret and use the information security policies and controls appropriately. However, this is not always the case. End-users exhibit a wide range of behaviours and their actual behaviour sometimes deviates from the expected behaviour (Stanovich & West, 2003; Furnell, 2010). This creates further problems for the organization. The effectiveness of the information security infrastructure is diminished and the organization may be exposed to further information security risks.

This chapter provides an overview of the typical information security behaviours displayed by end-users and attempts to understand the reasons behind these behaviours, particularly non-compliant behaviours. The next section comprises an overview of information security behaviours of end-users. The subsequent section attempts to understand these behaviours in the light of similar attempts in other streams of research such as 'thinking under risk', 'human error', 'loyalty and commitment' and 'behavioural psychology'.

2.2 Information security behaviours of end-users

When end-users use information and information systems during the discharge of their day-to-day activities in the organization, they come across information security tasks. With regard to these information security tasks, end-users display a range of information security behaviours – sometimes they fail to initiate the task; sometimes they fail to complete the task successfully; at other times they may be able to complete the task successfully. Stanton et al. (2003) define such behaviours as 'behavioural information security' consisting of *"complexes of human action that influence the availability, confidentiality and integrity of information systems"*. This end-user behaviour is critical to the success of information security efforts in the organization (Furnell & Thomson, 2009; Herath & Rao, 2009; Mauwa & Von Solms, 2007; Schneier, 2000; Thomson & Von Solms, 2006; Whitten & Tygar, 1999). Siponen (2000) states that even the best of security technologies lose their effectiveness if not properly used by end-users. End-users have both strengths and weaknesses in relation to information security tasks. Albrechtsen and Hovden (2009) characterize end-users as having the *"Janus face"* – i.e. end-users are a threat as well as a resource for information security. They are recognized as the *"human firewall"* (Wohnlich, 2006), but they are also maligned as the *"weakest link"* (Lineberry, 2007). Gonzalez and Sawicka (2002) call the end-users the *"Achilles heel of information security"*. In this backdrop of conflicting views of end-users, this section attempts to understand the wide range of information security behaviours, particularly non-compliant behaviours, exhibited by end-users as they interact with the information security infrastructure in the organization.

When faced with an information security task, end-users can be said to go through three stages in order to be able to undertake and complete the task, namely, knowledge or awareness regarding the task, intention or attitude towards the task, and lastly, skill to undertake and complete the task

successfully. These stages can be understood as follows. Firstly, the end-users need to be aware or have knowledge about the existence of the information security task and their responsibility regarding the task. Secondly, end-users have a choice – either to undertake the task or to bypass the task. This choice is determined by their intention or attitude towards the information security task. Thirdly, having decided to undertake the task, end-users may or may not be able to complete the task successfully. The awareness, intention and skill stages are used below to structure the discussion of the information security behaviours depicted by end-users.

2.2.1 The awareness stage

In the first stage, end-users need to be aware or to be knowledgeable about the information security concerns of the organization, and the existence of its information security policies and controls. The end-users need to be aware of their own role in the protection of information and how to behave in order to fulfill this role (Du Plessis & Von Solms, 2002). In the absence of this awareness, end-users may not undertake an information security task simply because of the lack of awareness; or end-users may misunderstand or misinterpret security guidance. Consequently, *"even an adequate security mechanism may become inadequate"* (Siponen, 2001). For example, Sasse, Brostoff and Weirich (2001) state that end-users sometimes underestimate the value of the information they work with and, therefore, wrongly believe that this information may not be useful to an intruder, or that no damage could be done to them or their organization if their privileged access were to be compromised. Erroneous action, or inaction, on the part of end-users might lead to a compromise of the information assets of the organization.

For creating awareness, organizations conduct awareness and training campaigns for their end-users. Organizations also document their information security policies and controls and disseminate these to their end-users. However, both these measures, aimed at improving end-user awareness and behaviour, remain ineffective and do not yield the expected dividends. Firstly, many organizations do not pay sufficient attention to the importance of awareness and the knowledge of end-users and consequently do not conduct regular training and awareness campaigns (Du Plessis & Von Solms, 2002; Mauwa & Von Solms, 2007; Albrechtsen & Hovden, 2009). Secondly, end-users continue to ignore the training and awareness campaigns and the information security documents (Albrechtsen, 2007; Albrechtsen & Hovden, 2009). End-users may regularly participate in the awareness campaigns, but they miss the message. They experience the campaign as one-way expert communication and, though, they may remember the campaign, they do not remember the content (Albrechtsen, 2007; Albrechtsen & Hovden, 2009). A similar fate befalls the effect of documentation. According to Albrechtsen (2007), documentation fails for the following reasons: lack of time to read the documents, lack of communication on the whereabouts of the documents, lack of incentives for studying the documents and lack of knowledge for understanding the instructions (Albrechtsen, 2007). End-

users may be aware of the existence of the policy documents, but they do not know the content, and seldom make any effort to read the documents. Even if the end-users attempt to read the documents, the technical- or security-oriented terminology discourages them (Furnell et al., 2006).

2.2.2 The intention stage

After crossing the hurdle of awareness or knowledge about the information security task, the end-user enters the second stage. In the second stage, the end-user is aware and knowledgeable about the information security task to be performed. The end-user now has a choice – either to undertake the task or to bypass it; this choice is shaped by the intention of the end-user or his/her attitude towards information security (Beautement, Sasse & Wonham, 2008). End-users are known to often bypass the information security task (Adams & Sasse, 1999; Dhillon, 2001b; Dourish et al., 2004). This deliberate act happens under the influence of personal and organizational factors. According to Beautement and Sasse (2009), the reasons for not complying include the negative effect of information security behaviours on personal and organizational productivity, the mis-perceived absence of risks and the culture of non-compliance pervasive in the organization. End-users see the information security task as an obstacle in the completion of their primary task which is completing the work at hand (Desouza & Vanapalli, 2005; Post & Kagan, 2007). The completion of the primary task is prioritized ahead of the information security task. The end-user may even feel that there is a mismatch between the actual work practice and the information security controls and policies. A conflict arises between the end-users desire to complete the primary work task and the restriction imposed by the information security policies and controls. Furthermore, if the task is perceived as difficult or requiring significant effort, then the task is perceived as an inconvenience, and ignored (Beautement & Sasse, 2009). As an example, one may consider the case of the use of USB sticks in the organization. An organization may severely restrict the use of USB sticks on account of their potential for misuse. This creates a disruption in the usual day-to-day work-life of end-users. The crisis may be aggravated by the lack of alternative mechanisms. Consequently, the convenience offered by these devices, and the consequent productivity gains, may prompt end-users to continue using them. In this situation, end-users may continue bypassing the policy for the following reasons: not using these devices may lead to a failure in completing the primary work task; secure, alternative mechanisms are not available in the organization; and finally, it may be a common, accepted practice amongst the group. Policies in direct conflict with the needs and practices of end-users will not promote information security, and may, in fact, lead to apathy towards it (Adams & Sasse, 1999; Whitten & Tygar, 1999). In certain circumstances, information security policies and controls may put end-users in conflict with their colleagues. Typically, organizations prohibit the sharing of passwords. However, end-users are known to violate this policy by sharing passwords with their colleagues. An end-user may feel uneasy about not sharing her

password as this might vitiate their relationship with colleagues (Sasse, Brostoff & Weirich, 2001). End-users may also feel that information security is not their job and that it is the job of the organization, and its information security staff, to take care of information security concerns (Albrechtsen, 2007). In the midst of all this, end-users continue to indulge in opportunistic behaviour, and side-step security policies and controls, exhibiting low levels of commitment to information security.

2.2.3 The skill stage

In the skill stage, the end-user has crossed the earlier hurdles of awareness and intention. In this stage, the end-user is aware or knowledgeable about the information security task and has also decided to undertake the task. The end-user may be able to complete the task successfully, or may fail. The successful completion of the task depends upon the skill of the end-user and the usability of the policy or control. At this stage, end-users face problems as they may have inadequate knowledge and skills needed to complete the information security task successfully. Or, the technical controls may have poor usability, thereby, reducing the effectiveness of the end-user's efforts. The problem of the usability and psychological acceptability of security policies and control has been understood for many years (Saltzer & Schroeder, 1975; Bishop, 2003). Ease of use of policies and controls has been seen to be of great importance. However, this aspect has been ignored in information security (Zurko & Simon, 1996) and information security policies and controls continue to be difficult for end-users to negotiate and comply with (Schultz et al., 2001; Furnell, 2010). According to Schultz et al. (2001), poor usability results in end-user resistance manifested as passive resistance, negative verbal behaviour, reluctance to perform tasks, failure to pay sustained attention to tasks, actions that cause damage to system components etc. Furnell et al. (2006) state that difficult-to-use policies and controls are underutilized by end-users and the *"usability gap translates into a usage gap"*. Furthermore, difficult-to-use policies and controls increase the chances of errors by end-users. The easier a policy or control is for the end-user to use, the more likely it will be for the end-user to undertake the task and to complete it successfully (Johnston, Eloff & Labuschagne, 2003). Adams and Sasse (1999) have discussed the use of passwords from the perspective of their usability. In their analysis, effective password usage is associated with factors such as 'multiple passwords', 'password content', 'perceived compatibility with work practices' and 'users' perceptions of organizational security and information sensitivity'. Adams and Sasse (1999) further argue that the consideration of passwords solely from a technical perspective, and ignoring the usability perspective, have reduced the effectiveness of the control. This ineffectiveness arising from the neglect of usability issues and human factors is reflected in the continued use of weak passwords by end-users (Imperva, 2010). Adams and Sasse (1999) conclude that the underlying difficulties associated with the use of passwords force end-users to exhibit non-compliance and even to *"circumvent the whole procedure"*. Furnell and Thomson (2009) describe 'security fatigue' as

one of the main reasons for end-user non-compliance where the fatigue potential of a policy or control is characterized by the levels of effort, difficulty and importance associated with the policy or control.

The above discussion has highlighted two critical aspects of information security in organizations. The first critical aspect is regarding the role of end-users. The effectiveness of information security policies and controls in the organization depends to a large extent upon secure actions by end-users. However, while end-users often complete their information security tasks, they are just as often guilty of improper behaviours leading to information security breaches in the organization. Hence, end-users are *"Janus-faced"* and may be characterized as both threats and resources, as firewall and weak link. The second critical aspect relates to the causes behind the insecure behaviours of end-users. When faced with an information security task, end-users may be said to pass through three stages, namely, awareness, intention and skill. At each stage, end-users face problems that can potentially make them deviate from the correct path. These problems are sometimes individual, but mostly can be traced to organizational or systemic factors and hence they are beyond the control of the end-users. Furnell (2010) terms these problems as 'hurdles' and states that they are of the following kinds: perception failings, priority or responsibility failings and capability or usability failings. Furnell (2010) further states that all these hurdles must be recognized and addressed in dealing effectively with the issues related to the non-compliance of end-users.

This section has discussed the information security behaviours, particularly the non-compliance, of end-users in the organization. The next section and its sub-sections will discuss studies of human behaviour in other streams of research in an attempt to understand the reasons behind the non-compliance of end-users in the organization.

2.3 Understanding the behaviour of humans and end-users

This section provides a brief overview of various theories in order to understand and explain the behaviour of humans in general, and end-users, in particular, in the context of information security. The theories are presented as follows:

- Thinking under risk – information security inherently involves risk, and therefore end-users are often faced with making a trade-off between the use of information and risk; this trade-off can be understood from the perspective of 'thinking under risk';
- Human error from the safety domain – when end-users interact with information security policies and controls, they are liable to commit errors, mistakes and violations; studies of human error in the safety domain can be used to understand end-user error in information security;

- Loyalty and commitment – loyalty and commitment bind people to a course of action; repeated compliance and completion of information security behaviours of end-users can be understood from the perspective of loyalty and commitment; and finally,
- Theory of Planned Behaviour (TPB) – human behaviour is driven by intentions, attitudes, beliefs and perceptions of control; this understanding helps in uncovering the factors that drive the information security behaviours of end-users in the context of information security in an organization.

2.3.1 Thinking under risk

Risk is an inherent aspect of information security. Information security deals with the management of risks to the information assets of an organization. Risk management involves trade-offs between the utilization and the protection of information assets. An asset that is not used will, in all likelihood, not pose any risks. However, such an asset will have no value for the organization. Value or use, risks and security are inter-linked. Information security emerges as a trade-off between use and risk (Schneier, 2008). Consequently, the effectiveness of information security hinges on the correctness of the trade-off.

According to Schneier (2008), various aspects of the security trade-off are related to: the severity of the risk, the probability of the risk, the magnitude of the costs, the effectiveness of countermeasures for mitigating the risk and how well disparate risks and costs can be compared. Schneier (2008) further goes on to say that people often get these trade-offs wrong, in fact people are *"hopelessly bad"* at these trade-offs. In the context of information security policies and controls in the organization, end-users have the potential to make mistakes while judging the value of the information assets, the existence of vulnerabilities and threats to the assets and themselves, the probability of attacks, and the effectiveness of policies and controls. End-users make seemingly irrational trade-offs. These irrational trade-offs have a psychological basis (Schneier, 2008).

In the idealized model of man, 'Homo Economicus' or the 'Economic Man' is seen as an intelligent and analytic entity who makes rational decisions regarding costs against benefits. This is the utility theory model in which feelings do not play any role. However, this is only an idealized model; and in reality, 'Homo Economicus' does not exist (Lambert, 2006). Instead, humans have only incomplete information and limited capability to process information. Humans rely on heuristics for decision-making under risk and uncertainty. Hillson and Murray-Webster (2005) define an heuristic as *"an approach to inferring a solution to a problem by reasoning from previous experience, when no relevant algorithm or dataset exists"*. Heuristics serve as a thumb-rule which may be used in place of elaborate information processing. Heuristics enable fast processing, however, they also introduce biases that can lead to incorrect evaluation of risks.

Heuristics operate in an automated manner at the sub-conscious level (Hillson & Murray-Webster, 2005).

The 'Prospect Theory', introduced by Kahneman and Tversky (1979), proposed the framing effect and the endowment effect. These effects influence the way people process risk-related information (Schneier, 2008). According to the framing effect, people make trade-offs depending on whether the associated risk information is presented as a gain or a loss. People's thinking is also affected by the immediacy or delay in gains and losses. The endowment effect ensures that people value more that which they have, when compared with that which they do not have. Various other heuristics exist such as the affect heuristic, the availability heuristic, representativeness heuristic, anchoring and adjustment heuristic and the confirmation trap heuristic (Hillson & Murray-Webster, 2005).

In the context of information security policies and controls in an organization, end-users are regularly faced with a security versus productivity trade-off. In one instance, the trade-off could involve non-compliance with the information security policies and controls versus completing the primary work task efficiently. In another instance, the trade-off could involve compliance with the information security policies and controls versus the inability to complete the primary work task efficiently. In this trade-off, the certainty and immediacy of gains of productivity win over the speculative losses from insecurity (Brostoff & Sasse, 2001). For example, an end-user may need to share a password with a colleague. In this situation, the gain of completing the primary work task is both certain and immediate. However, an information security breach, resulting from this sharing of a password, is an uncertain outcome.

As stated earlier, while heuristics enable people to make fast decisions under risk, heuristics may also lead to people having incorrect risk perceptions. These risk perceptions will differ from those of the organization and its information security managers. The risk perceptions of end-users will also be shaped by the transparency of information security measures and their effectiveness. The end-users do not see the defences, they do not see the risks materializing, and so they also fail to see the risk itself. This leads end-users to believe incorrectly that the risk does not exist, that they will not be the target of attack, that they do not have anything of value for an attacker, and that security policies and controls are an over-reaction. With this mind-set, end-users pay little heed to compliance with information security policies and controls and non-compliance seems more logical.

2.3.2 Human error

"Errare humanum est". To err is human. Error is a universal characteristic of human behaviour. When an individual executes a behaviour, two possibilities exist – either the behaviour is

completed successfully or there is failure. In any system, where human behaviour is crucial to successful operation, it becomes vital to understand failure so that its probability and impact can be mitigated.

Reason (1990) presented the GEMS (Generic Error-Modelling System) taxonomy for the classification of human error. In GEMS, human error is defined as *"a generic term to encompass all those occasions in which a planned sequence of mental or physical activities fails to achieve its intended outcome, and when these failures cannot be attributed to some chance agency"*. Reason (1990) proposed three major error types: skills-based slips and lapses, rule-based mistakes and knowledge-based mistakes. These error types are shown in Figure 2.1.

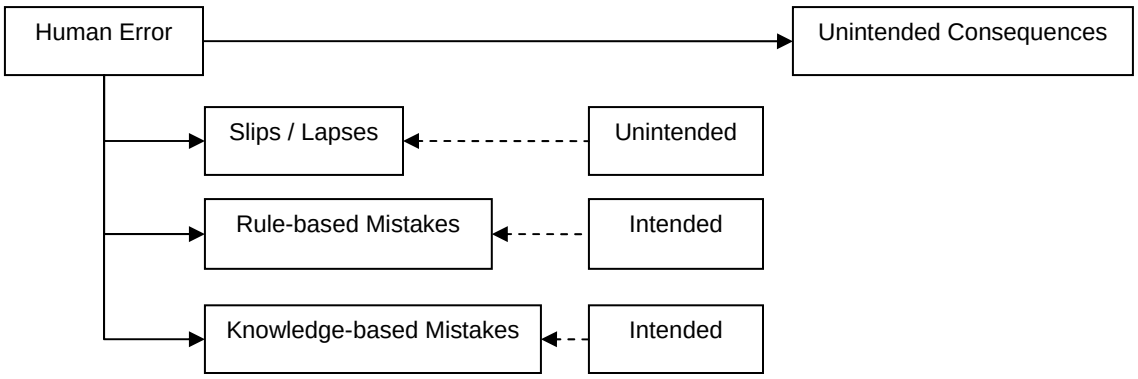


Figure 2.1: Human Errors (adapted from GEMS)

Slips and lapses occur at the skill-based level of execution of routine and familiar actions. Slips arise from failures of attention, while lapses arise from failures of memory. In both cases, the action (or lack of action) is unintended and leads to unintended results.

Mistakes are rule-based or knowledge-based and occur in the execution of problem-solving actions. These are intended actions that lead to unintended results. Rule-based mistakes arise from the misapplication of good rules or the application of bad rules. Knowledge-based mistakes arise from the lack of knowledge.

In the context of information security policies and controls in an organization, slips, lapses and mistakes occur when end-users interact with the policies and controls. A slip occurs when an end-user misses encrypting an email containing confidential information. A lapse occurs when an end-user forgets a password. A rule-based mistake occurs when an end-user creates a simple

password when the policy demanded a strong password. A knowledge-based mistake occurs when the end-user does not know how to create a strong password.

Slips, lapses and mistakes are inadvertent actions that have unintended consequences. But individuals, often, indulge in more deliberate acts that have the potential of unintended consequences. Such actions are called violations. Whittingham (2004) defines a violation as *"an intended action that has taken place in breach of a set of rules, whether or not these rules be written down, are implicit within the action, or have been developed as part of custom and practice"*. Whittingham (2004) further states that a violation meets the two conditions that the individual has prior knowledge of the rule being violated, and that the individual violates the rule willfully. In such a situation, the individual does not necessarily have any malicious intent and the violation may even be well-intended and meant for getting the job done. Often, organizations reward successful violations by terming them as initiatives (Hudson, Verschuur, Parker & Lawton, 2000; Santiago, 2007). According to Hudson et al. (2000), there are five types of violations, namely, unintentional, routine, situational, optimizing and exceptional violations. Unintentional violations are similar to errors. Routine violations are deviations that are practised so regularly that they have become common practice. Such violations become the accepted way of doing the work. Situational violations result from the factors present in the environment or workspace of the individual. Optimizing violations are related to job characteristics such as monotonous work or overly restrictive rules. Exceptional violations occur only in very unusual circumstances such as emergencies.

In the context of information security policies and controls in an organization, end-users often indulge in acts that are in violation of security policies and controls. These violations are not deliberate; they are not malicious and they are not intended to harm the organization. For example, sharing a password with a colleague is a violation, but it is intended to get the job done. This practice of sharing passwords may be accepted as regular practice amongst colleagues and so becomes a routine violation. Furthermore, even though the password policy forbids password sharing, password sharing may be seen as a positive act whereas resistance to password sharing may be seen as reflecting an unhealthy sense of distrust and paranoia.

Human errors and violations can be viewed in two ways: the person approach and the system approach (Reason, 2000). The approach depends on whether the focus of the analysis is on the human or on the system. In the words of Rasmussen (1997), *"the stop rule applied to identify 'root causes' depends on the aim of the analyst (to understand behaviour, to punish, or to improve system safety)"*. Consequently, the approach determines the philosophy of error management.

The person approach focuses on the errors and violations of people at the sharp end of operations. In this approach, the stop rule treats the human as the root cause of the failure and

blames the individual for aberrant mental processes such as carelessness, negligence, poor motivation etc. Consequently, countermeasures for mitigating failures are directed at reducing unwanted variability in human behaviour through education, rewards and penalties. The person approach blames individuals for all failures; and it, therefore, suffers from the inability to learn from failures. This approach impedes the development of safer systems.

The system approach looks beyond the people at the sharp end of operations and focuses on the blunt end. This approach treats people as inherently fallible and requires that defences be built to avert or mitigate failures. Errors and violations are seen as consequences rather than the cause of failure i.e. these originate not only from human nature, but also, from other organizational and systemic factors. Consequently, countermeasures for mitigating failures are directed at building sufficient defences in the system, and human variability is seen as a valuable resource.

Dekker (2002) identifies the 'old view' and the 'new view' of human error. These views closely match the person and system approaches of Reason (2000). In the 'old view', systems are inherently safe, failure is a result of human error and progress on safety can be made by protecting systems from unreliable humans. In the 'new view', safety is not inherent in systems, human error arises from factors within the system and progress on safety can only be made by understanding and influencing the connections between people, tools, tasks and the operating environment.

In the 'new view' or the system approach to human error, failure occurs when unsafe acts or active failures combine with underlying latent conditions. This is the *"Swiss cheese model of system accidents"* (Reason, 2000). The active failures are committed by people at the sharp end of the operation. The latent conditions are the 'resident pathogens' within the system that arise from decisions made by other people such as designers, developers, top-level managers, etc.

In the context of information security policies and controls in an organization, it is known that end-users undertake two kinds of unsafe acts – either they are unable to cope with the information security task, or they deliberately do not comply. End-users are the people at the sharp end of the operation and their unsafe acts are the active failures. The decisions made while formulating the information security policies and controls, while creating the work processes and procedures, while creating the IT systems, while rewarding performance etc. are the latent conditions.

According to the traditional view of information security, which matches the old view of human error or the person approach, the failure to undertake or complete the information security task is blamed on the end-user. This approach prevents the analysis from going deeper into understanding the underlying causes of end-user behaviour, and as a consequence, information security management keeps repeating its faulty decision-making with regard to information

security policies and controls. The cycle of faulty decision-making by management, unsafe acts by end-users and blaming end-users for failures completes a vicious circle.

Information security, as a discipline, needs to evolve its conception of the role of end-users in failures related to information security policies and controls in an organization. Information security must adopt the new view or the system approach towards unsafe acts by end-users. In the new view, end-users can be held responsible for only a few unsafe acts, most other unsafe acts can be traced back to earlier decisions in the life-time of information security policies and controls in the organization. Analysis according to this approach uncovers the latent conditions behind the unsafe acts. This understanding is used to improve the decision-making by management. Thus, a virtuous circle is created between decision-making that is responsive to end-user needs, improved compliance by end-users and a deeper understanding of end-user needs gained through a deeper analysis of failures.

2.3.3 Loyalty and commitment

"A committed person stays with the organization through thick and thin, puts in a full day and more, protects company assets, shares company's beliefs and goals" (Meyer & Allen, 1997).

As the above quote from Meyer and Allen (1997) shows, an organization would desire commitment from their employees. The committed employee, not only would complete his/her immediate responsibilities, but would do all that is required, and more. Such an employee would always work in the best interests of the organization, would always strive to protect the organization's assets and would have the same beliefs as the organization. In the context of information security policies and controls in an organization, it is understandable that commitment to information security is desirable in the end-users. End-users committed to information security in the organization will comply with the information security policies and controls and will exercise due diligence in using and protecting the organization's information assets. Since end-users frequently, do not comply with information security policies and controls in the organization, commitment to information security becomes a valuable construct.

Meyer and Herscovitch (2001) define commitment as:
"a force that binds an individual to a course of action of relevance to one or more targets. As such, commitment is distinguishable from exchange-based forms of motivation and from target-relevant attitudes, and can influence behaviour even in the absence of intrinsic motivation or positive attitudes."

Hence, commitment is the force of a psychological bond that causes an individual to continue a course of action. In the context of end-users, commitment to information security policies and

controls in the organization implies a psychological bond that causes end-users to persevere with information security tasks even though such perseverance might lead to personal inconvenience, inefficiency etc.

Meyer and Allen (1991) presented the 'Three-component' model of commitment of employees to their organization. According to this model, organizational commitment is a mind-set or psychological state concerning the employee's relationship with the organization and has implications for the decision to continue or discontinue membership in the organization. Commitment is seen as being composed of three components – affective, continuance and normative commitment (see Figure 2.2). Affective commitment refers to the employee's emotional attachment to, identification with, and involvement in the organization. Affective commitment reflects a desire to continue. Employees continue with the relationship because they want to continue. Continuance commitment refers to an awareness of the costs associated with discontinuing the relationship. Employees under continuance commitment, continue because they need to. Normative commitment reflects a feeling of obligation to continue the relationship. Employees under normative commitment, continue because they feel that they ought to.

In the three-component model, an employee can experience all three forms of commitment in varying degrees. The three components interact to influence behaviour. Meyer and Allen (1991) state that employees' willingness to contribute to organizational effectiveness will be influenced by the nature of the commitment they experience. Employees under affective commitment might be more likely to exert effort on behalf of the organization. Such employees exert more effort because they want to, rather than because they need to (continual commitment) or because they feel obligated to (normative commitment). Individuals under affective commitment may be more inclined to engage in behaviours that would benefit the organization than those under normative or continuance commitment. Morgan and Hunt (1994) stated that affective commitment is created when an individual internalizes, the values of the organization. Affective commitment reflects a sense of liking and of emotional attachment to the partnership. Calculative commitment (i.e. normative and continuance components) is based on gains and losses, rewards and punishments or plusses and minuses. Normative commitment is derived from a mind-set driven by the obligation to pursue a course of action; continuance commitment is derived from a mind-set driven by the rewards and costs associated with the particular course of action (Meyer & Herscovitch, 2001).

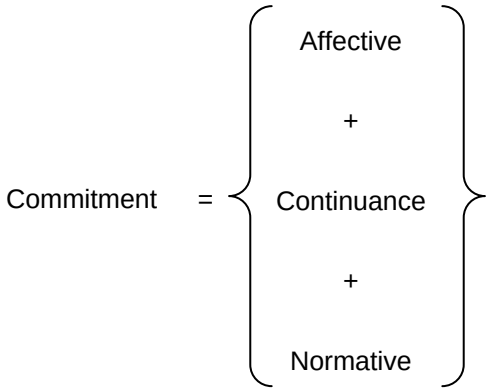


Figure 2.2: Three-component Model of Commitment (from Meyer and Allen, 1991)

Loyalty is a concept similar to commitment. Businesses often strive to obtain customer loyalty. Customer loyalty results in greater repeat purchases by existing customers. Further, loyal customers are less likely to switch to competitors solely because of price (Bowen & Shoemaker, 1998). In the context of information security policies and controls in an organization, end-user loyalty to information security signifies that end-users will regularly comply with their information security tasks. Loyal end-users will have a positive attitude towards the information security policies and controls in the organization, in spite of various difficulties and inconveniences.

Jacoby and Chestnut (1978) state that loyalty is represented by a set of six conditions:
"Loyalty is (1) the biased (i.e. nonrandom), (2) behavioural response (i.e. purchase), (3) expressed over time, (4) by some decision-making unit, (5) with respect to one or more alternative brands out of a set of brands, and (6) is a function of psychological (decision-making evaluative) processes."

Thus, a loyal individual exhibits the behavioural consistency of repeat purchase driven by psychological evaluative processes. Loyalty is a construct that combines both behavioural consistency and psychological commitment (see Figure 2.3). Behavioural consistency combined with psychological commitment leads to 'true loyalty', whereas behavioural consistency without psychological commitment leads to 'spurious loyalty' (Day, 1969). 'True loyalty' customers exhibit a strong psychological commitment and will exhibit repeat purchasing behaviour. Such customers are also unlikely to switch to competing brands. 'Spurious loyalty' customers exhibit a lack of psychological commitment to the brand. Though such customers may exhibit behavioural consistency, these customers are likely to shift to competing brands at the slightest opportunity.

This combined construct of loyalty is useful in not only understanding past behaviour, but also predicting future patronage (Evanschitzky, Iyer, Plassmann, Niessing, & Meffert, 2006).

In the context of information security policies and controls in an organization, end-users are influenced by a multitude of factors that prevent them from complying with the information security policies and controls. Influenced by these factors, end-users find that non-compliance is often easier than compliance. Under these circumstances, commitment and loyalty are useful concepts as they represent a desire to continue with a course of action in spite of any difficulties. Committed and loyal end-users will be more inclined towards compliance than non-compliance, thereby contributing towards maintaining the effectiveness of information security policies and controls in the organization. End-users who demonstrate both commitment and repeated compliant behaviour are truly loyal to the information security policies and controls in the organization.

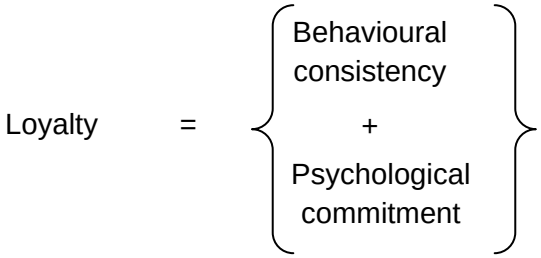


Figure 2.3: The construct of Loyalty (from Jacoby & Chestnut, 1978)

2.3.4 Theory of Planned Behaviour

Behaviour may be defined as the *"observed overt acts"* undertaken by individual end-users (Fishbein & Ajzen, 1975). The Theory of Planned Behaviour (Ajzen, 1991, 2005) provides an explanation of the underlying causes of human behaviour. In the context of information security, the Theory of Planned Behaviour (TPB) can be used to understand the behaviour of end-users related to information security policies and controls in the organization. This section provides a brief overview of the TPB based on Fishbein and Ajzen (1975) and Ajzen (1991, 2005).

Human behaviour is complex and is subject to a large number of factors. It can be understood in terms of an individual's physiological responses and also in terms of socio-cultural influences on the individual (Ajzen, 1991). TPB links these underlying causes to the actual behaviour. The

model of TPB is shown in Figure 2.4. According to this model, to understand behaviour, one has to understand the underlying causes and their links.

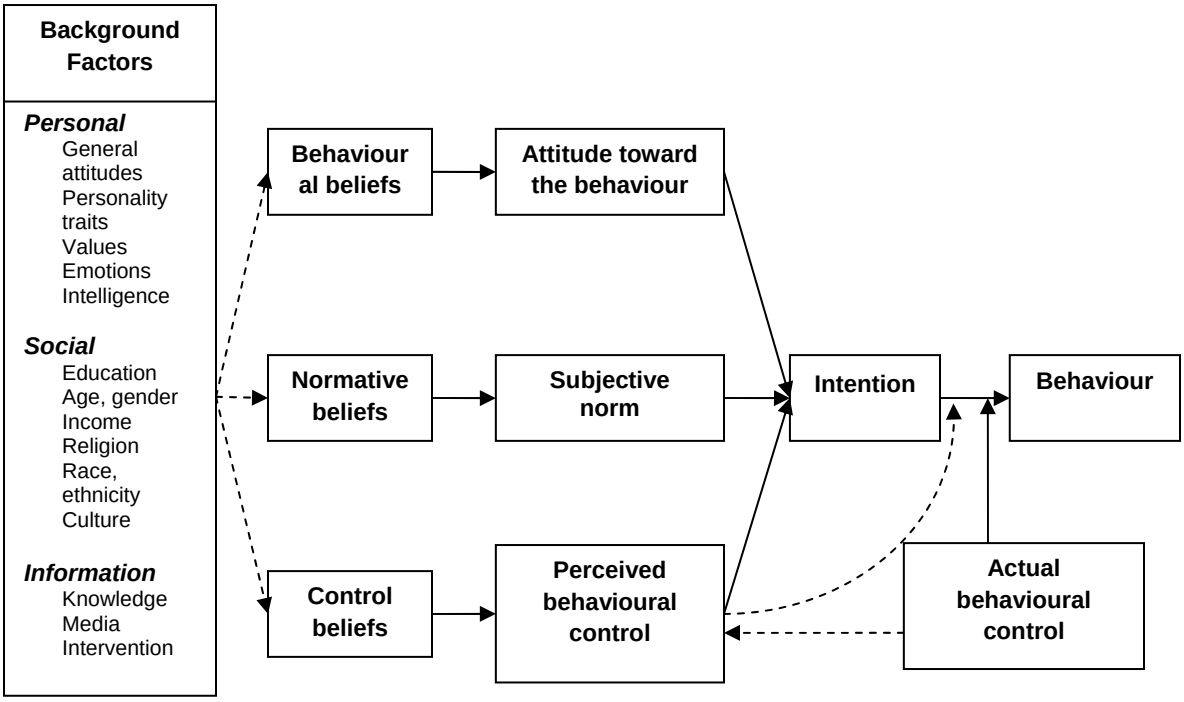


Figure 2.4: The Theory of Planned Behaviour (from Ajzen, 2005)

In TPB, the immediate precursor of actual behaviour is 'intention'. Intention is an indication of an individual's readiness to performs a behaviour. It is determined by the individual's attitude towards the behaviour, subjective norm and the individual's perceived behavioural control. The determinants of attitudes, norms and perceived control are themselves determined by underlying behavioural, normative and control beliefs. These beliefs represent the information that the individual possesses about the behaviour; and they may vary based on a wide range of background factors such as personality, emotion, age, race, gender, etc. Finally, once an individual has decided to undertake an action, i.e. the intention for the behaviours has crystallized, the execution of the actual behaviour is subject to the individual's capacity to undertake that behaviour successfully. Thus, once an individual has decided to perform the behaviour, and if the required opportunity and resources are available, the individual should succeed in doing so.

Attitude refers to the positive or negative value that the individual attaches to the behaviour and its outcomes. Attitude is based on behavioural beliefs that represent the information the individual possesses on the outcomes of the behaviour. The beliefs link the behaviour to the benefits and the costs of the behaviour. Over a period of time, individuals form favorable attitudes towards behaviours with desirable outcomes and unfavourable attitudes towards other behaviours with undesirable outcomes. French et al. (2005) maintain that attitude has two components, namely, affective or emotional and instrumental or cognitive. In TPB, beliefs are cognitive in nature, whereas attitude is affective in nature and represents the individual's 'feeling' of being favorably or unfavourably inclined towards the behaviour (Fishbein & Ajzen, 1975). According to Olson and Maio (2003), attitudes are subjective and *"reflect how a person sees an object and not necessarily how the object actually exists"*. Attitude captures summary evaluations such as good-bad, easy-difficult, harmful-beneficial etc. regarding a particular behaviour (Ajzen, 2001). In the context of information security in an organization, attitude of an end-user towards information security policies and controls would reflect his/her 'feeling' towards undertaking the specified security behaviours. For example, an end-user may develop an unfavourable feeling towards restrictions on file sharing and a favorable feeling towards bypassing the restrictions as this behaviour is more productive and beneficial, in spite of having knowledge regarding the risks that may arise.

The social factors, that influence an individual's preference for a particular behaviour, are grouped under 'subjective norms'. The normative beliefs reflect the individual's beliefs about the approval or disapproval of important referent individuals or groups regarding the proposed behaviour. In the context of information security in an organization, the normative beliefs of an end-user would reflect the end-user's understanding of the prevailing information security culture in the organization and the management's commitment to information security.

Perceived behavioural control refers to *"people's perception of the ease or difficulty of performing the behaviour of interest"* (Ajzen, 1991). Thus, it is an individual's perception of his or her ability to successfully undertake the behaviour, given the availability of opportunity, skills and resources. The control beliefs are based upon the individual's past experience as well as the second-hand information obtained from sources such as acquaintances and friends. In the context of information security in an organization, perceived behavioural control refers to an end-user's beliefs about his or her ability to undertake a security behaviour as mandated by the organization's information security policies and controls. These beliefs are shaped, in part, by the end-user's past success or failure with respect to information security policies and controls.

Actual behavioural control refers to the opportunity, skills and resources available to the individual to successfully undertake the behaviour after having decided to do so. It may so happen, that even though an individual intends to undertake a particular behaviour, he/she fails because of the absence of these factors. In the context of information security in an organization,

an end-user may intend to keep a strong password but fails simply because he/she does not know how to do so.

According to Ajzen (1991), *"explaining human behaviour in all its complexity is a difficult task"*. An individual's behaviour is determined by his/her feeling towards the behaviour, his/her perception of how others would behave in a similar situation and finally, his/her perception of the ease of undertaking the behaviour. Furtherore, all these determinants are influenced by a multitude of the individual's background factors such as personality, knowledge, age, race, gender, etc. Ajzen and Fishbein (2005) state that the relative weights or importance of attitude, subjective norm and perceived control in the formation of intention vary as a function of the behaviour and the individual. It may so happen that one or another of the factors does not contribute significantly to the formation of intention. Trafimow et al. (2004) found that affect (i.e. attitude) influences behaviour more than cognition does. Ajzen and Fishbein (2005) also state that, over time, individuals develop attitudes, norms, perceptions of control and intentions that guide their automatic performance of the behaviour. Such automatic behaviour, performed repeatedly over time, is termed as a habit. Habits may be defined as *"learned sequences of acts that have become automatic responses to specific cues, and are functional in obtaining certain goals or end-states"* (Verplanken & Aarts, 1999). According to Verplanken and Orbell (2003), habits have a history of repetition, are associated with a satisfactory pairing of goals and behaviours and habitual behaviours do not require any conscious decision-making. In the absence of conscious decision-making, according to Fazio's MODE model (Fazio & Towles-Schwein, 1999), such automatic or spontaneous behaviour is influenced by strong attitudes towards the behaviour.

In the context of information security in an organization, the behaviour of end-users regarding information security policies and controls is determined by their attitude, their perception of what others would do in the situation and also by their perception of control towards the specific behaviour. Typically, end-users recognize that complying with policies and controls is more troublesome than bypassing them; that their colleagues and seniors also often sacrifice security for productivity; and that they can successfully cope with the results of insecure behaviour. Under these circumstances, and over time, successfully indulging in insecure behaviours, end-users develop attitudes, subjective norms, perceptions of control and intentions that readily guide them towards insecure behaviour and away from compliance with organizational information security policies and controls. Such repeated insecure behaviour becomes a habit of non-compliance with information security policies and controls in the organization.

2.4 Conclusion

This chapter began as an attempt to understand the information security behaviours, particularly the non-compliance, of end-users in an organization. When end-users are confronted with an information security task, they pass through three stages. These stages are: awareness or knowledge regarding the task, the intention to initiate the task, and finally, the skill to successfully complete the task. Furnell (2010) called these the hurdles of perception failings, priority or responsibility failings and capability or usability failings. It was also discussed that a difficulty in any of the stages would force the end-users away from compliance towards non-compliance.

Studies of human behaviour in various other disciplines were also discussed. 'Thinking under risk' indicated that end-users are often faced with a trade-off – that of non-compliance versus productivity or of compliance versus lost productivity. The use of heuristics, often incorrect estimates of risk and the immediacy of benefits from productivity gains will ensure that end-users tend to decide the trade-off in favour of productivity, and hence, non-compliance. This underlines the falsity of the assumption of 'Homo Economicus' regarding end-users.

End-users, as error-prone humans, further have the potential of causing information security breaches through inadvertent errors leading to unintended consequences. The sub-section on the discussion on human error highlighted how organizational factors are often the true cause of these inadvertent errors. Organizations can mitigate the occurrence of error through essentially two approaches: the 'person' or 'system' approach of Reason (2000); or the 'old view' or the 'new view' of Dekker (2002). In the person approach, or the old view, the end-user is the cause of the error. In the system approach or the new view, the end-user is to be seen only as the immediate cause of the error; but, it is generally, believed that the error originates in the system or the organization. In the context of information security in the organization, adopting the person approach or the old view would lead to blaming the end-user for non-compliance. On the contrary, and more fruitfully, adopting the system approach or new view would take the analysis beyond the end-user into uncovering organizational and systemic factors leading to non-compliance, e.g., the lack of fit between an information security policy or control and the working practices of the end-users.

Loyal and committed end-users would tend to comply with the information security policies and controls in the organization. Thus, loyalty or commitment is a desirable characteristic. The loyalty or commitment of end-users would ensure that end-users would be willing to tolerate the inconvenience or fatigue associated with compliance.

The chapter finally discussed the Theory of Planned Behaviour (TPB). TPB seeks to explain the factors that drive human behaviour in any given situation. This theory ties up together all the other results from the preceding discussions. According to the TPB, human behaviour is determined by a cluster of underlying factors. These factors include the beliefs and attitude of the person, the socio-cultural influences on the person, and the perceived control beliefs of the person. It was also shown that in the context of information security in the organization, the situation is such that all these factors conspire to take end-users towards non-compliance.

This chapter has thus shown that it may be inappropriate to blame the end-user for non-compliance and the resultant information security breaches. It is probable, however, that it would be more meaningful to investigate more deeply into the organization. Further, the chapter also indicated that the problem of non-compliance arises from a multitude of factors. Non-compliance, consequently, requires a comprehensive treatment – identifying and resolving individual issues, e.g., awareness or usability or culture, may not yield the desired results. Since the managerial style in an organization gives shape to factors that influence the behaviour of people in the organization, the next chapter will carry this investigation forward, and will discuss various managerial styles and the resultant patterns of employee behaviours in the organization.

CHAPTER 3

The management of people in the organization

"'Our most important resource is our people.'
'Organizations exploit people, chew them up, and spit them out.'
Both of these views of the relationship between people and organizations are often expressed, but which is true? How you answer affects everything you do at work."

- Bolman and Deal (2003)

3.1 Introduction

People are the central constituents of any organization (Schein, 1980). Schein (1980) defined an organization as the *"rational coordination of the activities of a number of people for the achievement of some common explicit purpose or goal"*. Likewise, Schein (2004) defines organizations as *"the result of people doing things for a common purpose"*. Both definitions emphasize the role of people in achieving the objectives of the organization. Accordingly, it can be said that people are fundamentally important for any organization.

Mintzberg (1980) states that there are five basic parts of the organization, namely, the operating core, the strategic apex, the middle line, the technostructure and the support staff. Interestingly, all these parts are composed of people (Mintzberg, 1980). Mintzberg's 'operating core' consists of the employees of the organization who are directly involved in the production of the basic products and services of the organization. This operating core and its management are the focus of this chapter.

In view of the importance of people to the organization, the management of people, as workers or the operating core, in the organization assumes significant importance. According to Drucker (1954), the management of workers is one of the main jobs of management. But how a manager treats the working people in the organization depends on the manager's perception of the 'organizational world' about him (Davis, 1968). This view colours the manager's view of people

and his/her interpretation of various events, and acts as an 'unconscious guide' to his/her behaviour (Davis, 1968). Further, according to Davis (1968), the mental model that a manager holds *"affects the quality of human relations and productivity"* in the organization and determines the success of the organization. It is, therefore, instructive to understand the various mental models that managers hold regarding people in the organization. The link between managerial assumptions or mental models and employee performance is shown in Figure 3.1.

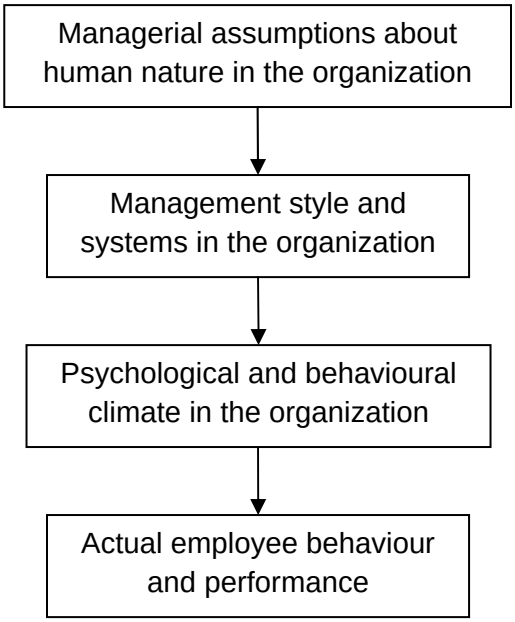


Figure 3.1: Influence of managerial assumptions on human nature upon actual employee behaviour (based on Davis, 1968)

This chapter explores this link between managerial assumptions regarding human nature in the organization and the consequential effects on managerial styles and actual employee behaviour in the organization. The next section establishes the validity of this link. Subsequent sections provide a brief overview of various organizational typologies, namely, those proposed by Davis (1968), Etzioni (1975), Pheysey (1993) and Schein (2004). These typologies reflect the mental models of managers in the organization. This overview is followed by an overview of the developments in management thought – from Taylor's 'scientific management' and Weber's 'bureaucracy' through the 'human relations' approach to McGregor's 'Theory X' and 'Theory Y'. All these typologies and approaches depict the growing trend of democratization and the participatory nature of models of management vis. a vis. the operating core in the organization.

In the remaining portion of this chapter, the terms 'employee', 'individual', 'man', 'people', 'employee' and 'worker' are synonymous and will be used inter-changeably. These terms refer to the 'operating core' of the organization.

3.2 The link between managerial assumptions and employee behaviour

In the early pages of his book *"Organizational Culture and Leadership"* (Schein, 2004), Schein provides an example of how managerial assumptions on the nature of workers in the organization influence the shape of the management style and control systems in the organization. Schein further quotes McGregor (1960) to reinforce how these assumptions influence the behaviour of workers in the organization. According to McGregor (1960), managerial assumptions regarding human nature have a considerable influence upon the organization as they determine the management and control systems used in the organization; further, people in the organization eventually come to behave in the manner consistent with these systems and their underlying assumptions (Schein, 2004).

This above view – of managerial assumptions influencing both managerial styles and control systems, which in turn influence the behaviour of workers in the organization – has been espoused for a long time in management theory, e.g., Davis (1968) and Harrison (1972). Davis (1968) described the managerial assumptions as the *"models of organizational behaviour"*. According to Davis (1968), these assumptions or models determine how managers perceive their organizational world, how they perceive people, how they interpret events – in short, the assumptions or models act as guides to the behaviour of managers. The managerial behaviour in turn influences the quality of human relations and worker productivity.

Harrison (1972) used the term 'organization ideologies' for managerial assumptions. According to Harrison (1972), organization ideologies refer to *"the systems of thought that are central determinants of the character of organizations"*. The importance of the organization ideology lies in the influence that it has on the behaviour of people in the organization, and the organization's capabilities to effectively meet the demands and needs of its people and to cope with the external environment. Harrison (1972) further states that organizational conflict can often be traced back to organization ideologies. The organization ideology performs the following functions (Harrison, 1972):

- Specifies the goals and values toward which the organization should be directed.
- Prescribes the appropriate relationships between individuals and the organization and what they can expect from each other.
- Indicates how behaviour should be controlled in the organization and identifies the kinds of controls that are legitimate, as well as those that are illegitimate.

- Depicts which qualities and characteristics of people in the organization are to be valued or vilified.
- Indicates how people in the organization treat others in the organization – competitively or collaboratively, honestly or dishonestly, closely or distantly.
- Establishes appropriate methods of coping with the external environment.

Various authors, as discussed above, have highlighted the role of managerial assumptions or mental models in determining the managerial styles and consequently employee behaviour in the organization. The next section discusses some of these mental models held by managers.

3.3 The typologies of organizational behaviour

Organizational typologies or managerial mental models represent the perceptions of managers in an organization regarding the 'organizational world' (Davis, 1968). These perceptions influence the way that the managers relate to their employees in terms of controlling their performance. Each model consists of a set of perceptions and assumptions and leads to a particular type of behavioural climate in the organization (Davis, 1968). According to Pheysey (1993), the model affects various facets of the organization such as control, job design, the motivation of employees etc. Harrison (1972) described these mental models as 'organization ideologies' that can be defined as *"the systems of thought that are central determinants of the character of organizations"*. These ideologies perform the following functions: they identify the goals and values that the organization strives for; they identify the relationships between individuals and the organization and between individuals; they identify legitimate and illegitimate forms of control; and they identify the desirable and undesirable qualities and characteristics of individuals (Harrison, 1972). This section discusses the typologies, models or ideologies as proposed by Davis (1968), Etzioni (1975), Pheysey (1993) and Schein (2004) (see Table 3.1). It is important to note here the different terms used by these authors for very much the same concept. In the discussion here, the author's preferred term is retained for each author, though the concept being discussed remains the same, namely, the organizational typologies or managerial mental models.

Davis (1968) Models of Organizational Behaviour	Etzioni (1975) Types of Organizations	Pheysey (1993) Types of Organizational Cultures	Schein (2004) Cultures of Management
Autocratic	Coercive	Role	Operator
Custodial	Utilitarian	Power	Engineering
Supportive	Normative	Achievement	Executive
Collegial		Support	

Table 3.1: Organizational Typologies (based on Davis, 1968; Etzioni, 1975; Pheysey, 1993 and Schein, 2004)

3.3.1 Davis' models of organizational behaviour

Davis (1968) proposed four models of organizational behaviour. These models are the autocratic, the custodial, the supportive and the collegial models (Table 3.1). Each model depicts the underlying mental model of the managers regarding the workers and the organization. According to Davis (1968), each of the four models may be present in an organization; however, the one model that predominates would determine the overall interaction between the manager and his workers. Below is a brief overview of each model from Davis (1968).

The autocratic model is based on the power exercised by the managers over their workers. This takes a threatening approach wherein workers can be penalized for not complying with orders. Compliance is achieved through fear and negative motivation. In the autocratic model, management assumes that it knows what is best and that it is the workers' obligation to comply with orders. Further, management assumes that workers are inherently passive and that management's primary responsibility is to persuade the workers to perform. This antagonistic approach towards workers engenders an equally antagonistic reaction amongst workers towards management. Hence, in the autocratic model, workers tend to resent the absolute power of their managers and they are motivated to give only minimal performance.

The autocratic model can lead to an unhealthy divide in the organization, namely, the overly-powerful managers versus their resentful workers. An improvement on this model is the custodial model, where it is believed that a happy employee is a better and more productive employee. The custodial model is based on economic and other material benefits provided by an organization to its employees. A limitation of the custodial model is that though it results in happy and satisfied employees, it does not necessarily lead to workers who are highly motivated or most productive.

The supportive model extended the custodial model by making the manager a source of psychological support for the workers, rather than being merely a source of economic support as in the custodial model. In the supportive model, managers provide leadership for creating an environment of personal growth and work performance. In this model, workers are not assumed to be passive; on the contrary it is believed that workers want to perform but are constrained by the organizational environment around them. Hence, the manager's primary responsibility is to create conditions that support the workers and allow them to perform at their best. In reciprocation, the workers do not just want to follow orders; rather, they become highly motivated and genuinely want to contribute towards achieving the organizational goals.

The collegial model further builds on the supportive model. In the collegial model, managers become integrators rather than bosses driven by power. The managerial orientation is towards teamwork in which both managers and workers are playing out their specific roles. Whereas workers are tasked with production, managers are tasked with integrating all the contributions of the team. The collegial model leads to workers who are driven by self-discipline – the worker feels responsible and wanted and, therefore, becomes highly motivated towards performance.

The four models can be said to follow a sequential path towards greater democratization, greater participation by workers in management and greater worker motivation towards achieving organizational objectives. According to Davis (1968), all four models typically co-exist in any organization and each model is well suited to a particular context. For example, the autocratic and custodial models are better suited for workers performing routine and low-skilled jobs. However, the supportive and collegial models are better suited for jobs that are intellectual in nature and require teamwork and self-motivation.

Four Models of Organizational Behaviour				
	Autocratic	**Custodial**	**Supportive**	**Collegial**
Depends on:	Power	Economic resources	Leadership	Mutual contribution
Managerial orientation:	Authority	Material rewards	Support	Integration and teamwork
Employee orientation:	Obedience	Security	Performance	Responsibility
Employee psychological result:	Personal dependency	Organizational dependency	Participation	Self-discipline
Employee needs met:	Subsistence	Maintenance	Higher-order	Self-realization
Performance result:	Minimum	Passive cooperation	Awakened drive	Enthusiasm
Morale measure:	Compliance	Satisfaction	Motivation	Commitment to task and team

Table 3.2: Four Models of Organizational Behaviour (from Davis, 1968)

3.3.2 Etzioni's types of organizations and Schein's cultures of management

According to Schein (2004), Etzioni (1975) proposed three types of organizations based on the relationship between the employee and the organization. These three types are: the coercive organization, the utilitarian organization and the normative organization.

In the coercive organization, the individual exists in the organization for purely physical and economic reasons. In such organizations, employees feel alienated and would exit if this were possible. Further, peer relationships develop for self-protection in defence against authority. In the coercive organization, employees work because they have to, rather than because they enjoy the work.

In the utilitarian organization, employees are assumed to be rational, calculative economic agents who work for incentives and rewards. In such organizations, employees work for compensation. Coercive and utilitarian organizations are similar in that they do not engender employee satisfaction and commitment.

Normative organizations engender employee commitment to organizational goals. Such organizations differ starkly from coercive and utilitarian organizations in the level of employee commitment. In normative organizations employees work because they want to, rather than because they have to.

Schein (2004) also proposed the three cultures of management. These are: the operator culture, the engineering culture and the executive culture. These cultures are based on the combination of the task to be performed and the occupational reference group involved. These subcultures are generic and they exist in all organizations. According to Schein (2004), conflicts often exist between these three subcultures, and these conflicts lead to reduced organizational effectiveness. The operator culture involves the line organization or the people who get the work done. This corresponds to Mintzberg's operating core group. The engineering culture belongs to the people or engineers who design the work products and processes. The executive culture involves the senior management of the organization whose job it is to maintain the financial health of the organization.

The executive and engineering cultures are similar in that they view the employees impersonally. They treat people as resources to be managed and persuaded to perform and achieve the organizational goals. Both cultures see employees as sources of conflict and problems that need to be managed. This view is in contrast to the view of the operator culture. The operator culture assumes that the action of the organization is the result of the action by operators and that the success of the organization depends on their knowledge, skill and commitment. Further, the operator culture assumes that carefully engineered rules and processes alone cannot solve all

problems and that operators will regularly have to deal with unpredictable contingencies. According to Schein (2004), conflicts often arise between these three cultures. Conflicts lead to undermining and devaluing each others' role in the organization. Often, operators assume that the executives and engineers do not understand their work and environment and so the operators resist and break the rules. In response, executives and engineers assume that the operators need to be controlled, and so they make tighter policies and manuals of procedure.

3.3.3 Pheysey's organizational cultures

In her book *"Organizational Cultures - Types and Transformations"* (Pheysey, 1993), Diana C. Pheysey presents four types of organizational cultures. These four types are: the role culture, the achievement culture, the power culture and the support culture. According to Pheysey, an organizational culture includes values, beliefs and attitudes commonly held by the people in the organization. An organizational culture prescribes *"the way we do things around here"* and serves as a pattern that governs the interactions between managers and workers in the organization.

A 'role culture' emphasizes conformity to expectations. In a role culture, the organization consists of hierarchies and divisions. Job descriptions, rules and procedures, in addition to principles for fixing remuneration, are the key constituents. The word 'role' refers to the way each employee occupying a position is expected to act. In such an organization, the employees are rewarded for conforming to their role.

An organization with an 'achievement culture' focuses on the achievement of work rather than on the conformity to rules. An achievement culture requires employees who are highly motivated and interested in the work itself. Contrary to the 'role culture', in achievement culture conformity to rules is not important.

The 'power culture' relies on the power vested in dominant individuals in the organization, whereas the other individuals have to be subservient. The dominant individuals are the leaders who decide unilaterally on what is best for the employees and the organization. The employees are expected to merely follow.

An organization following the 'support culture' exists as a community or group. Employees and managers exist as members of this community. In this culture, there is mutual trust and support. Communication, collaboration and cooperation govern the interactions between the people in the organization.

Pheysey (1993) has applied these organizational cultural forms in order to understand the beliefs and perceptions of managers regarding their workers in the organization. In role and power cultures, managers tend to motivate workers through control, whereas in achievement and support cultures, managers motivate their workers through appreciation and encouragement. In the role and power cultures, managers view workers as inherently lazy and unwilling to work. In this view, workers are to be persuaded to work through factors of extrinsic motivation such as rewards and penalties. Achievement and support cultures are marked by managers' belief that workers are intrinsically motivated towards the performance of their work. In these cultures, workers are assumed to work for the sake of satisfaction and enjoyment. Managers' beliefs regarding the motivation of workers in various organizational cultures are shown in Table 3.2.

By Control	By Encouragement
Role Culture: "Work is performed out of a respect for contractual obligations backed up by sanctions and personal loyalty towards the organization or system".	**Achievement Culture**: "Work is performed out of satisfaction in excellence of work and achievement and/or personal commitment to the task or goal".
Power Culture: "Work is performed out of hoe of reward, fear of punishment or personal loyalty towards a powerful individual".	**Support Culture**: "Work is performed out of enjoyment of the activity for its own sake and concern and respect for the needs and values of the other persons involved".

Table 3.3: Managers' beliefs on how to motivate subordinates (from Pheysey, 1993)

3.4 Scientific Management, Bureaucracy, Human Relations, Theory X and Theory Y

Scientific management (or Taylorism, after the name of Frederick Winslow Taylor) is a theory of management that was developed by Taylor (1911). The main objective of scientific management is to improve worker efficiency through an improved understanding of the work being done. According to Keir (1918), the basic elements of scientific management are: standardization, exact knowledge, functionalization, incentive and selected personnel. Standardization is the starting point of the scientific management approach. Standardization involves identifying the

best way to complete the given work. Exact knowledge is gained by studying the work being done. Management then uses this knowledge to govern instead of following 'rules of thumb'. Functionalization refers to the division of labour and the application of the rightly qualified workers to do the work. Incentives involve rewarding workers for doing their work sincerely. This involves managers taking over the work of designing and engineering, whereas the actual work of production is for the workers. Finally, scientific management requires careful selection of workers matching the needs of the work to be done.

According to Pheysey (1993), Weber (1947) developed the concept of 'bureaucracy' as an organization with a rational-legal basis. A bureaucracy has six major principles (Johnston, 1993). A bureaucratic organization has a distinct, formal hierarchical structure. Each level exercises control over the level below it. Control is exercised through formal rules and procedures that tie the levels together. Work is to be performed by the specialists. The organization is internally focused with scant regard for its customers. The organization operates impersonally, i.e. all employees are treated equally. Finally, employment is based on technical qualifications.

While both scientific management and bureaucracy had their advantages, both also suffered from several problems. According to Mullins (2004), these problems resulted from their implicit model of the worker. In Taylor's model of workers, workers could be treated as rational, economic beings who could be motivated by incentives to do work; they were to be given standardized tasks for completion; workers were to be provided with training, instructions and incentives for doing the work; and they were not to be involved in any decision-making related to the design of their work (Mullins, 2004). The problems that result include the dehumanization of work; worker deskilling; lack of worker motivation and commitment owing to an excessive focus on worker efficiency; and deterioration of the worker-management relationship (Mullins, 2004; Sandrone, n.d.). Bureaucracies too suffer from several dysfunctions. Mullins (2004) states that these are an over-emphasis on rules and procedures; initiative is stifled; impersonal relations in the organization; dependence on bureaucratic status, rules and symbols; and officious bureaucratic behaviour. Dayal (1981) stated that bureaucratic organizations suffer from delays, from mediocrity, from lack of innovation and from problems in the coordination of work due to the creation of barriers between functions.

The difficulties arising from scientific management and bureaucratic control led to the development of the human relations movement initiated by Elton Mayo. The human relations approach seeks to humanize the work organization through a better understanding of the social and psychological needs of workers (Mullins, 2004). In this approach, it is assumed that workers in an organization are influenced not only by the incentives they get for work, but also by their network of relationships in the organization and the values and attitudes of their colleagues. The level of workers' motivation depends on their view of their organization. According to Mullins (2004), the human relations approach was based on the recognition that an organization exists as

a social organization consisting of groups, group values and group norms. Whereas scientific management emphasized the rationalization of work, the human relations approach sought to humanize the organization (Mullins, 2004).

Douglas M. McGregor summarized the opposing perspectives of scientific management and human relations approach in his theories X and Y for the management of workers. McGregor (1957) described scientific management, or the conventional view of management, as 'Theory X'. The assumptions of this theory are that people are inherently lazy and indolent, and they lack the motivation to work. Hence, management is responsible for organizing the elements of production, and motivating, directing, controlling people for the completion of the work. In Theory X, the tools of management include incentives and the coercion of workers. McGregor (1957) stated that the carrot-and-stick approach leads to worker behaviour consisting of indolence, passivity, resistance to change, lack of responsibility, willingness to follow the demagogue and unreasonable demands for economic benefits. McGregor (1957) also proposed an alternative theory, namely, 'Theory Y'. In this theory, people's passivity and indolence are assumed to be the results of their organizational experiences; otherwise, people, by nature, are willing and motivated to work and take responsibility. Consequently, under Theory Y, the main task of management is to arrange organizational conditions and the methods of operation in order to enable people to achieve their goals.

The various theories of management discussed above are all based on a certain assumption regarding human nature, particularly in the context of work in organizations. Scientific management, bureaucracy and Theory X are based on the view that the people in an organization are passive, indolent and not wanting to work. Theory Y is based on an alternative view in which people are inherently willing to work. Dayal (1981) identified three views of man in management: the rabble hypothesis, the social man hypothesis and the complex man hypothesis. In the rabble hypothesis, the employee is disorganized and works primarily for his personal ends; and he will do his manager's bidding only for the sake of earning incentives. In this hypothesis, the work of management is to determine what is best for the man and the organization and to plan and organize the doer's behaviour to achieve the mission of the organization. The social man hypothesis questioned the 'economic man' concept and proposed that worker's performance is influenced by their satisfaction and happiness in the workplace. In this hypothesis, the essential task of management is to understand the social and technical factors influencing the worker and to create conditions in which the worker would be at his/her best. This gave rise to welfare programs, home visits, counselling etc. The complex man hypothesis extends the concept of man further by including his past personal experiences, his interpersonal and intergroup relations and his work context. In this hypothesis, the essential tasks of management are to: provide leadership that is capable of analyzing the dynamics of human situations at work; design and develop an appropriate organization congruent with the work; and implement policies and practices that support the behaviour that is best on the job (Dayal, 1981).

Similarly to Dayal (1981), Schein presented four assumptions regarding human nature that are shared by all cultures (Schein, 2004). These are:

- Humans as rational-economic actors: man is primarily motivated by economic incentives and will do those things that will give him the greatest gains.
- Humans as social animals with primarily social needs: man is basically motivated by social needs and obtains his basic sense of identity through his relationships with others.
- Humans as problem-solvers and self-actualizers, with primary needs to be challenged and to use their talents: man is motivated by a hierarchy of needs and is primarily self-motivated and self-controlled.
- Humans as complex and malleable: man is both complex and variable and it is difficult to generalize.

Ugboaja (2006) states that these assumptions have an *"extremely significant effect on any organization"* and that *"many of the really significant decisions in the organization are based on assumptions and values rather than logic and hard facts"*. Ugboaja (2006) shows how these managerial assumptions have implications for management styles and strategy. The observations of Ugboaja (2006) are summarized in Table 3.4.

Assumptions of Human nature	**Implications for Management Strategy**
Rational economic man	Organizations see themselves as buying the services and obedience of their employees. Motivation for work is through rewards; performance is regulated through a system of authority and control. Employees have to respect whoever occupies a position of authority. Management has four principal functions: plan, organize, motivate and control.
Social man	The manager's role shifts to understanding the needs and feeling of subordinates. The manager becomes a facilitator and sympathetic supporter rather than just being the creator of work, motivator and controller.
Self-actualizing man	The manager worries less about being considerate to employees; but, rather, he is more concerned with making work for the employees more challenging and more satisfying. The manager has to adjust to the individual needs and talents of the employees.
Complex man	The manager needs to be a good diagnostician and must be able to both sense and utilize the differences in individuals.

Table 3.4: Assumptions regarding human nature and the implications for management strategy (based on Ugboaja, 2006)

This section has provided a brief overview of various management theories, particularly as they apply to the relationship between managers and workers. Taylor's scientific management, Weber's bureaucracy, Mayo's human relations approach and McGregor's theories X and Y were discussed. Dayal's hypotheses on the concept of man in management theories and Schein's observations on human nature were also discussed.

3.5 Conclusion

This chapter has provided an overview of various organizational typologies and management theories. The typologies discussed include those proposed by Davis (1968), Etzioni (1975), Pheysey (1993) and Schein (2004). All the typologies indicate that organizations can be classified according to their perception of human motivation and behaviour. Depending on this perception, organizations have variable degrees of democratization and participation of employees in management.

Later, the chapter provided an overview of management theories including Taylor's scientific management, Weber's bureaucracy, Mayo's human relations model and finally, McGregor's theories X and Y. Each management theory is based on a particular perception of workers beliefs and motivations regarding their work. These perceptions are important as they determine the strategies that managers adopt for motivating workers. Finally, these management strategies lead to the creation of a psychological and behavioural environment in the organization that either supports or hinders the achievement of organizational goals.

This chapter has focused on how organizations treat those people who are their employees or workers. This focus uncovered the fact that the way management in an organization treats its people determines how these people behave in the organization. Chapter 2 discussed the information security behaviours of end-users and revealed the fact that the non-compliance of end-users originates not only from their actions (or inactions) but also from other organizational factors. The next chapter takes these two 'discoveries' (from Chapters 2 and 3) together and seeks to find out whether the style of information security management in the organization could be leading to non-compliance by end-users. The next chapter discusses the present-day approach to information security management.

CHAPTER 4

Information Security Management

"An information security digital divide between users and information security managers with regard to skills, knowledge and responsibilities is therefore to be expected".

- Albrechtsen and Hovden (2009)

4.1 Introduction

The previous two chapters highlighted the role of end-users in information security in the organization and the role of managerial mental models in shaping managerial systems and employee behaviour in the organization. Chapter 2 established that information security behaviours exhibited by end-users range from compliance to non-compliance. Non-compliant behaviours are particularly important to this study as non-compliance has the potential to lead to information security breaches in the organization. Chapter 2 also established that while the actions (or inactions) of end-users may be the immediate cause of non-compliance, the non-compliance actually originates in organizational and systemic factors beyond the control of end-users. Consequently, it is inappropriate to blame the end-users alone for non-compliance and to target remedial measures at the end-users only. What is needed is a more holistic approach that targets the end-users and also those organizational and systemic factors that lead to such non-compliance.

Chapter 3 took up this challenge and investigated the role of management in an organization. The analysis revealed that the managerial style in an organization has a significant influence on the behaviour of employees in the organization. Depending upon the managerial style existing in the organization, the organization develops a psychological and behavioural climate that determines how the employees in the organization behave in their day-to-day work in the organization. Chapter 3 indicated that a managerial style based on the principles of scientific management and bureaucracy treats employees under the assumptions of Theory X of McGregor (1957) and thus leads to the erosion of commitment of the employees to the organization. In contrast, a

managerial style based on Theory Y assumptions has the potential to lead to a much healthier organization in which employees are motivated and committed to the organization and their work.

This chapter examines the nature of the present-day approach to information security management (or information security management system) in the organization. Information security management (ISM) is implemented in the organization through the organizational structure of an information security management system (ISMS); consequently, this thesis treats the terms ISM and ISMS synonymously. The analysis in this chapter attempts to discover whether the non-compliance of end-users can be traced back to the managerial style of information security managers in the organization. The next two sections will discuss the role, and importance of information security management in the organization and its process. The subsequent two sections will discuss the evolution of information security and the problems associated with present-day information security management systems. This chapter firmly establishes that the present-day approach to information security management in the organization is bureaucratic in nature and thus, by implication, largely responsible for the non-compliance exhibited by the end-users in the organization.

4.2 The role of information security management

According to Von Solms (2001), information security is a multidimensional discipline. One of the dimensions of information security is the 'Governance/Organizational dimension'. This dimension refers to the way that information security is organized, structured and managed in an organization. According to Von Solms (2001), information security management is an important dimension underlined by the availability of various international best practices, standards and guidelines which all stress the importance of an organizational structure for information security. The 'Governance/Organizational' dimension of information security establishes information security related job roles and responsibilities, communication between these roles and top management commitment and involvement with information security in the organization.

Eloff and Eloff (2003) define an information security management system (ISMS) as *"a management system used for establishing and maintaining a secure information environment"*. The ISMS establishes the processes and procedures required to manage information security. The aim of these processes and procedures is to preserve the security of the information assets of the organization and to work towards the continual improvement of information security in the organization (Posthumus & Von Solms, 2005). The international standard on ISMS, ISO/IEC 27001:2005 (ISO/IEC 27001, 2005) defines information security management system as *"that part of the overall management system, based on a business risk approach, to establish, implement, operate, monitor, review, maintain and improve information security"*. In a note to

the definition, it says that *"the management system includes organizational structure, policies, planning activities, responsibilities, practices, procedures, processes and resources"* (ISO/IEC 27001, 2005).

ISMS can be viewed from different perspectives (Eloff & Eloff, 2003):

- Strategic perspective: addressing corporate governance, policies and pure management issues;
- Human perspective: addressing security culture, awareness, training ethics and other human-related issues;
- Technology perspective: addressing issues related to hardware and software products; and
- Process perspective: addressing the implementation of controls as contained in a standard or code of practice and compliance with these controls.

Eloff and Eloff (2003) further state that information security management should take a holistic approach consisting of the integration of all the four perspectives in implementing ISMS in the organization.

Information security management in an organization plays a vital role in establishing an environment of information security in the organization. Through its organizational structures, processes and procedures, the ISMS attempts to preserve the security of vital information assets of the organization. As stated by Eloff and Eloff (2003), the ISMS has a human side as well; however, this aspect is not well developed, as will be discussed later in this chapter. The next section discusses how information security management operates in the organization.

4.3 The process of information security management

Eloff and Eloff (2003) state that the process of ISMS consists of two phases, namely, planning and then implementing management practices, procedures and processes for establishing and maintaining information security. According to Posthumus and Von Solms (2005), the ISMS process consists of:

- Obtaining clear direction from guidance available in security standards or codes of practice. Additional guidance is available from the corporate information security policy.
- Assessment of various potential risks to the information.
- Formulation of a risk management strategy resulting in the identification and implementation of physical, technical and operational security controls.
- Staff training in security practices.
- Testing the security infrastructure.
- Detecting and responding to security incidents.

- Auditing the security function and reporting to the board on its effectiveness.

ISO/IEC 27001:2005 (ISO/IEC 27001, 2005) adopts a 'process approach' for implementing ISMS in the organization. This process approach consists of the Plan-Do-Check-Act (PDCA) model (see Fig. 4.1).

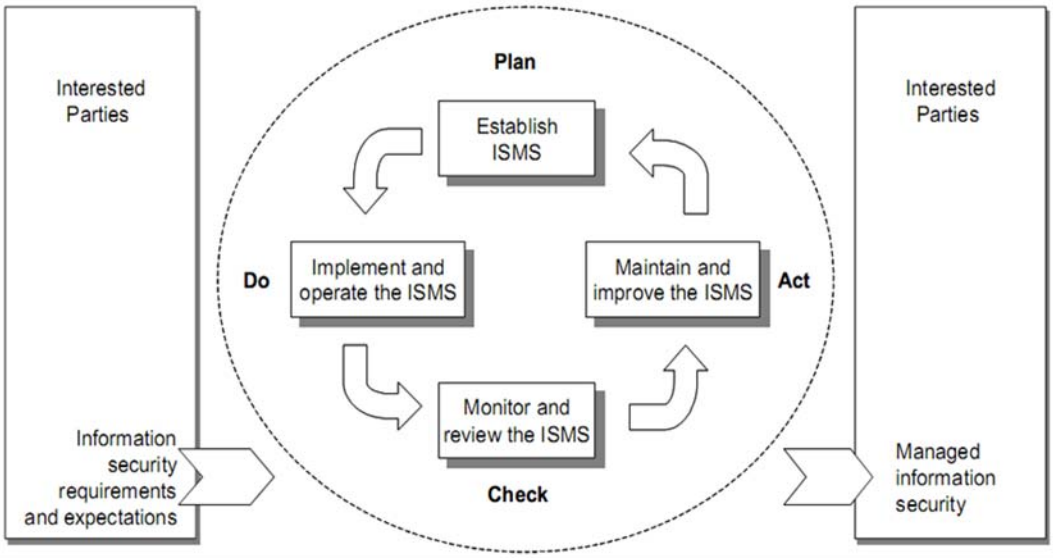


Figure 4.1: PDCA Model applied to ISMS Processes (from ISO/IEC 27001:2005)

As shown in Figure 4.1, the ISMS takes as input the information security requirements and expectations from the interested parties and then delivers managed information security to these parties. This transformation from needs to managed security takes place through the operation of the ISMS. The process provided in ISO/IEC 27001:2005 for establishing and maintaining the ISMS is as follows (also see Table 4.1):

- Establish the ISMS: identify its scope; analyse the risks; select control objectives and controls; obtain management authorization to implement and operate the ISMS.
- Implement and operate the ISMS: implement the controls; implement training and awareness program; manage operation and resources for the ISMS.
- Monitor and review the ISMS: review and measure the effectiveness of controls and the ISMS; conduct internal ISMS audits.
- Maintain and improve the ISMS: implement identified improvements in the ISMS and inform all interested parties; ensure that improvements achieve the intended results.

Plan **(establish the ISMS)**	Establish ISMS policy, objectives, processes and procedures relevant to managing risk and improving information security to deliver results in accordance with an organization's overall policies and objectives.
Do **(implement and operate the ISMS)**	Implement and operate the ISMS policy, controls, processes and procedures.
Check **(monitor and review the ISMS)**	Assess and, where applicable, measure process performance against ISMS policy, objectives and practical experience and report the results to management for review.
Act **(maintain and improve the ISMS)**	Take corrective and preventive actions, based on the results of the internal ISMS audit and management review or other relevant information, to achieve continual improvement of the ISMS.

Table 4.1: PDCA Model for ISMS (from ISO/IEC 27001:2005)

The companion standard ISO/IEC 27002:2005 (ISO/IEC 27002, 2005) provides further guidance for the training and awareness program for employees of the organization. The standard says that during the period of their employment, it is management's responsibility to ensure that all employees or users of the organization are provided with guidance, training and education regarding the sensitivity of the information they handle and the policies and procedures in place. The standard further states that there should be a formal disciplinary process for employees who commit a security breach.

Von Solms and Von Solms (2004) have listed the factors crucial to the success of ISMS in an organization. These factors have been labelled as 'sins' since missing these factors severely affects the effectiveness of ISMS implementation. These factors are:

- Not realizing that information security is a corporate governance responsibility (the buck stops right at the top).
- Not realizing that information security is a business issue and not a technical issue.
- Not realizing the fact that information security governance is a multi-dimensional discipline (information security governance is a complex issue, and there is no silver bullet or single 'off the shelf' solution).
- Not realizing that an information security plan must be based on identified risks.

- Not realizing (and leveraging) the important role of international best practices for information security management.
- Not realizing that a corporate information security policy is absolutely essential.
- Not realizing that information security compliance enforcement and monitoring is absolutely essential.
- Not realizing that a proper information security governance structure (organization) is absolutely essential.
- Not realizing the core importance of information security awareness amongst users.
- Not empowering information security managers with the infrastructure, tools and supporting mechanisms to properly perform their responsibilities.

Similarly, ISO/IEC 27002:2005 (ISO/IEC 27002, 2005) has listed critical success factors for ISMS implementation. These are:

- Information security policy, objectives, and activities that reflect business objectives;
- An approach and framework to implementing, maintaining, monitoring, and improving information security that is consistent with the organizational culture;
- Visible support and commitment from all levels of management;
- A good understanding of the information security requirements, risk assessment, and risk management;
- Effective marketing of information security to all managers, employees, and other parties to achieve awareness;
- Distribution of guidance on information security policy and standards to all managers, employees and other parties;
- Provision to fund information security management activities;
- Providing appropriate awareness, training, and education;
- Establishing an effective information security incident management process;
- Implementation of a measurement system that is used to evaluate performance in information security management and feedback suggestions for improvement.

At this point, in relation to the problem of end-user non-compliance, it is vital to note the near-total neglect by the present-day approach to ISM regarding the consideration of the human aspect of information security. The present-day approach to ISM, as evidenced by the role and process of ISMS discussed above, treats end-users in a rather simplistic manner – it assumes that compliance of end-users to information security policies and controls in the organization can simply be achieved by improving the awareness and skill levels of end-users. Beyond this, if end-user non-compliance persists, then end-users are to be blamed and treated through a disciplinary process. This approach is akin to the ‘person’ approach or the ‘old view’ of human error, as discussed in Chapter 2. Against this backdrop, the next section discusses the evolution of information security.

4.4 The four waves of information security

Since its inception, some decades ago now, information security and its management have continued to evolve. Von Solms (2000 & 2006) describe this evolution in terms of four waves. These waves are: the technical wave, the management wave, the institutionalization wave and the governance wave (Von Solms, 2000 & 2006). Von Solms (2000) presented the first three waves while Von Solms (2006) presented the fourth wave. This section presents an overview of these waves of development as presented in Von Solms (2000 & 2006).

The first wave is the technical wave which lasted until the early eighties and represents the highly technical approach to information security. This was the era of mainframe-based computing and highly technical users. In this era, information security consisted largely of securing the IT assets through the use of built-in access control lists, user-ids and passwords. People-related aspects such as information security policies, information security awareness of users etc. were not even acknowledged. Information security was a technical issue and dedicated to the needs of technical people. However, the people responsible for implementing information security began to realize that this approach was not appropriate and that they needed management's commitment and involvement to guarantee the effectiveness of information security.

The second wave is the management wave which lasted from the early eighties to the middle nineties. This wave is characterized by the growing management realization of the importance of information security to the survival of the organization and the consequent involvement of management in the implementation of information security. The era of the second wave coincided with the development of organizational computing from mainframe-based computing to distributed computing and the arrival of technologies such as the Internet, WWW and E-commerce. As these technologies became more and more important for the organizations, information security too gained prominence and the top managements of organizations began to get involved. Information security policies, information security managers and organizational structures for information security were established. As top management became involved with information security, the information security people not only got the sanction to go ahead with securing the organization's information assets, but they also got questioned about issues such as progress and results. Information security managers were saddled with the responsibility of drafting policies and procedures, and they started to report to top management through organizational structures.

The second wave overcame some of the shortcomings of the first wave and management involvement led to improvements in the effectiveness of information security in the organization. However, now organizations wanted to know how well they were doing in their information

security efforts and how they could benchmark themselves against other organizations. Another significant realization was that the human aspect of information security was perhaps the biggest impediment to the effectiveness of information security in the organization.

The third wave began in the late nineties and lasted until the mid-2000s when the fourth wave began. This is the wave of the institutionalization of information security. This wave is characterized by aspects like best practices and codes of practice for information security management, international information security certification, cultivating information security as a corporate culture, and dynamic and continuous information security measurement. The third wave filled the gap that was felt in the second wave, namely, that of the availability of guidance for the implementation of information security in the organization. The fourth wave consisted of the following components, each component addressing a particular syndrome:

- Information Security Standardization: availability of guidance in the form of international best practices addressing the syndrome *"how do I know I am not missing something?"*
- International Information Security Certification: availability of audit and certification bodies to address the twin syndromes of *"how do I prove my security preparedness to an E-commerce partner?"* and *"how can I allow a potential E-commerce partner into my system if I know nothing about his information security preparedness?"*
- Cultivating an information security culture throughout a company: this consists mainly of comprehensive information security awareness programs and addressed the syndrome *"my own users may be my biggest enemy?"*
- Implementing metrics to continuously and dynamically measure information security aspects in a company: this consists of continuous measurement of the state of information security in the organization and addresses the syndrome *"how do I know how well our information security policies, procedures etc. are complied with?"*

The third wave, in parallel with the first and second waves, established a more mature discipline of information security. The technical measures of the first wave and the managerial involvement of the second wave were supplemented by guidance in the form of standards and certifying bodies. Additionally, the implementation of information security was further enhanced with the introduction of culture and awareness programs in recognition of the importance of people for information security.

The fourth wave began in the mid-2000s and consists of the development of information security governance. This is the era in which IT has become pervasive and is crucial to the operation, growth and survival of organizations. This dependence has led to developments in the field of corporate governance which make top management and boards of directors of organizations directly responsible for the health and security of their IT systems. Consequently, the responsibility for information security in the organization has risen to the top echelons of the organization. This has led to information security governance becoming an integral part of

corporate governance. The fourth wave is characterized by another crucial realization, namely, that the use of IT systems by humans, i.e. employees, clients and customers, can lead to serious information security risks. Organizations and their management have realized that technical measures alone cannot solve this problem and that this requires strategic decisions at a high-level to improve the awareness of all the end-users.

The four waves in the development of information security, as put forward by Von Solms (2000 & 2006) represent a maturing of the information security discipline. These waves operate in parallel and, together, these developments ensure that not only technical means and controls are available for information security, but policies, procedures and guidance in the form of best practices and standards are also available for practitioners. Furthermore, organizations can measure and benchmark their information security efforts. These waves have seen the responsibility for information security escalate from the technical IT staff to the top echelons of the organization. Another important aspect has been the realization regarding the importance of user awareness and compliance to the effectiveness of information security. This has led to the development of awareness programs and efforts to create an information security culture in the organization such that information security becomes a way of life for the people in the organization.

As stated towards the end of the previous section, information security management has tended to take a simplistic approach to end-users. This fact is further reinforced by the delineation of the evolution of information security through the four waves. As discussed in Chapters 2 and 3 earlier, the behaviour of people (as employees or end-users) in the organization is complex and, hence, requires a comprehensive managerial approach. However, information security has failed to acknowledge this understanding and focuses only upon the awareness and training needs of end-users. This failure is further discussed in the next section.

4.5 The bureaucratic nature of present-day ISMS

This section discusses the incompleteness or the shortcomings of the present-day approach to ISM in regard to the management of end-users aspects of information security. The earlier discussions in the previous chapters and this chapter have prepared the grounds as follows:

- End-user compliance with information security policies and controls is crucial to the success of information security in the organization. End-user non-compliance has the potential to lead to information security breaches. Further, this non-compliance emerges from a cluster of factors which are not entirely under the control of end-users. Consequently, it may be inappropriate to blame end-users alone and the remediation of non-compliance requires a more comprehensive approach.

- The managerial style in an organization has a significant influence on the employee behaviour in the organization. Managerial styles based on Theory X assumptions of human nature, such as scientific management or bureaucracy, lead to the erosion of commitment and an unhealthy work culture. Alternative managerial styles, such as those based on Theory Y assumptions, lead to a more committed work force.
- Information security management plays a vital role in the establishment of information security in the organization. However, even as information security has evolved, and even as there are international standards and best practices guiding the implementation of information security in the organization, only a very narrow approach is adopted towards dealing with end-users in information security. The major aspect of the approach towards end-users may be summarized as follows: provide awareness and training to end-users to enable them to comply; if non-compliance persists then treat it through a disciplinary process.

The present-day approach of ISM is reminiscent of scientific management and bureaucracy. Hence, it may be that the present-day approach is, in fact, contributing to end-user non-compliance, rather than restraining it. This aspect is discussed further in this section.

Frangopoulos (2007) states that today's ISMS can be characterized by the following:

- Use of rules and regulations aiming to provide a secure environment.
- Commitment of everyone involved to a set of prescribed guidelines, i.e. behaviour control.
- Use of technical measures for controlling the application of rules and regulations and the upholding of behaviour control.
- Use of non-technical measures to complement the technical measures.
- De facto existence of a technocratic elite of information security professionals.

Frangopoulos (2007) further states that such ISMS correspond to a well-oiled machine according to the *"organization as machine"* metaphor of Morgan (1996). Thus, the ISMS is expected to function as a machine, in a *"precise, repeatable and predictable manner"* (Frangopoulos, 2007) ignoring the inherent variability of humans and their impact on the ISMS. Thus, *"despite being complete from a technical viewpoint"*, the present-day approach to ISM falls short on the treatment of the *"idiosyncratic nature of the human element, especially within a social context"* (Frangopoulos, 2007). Consequently, present-day ISMS suffer from *"fallacious working assumptions"* that *"imposed technical and physical controls can mitigate all identified risks"* (Frangopoulos, 2007). Frangopoulos (2007) further argues that *"modern day ISMS implementation still relies on bureaucracy for its fundamental functions"* and that *"a bureaucratic structure through which regulation and control are applied is a necessary pre-requisite for an ISMS to exist"*. According to Frangopoulos (2007), present-day ISMS represents an oxymoron, as it applies the Weberian principles of the 19th century to resolve the issue of

securing information in the 21st century. Hence, present-day ISMS is fundamentally bureaucratic and does not employ democratic processes.

Albrechtsen (2008) provides a similar analysis of present-day ISMS. Albrechtsen (2008) concurs that present-day ISMS is bureaucratic in nature and it can be characterized as follows:

- Use of technology to control and monitor user behaviour in addition to function as a fool-proof system.
- Use of documented descriptions of expected individual and organizational behaviour.
- Use of formal, one-way communicated, expert-based training and education of employees.
- Modest involvement of employees in the information security work.
- Lack of dialogue and interaction between information security professionals and users.
- Centralized management, with expert knowledge on information security and modest knowledge on actual work context at the sharp-end.

Albrechtsen (2008) states that bureaucratic ISMS suffers from two problems:

- Its inability to adjust to the dynamic nature of IT, organizations and threats; and
- It is inappropriate for handling the human aspect of information security.

According to Albrechtsen (2008), traditional management is based on the use of technological and bureaucratic means for the control of users. Echoing Frangopoulos (2007), Albrechtsen (2008) too states that present-day ISMS represents a paradox since it attempts to manage the security of modern and dynamic IT through traditionally structured approaches and perspectives.

Albrechtsen (2007) explored the relationship between users and information security managers. The results of this study indicate the divide between users and information security management. The results were as follows:

- Documented rules and guidelines have only a limited effect on users' information security behaviour.
- Uses feel that information security managers are invisible and inaccessible.
- Users experience their interactions with information security managers as expert-based, top-down interactions with no or moderate involvement of users.
- Users' perceptions of risk differ from those of information security managers.

Ashenden (2008) states that the role of information security managers in an organization is that of a technical specialist and that information security management is approached in a 'command and control' style. Information security is treated as a technical subject and best managed by technical staff. In pursuance of this approach, information security managers tend to ignore the end-users – *"they focus on talking, presenting and reinforcing ideas"* and *"not listening to end-users"* (Ashenden, 2008). The neglect of end-users is further reinforced by incorrect perceptions as information security managers do not engage with end-users and they do not try to understand

how end-users perceive information security; rather, information security managers rely on *"how they think"* end-users perceive information security. Ashenden (2008) states that this view is *"unlikely to be neutral"*.

Sensing the difficulties as discussed above, Dhillon (2001a) has provided the principles for information security management more suitable to today's needs. These principles are:

- Principles for managing the pragmatic aspects
  - Education, training and awareness, although important, are not sufficient conditions for managing information security. A focus on developing a security culture goes a long way in developing and sustaining a secure environment.
  - Responsibility, integrity, trust and ethicality are the cornerstones for maintaining a secure environment.
- Principles for managing the formal rule-based aspects
  - Establishing a boundary between what can be formalized and what should be norm based is the basis for establishing appropriate control measures.
  - Rules for managing information security have little relevance unless they are contextualized.
- Principles for managing the technical systems
  - In managing the security of technical systems, a rationally planned grandiose strategy would fall short of achieving the purpose.
  - Formal models for maintaining the confidentiality, integrity and availability (CIA) of information cannot be applied to commercial organizations on a grand scale. Micro-management for achieving CIA is the way forward.

In the principles proposed by Dhillon (2001a), it is stated that awareness and skills alone are insufficient for ensuring compliance by end-users. A more comprehensive approach is needed, based on a richer role for end-users in the organization. Furthermore, information security policies and controls need to be contextualized.

Finally, Schlienger and Teufel (2002) underline the problem with today's approach to information security management. According to Schlienger and Teufel (2002), the problem lies in the conception of the human dimension of information security. In the present-day, information security management is mainly focused on technical measures. In this approach, the users are seen as a threat. There is distrust between information security management and users. In this scenario, information security management treats users as the *"enemy"* and there is no inclination to discuss the human aspect of information security. However, Schlienger and Teufel (2002) also propose a solution to this imbroglio. According to Schlienger and Teufel (2002), the solution lies in information security management undergoing a paradigm shift in regard to its conception of the human dimension. Information security management needs to shift from a technical to a human-centric focus. This approach requires a cultural change in information security management. In the new approach, the user is no longer the enemy; rather, the user

becomes a *"security asset"* (Schlienger & Teufel, 2002). As Schlienger and Teufel (2002) put it, the new information security management approach should be *"a socio-cultural, human centric approach that is based on trust and partnership, accompanied by appropriate security technology"*.

This section has firmly established the bureaucratic nature of the present-day approach to information security management. This means that the non-compliance of end-users can be traced back to information security management itself. Authors such as Dhillon, Schlienger and Teufel have provided a way forward from this malaise – that of a human-centric approach to information security management in the organization.

4.6 Conclusion

This chapter has provided an overview of present-day information security management in the organization. Information security management is essential for effective information security in the organization. However, the present-day approach to information security management in the organization is bureaucratic in nature and technically oriented and, hence, it fails to meet its objectives. The present-day approach, it may be said, actually contributes to the non-compliance of end-users. Hence, if non-compliance is to be remedied, then the present-day approach to information security management too must be enhanced – as stated by Frangopoulos (2007), it is improper to use 19th century principles to manage 21st century issues. Dhillon (2001a) and Schlienger and Teufel (2002) have pointed a way forward towards adopting a *"human-centric"* approach. The way out is an ISMS with a human-centric focus.

The next chapter will provide an overview of a management approach that is human-centric. This approach is that of service management. Service management is a customer-centric approach to management. It can be applied to internal services and to internal employees also. Thus, service management holds the potential for being applied to information security management. This will be discussed in the next chapter.

CHAPTER 5

Service Management

"The shift to services in focus is a shift from the means and the producer perspective to the utilization and the customer perspective."

- Gummesson (1994)

5.1 Introduction

The concept of service(s) has varied meanings. Services represent a class of products (a good or a service) with particular characteristics that differentiate them from goods. On the other hand, service is a mind-set, an approach wherein the organization is focused on serving its customers. As a mind-set, service is applicable to almost any kind of activity.

The objective of this chapter is to provide an overview of the concept of services, service and service management. This chapter concludes by exploring how service management principles have been extrapolated and applied to operations within an organization, namely, internal services and IT services.

5.2 Service and services

The American Marketing Association provides a rather lengthy definition of service(s) as *"products, such as a bank loan or home security, that are intangible or at least substantially so. If totally intangible, they are exchanged directly from producer to user, cannot be transported or stored, and are almost instantly perishable. Service products are often difficult to identify, because they come into existence at the same time they are bought and consumed. They comprise intangible elements that are inseparable; they usually involve customer participation in some important way; they cannot be sold in the sense of ownership transfer; and they have no title.*

Today, however, most products are partly tangible and partly intangible, and the dominant form is used to classify them as either goods or services (all are products). These common, hybrid forms, whatever they are called, may or may not have the attributes just given for totally intangible services. 2. Services, as a term, is also used to describe activities performed by sellers and others that accompany the sale of a product and aid in its exchange or its utilization (e.g., shoe fitting, financing, an 800 number). Such services are either presale or post-sale and supplement the product, not comprise it. If performed during sale, they are considered to be intangible parts of the product" (AMA, 2010b). This definition contains several elements, namely:

- Services are products which are largely intangible, e.g. a bank loan. In addition to intangibility, such products share certain common characteristics such as:
    - not capable of being stored or transported, and coming into existence at the time of consumption;
    - involve customer involvement in some important way;
    - they are intangible and hence difficult to identify;
    - they are not sold in the sense of ownership transfer; and
    - they can also be a hybrid product with both tangible and intangible components.
- Service represents activities that aid in the exchange or utilization of products.

According to the above definition, service exists in two forms: i.e. services as a largely intangible product, or service as an activity that supports the utilization of a product. This section first provides an overview of the characteristics of services as products (as distinct from products that are goods); and it, then provides an overview of the service as a product-supporting activity. It is important here to note the difference between the terms 'services' (as product) and 'service' (as product-supporting activity).

Various authors have commented on the four distinguishing characteristics of services, namely, the *IHIP* characteristics. The IHIP characteristics stand for intangibility, heterogeneity, inseparability and perishability (Gummesson, 2004; Kotler & Keller, 2006; Zeithaml, Bitner, Gremler & Pandit, 2008). Table 4.1 provides a comparison between goods and services based on the IHIP characteristics.

Goods	Services	Resulting implications
Tangible	Intangible	Services cannot be inventoried, patented, displayed or communicated.
Standardized	Heterogeneous	Delivery of services depends upon both on provider and customer actions and hence quality of services is variable.
Production separate from consumption	Production and consumption are inseparable	Customers participate in and affect the transaction; customers affect each other; employees affect the outcome of services.
Nonperishable	Perishable	With services, it is difficult to synchronize supply and demand; services cannot be returned or resold.

Table 5.1: Goods and Services (from Parasuraman, Zeithaml & Berry, 1985)

According to Zeithaml et al. (2008), the most distinguishing characteristic of services is intangibility. In this sense, services are performances or actions rather than objects. Consequently, services cannot be seen, felt, tasted or touched and hence are intangible. Intangiblity can be found in two dimensions i.e. physical intangibility and mental intangibility (Lovelock & Gummesson, 2004). Physical intangibility refers to the degree of materiality of the services product. Mental intangibility refers to the extent of difficulty involved in defining and evaluating the services product. Intangibility presents several challenges for services. Services cannot be inventoried, demand and supply cannot be matched, services cannot be easily advertised or communicated to customers and so customers may find it difficult to evaluate services (Zeithaml et al., 2008).

Services arise from the interaction between employees and customers. The heterogeneity of services is largely the result of the inherent variability in these interactions (Zeithaml, et al., 2008). Services are performances enacted by employees. Employees may be influenced by a multitude of factors. Further, customers may experience the performance under the influence of their own multiple factors. Heterogeneity also leads to several challenges. Because of the inherently variable nature of human interactions, ensuring consistent quality of services is difficult. The quality of services depends on both the customer and the provider. Whereas, the provider factors may be under the control of service managers, the quality may be affected by customer factors, over which the service manager may have no control.

Goods are typically first produced, then sold, and finally consumed. However, with services, the chain is a little different. Services are often first sold and then simultaneously produced and consumed (Zeithaml et al., 2008). This is the inseparability characteristic of services, whereby, services are simultaneously produced and consumed. This means that often the customer is present during the production of services. Furthermore, the customer may also often participate in the production process. According to Lovelock and Gummesson (2004), inseparability involves the presence of customers, the customer's role in production and customer-to-employee and customer-to-customer interactions. Customers take on the role of coproducer or 'partial employee' involving the transfer of work from provider to customer (Lovelock & Gummesson, 2004). Inseparability and simultaneity of production and consumption of services means that quality of services and customer satisfaction depends on what happens in 'real time' between employees and customers. Thus, inseparability poses challenges regarding mass production, customization, decentralization and delivery of services at convenient locations (Zeithaml et al., 2008).

Perishability of services implies that services cannot be saved, stored, resold or returned. This is in contrast to goods that can be stored. For service managers, perishability poses challenges regarding demand forecasting and capacity utilization.

Kotler and Keller (2006) define service as *"any act or performance that one party can offer to another that is essentially intangible and does not result in the ownership of anything. Its production may or may not be tied to a physical product"*. According to Kotler and Keller (2006), the offerings of a company can be categorized on the basis of the extent of the service component as part of the total offering of the company: pure tangible good, tangible good with accompanying services, hybrid, major service with accompanying minor goods and services and pure service. The second category echoes the second part of the definition of service as propounded by AMA (2010b) in which the service supports the utilization of the product. Such a service exists as a product support service.

The above definitions and characteristics describe service(s) in terms of the 'product' that is provided to customers. According to Vargo and Akaka (2009), this is reminiscent of the 'goods-dominant logic' or 'G-D Logic' in which services are conceptualized as output. In G-D logic *"services are what goods are not - somewhat less-than-ideal products or 'not-such-good goods'"* (Vargo & Akaka, 2009). An alternate conceptualization of service is also possible. In the 'service-dominant logic' or 'S-D Logic', service is defined as *"the application of specialized competencies (knowledge and skills), through deeds, processes and performances for the benefit of another entity or the entity itself"* (Vargo & Lusch, 2004). In terms of this logic, service is the fundamental unit of value creation, and goods exist only as service-provision vehicles (Vargo & Akaka, 2009). The first foundational premise of S-D logic is that the application of specialized

skills and knowledge for value creation is the fundamental unit of exchange between providers and customers (Vargo & Lusch, 2004). Gummesson (1994) stated that customers do not buy goods or services; rather, they buy an offering that creates value for the customer. Consequently, Gummesson (1994) rejected the separation between goods and services, and posited service as activities seen from the customer perspective.

In a similar vein, Grönroos (2007) states that service offers value-creating support to customers in their everyday activities and processes. In this view, customers are not concerned with goods or services; but, rather, customers look for solutions that serve their own value-generating processes. In response, firms have to choose from among four strategic perspectives: core product perspective, price perspective, image perspective and service perspective. In the first three perspectives, the firm focuses on the development of a core solution, whether as a physical product or as services, for the customer; additional services may be provided but only to aid in the use of the core solution (Grönroos, 2007). The service component is not strategic. In the service perspective, service attains strategic importance. The service perspective leads to the conceptualization of 'service competition' in which *"the core solution is the prerequisite for success, but where the management of a number of services, together with the core solution, forms a total service offering and determines whether or not the firm will be successful"* (Grönroos, 2007). The service perspective matches most closely to that which the customer seeks.

This section has provided an overview of the concept of service and services. Over the years, the concept has undergone changes. From its modest beginning as being what-goods-are-not, the concept has evolved into a new logic, a new perspective for business. In this perspective the difference between goods and services no longer exists, and service comprises two aspects: the application of provider competences and the benefit of customers. This is the view of service that is adopted in this thesis. The next section provides an overview of the service management approach of Grönroos (2007).

5.3 Service management

In the realm of the management of organizations, different management paradigms or perspectives have been identified. Three paradigms identified by Gummesson (1993, cited in Gummesson, 1994) are, namely:

- The manufacturing paradigm – the focus is on goods. Productivity and cost are important parameters to be controlled. Quality is only about technical standards and specifications.
- The bureaucratic-legal paradigm – the focus is on compliance with regulations and rituals, rather than on end results.

- The service paradigm – the focus is on the customer and the customer's interactions with the provider. Process thinking is the core of service delivery. Quality is not just about conforming to technical standards and specifications, it revolves around customer satisfaction.

Gummesson further states that all types of organizations are undergoing a shift towards the service paradigm and that service paradigm will be the management style of most businesses in the future (Gummesson, 1994).

According to Grönroos (1994), traditional management suffers from an overemphasis on cost reduction and economies of scale. Grönroos (1990) goes to the extent of saying that this thinking is a trap in service context. If, in a service context, firms do not adopt service management and continue with traditional management, the firm will fail to meet customers' expectations and *"will in the long run disappear from the market"* (Grönroos, 2007). To resolve this crisis, Grönroos has propounded the service management approach (Grönroos, 1990, 1994 and 2007). According to Grönroos (1990), service management is a management philosophy accompanied by two general shifts in traditional management thinking: (1) a shift from being concerned with the internal consequences of performance to external consequences from the customers' perspective; and (2) a shift in focus from structure to process. According to Grönroos (1990), service management approach differs from the focus of traditional management in the following ways:

(1) Form product-based utility to total quality utility in the customer relationship.
(2) From short-term transactions to long-term relationships.
(3) From core product (goods or services) quality or the mere technical quality of the outcome to total customer-perceived quality in enduring customer relationships.
(4) From production of the technical quality of products (goods or services) as the key process in the organization to developing and managing total utility and total quality as the key process (see Figure 5.1).

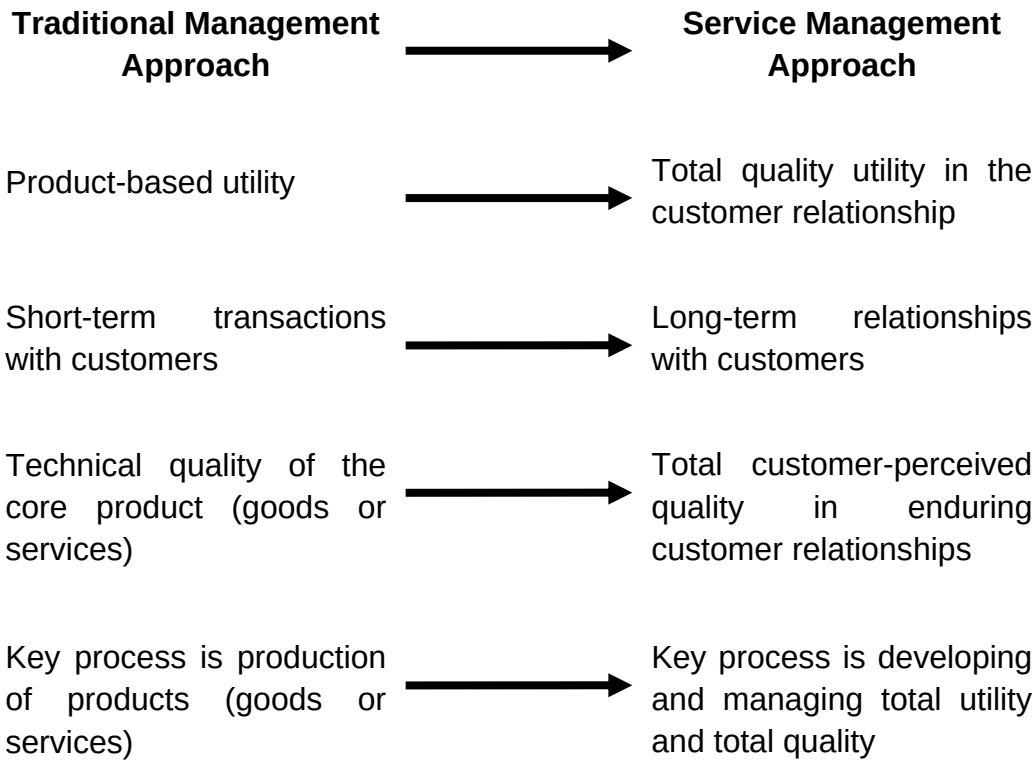


Figure 5.1: Shifts in focus from traditional management to service management (based on Grönroos, 1990)

Grönroos (1990) defined service management as, "*service management is to:*

(1) Understand the utility or value customers receive by consuming or using the offerings of the organization and how services alone or together with physical goods or other kinds of tangibles contribute to this utility that is, to understand how total quality is perceived in customer relationships and how it changes over time;

(2) Understand how the organization (personnel, technology and physical resources, systems and customers) will be able to produce and deliver this utility or quality;

(3) Understand how the organization should be developed and managed so that the intended utility or quality is achieved; and

(4) *Make the organization function so that this utility or quality is achieved and the objectives of the parties involved (the organization, the customers, other partners, the society, etc.) are met."*

Grönroos (1990) further stated that service management is a total organizational approach that focuses on the quality of service, as perceived by the customer. According to this definition,

service management applies not only to service businesses, but to all types of organizations (Grönroos, 1994). The above definition of service management has five key aspects: overall management perspective, customer focus, holistic approach, quality focus and internal development and reinforcement (Grönroos, 1994). The overall management perspective implies that service management philosophy guides management decisions in all areas of management and not just in the separate functions of the organization. Furthermore, service management is customer-focused and quality focused. To deliver on these foci, service management takes a holistic view by emphasizing intra-organizational and cross-functional collaboration and the development of personnel.

This section has provided an overview of service management as propounded by Grönroos (1990, 1994 and 2007). Service management is essentially a management perspective, philosophy or mind-set that revolves around long-term, enduring customer satisfaction. Since it is a management philosophy, service management can be adopted by all types of organizations or businesses. The next section provides an overview of the six principles of service management in order to understand how an organization may adopt and implement the service management approach.

5.4 Service management principles

Grönroos (1990, 2007) has provided six principles of service management. These principles signal the shifts in traditional management along six dimensions: (1) the business logic and driver of profit; (2) decision-making authority; (3) organizational focus; (4) supervisory control; (5) reward systems and (6) the monitoring and measurement of tasks and achievements. These principles are discussed below. A summary is provided in Table 5.2.

Dimension	Principle of Service Management
The business logic	**Customer perceived service quality drives profit.** Managing customer relationships and customer perceived quality are critically important to success. Interest in cost and productivity become secondary.
Decision-making authority	**Decision-making has to be decentralized as close as possible to the organization-customer interface.** Employees are empowered, encouraged, and trained, to solve problems arising from deviations from standard procedures so that customer satisfaction is created.
Organizational Focus	**The organization has to be structured and functioning so that its main goal is the mobilization of resources to support the front-line operations.** Focus shifts away from structure and control procedures to process and customer perceived quality.
Supervisory Control (or rather Supervisory Support)	**Managers and supervisors have to focus on the encouragement and support of employees.** Supervisory focus has to be on encouragement and enablement of employees so they can deliver quality service.
Reward Systems	**Production of customer perceived quality has to be the focus of reward systems.** Efforts at producing customer perceived excellence are rewarded rather than compliance to predetermined standards.
Measurement Focus	**Customer satisfaction with service quality has to be the focus of measurement of achievements.** The primary variable to be measured becomes customer satisfaction with service quality.

Table 5.2: Principles of Service Management (based on Grönroos, 1990 and 2007)

The profit equation and business logic. Traditionally, the focus of a business has been on making economic gains through management of the internal efficiency of the productivity of capital and labour. This, in turn, leads to an emphasis on economies of scale. According to Grönroos (1990, 2007), this approach can often lead an operation towards disaster (Figure 5.2). The shift to service management encompasses a shift in focus towards the notion that customer perceived quality, and not just internal efficiency, drives business profits. This means that the strategic focus of the organization shifts from cost considerations and internal efficiency towards management of customer interactions and relationships. Internal efficiency is still important, but it is not the top priority. The top priority is the management of customer perceived quality, customer interactions and customer relationships. The vicious circle of strategic management is transformed into the virtuous circle of service management (Figure 5.3).

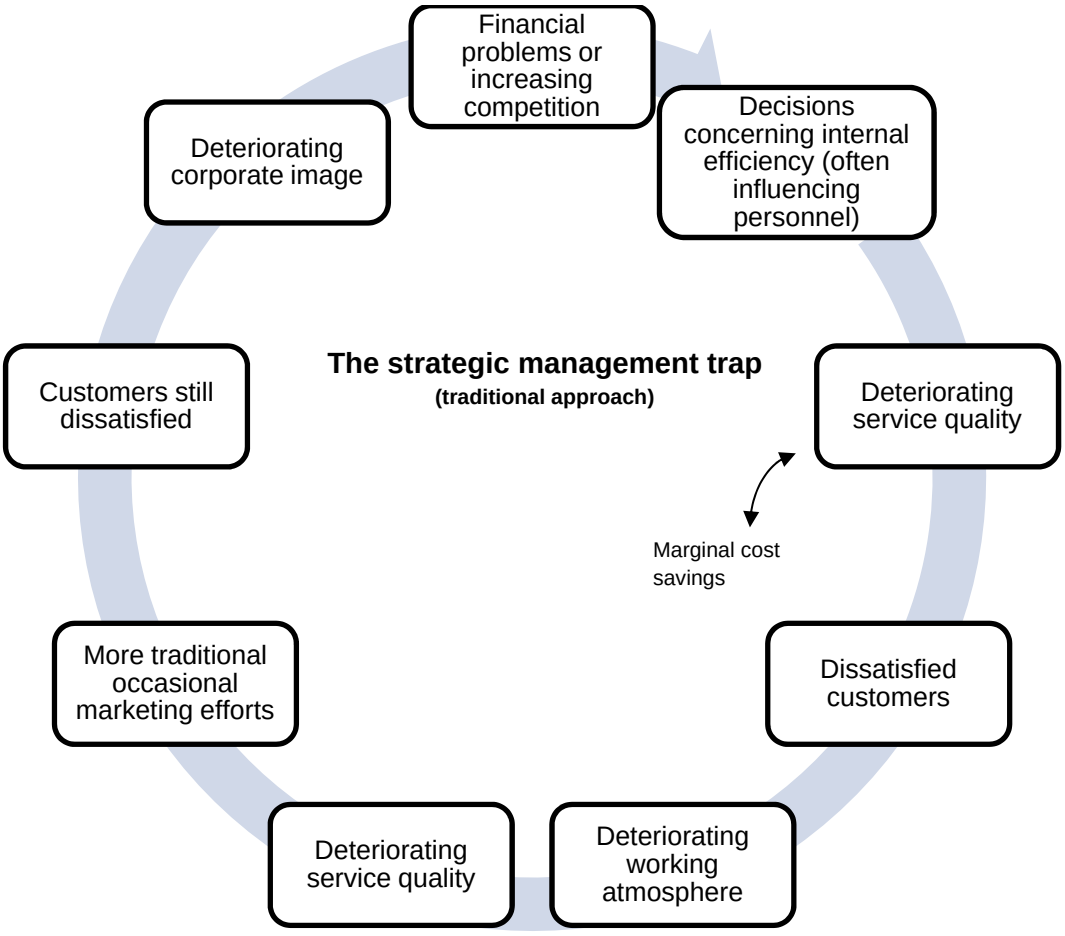


Figure 5.2: The strategic management trap (from Grönroos, 1990 & 2007)

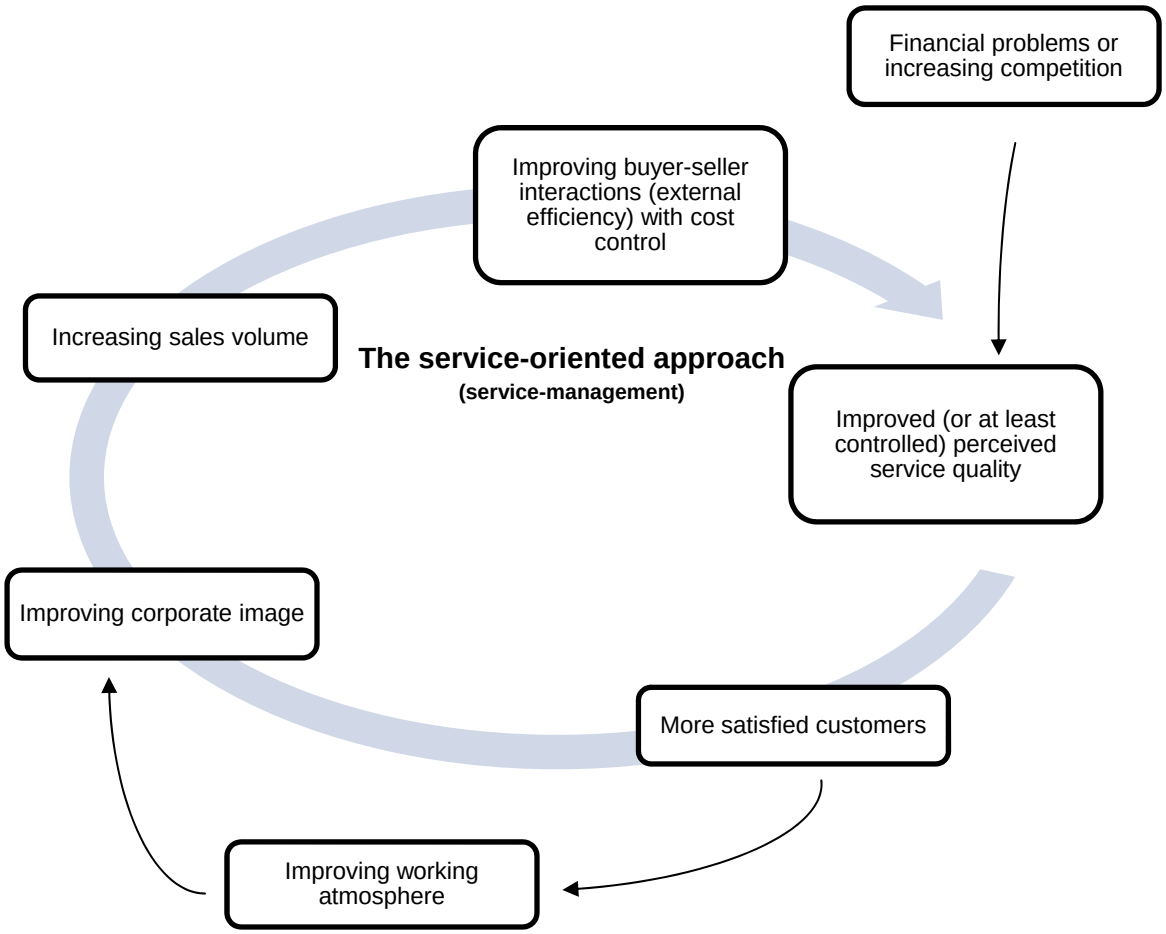


Figure 5.3: The service-oriented approach (from Grönroos, 1990 & 2007)

Decision-making authority. Services are characterized by inseparability between production and consumption. Further, in services, quality depends upon how customers perceive the service to be. Also, as stated earlier, service management requires a strategic focus on customer interactions and relationships. All the factors combine to elevate the importance of front-line employees, or customer contact employees, who interact with customers. These employees are the interface between the organization and the customers. Customer contact employees need to be empowered to take operational decisions to ensure the satisfaction of the customers. Strategically important decisions may still be centralized, however, certain decisions are best taken by customer contact employees. This means that the organization should place a special emphasis on training customer contact employees to use their judgment in tackling tricky

situations that may arise with any deviations from standard procedures for the benefit of customer satisfaction.

Organizational focus. In traditional management, the organizational focus is on creating and maintaining an organizational structure where management decisions are cascaded through processes involving legislative control. This approach is dysfunctional, and creates a lack of flexibility; it leads to centralization and prevents the easy flow of information throughout the organization. Service management removes this focus on structure and control procedures and instead places it on improved customer perceived quality. The organizational structure needs to be flexible in order to meet the needs of the customers.

Supervisory control. Traditional management requires the supervisory systems to closely monitor the capability of the organization and its various departments in performing their activities to predetermined standards. This rigidity is however unsuitable for service management. By their very nature, services cannot be standardized and there always remains an element of flexibility. In this situation, guidelines and vision are better than pre-determined standards. Thus, instead of monitoring performance in comparison with pre-determined standards, service management requires that the supervisory focus is on the support and encouragement of employees, particularly customer contact employees. In a way, supervisory control could be labelled as 'supervisory support' in which the job of management is to both empower and enable their employees to deliver services for the benefit of the organization's customers.

Reward systems. Reward systems are tied to supervisory focus. With a shift in supervisory focus from control to support, reward systems also need to reflect this shift. Service management requires that the production of customer perceived quality should be rewarded rather than mere compliance with pre-determined standards. Often organizations reward internal efficiency, but this forces employees to shift their focus from customer satisfaction to internal issues. This, frequently, leads to deterioration in customer perceived quality.

Monitoring and measurement of tasks and achievements or measurement focus. For supervisory focus and reward systems to be effective in promoting the service management approach, the measurement focus must also shift. In service management, the *"ultimate signs of success are customer satisfaction with total perceived quality, loyal customers and improved profits"* (Grönroos, 1990 and 2007). This implies that the focus should be on measuring efforts that boost customer satisfaction and loyalty. Internal efficiency must also be measured, but external efficiency criteria should dominate.

5.5 Internal service and internal customers

According to the *"six markets"* model of Christopher, Payne and Ballantyne (1991), an organization needs to be concerned with six markets, namely, customer markets, referral markets, influencer markets, employee markets, supplier markets and internal markets (Payne, Ballantyne & Christopher, 2005). While customer markets refer to existing and prospective customers of the organization, internal markets refer to the organization itself, including its different departments and staff (Payne et al., 2005). For the purpose of this section, only 'customer markets' and 'internal markets' are of interest. Since both customers and internal employees constitute markets for the organization, both can be managed through similar approaches. This approach consists of the following stages:

(1) Identify key participants, or segments, within each of the market domains;
(2) Review the expectations and needs of key participants;
(3) Review current and proposed levels of emphasis in each market; and
(4) Formulate an appropriate relationship strategy.

In the customer market, the organization acts as the service provider for its traditional customers or external customers. In the internal market, various departments or functions of the organization become both customers and service providers to each other, i.e. various internal service providers provide internal services to internal customers. Gremler, Bitner and Evans (1995) defined an internal customer as *"anyone in an organization who is supplied with products or services by others in the organization. That is, the employees of an organization can be considered as internal customers who, like external customers, are looking to get their needs satisfied"*.

Vandermerwe and Gilbert (1989) stated that firms typically take one of three approaches towards management of internal services: the accounting approach, the organizational approach and the operational approach. Vandermerwe and Gilbert (1989) also proposed a fourth approach, namely, the market-driven approach to improve upon the existing three approaches (see Tables 5.3 and 5.4). The following discussion of the four approaches is based on Vandermerwe and Gilbert (1989).

	Cost	Communications	Efficiency	Users & Usage
Accounting	X			
Organizational	X	X		
Operational	X	X	X	
Market-driven	X	X	X	X

Table 5.3: A shift in focus between the approaches of internal service management (from Vandermerwe & Gilbert, 1989)

Approach	Focus	Buyer / Seller relationship
Accounting	Cost	Rigid • Low customer commitment • Financially based
Organizational	Information	Structured • Defined relationship • Task-oriented
Operational	Efficiency	Periodic • Limited involvement • Process-base
Market-driven	Users and usage	Ongoing • Flexible • Market-based

Table 5.4: Aspects of approaches of internal service management (from Vandermerwe & Gilbert, 1989)

In the accounting approach, the focus is on minimizing the costs of internal services. This focus becomes dysfunctional and leads to several shortcomings. In this approach, service providers become insensitive towards their customers. Offered services become undifferentiated and inflexible and fail to meet the requirements of the customers. Since these customers are internal to the organization, the organization as a whole suffers.

In the organizational approach, the focus shifts from minimizing costs to creating a structure that facilitates relationships and communication between internal customers and internal service providers. Though this approach often works, it limits the interaction between internal service providers and internal customers to functional issues only.

The operational approach takes a 'service-factory' orientation towards internal services. In this approach, the focus is not on minimizing cost but rather on maximizing the efficiency of internal service production and delivery across the organization. The operational approach results in routine, standardized service offerings. This approach limits the interaction between internal service providers and internal customers to only those issues that are relevant to efficient production.

The above three approaches suffer from two problems: (1) internal service providers are insensitive to the needs of their internal customers, and (2) they often do not realize this. Consequently, the internal services fail to meet the requirements of internal customers and often do not adapt to their changing needs. This is the result of a focus on the service itself and a lack of sensitivity towards the users.

To alleviate the short-comings of the three approaches to internal services, Vandermerwe and Gilbert (1989) have proposed the market-driven approach. This approach shifts the focus from the internal service offering to the customer of the service; the approach forces the internal service providers to ask and answer two questions: who uses our services, and for what purpose? In the market-driven approach, the internal service providers align themselves with the internal customers' needs, thereby increasing the overall effectiveness of the organization. The market-driven approach to internal services necessitates the following:

(1) Providers and receivers become sellers and buyers. This radically changes attitudes and the providers realize that they exist to serve an end-market.
(2) Sellers want to understand the needs of their customers and adapt to their changing needs.
(3) Providers are focused on adding value to their customers, and thus to the overall organization.
(4) The operations become 'flexible service factories' emphasizing routinization and standardization, but at the same time remaining flexible to meet specific customer needs.

Earlier sections have provided an overview of the service management approach, as it is applied to the relationship between the organization and its customers. Here, the organization is the service provider and the customer is external to the organization. Service management is inherently customer-focused. This section has provided an overview of a customer-focused, market-driven approach to internal services. In internal services, the concepts of service management are equally applicable, the only difference being that both service providers and customers are employees, and hence internal to the organization.

Information technology (IT) operations in organizations are frequently managed as an internal service. The next section provides an overview of IT service management.

5.6 IT service management

Information and Information Technology (IT) provide a range of benefits to organizations (Dewett & Jones, 2001; Peppard, 2003; Porter & Millar, 1985; Whyte & Bytheway, 1996). The dependence of organizations on their IT has grown so much that failure of IT can cripple the parent organization (Peppard, 2003).

According to Whyte and Bytheway (1996), IT systems have failed to live up to expectations and there have been more failures than successes. Whyte and Bytheway (1996) provide a long list of factors responsible for these failures, culled from a review of the relevant literature. Their list of reasons for failure include: over-optimistic estimates, ill-defined project objectives, poor communication between users and the development staff, lack of user commitment to the project and the system, technical limitations of a system, systems which are unfriendly and inflexible, and the use of inexperienced staff for development. Conflicts between users, developers, tools and technologies in an information system or IT project are a key risk to the success of the project (Whyte & Bytheway, 1996). User-related problems with IT (or information systems) have been captured for some time now, e.g. Galloway and White (1993) stated that *"mutual dissatisfaction of users and data processing (DP) specialists continues to be a major problem"*. According to Galloway and White (1993), complaints from users' perspective are: over-run on budget, late delivery, failure to meet performance criteria, DP specialists' failure to communicate with users and insufficient maintenance provision. DP specialists complain about users' failure to specify needs adequately, failure to attend progress meetings, failure to assimilate training and failure to use the system properly (Galloway & White, 1993). Galloway and White (1993) further state that *"the situation is so common that both tend to assume that it is inevitable"*.

Whyte and Bytheway (1996) state that there are three perspectives regarding the development and delivery of IT systems in organizations. Each perspective has a different view of the problem of system development, delivery, and improvement. These perspectives are the product perspective, the process perspective and the service perspective. In the product perspective, the focus is on the product delivered to the users, e.g. hardware, software, documentation, training courses etc. The process perspective focuses on the process used for system development. The service perspective deals with the softer issues, e.g. answering questions, dealing with problems and addressing concerns of users. Whyte and Bytheway (1996) further state that IT managers are typically more concerned with monitoring of product and process aspects of their operation, rather than with the service aspects related to users.

Recently, user orientation is being seen as an important aspect of strategic IT management in organizations (Braun & Winter, 2007; Hochstein, Tamm & Brenner, 2005). Hirschheim et al. (2006) state that user participation and involvement in system development are important for successful projects. However, they also state that IT managers find managing this involvement very challenging. To resolve this difficulty, Hirschheim et al. (2006) propose a marketing perspective to IT management. In the marketing perspective, the users are the internal customers of the IT function and the IT function focuses its attention on *"determining the needs and wants of the target customers and then delivering satisfaction more effectively and efficiently than competitors"* (Hirschheim et al., 2006). According to Hirschheim et al. (2006), the marketing perspective delivers its benefits by making the IT function into a service organization that delivers ongoing services to its customers, namely, the users of the organization.

Hochstein et al. (2005) state that the transformation of the IT function from a technology oriented function to a client-focused IT service provider is possible only with a service management approach. Keel, Orr, Hernandez, Patrocinio and Bouchard (2007) also state that taking a customer perspective *"implies a shift from a technology-oriented to a service-oriented approach to IT management"*. Similarly, Braun and Winter (2007) state that *"this transformation from a technology oriented IT shop towards a customer oriented service provider that engineers its IT processes in a systematic, methodical manner"* is only possible by adopting a service management approach to IT. In a similar manner, Tan, Cater-Steel and Toleman (2009) state that ITSM represents a *"paradigm shift for IT functions as it deemphasizes the management of IT assets and focuses on the provision of quality end-to-end IT services"*.

Consequently, IT Service Management (ITSM) has gained prominence (Hochstein et al., 2005; Iden, 2009; McNaughton, Ray & Lewis, 2010). Tan et al. (2009) state that ITSM is the provision of quality customer service by ensuring that customer requirements and expectations with respect to IT are met at all times. In ITSM, the IT function in an organization is treated as a service organization delivering services to the organization (McBride, 2009; Peppard, 2003; Whyte & Bytheway, 1996). The users of the organization constitute the customers of the service. The IT function then directs its attention away from IT and outwards towards the customers and their need for services (McBride, 2009). This leads to few key effects. Firstly, the IT function becomes focused on the business process and the IT services needed to support this process. Secondly, the IT function needs to be staffed with people having skills in both IT and the business domain (McBride, 2009).

ITSM has proven beneficial to organizations. According to Potgieter, Botha and Lew (2005), the benefits include both enhanced customer satisfaction as well as improved operational performance. Hochstein et al. (2005) state that ITSM leads to improved client/server orientation and quality of IT services; higher efficiency of IT operations; and better transparency and

comparability through process documentation and monitoring. Tan et al. (2009) reported the following benefits: improved focus on IT service management; more predictable infrastructure, improved consultation with IT groups within the organization; smoother negotiation of service level agreements and seamless end-to-end service (Cater-Steel et al., 2006).

This section has provided an overview of IT service management, which is a service management approach to IT management. The IT service is similar to other internal services in an organization and possesses the IHIP characteristics of services (Peppard, 2003; Whyte and Bytheway, 1996), as discussed in the earlier sections. ITSM leads to several benefits for the organization, arising chiefly from the increased customer-orientation of the IT function.

5.7 Conclusion

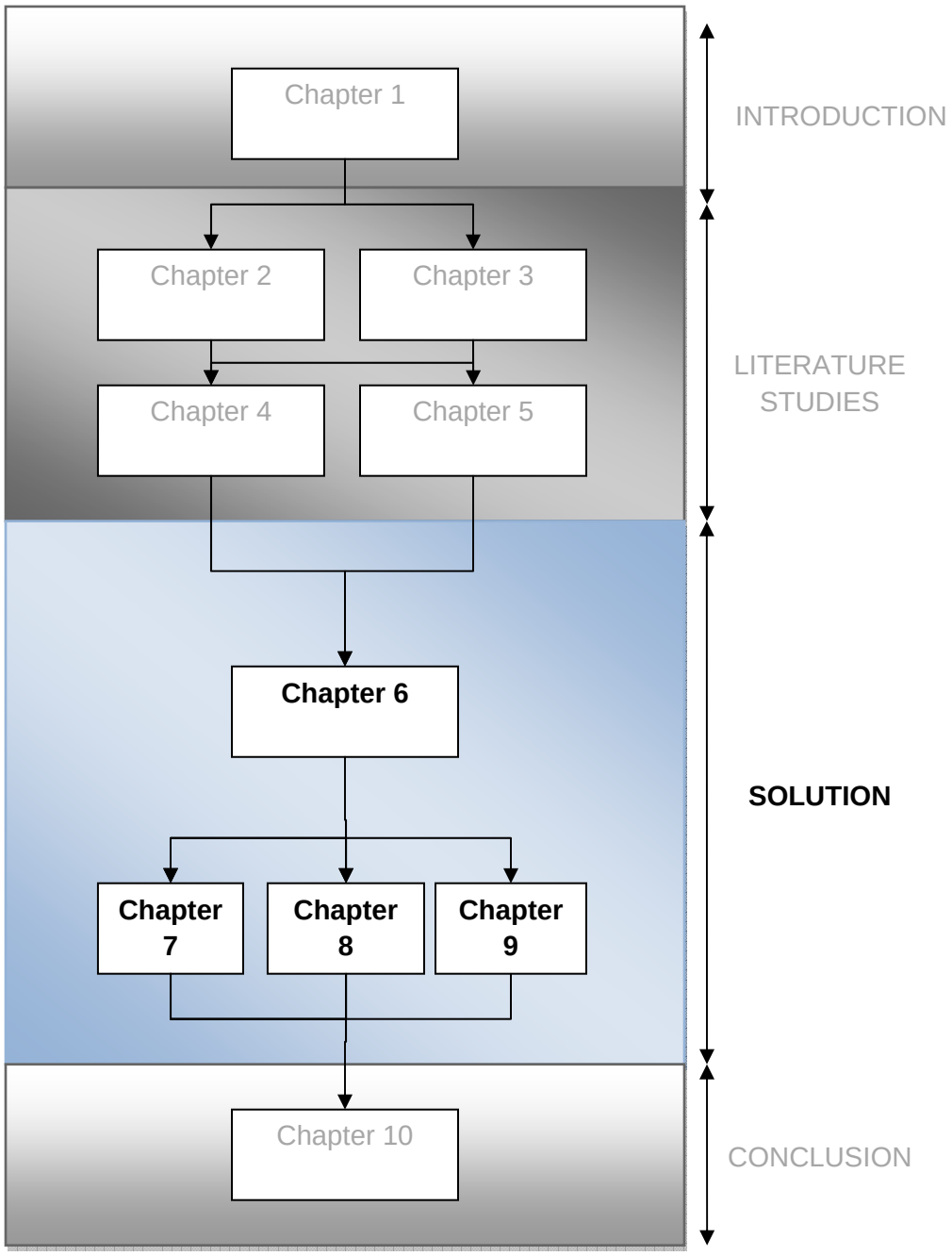
This chapter has provided an overview of the concepts of services and service management. Services are a particular kind of product; they possess the IHIP characteristics, making them distinct from goods. Service management is a mind-set that enables organizations to focus on their customers. As a mind-set, the concept of service management is applicable to all types of businesses and activities. This chapter has included an overview of the applicability of service management to internal services in which an internal function of the organization becomes a service provider to other employees, who in turn become its customers. The chapter finally provided an overview of IT service management which represents a case of service management being applied to an internal service.

This chapter is the concluding chapter in the literature overview that includes the previous three chapters also. This literature overview has covered various concepts and topics that have a bearing on this thesis.

The next chapter will apply these concepts to the problem of the end-user aspects of information security management; and it proposes a service management approach to information security management as a solution.

SECTION III

SOLUTION



CHAPTER 6

Information Security Service Management

"A customer is the most important visitor on our premises. He is not dependent on us. We are dependent on him. He is not an interruption in our work. He is the purpose of it. He is not an outsider in our business. He is part of it. We are not doing him a favor by serving him. He is doing us a favor by giving us an opportunity to do so."

- Mahatma Gandhi

6.1 Introduction

The above quote by Mahatma Gandhi underlines the importance of customers for an organization. Many in the organization management would swear by it as the mantra for success. However, with slight changes, such as replacing the word 'customer' with 'end-user', the quote may sound very startling and unexpected to information security managers in the organization. The quote, in the context of information security in the organization, would thus become (with some further minor changes):

"An end-user is the most important component of securing information in the organization. He is not dependent on us. We are dependent on him. He is not an interruption in our work. He is the purpose of it. He is not an outsider in our security effort. He is part of it. We are not doing him a favor by serving him. He is doing us a favor by giving us an opportunity to do so."

The quote, now, reflects a mind-set in which the end-user is supreme and information security management, policies and controls are subservient to his/her needs. This view is quite at variance with the dominant view in present-day information security management. Traditionally, information security management has been besieged by the idea that end-users represent a disruptive element that threatens the effectiveness of information security policies and controls in the organization. This mind-set leads to a bureaucratic information security management system and ever more stringent policies and controls that attempt to control the deviant end-users. The

vicious circle is completed when end-users, as it is unable to cope with the demands of information security, further reinforce management's assumptions about them through their increasing non-compliance with increasingly stringent information security policies and controls (Figure 6.1).

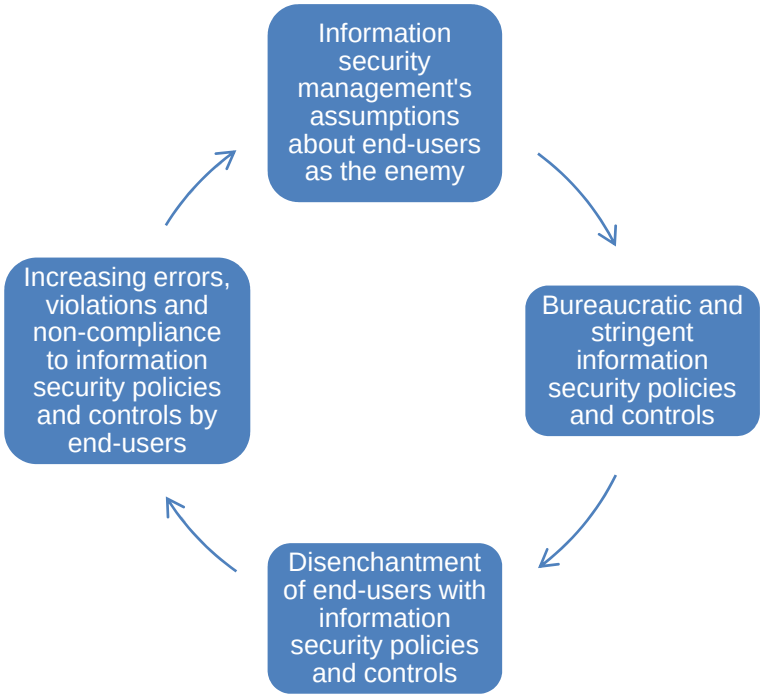


Figure 6.1: The vicious circle of bureaucratic information security

It is the purpose of this chapter to propose a solution for breaking out of the vicious circle which afflicts present-day information security management. The solution lies in Information Security Service Management (ISSM) which consists of applying the service management approach to information security management. The virtuous circle of ISSM is shown in Figure 6.2. In this virtuous circle, ISSM treats end-users as an asset and as partners. This mind-set leads to a management system that focuses on end-user friendly information security policies and controls and on providing a support system to the end-users. The virtuous circle is completed when end-users, already involved in information security efforts, further reinforce management's assumptions about them through their increasing compliance with information security policies and controls (Figure 6.2).

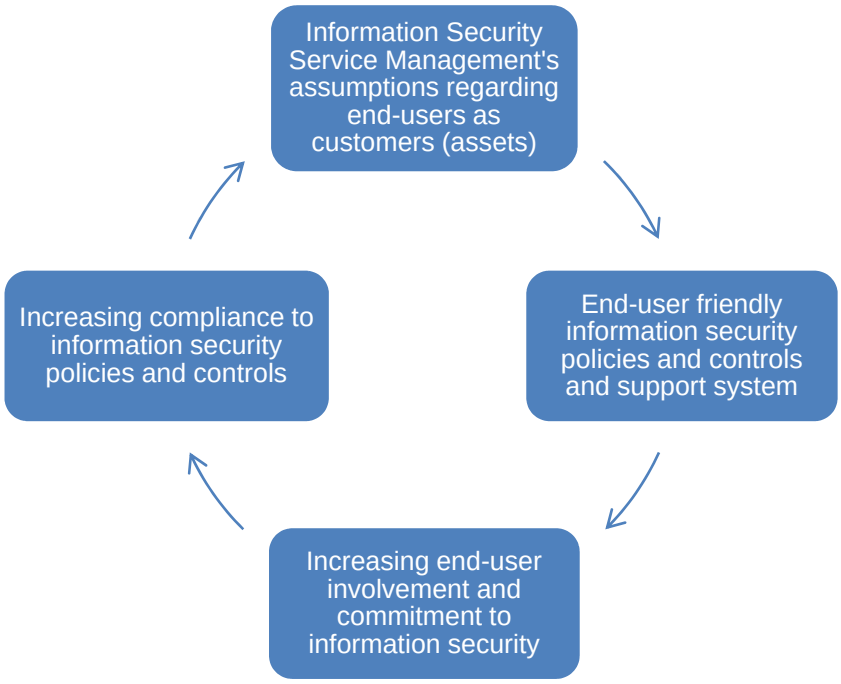


Figure 6.2: The virtuous circle of Information Security Service Management

The previous chapters have highlighted the issues pertaining to the human aspect of information security. This chapter brings all the issues together and uses argumentation to establish the validity of Information Security Service Management as an improved alternative to present-day information security management.

6.2 Making an argument for Information Security Service Management

Section 1.5.3 discussed the concepts of argument and argumentation, particularly Toulmin's layout of an argument. The section highlighted the role of argumentation in reasoning about the theory that results from theory building. In Toulmin's layout of an argument (see Figure 6.3), an argument links grounds or data to claims, with the support of warrants. This section applies Toulmin's layout of argument to establish the veracity of the claims made in this thesis.

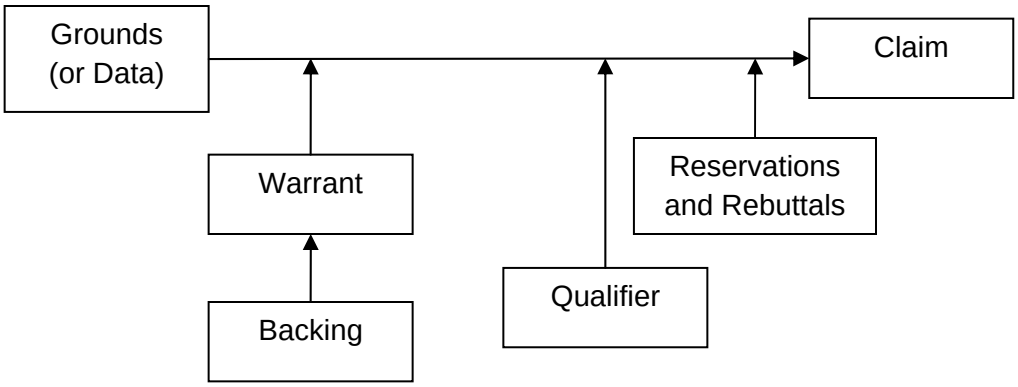


Figure 6.3: Toulmin's layout of argument (based on UNL, 1998)

This thesis essentially makes two claims – the first one establishing the problem and the second one establishing a solution; these claims are as follows:

- C1: The present-day approach to information security management (ISM) alienates end-users and fails to achieve the commitment and loyalty of end-users to information security in the organization; it creates a digital divide between end-users and information security managers and, thereby, fails to obtain end-users' compliance to information security policies and controls in the organization;
- C2: Information Security Service Management (ISSM) will overcome the short-comings of the present-day approach to ISM and will lead to improved compliance of end-users with information security policies and controls in the organization.

In Toulmin's layout of an argument, it is important to state the strength of the assertion regarding the claim of the argument. Following this, and before really launching into the process of argumentation, this thesis asserts that it makes 'strong' claims, i.e. these claims are highly probable given the grounds and warrants which are presented later.

The process of argumentation for establishing the two claims made above follows a two-step process. Step 1 establishes claim C1 regarding the failure of the present-day approach to ISM. Step 2 uses the claim C1 as ground or data and establishes claim C2 regarding the effectiveness of ISSM as a service-management approach to information security management.

Step 1: For this step, the layout of the argument A1 is as follows. The claim is C1 stated above, i.e. that the present-day ISM is leading to non-compliance of end-users rather than resolving this issue. The ground or data G1 for this claim is that end-users exhibit non-compliance with

information security policies and controls in the organization. The warrants for this argument are as follows:

- W1: End-user behaviour is complex and influenced by the circumstances prevailing in the organization.
- W2: A managerial style based on the principles of scientific management and bureaucracy leads to an unmotivated and uncommitted work-force and a deterioration of the worker-management relationship.
- W3: The present-day approach to ISM is based on the principles of scientific management and is bureaucratic in nature.

The backing to the argument and the warrants is provided by the literature overviews contained in Chapter 2 (W1 regarding end-user behaviour), Chapter 3 (W2 regarding the influence of managerial style) and Chapter 4 (W3 regarding the nature of present-day approach to ISM). The literature overviews present results from the works of various researchers who may be regarded as experts.

One of the possible reservations regarding the claim C1 can be that the present-day approach to ISM may not be the sole or major cause of the non-compliance of end-users with information security policies and controls in the organization; rather the non-compliance may be caused by other factors. In rebuttal to this reservation, it may be stated that the managerial style prevailing in an organization wields an over-arching influence over conditions prevailing in the organization; and that instead of denying the existence of other causal factors, this 'macro' factor incorporates and subsumes other 'micro' factors that may have influence over end-user behaviour.

Step 2: For this step, the layout of the argument A2 is as follows. The claim is C2 stated above, i.e. ISSM will lead to improved compliance of end-users with information security policies and controls in the organization. The ground or data G2 for this claim is claim C1 (i.e. G2=C1) which asserts that the present-day approach to ISM is proving unsuccessful in meeting the challenge of end-user non-compliance. The warrants for this argument are as follows:

- W4: An employee-centric managerial style which is based on the principles of Theory Y of McGregor leads to a motivated and committed work-force and improved worker-management relationship.
- W5: Service management is a philosophy focused on customer satisfaction; it can be applied to internal services focusing on employee satisfaction; ITSM applies the service management approach to IT management in the organization and delivers substantial benefits to the organization.
- W6: Information security shares the IHIP characteristics of services and the concept of service management is applicable to information security management; information security

managed as an internal service with end-users as customers will lead to end-user centric information security and thus to improved levels of compliance.

The backing to the argument and the warrants is provided by the literature overviews contained in Chapter 3 (W4 regarding managerial style), Chapter 5 (W5 regarding service management) and this chapter (W6 regarding information security as a service). The literature overviews present results from the works of various researchers who may be regarded as experts. This chapter further motivates the applicability of service management to information security management.

One of the possible reservations regarding the claim C2 can be that the service management approach may not deliver improved end-user compliance and might consume extra resources for its implementation. In rebuttal to this reservation, it may be stated that argument A2 makes a strong claim C2. As for any other managerial style, the results cannot be guaranteed for ISSM also; however, ISSM is an improvement upon the present-day approach to ISM as it mitigates its shortcoming of not focusing on the end-users.

This section has framed an argument in favour of ISSM. This argument utilizes Toulmin's layout of an argument. The argument consists of claims and supporting grounds and warrants. As stated above, the literature overviews in the previous Chapters 2 to 5 discuss material that can be used to reason towards making a case for ISSM. The next three sections present a firmer reasoning for the argument and discuss the drive towards ISSM in greater detail.

6.3 Arguing for Information Security Service Management

This section first provides a brief summary of the literature overview in Chapters 2 to 5. The section then uses this information to argue in favour of ISSM according to the argument framed in the previous section. As stated earlier, these chapters help illustrate the problem i.e. the weakness of the present-day approach to ISM. These chapters also provide support material for identifying the solution, namely, ISSM. This section concludes by stating that there is an urgent need to both re-conceptualize the end-user in information security and then define an information security management approach based on this re-conceptualization.

The previous section framed the argument as a two-step process. The first step establishes the problem by illustrating the weakness of the present-day approach to ISM in tackling the end-user aspect of information security. The second step establishes ISSM as a solution to this weakness. The previous section also broadly identified the reasoning followed for the argument. This reasoning is discussed below in greater detail.

6.3.1 Arguing for establishing the problem

For this argument, the ground or data is the non-compliance that end-users exhibit in regard to information security policies and controls in the organization. The claim is that the present-day approach to ISM is failing and rather than resolving the end-user issue, it is in fact alienating end-users and exacerbating the issue. The reasoning, based on Chapters 2, 3 and 4, is discussed below.

In an organization, when end-users use information and information systems during the discharge of their day-to-day activities in the organization, they come across a variety of information security tasks. With regard to these information security tasks, end-users display a range of behaviours as they interact with information security policies and controls in the organization. Stanton et al. (2003) define such behaviours as 'behavioural information security' consisting of *"complexes of human action that influence the availability, confidentiality and integrity of information systems"*. Chapter 2 discussed these behaviours and illustrated that end-users in an organization often indulge in unsafe information security behaviours. Chapter 2 also demonstrated that end-users exhibit unsafe behaviours and non-compliance with information security policies and controls under the influence of various factors – sometimes because of a lack of awareness, other times because of a lack of intention and motivation to comply and sometimes because of a lack of skill. Chapter 2 further drew upon other streams of research to illustrate the complexity of human behaviour. According to the discussion in Chapter 2, a confluence of factors determines the final behaviour that an end-user undertakes in a given situation, often leading end-users towards non-compliance. The discussion on human behaviour under risk showed that end-users often have incorrect perceptions of value and risk. End-users, thus fail to develop an appreciation of the information security policies and controls in the organization. This factor is compounded by the existence of human error in the form of slips, lapses, mistakes and violations. Human error is an inescapable aspect of human existence and cannot be eradicated. These errors result from various systemic factors in the organization. The subsequent discussion on loyalty and commitment in Chapter 2 underlined the importance of these factors in determining end-user behaviour. It is shown that 'spurious loyalty' alone is inadequate and that obtaining the 'true loyalty' of end-users should be the objective of information security management. Committed and loyal end-users will be more inclined towards compliance than non-compliance, thereby contributing towards maintaining the effectiveness of information security policies and controls in the organization. Finally, the discussion on the Theory of Planned Behaviour brings together all these factors and shows that the behaviour of end-users regarding information security policies and controls is determined by their attitude, their perception of what others would do in the situation and by their perception of control towards the specific behaviour. Chapter 2 concluded by establishing the multiplicity of factors behind the behaviours of end-users. Typically, under the circumstances prevailing in

organizations, and over time, these factors lead end-users towards insecure behaviour patterns and away from compliance with organizational information security policies and controls.

The rebuttal in the argument A1 in step-1 discussed in the previous section stated that managerial style has over-arching influence over the conditions prevailing in the organization. Since the information security behaviours of end-users in an organization are determined by a multiplicity of factors prevailing in the organization, Chapter 3 probed various management theories and the managerial mental models in an attempt to understand the genesis of these organizational factors. According to the discussion in Chapter 3, the assumptions that managers hold regarding human nature of their employees or workers determine not only their management style but, finally, the behaviour that the employees display. The discussion covered several models of managerial assumptions regarding human nature. Chapter 3 also provided an overview of the various management theories, namely, scientific management, bureaucracy, Theory X and Theory Y. This overview highlighted the problems associated with scientific management and bureaucracy. A key point to emerge from the discussion in Chapter 3 was that the problems associated with scientific management and bureaucracy could be traced back to the implicit model that managers held of their employees. In scientific management, managers believe that their employees can be treated as rational, economic beings whose performance is to be controlled through training, rewards and punishment and who are not to be involved in any decision-making related to the design of their work. The main problems that result include the lack of worker motivation and commitment and deterioration in the worker-management relationship. The problems with bureaucracies include an over-emphasis on rules and procedures; a lack of initiative by employees; impersonal relations in the organization; dependence on bureaucratic status, rules and symbols; and officious bureaucratic behaviour.

As a follow-up to the discussions in Chapters 2 and 3, Chapter 4 probed the role of information security management in influencing the information security behaviours of end-users. The chapter indicated the importance of information security management in establishing, maintaining and improving the state of information security in the organization. Chapter 4 also discussed the evolution of information security over four waves. The four waves of evolution represent the maturing of the information security field. The developments in the field indicate that today technical means and controls along with policies, procedures and guidance in the form of best practices and standards are available for practitioners of information security. Furthermore, the responsibility for information security has escalated from the technical IT staff to the top echelons of the organization. Another important aspect of the maturing of information security has been the realization regarding the importance of user awareness and compliance to the effectiveness of information security. This has led to the development of awareness programs and efforts to create an information security culture in the organization such that information security becomes a way of life for the people in the organization. Chapter 4 concluded by identifying the weaknesses in the present-day approach to ISM. According to the discussion in

Chapter 4, the present-day approach to ISM is based on the principles of scientific management and bureaucracy. The present-day approach to ISM focuses on technical measures and ignores the variability in human behaviour. Further, this approach assumes that end-users are the enemy and need to be controlled. This leads to the vicious circle of bureaucratic information security management (already shown earlier in Figure 6.1). Chapter 4 also indicated the changes required for improving the state of information security management. According to the discussion, the present-day approach to ISM needs to be reoriented from its technical approach to an end-user centric approach.

The above reasoning links the information security behaviours of end-users with the nature and style of the present-day approach of information security management in the organization. The present-day approach to ISM is based on the principles of scientific management and bureaucracy and hence the non-compliance of end-users is to be expected, since it has also been shown that a management style based on the principles of scientific management and bureaucracy leads to similar problems. Consequently, it may be said, that the above reasoning establishes the claim regarding the weakness or problem associated with the present-day approach to ISM. The next sub-section establishes the claim for the solution.

6.3.2 Arguing for establishing the solution of ISSM

For this argument, the ground or data is the claim of the problem established in the previous sub-section, namely, the problem with the present-day approach to ISM in the context of non-compliant information security behaviours of end-users. The claim is that ISSM is will overcome this short-coming and lead to improved compliance by end-users. The reasoning, based on Chapters 3, 4 and 5, is discussed below.

The reasoning behind the claim established in the previous sub-section is that the present-day approach to ISM fails primarily because it is based on the principles of scientific management and bureaucracy and while it is technology-focused, it ignores the end-users. Chapter 3 discussed various management theories and managerial mental models and showed that there are alternatives to scientific management and bureaucracy. These alternatives have a different conception or assumptions on human nature and lead to the creation of improved organizational conditions. Theory Y of McGregor assumes that employees are committed, motivated and willing to take responsibility and these assumptions lead to improved performance and better relationship between management and the employees. Chapter 4 indicated that information security management too could benefit by adopting a different conception of end-users leading to a more end-user centric approach to ISM. Chapter 5 then presented service management as a management approach that is focused on customer satisfaction. The chapter also demonstrated that the concept is applicable to internal services as well in which employees become customers

and service providers to each other. The application of service management to IT Service Management (ITSM) is also discussed. ITSM provides several benefits to the organization. By analogy, it can be said that service management concepts may be fruitfully applied to ISM in the organization. The service management approach to ISM, called Information Security Service Management (ISSM), will be an end-user centric approach to ISM in the organization and will lead to improved commitment of end-users to information security, improved levels of compliance of end-users with information security polices and controls in the organization and to improved relationship between information security managers and end-users in the organization. This leads to the virtuous circle of end-user centric Information Security Service Management (already shown earlier in Figure 6.1). This reasoning establishes the claim of the solution, namely, that ISSM is an improvement over the present-day approach to ISM.

This section has completed the argument framed in the previous section. It has established the two claims set out earlier, namely, that of the problem of present-day ISM and that of the solution in the form of ISSM. This section has established firmly the claim that ISSM will lead to improved compliance of end-users with information security policies and controls in the organization. Consequently, an organization will benefit by adopting ISSM as the approach for information security management. The following sections answer some questions regarding ISSM:

- Can the service management approach be applied to information security management?
- What does it mean to be end-user centric in approach?
- What is ISSM and what does service management mean for ISM?
- How can ISSM be implemented by an organization?

The next section answers the question regarding the applicability of service management to ISM.

6.4 The applicability of service management to information security management

The previous sections have established the credentials of ISSM as an improvement over the present-day approach to ISM. However, the conceptualization of ISSM first requires the question to be answered – can the service management approach be applied to ISM or not? The answer to this question is in the affirmative – this section provides the answer.

It was discussed in Chapter 5 that the service management approach is a management philosophy that can be applied in all kinds of organizations and not just service businesses (Grönroos, 1994). Service management is a total organizational approach and views service from the perspective of the customer (Grönroos, 1990). It was also discussed in Chapter 5 that the service management

approach can be applied to internal services and to ITSM. In both these scenarios, the employees in the organization become both customers and service providers to each other. In service management, organizations become focused on customer satisfaction; similarly, organizations become focused on employee satisfaction in internal services. Similarly, and by analogy, service management approach can be applied to ISM wherein ISM becomes an internal service and the end-users the customers of the information security service. In this approach, the focus of ISM shifts towards the satisfaction of end-users. Further, in section 5.2, services have been described as possessing the distinguishing characteristics of IHIP. The IHIP characteristics stand for intangibility, heterogeneity, inseparability and perishability (x Kotler & Keller, 2006; Lovelock & Gummesson, 2004; Zeithaml, et al., 2008). Information security too possesses the IHIP characteristics and hence can be classified as a service (see Table 6.1). The following discussion describes the IHIP characteristics of information security.

Characteristic	Services	Information Security
Intangible	Services cannot be inventoried, patented, displayed or communicated.	Information security policies and controls are both physically and mentally intangible. This makes it difficult for information security management to advertize and communicate to end-users. End-users find it difficult to define and evaluate information security.
Heterogeneous	Delivery of services depends upon both on provider and customer actions and hence quality of services is variable.	The quality of information security depends upon the successful completion of information security behaviours by end-users. End-user actions are variable and hence the quality of information security is variable.
Inseparable (Production and consumption are inseparable)	Customers participate in and affect the transaction; customers affect each other; employees affect the outcome of services.	End-users are coproducers of the information security service along with information security management.
Perishable	With services, it is difficult to synchronize supply and demand; services cannot be returned or resold.	Appropriate information security behaviours are perishable and need to be reproduced every time.

Table 6.1: IHIP Characteristics of Services and Information Security (based on Parasuraman, Zeithaml & Berry, 1985)

Heterogeneity of services refers to the variation in the quality of services rendered to the customers. This heterogeneity is largely the result of the inherent variability in the interactions between service employees and customers. Both service employees and customers may be under the influence of a multitude of factors, and so the quality of the interaction (or the service) is variable and heterogeneous. Information security too involves the interaction of end-users with policies and controls. End-users bring to bear their own characteristics on this interaction. Their level of awareness and skill, as well as their intention to perform an information security behaviour, and the various contextual factors, all are variables that affect the quality of the end-users' interactions with information security policies and controls. This affects the perception of the quality of information security policies and controls. Thus, it can be said that information security possesses the characteristic of heterogeneity.

Inseparability refers to the involvement of customers in the production of services. In services, customers participate actively in the production process; they become co-producers or partial employees and work is transferred from the provider to the customer. Information security too requires the active participation of end-users in the operation of policies and controls. Information security policies and controls require the end-users to participate and complete the necessary information security behaviours. Thus, it can be said that information security possesses the characteristic of inseparability.

Perishability of services implies that services cannot be saved, stored, resold or returned. This means that whenever the service is to be produced, a new interaction will have to occur between the service provider and the customer, along with all the inherent vagaries. Information security too requires a new interaction between end-users and policies and controls to occur whenever the service is to be produced. A good interaction, i.e. an appropriate instance of an information security behaviour, cannot be saved for later use. In this sense, information security possesses the characteristic of perishability.

The above discussion has indicated the 'service' nature of information security. Information security possesses the IHIP characteristics and can thus be treated as a service. This service nature of information security leads to certain challenges for information security management. Intangibility of information security implies that information security management will find it difficult to advertise or communicate about information security to the end-users. Further, the intangibility ensures that end-users too find it difficult to evaluate and appreciate information security. The heterogeneity of information security implies that information security management will find it difficult to control the quality of interactions between end-users and policies and controls. This, in turn, will lead to variable quality of information security in the organization. Whereas, information security managers are able to control the quality of policies and controls, the quality depends to a large extent on end-users over whom the information

security managers have no control. Inseparability and perishability too pose problems for information security managers. Inseparability implies that information security managers have to understand the co-production role of end-users. The information security managers have to realize that by designing or formulating information security policies and controls, they perform only half the task of completing information security behaviours. The remaining part is completed by end-users as they interact with policies and controls and undertake the necessary actions. Furthermore, not only do end-users thus act as co-producers, but their own satisfaction with policies and controls depends upon this interaction. Finally, these behaviours are perishable and cannot be inventoried. Hence, these behaviours have to be produced every time they are needed.

This section has discussed the applicability of service management approach to ISM. Information security possesses the IHIP characteristics of services. Further, information security can be managed as an internal service with end-users as the customers. The discussion also identified several challenges for ISM. These challenges are intrinsic to information security; ISSM can offer a way to meet these challenges. The primary method for meeting these challenges is end-user centricity. The next section discusses what it means for ISM to be end-user centric.

6.5 The end-user centricity of ISSM – the CARE Principles

In the introduction to this Chapter, the vicious and virtuous circles of information security management were presented. The two circles can be combined as shown in Figure 6.4. According to this figure, depending upon their assumption regarding the nature of end-users in the organization, information security managers create the information security management systems (ISMS) and its constituent information security policies and controls. The nature of the ISMS, and specifically its constituent policies and controls, creates a psychological and behavioural climate in the organization that can either promote commitment and compliance by end-users or drive them towards disenchantment and non-compliance. The end-users are affected by the surrounding climate and the available policies and controls. Finally, the end-users demonstrate either compliance or non-compliance and this feeds back and reinforces the assumptions that information security managers hold about their nature. As can be seen from Figure 6.4, the genesis of both circles lies in the view that information security managers in the organization hold regarding the nature of end-users in the organization.

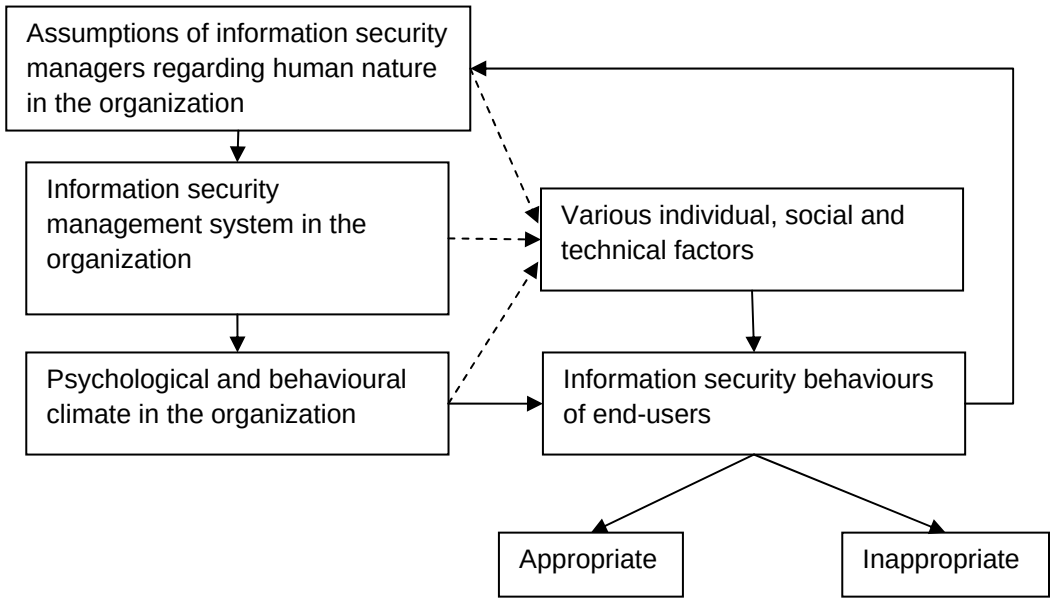


Figure 6.4: Influence of managerial assumptions of human nature upon the information security behaviours of end-users

The present-day approach to ISM has a blinkered view of end-users. In this view, present-day information security management in organizations is still focused on technology; end-users are the enemy and are treated merely as adjuncts to this technology. Furthermore, end-users can be motivated towards compliance through training, rewards and punishment. Information security is further improved and enhanced through enforcing stronger policies and controls. The information security efforts are based on the assumption that end-users behave as 'homo economicus'. But as shown earlier in Chapter 2, this assumption is false, and consequently, information security efforts are liable to fail. Currently, efforts to motivate end-users are directed towards their rational and calculative side. However, when it comes to information security behaviours, end-users are motivated by a complex set of factors including commitment and loyalty, social norms, perceptions of control, heuristics, habits etc. Thus, an incorrect conception of end-users directs, or rather misdirects, present-day information security management in the organization which is unable to yield improved end-user compliance with information security policies and controls in the organization.

The end-user centric approach of ISSM requires information security managers to re-conceptualize the notion of end-users in the organization. In this re-conceptualization, end-users are not the enemy but an invaluable asset in securing information in the organization; end-users

are knowledgeable about their information needs and practices, and the inherent business risks in these practices. Furthermore, given the right environment and tools, end-users would rather comply than not comply with information security policies and controls in the organization; end-users can be held responsible for only a few insecure acts, most other insecure acts can be traced back to earlier decisions concerning the formulation and implementation of information security policies and controls in the organization. Thus, while the actions (or inactions) of end-users may be the immediate cause of non-compliance, the non-compliance actually originates from other organizational and systemic factors created by decisions made by other people such as information security managers, designers, developers, IT managers, business managers, etc.

In the end-user centric approach, the focus of information security managers shifts from *compliance* to *commitment* of end-users to information security policies and controls in the organization. This shift occurs with information security managers adopting the CARE principles (Figure 6.5). The CARE principles, as the name suggests, ensure that end-users are handled with due care. The remainder of this section discusses the CARE principles.

The CARE principles are as follows:

- **C**ommunicate with end-users: to win their commitment to information security policies and controls, to give them the required skills and to learn and understand their practices and needs.
- **A**ccommodate the end-user perspective: to formulate the information security policies and controls around the practices and needs of end-users and to provide them with the tools required for doing their primary work tasks in a secure manner.
- **Re**spond to the difficulties experienced by end-users: to provide support to end-users as they navigate through the maze of information security policies and controls.

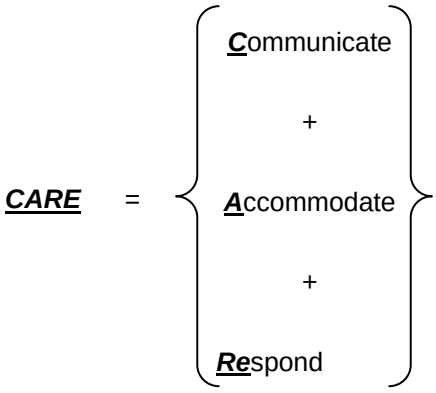


Figure 6.5: The CARE principles

Communication provides the link between end-users and information security management and enables the exchange of information between the information security management and end-users. This communication allows the concerns of management and the limitations of technology to be conveyed to the end-users while escalating their issues and needs to business, IT and information security managers. Traditionally, information security managers have used communication uni-directionally i.e. to deliver expert-driven information to end-users. This information consists of awareness and training guidance. Information security managers are the providers, while end-users are the consumers of this information. The purpose of this communication is to inform the end-users about the information security policies and controls and to give them the skills required to successfully complete their information security tasks. The CARE principles redefine the scope and purpose of communication. The communication is bi-directional and it is as much driven by experts as by the end-users. In addition to the above mentioned purpose of communication, the CARE principles enhance the purpose of communication to learn about users and to provide them with a forum to voice their concerns and needs and to share their experiences. In the CARE principles, the objectives of communication are to win the commitment of end-users to information security and to allow information security managers to learn about the practices, needs and concerns of end-users.

In the present-day approach to ISM, policies and controls are designed or formulated on the basis of risk analysis related to the information assets of the organization. End-users are expected to comply and modify their day-to-day working practices, as required. According to the 'Accommodate' element of the CARE principles, the traditional design approach is enhanced to ensure that information security policies and controls are built around the practices and behaviours of end-users, including the prevailing culture and social practices in the organization. The main objective of the 'Accommodate' element is to minimize the conflict between the information security policies and controls and the day-to-day practices of end-users. Another objective is to ensure that information security policies and controls are easy to understand and use. However, it may not always be possible to accommodate all end-user requirements. Einstein said, *"Make everything as simple as possible, but not simpler"*. Likewise, end-user practices can be accommodated only to a certain point. Beyond this point, the practices take the organization into the area of unacceptable risk, where the practice needs to be curbed. In this situation, the 'Communicate' and 'Respond' elements are expected to combine to resolve the issue.

The last element of the CARE principles is the 'Respond' element. During their day-to-day life in the organization, end-users come across the information security policies and controls as they interact with information and information systems in the organization. The end-users' willingness to undertake their information security tasks and their ability to complete these tasks, both are influenced by their perception of the level of difficulty of the tasks. Also, past experience of difficulty may prompt the end-users to ignore their information security tasks. Thus, it is imperative to provide adequate support to the end-users in an on-going manner. The

'Respond' element of the CARE principles embodies this support. The 'Respond' element requires that the organization creates a support function consisting of support-employees. The support-employees interact with the end-users on a regular basis and help and advise them in the conduct of their information security tasks. End-users should find it convenient to contact the support-employees in case of any difficulty or doubt. The conduct of the support-employees should be such as to make the end-users feel comfortable in seeking help. The objective of the support function is to give comfort and confidence to end-users and to assist them in the conduct of their information security behaviours.

This section has discussed the end-user centric approach of ISSM. The basis for this approach is the re-conceptualization of the notion of end-users in information security. End-users are to be treated as partners rather than as enemies to be controlled. This view of end-users negates the bureaucratic style of present-day information security management and paves the way for a service management approach for end-user centric information security management based upon the CARE principles. The following two sections will discuss ISSM in greater detail and how the service management approach is utilized to implement the CARE principles.

6.6 Information Security Service Management

As previous discussions have shown, present-day information security management has two urgent needs: firstly, to revamp its blinkered view of end-users as the enemy, and secondly, to develop an end-user centric approach to information security management based on this revamped view of end-users. The previous section discussed the re-conceptualization of the notion of end-users and delineated the CARE principles for meeting the needs of end-users. This section describes Information Security Service Management (ISSM) as the new end-user centric approach to information security management based on the CARE principles.

ISSM is the application of the service management approach to information security management in the organization. In keeping with the customer-centric approach of service management, ISSM entails a shift in focus from the formulation and enforcement of security policies and controls towards the satisfaction of the customers of the information security service. This shift is aimed at obtaining long-term commitment and loyalty of end-users to the organizational information security policies and controls, which in turn will lead to improved compliance. ISSM becomes an internal service consisting of information security service managers and staff that provide information security service to their customers. The customers are the end-users in the organization.

As stated in section 5.3, service management is a management philosophy accompanied by a shift from being concerned with the internal consequences of performance to the external

consequences from the customers' perspective. The service management approach differs from the focus of traditional management in the following ways (Grönroos, 1990):

(1) From product-based utility to total quality utility in the customer relationship.
(2) From short-term transactions to long-term relationships.
(3) From core product (goods or services) quality or the mere technical quality of the outcome to total customer-perceived quality in enduring customer relationships.
(4) From production of the technical quality of products (goods or services) as the key process in the organization to developing and managing total utility and total quality as the key process.

Similarly, ISSM too differs from present-day information security management in terms of the philosophy of its approach towards end-users and information security policies and controls. The present-day approach to ISM focuses on the strength and coverage of information security policies and controls over information assets, while it ignores the needs and the requirements of the end-users. ISSM shifts this focus to the consequences and the impact that these policies and controls have on end-users, their psychological state of commitment to information security and their information security behaviours; the focus shifts from controlling and restricting end-users to enabling end-users to complete their day-to-day work in a secure manner. Similar to the shifts mentioned by Grönroos (1990) as stated above, the shifts that occur in ISSM are:

(1) Form product-based utility to total quality utility in the customer relationship: it is unrealistic to believe that information security policies and controls alone will deliver information security to the organization; rather, the end-users are to be seen as partners and their commitment as key to information security in the organization. This entails a shift in focus from compliance to commitment.
(2) From short-term transactions to long-term relationships: it is not sufficient to focus only on the formulation and deployment of information security policies and controls; rather, it is more important to provide ongoing training, support, and reformulation etc. to the end-users.
(3) From core product (goods or services) quality or the mere technical quality of the outcome to total customer-perceived quality in enduring customer relationships: it is no longer sufficient to focus only on the strength and coverage of information security policies and controls; rather, it is more important to focus on the effects of these policies and controls on end-users, their working practices, their psychological state and their behaviours.
(4) From the production of the technical quality of products (goods or services) as the key process in the organization to developing and managing total utility and total quality as the key process: in present-day ISM, the key processes include risk analysis and formulation of information security policies and controls; in ISSM the key processes should include the total management of the end-user aspect of information security, in terms of the CARE principles stated earlier.

Section 5.4 also stated the principles of service management as formulated by Grönroos (1990 and 2007). These principles reflect the shifts in traditional management along six dimensions: (1) the business logic and driver of profit; (2) decision-making authority; (3) organizational focus; (4) supervisory control; (5) reward systems and (6) monitoring and measurement of tasks and achievements. The application of these principles to ISSM is discussed below (see also Table 6.2).

- **Business logic and driver of profit.** In the present-day approach to information security management, the business logic is considered only through the lens of protecting the information assets of the organization. The security of information assets become of primary importance. Various kinds of information security policies and controls are formulated and implemented in the organization to maintain the security properties of the information assets. End-users are expected to comply at the risk of punitive measures for non-compliance. The business logic is very much a top-down and 'control-based' approach. In contrast, the business logic of ISSM is 'commitment-based'. It is focused not just on formulating security policies and controls, but the ISSM function sees itself as providing a complete support system to its customers, i.e. the end-users. The ISSM approach is based on the belief that satisfied and loyal end-users will lead to a more effective state of information security in the organization and that the user satisfaction is derived from the service experience or the users' encounters with the information security service. In the ISSM approach, factors such as costs, strength of security architecture, efficiency of operations etc. become secondary to the user experience.
- **Organizational focus.** In conjunction with the new business logic, the organizational focus of ISSM shifts from formulating security policies and controls to establishing, maintaining and continuously enhancing the relationships with its customers and partners i.e. the end-users and the managements of business and IT. ISSM must also initiate a feedback loop between all these segments, thereby ensuring that each segment understands and appreciates each others' views on Information Security. With the IT Management and end-users, understanding their needs and converting them to the Business Management's view on information security become crucial. At the same time, Business Management's views on information security must be informed about the perspectives of IT Management and those of end-users. For ISSM, obtaining end-user commitment to the organization's information security policies and controls becomes top priority. This necessitates not just communication of the organization's policies to end-users but also communicating and incorporating the end-users' needs and perspective into the security policies and controls.

Dimension	Principle of Service Management	Principle applied to Information Security Service Management (ISSM)
The business logic	Managing customer relationships and customer perceived quality are critically important to success. Interest in cost and productivity become secondary.	ISSM realizes that formulation and enforcement of security policies and controls are insufficient for effective security. Managing relationships and obtaining long-term commitment of Business Management, IT Management and end-users are seen as critical to success.
Decision-making authority	Employees are empowered, encouraged, and trained, to solve problems following from deviations from standard procedures so that customer satisfaction is created.	Maintaining a state of "lock-down" is not the sole purpose of Information Security staff. Staff must understand that their responsibility is to provide support to the users to enable them to understand and work with security policies and controls.
Organizational Focus	Focus shifts away from structure and control procedures to process and customer perceived quality.	ISSM realizes that customer perceives quality not by the technical strength of security controls and technical competence of staff. ISSM realizes that customer perceives quality on the basis of his/her experience in dealing with security policies and controls and the behaviour of the security support staff.
Supervisory Control (or rather Supervisory Support)	Supervisory focus has to be on encouragement and enablement of employees so they can deliver quality service.	ISSM has to encourage not just its own staff but also end-users to practice secure behaviour. Regular training and feedback sessions are crucial. Both staff and end-users must understand and appreciate each other's compulsions.
Reward Systems	Efforts at producing customer perceived excellence are rewarded rather than compliance to predetermined standards.	User satisfaction rating of security and security staff is considered more important than the traditional security metrics such as number of patched systems, number of viruses stopped etc.
Measurement Focus	The primary variable to be measured becomes customer satisfaction with service quality.	The primary variable to be measured is user satisfaction. Metrics, such as number of patched systems, number of viruses stopped etc., become secondary.

Table 6.2: Principles of Service Management applied to Information Security Service Management (ISSM)

- **Decision-making authority.** The shifts in business logic and organization focus lead to a shift in decision making. In the ISSM approach, the information security function no longer merely consists of security architects and experts, but also end-user facing support personnel. Decision-making occurs at both levels – at the level of formulation and deployment of information security policies and controls, and also at the level of providing support to the end-users. These support personnel must not only be trained to understand the information security policies and controls, but must also be empowered to use their discretion in helping the end-users navigate through these policies and controls. These personnel also understand the crucial role of their own behaviour when dealing with the end-users. Appropriate technology may also be used to make it easy for end-users to seek help and enable the support personnel to provide friendly and efficient service.
- **Supervisory control, reward systems and measurement focus.** The supervisory control, reward system and measurement focus are all geared to ensure that the ISSM function delivers on the end-user centric directions provided by the business logic and the organizational focus. For example, in the ISSM approach, the role of supervisors is not so much to control the support personnel, as to enable and empower them in maintaining relationships with the end-users. The reward system and the measurement focus should also reflect this focus on end-user relationships and satisfaction. The reward system does not reward maintaining an adequate level of 'lock-down', but it rewards excellence in end-user service. Measurement focus is then on customer perceived quality based on their experiences with the security policies, controls, support personnel and the rest of the ISSM function.

ISSM leads to several benefits as compared with the present-day approach to information security management. A vital outcome of ISSM is that the vicious circle of bureaucratic ISM is converted to the virtuous circle of ISSM. The resulting benefits and outcomes that ISSM hopes to achieve include: a user-centric approach to information security; formulation of information security policies that support the day-to-day activities of end-users, and hence, are more amenable; end-user friendly policies and controls; improved commitment of end-users to information security efforts in the organization; reduced incidence of end-user violations and errors related to the information security policies and controls; improved levels of compliance; and finally, a more effective state of information security in the organization.

This section has discussed ISSM and what service management means for ISM. The next section will provide more details on how ISSM can be implemented in an organization.

6.7 Implementing ISSM in the organization

The previous sections have delineated the CARE principles, the re-conceptualization of the notion of end-user in information security and ISSM as the service management approach for end-user centric information security management in the organization. This section brings all these elements together in the form of the ISSMCube in order to indicate how ISSM can be implemented in the organization. The next three chapters provide further details of the three components of ISSM.

March and Smith (1995) stated that a model is a representation of reality. According to Hevner et al. (2004), a model is a combination of constructs that aids in the understanding of a problem and its solution. March and Smith (1995) also contrasted the term 'model' with 'theory' – whereas a model is concerned with utility, a theory is concerned with truth. Since utility, and not truth, is the chief concern of models, March and Smith (1995) state that a model can be silent or inaccurate about the details, but it must be a useful representation. In this sense, the ISSMCube is a model that depicts the various issues associated with ISSM and serves the utility of understanding and guiding the implementation of ISSM in the organization.

The six faces of the ISSMCube are shown in Figure 6.6 (parts a and b).

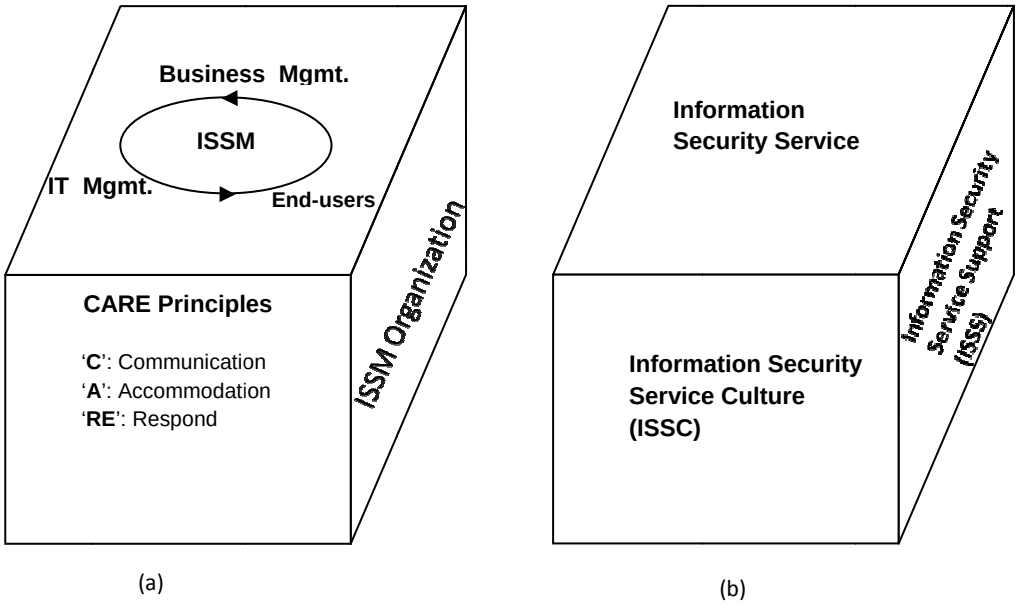


Figure 6.6: The six faces of the ISSMCube [parts (a) and (b)]

These faces, discussed later, are as follows:

(1) The CARE Principles.
(2) The position of ISSM in the organization in the midst of Business Management, IT Management and end-users in the organization.
(3) The internal organization of ISSM so as to be able to deliver information security as a service.
(4) Information Security Service Branding (ISSB).
(5) Information Security Service Culture (ISSC).
(6) Information Security Service Support (ISSS).

The 'CARE' principles. these principles define the essence of ISSM and serve as its foundation. The role of the CARE principles as the foundation of ISSM is shown in Figure 6.7. The CARE principles guide the implementation of ISSM ensuring the delivery of an end-user centric information security management to the organization which is in tune with the re-conceptualization of the notion of an end-user as discussed earlier. Adherence to the principles ensures institutionalization of the human aspect of information security in the organization.

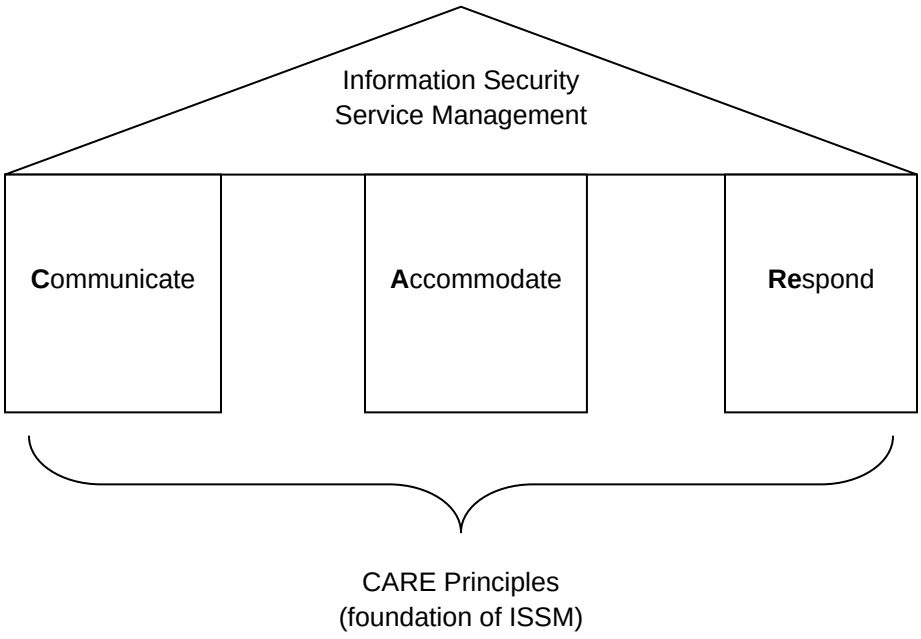


Figure 6.7: The CARE principles as foundation of ISSM

The position of ISSM in the organization. ISSM lies in the organization in the midst of Business Management, IT Management and end-users in the organization. These are the stakeholders in information security and they are linked together by ISSM in a web of relationships. This face depicts the importance of the partnership between the stakeholders in delivering effective information security to the organization. Unless, there is agreement and alignment amongst the stakeholders regarding the primacy of the end-user in information security, ISSM cannot be successfully implemented. ISSM links all these stakeholders in an ongoing process of interaction. The role of business management is to provide the directives to establish the strategic importance of information security for the organization and to ensure that all stakeholders combine together to implement the end-user centric nature of information security. Business management also plays a vital role in helping develop a culture of information security in the organization. IT management has to ensure that the IT facilities deployed in the organization are end-user centric and provide a secure environment for the day-to-day work of the end-users. The end-users on their part have to be committed to information security in the organization and engage with the process of information security management in the organization. The role of ISSM is to establish and maintain the partner relationships with business management, IT management and end-users. Figure 6.8 indicates the web of relationships between business management, IT management, end-users and Information Security Service Management.

The ISSM organization. This face represents the internal organization of the ISSM function. The internal organization is vital as it is the instrument for the implementation of the service management approach. As stated in the previous section, the adoption of a service management approach requires shifts in the six dimensions of the internal organization, namely, the business logic, decision-making authority, organizational focus, supervisory control, reward systems and measurement focus. These shifts institutionalize the implementation of ISSM in the organization. The ISSM organization requires new structures and processes in order to implement the three components of ISSM. These components are discussed below.

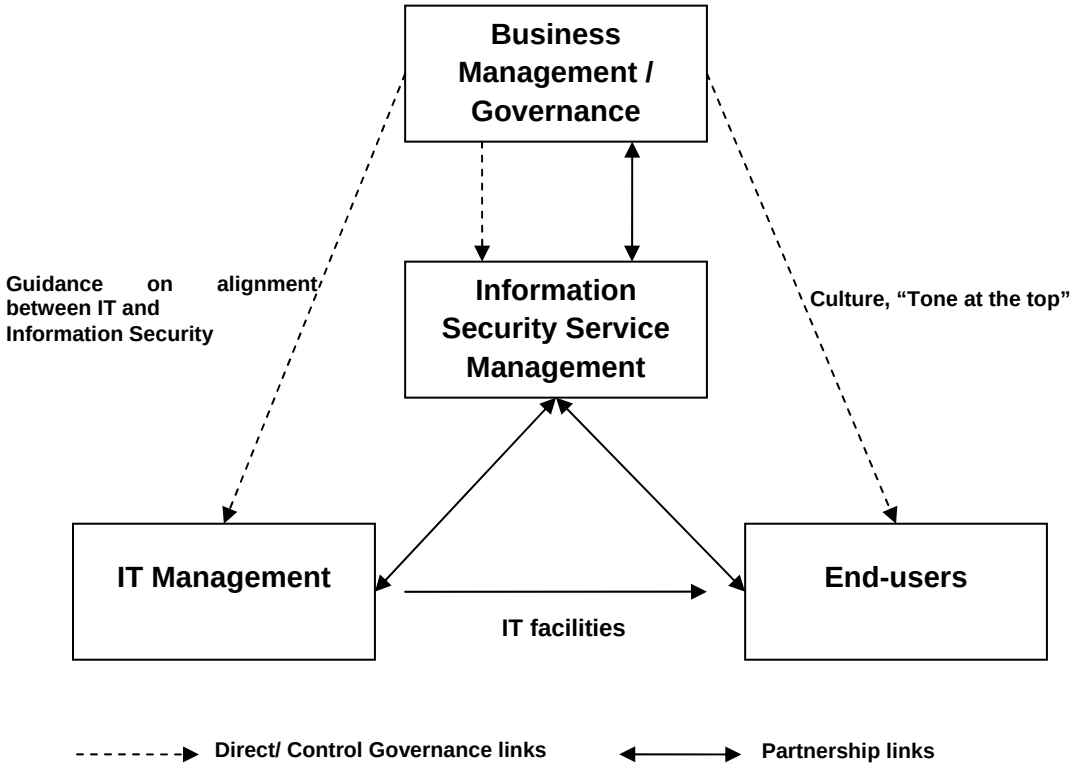


Figure 6.8: The web of ISSM relationships

The three components of ISSM – ISSB, ISSC and ISSS. ISSM implements the CARE principles via three components. These components are Information Security Service Branding (ISSB), Information Security Service Culture (ISSC) and Information Security Service Support (ISSS) and they are shown in Figure 6.6 (b).

- Information Security Service Branding (ISSB) that 'wins' the hearts of end-users for information security. The purpose of branding is to create a positive image for information security in the minds of end-users and thereby to evoke commitment in the end-users to information security in the organization. This also includes branding research that provides information on end-user behaviour so as to fine-tune ISS Management's perceptions of end-users and their behaviours. ISSM is end-user centric and needs to understand the practices, needs and requirements of the end-users in the organization.
- Information Security Service Culture (ISSC) leads to the formulation of information security policies and controls in active coordination with the end-users. This ensures that policies and controls are built around end-user behaviours and practices. This component also manages the web of relationships or partnerships of ISSM so as to enable successful delivery of ISSM.

- Information Security Service Support (ISSS) that provides assistance to the end-users in their interaction with information security policies and controls. This eases the interactions between the end-users and the information security policies and controls, and supports the end-users in successfully undertaking and completing their information security tasks.

These components work together in synergy to deliver end-user centric information security management to the organization. End-user centricity is achieved throughout the cycle of use of information security:

- Information security policies and controls are designed in an end-user centric manner.
- Efforts are made to evoke a positive image for information security in the hearts of end-users so as to obtain their commitment and compliance.
- Finally, when end-users attempt to complete their information security tasks, they are supported and guided in their efforts.

The interaction of these components is shown in Figure 6.9. These components will be discussed in greater detail in the subsequent chapters.

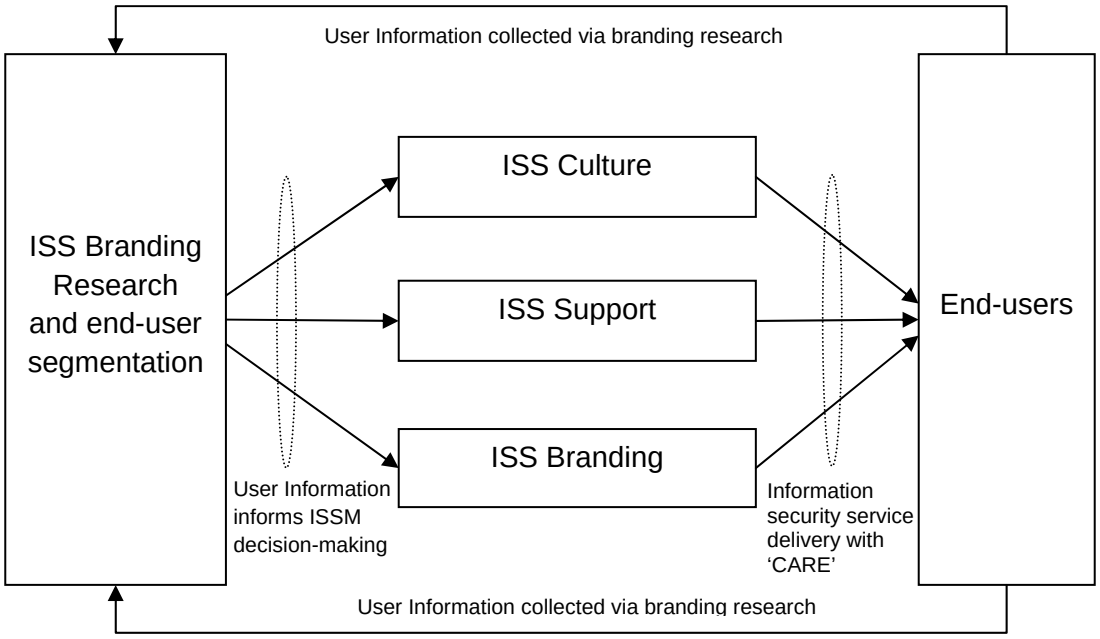


Figure 6.9: Culture, Support and Branding of the Information Security Service

6.8 Conclusion

This chapter began with a quote from Mahatma Gandhi underlining the importance of customers to the organization. The quote served another important purpose – that of highlighting the weakness of the 'end-users are the enemy' mind-set in information security. This is the dominant mind-set of information security managers and prevents present-day ISM from realizing effective information security in the organization; in fact it may be said that non-compliance results from the bureaucratic nature of present-day ISM. From the discussions in the previous chapters, it has emerged that employee behaviour is to a large extent determined by the managerial assumptions regarding the human nature of employees in the organization. Consequently, if one wants to improve employee behaviour in the organization, then one has to improve the managerial assumptions which lead to improved management systems. In the context of information security, this means that to improve the information security behaviours of the end-users, it is firstly necessary to re-conceptualize the notion of the end-user and then provide an end-user centric information security management system. This chapter then proceeded to delineate the 'CARE' principles and ISSM as the answer to these two issues. This chapter further discussed the ISSMCube as the model for implementing ISSM in the organization. ISSM consists of the components of ISS Branding, ISS Culture and ISS Support. Together and working in synergy, these components ensure that ISSM delivers an end-user centric information security service to the organization. These components will be discussed further in subsequent chapters.

CHAPTER 7

Information Security Service Branding – a question of image

"A favorable and well-known image, overall company image and/or local image, is an asset to any firm, because image has an impact on customer perceptions of the communications and operations of the firm in many respects".

- Grönroos (2007)

"One significant challenge is the image of security, in the sense that no one ever really encounters it for a good reason".

- Chipperfield & Furnell (2010)

7.1 Introduction

Chapter 6 presented the CARE principles. These principles serve as the foundation of Information Security Service Management (ISSM). The CARE principles embody the essence of a human-centric approach to information security in the organization. The CARE principles consist of 'Communicate', 'Accommodate' and 'Respond' elements. The 'Communicate' element of the CARE principles embodies the need of communicating to end-users. The objective of this communication is to win the commitment of end-users to information security in the organization. This principle will be the focus of this chapter.

Organizations use branding as a communication tool to establish the identity of the organization or a product in the minds of consumers. Likewise, ISSM utilizes Information Security Service Branding (ISSB) as a communication tool to establish the information security service brand in the minds of its consumers, namely, the end-users in the organization. In this way, ISSB implements the 'Communicate' function. Typically, as stated by Chipperfield and Furnell (2010), *"many people do not find security to be a naturally exciting or engaging topic, and it is therefore unrealistic to expect that the mere mention of its name will automatically drum up much enthusiasm"*. Thus, as discussed later, information security has a neutral or negative image

in the minds of most end-users. This image influences all exchanges and interactions between information security and end-users in the organization. The negative image of information security reduces the effectiveness of all other information security efforts. ISSB attempts to reverse this image leading to a positive image of information security in the organization. Branding is also required because ISSM is very different from the traditional approaches to information security management, particularly in its focus on the end-users.

As discussed in the previous chapter, ISSM implements the CARE principles through its components, namely, Information Security Service Branding (ISSB), Information Security Service Culture (ISSC) and Information Security Service Support (ISSS). ISSB performs the function of the branding of information security, as discussed above. Branding is an overarching concept and requires that all activities of an organization should be integrated and consistent with the espoused brand. In this sense, branding subsumes all activities of the organization, both internal as well as customer-facing. Thus, it can be said that ISSB subsumes ISSC and ISSS. However, for the purpose of this thesis, ISSB is restricted to the creation of a brand image through communication with the end-users; the other aspects are covered through ISSC and ISSS and will be discussed in subsequent chapters.

Information security awareness (ISA) is already an important communication tool used by information security management in organizations to influence end-users. However, as discussed later in section 7.5, ISA limits itself to a concentration on raising awareness, knowledge and skill levels of end-users; ISA does not focus on repairing the problems caused by the negative image of information security. In this sense, ISSB is complementary to ISA; in fact, if ISSB is considered as the overarching concept mentioned above, ISA may be said to be a part of ISSB. For the purpose of this thesis, ISSB is discussed only from the perspective of creating a positive image of information security; thus, ISSB may be said to exist in addition to, and as a complement of ISA efforts in the organization.

This chapter is organized as follows. The next section discusses the question of image and how this image is important for information security in the organization. The subsequent section discusses the negative image of information security in the perception of end-users in the organization. Then the chapter discusses what a positive image of information security could be. This discussion is followed by an overview of the literature on traditional approaches to ISA. ISA as a communication tool is accorded great importance in information security management. However, this undeniable importance of ISA is simultaneously accompanied by its inability to correct the negative image of information security and gain end-user commitment. The subsequent section provides an overview of branding in the business domain. Finally, the chapter describes ISSB and provides a process for its implementation in the organization.

7.2 The question of image

According to Grönroos (2007), the positive image of an organization is an asset for the organization. The image has an impact on how customers perceive the communications and operations of the organization. Grönroos (2007) says that image has the following impacts on customers: the image creates expectations and it also acts as a filter influencing perceptions. The image of the organization exists in the minds of its customers. This image combines with the other communication, or marketing, and operational efforts of the organization. The image is based on the past and it influences how customers evaluate the organization in the present and in the future. A positive image increases the effectiveness of the communications by the organization by making the customers more receptive. A negative image has the opposite effect, while a neutral image has no impact. The image also acts as a filter through which customers perceive the performance of the organization. A positive image acts as a shelter. Due to this sheltering effect, customers can often overlook minor, and sometimes even serious, performance issues with the organization. On the contrary, a negative or an unfavourable image results in performance issues further reinforcing the negative perception of customers. Customers having a negative image feel more dissatisfied and angrier at performance problems, than they would otherwise.

In the context of information security in the organization, it may be said that information security in the organization occupies a queer space. While information security needs the active co-operation from end-users, it is crippled by the negative perceptions of end-users regarding information security. This negative image will be discussed further in the next section, and it suffices for this section to state that most end-users have a negative image, while some end-users, at best, have a neutral image. Consequently, following on from Grönroos (2007), the negative image has a debilitating impact on the efforts of the organization to achieve the cooperation of end-users; thus the cooperation of end-users is not readily forthcoming. This negative image of information security is spawned by the experiences that end-users have as they interact with information security management and information security policies and controls in the organization. So, while information security depends upon the end-users for its effectiveness, information security is unable to win the end-user's commitment and cooperation. This, in turn, leads to non-compliance as end-users intentionally ignore or bypass information security policies and controls (Adams & Sasse, 1999; Dhillon, 2001b; Dourish et al., 2004). This sets up the queer space for information security in the organization. To remain effective, information security in the organization needs to resolve the tension in the queer space (see Fig. 7.1).

Figure 7.1: The queer space of information security in the organization

In the context of the queer space, the question for information security management in the organization becomes one of creating a positive image for itself in the eyes of the end-users. This positive image will create a fertile ground for information security – not only will end-users be emotionally committed to information security, but they will also be more receptive to other information security efforts such as awareness campaigns and information dissemination. Furthermore, the sheltering effect will make them overlook any difficulties with information security.

The answer to the issue of creating a positive image for information security can be found in the concept of branding. In the domain of business, branding operates by creating images in the minds of customers (Keller, 2001). This image can be said to consist of *"a cluster of values that enables a promise to be made about a unique and welcomed experience"* (De Chernatony, 2009). Brands provide several benefits to the firm. These include greater customer loyalty, increased effectiveness of marketing communication, less vulnerability to competitors, and greater customer tolerance of any glitches (Kapferer, 2008; Keller, 2001).

In the context of information security in the organization, branding would refer to the creation of a positive image of information security in the minds of the end-users. Similar to the benefits that branding provides to businesses, the positive image of information security in the organization should translate into benefits that would include greater end-user loyalty and compliance with information security policies and controls; increased effectiveness of awareness, training and education campaigns; reduced vulnerability of end-users to opportunistic behaviour and non-compliance, together with greater tolerance of lack of usability and imperfections of information security policies and controls (see Figure 7.2). Thus, it is worthwhile to utilize the principles of branding to create a positive image of information security in the minds of the end-users in the organization.

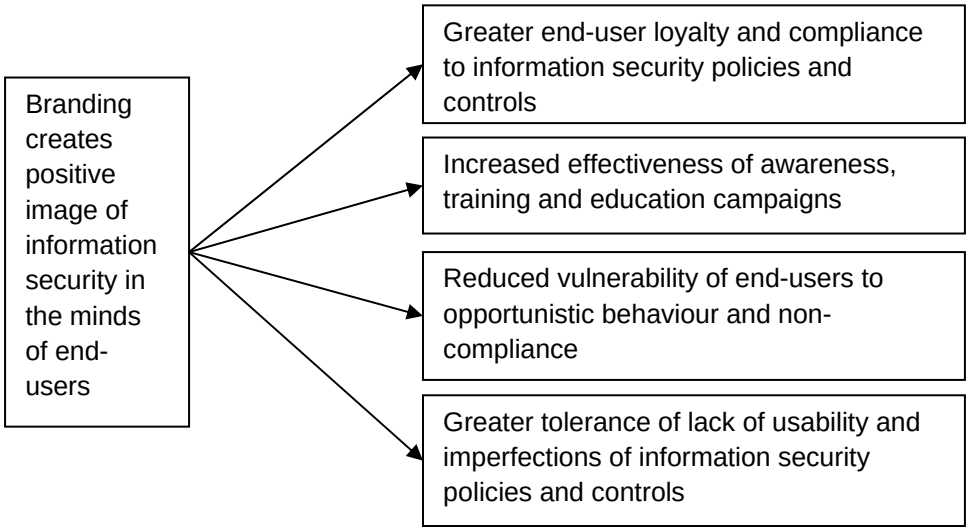


Figure 7.2: Benefits of branding for information security

Before discussing ISSB, it is important to understand the negative image of information security in the organization and the reasons for it. The next section discusses the negative image of information security in the organization. The subsequent section discusses what a possible positive image for information security might be.

7.3 The negative image of information security in the organization

Information and information technology (IT) are believed to provide significant advantages to organizations. These advantages are posited upon diverse capabilities for acquiring, processing and sharing information. Some of the buzzwords for IT are flexibility, collaboration, information sharing, just-in-time, sense-and-respond, etc. Against IT and its advantages, information security, with its policies, controls and restrictions, comes in as a poor second. With developments in IT, the situation has only worsened over the years. Nearly two decades ago, Baskerville (1993) stated that restrictions imposed by information security are detrimental to the spontaneity provided by IT. More recently, Chipperfield and Furnell (2010) echo the same sentiment when they state that information security is not something that end-users want on their own; according to the authors, end-users continue to find information security policies and controls as time consuming, inconvenient and generally an obstacle in getting their work done. In this context, end-users, more often than not, develop a negative image of information security (Chipperfield & Furnell, 2010). This leads to a resistance towards information security and an inclination to

readily switch to insecure behaviours (Adams & Sasse, 1999; Albrechtsen, 2007; Besnard & Arief, 2004; Chipperfield & Furnell, 2010; Dourish et al., 2004; Whitten & Tygar, 1999).

Albrechtsen (2006) states that end-users' perception of information security is shaped by organizational, technological and individual factors. These factors include the trade-offs made during day-to-day work; the existence of social norms and the interactions between individuals; the quality of information security management; the technological solutions implemented; and individual factors such as knowledge, attitudes, values, risk perceptions, etc. The remainder of this section discusses the negative image of information security in the organization along the axes of: security as an obstacle or hindrance to work; the delegation of security responsibility or 'security is not my responsibility'; and negative views on information security management (or managers).

7.3.1 Security as an obstacle or hindrance to work

The first and foremost problem that information security creates for the end-users is that it gets in their way when completing their day-to-day activities. Post and Kagan (2006) state that restricting access to information and IT systems can lead to interference in the completion of end-user activities. The authors label the restrictions as 'security hindrances' that represent the problems faced by the end-users since such security procedures and controls interfere with their work. In such situations, security is often sacrificed in the pursuit of work (Desouza & Vanapalli, 2005).

The primary task for most end-users is to complete their day-to-day business activities; security is only a secondary activity. According to Whitten and Tygar (1999), this leads to the 'unmotivated user property' of security in which the end-users optimistically, and often mistakenly, assume that security is working; further, if complying with security is too difficult or annoying, then end-users simply give up trying to comply. Often, the end-users develop their own ways and means for compliance which may have the side-effect of weakening the control, e.g. writing down passwords (Adams & Sasse, 1999).

Sometimes, information security policies and controls may be inappropriate for the way in which certain activities or tasks are conducted in the organization, or in certain end-user groups. Adams and Sasse (1999) stated that while individual password ownership is a best practice, it is incompatible with group work in organizations.

It is also possible that restrictions imposed by information security may be unacceptable to end-users and these may lead to a creation of a feeling of animosity towards information security. The monitoring of access or restrictions on Internet access may be unacceptable to end-users and

they may feel that these are unfair and overly restrictive. Monitoring may cause the end-users to feel threatened and lead to a loss of trust (Adams & Sasse, 1999).

Frequently, the risk perceptions of end-users may not be aligned with the risk perceptions of the organization. In this situation, end-users may feel that controls and restrictions are unnecessary. While sharing passwords or confidential information with colleagues, end-users may not appreciate the risks that could well arise from these acts; and therefore, they will tend to ignore the controls and restrictions on these practices.

7.3.2 Delegation of security responsibility or 'security is not my responsibility'

According to Dourish et al. (2004), end-users, in the course of their day-to-day activities, may abdicate their security responsibilities and delegate them to other entities such as technology or the organization. After the abdication and delegation of security responsibility, end-users continue with their day-to-day work without caring about information security and without making any additional effort required to enforce information security.

7.3.3 Negative views on information security management (or managers).

Albrechtsen and Hovden (2009) state that there is a *"digital divide"* between end-users and information security managers in the organization. End-users perceive information security managers as invisible and unapproachable and this has made it difficult to report problems or to ask questions. Furthermore, the security documentation is usually overly technical in nature; the content is poorly presented; and the tone of the documentation is admonitory and puts end-users off. Because of these difficulties, end-users often give up on reading the security documentation and continue with low levels of awareness.

This section has highlighted the negative perception of information security in the eyes of end-users in the organization. End-users form a variety of such images. These images are shaped by how end-users experience information security and its management in the organization. The images refer to information security as an obstacle, as a low priority activity, as unnecessary, as intrusive, as unapproachable, etc. Because of this, end-users continue to remain indifferent to information security in the organization. The focus of this chapter is on ISS Branding as a tool to counter this negativity. But before ISS Branding can address this problem, it is important to identify and discuss what a positive image for information security should be. This is the subject of the next section.

7.4 Identifying a positive image for information security in the organization

As stated earlier in Chapter 1, information security suffers from two problems. The first problem is with regard to the negative perception of end-users by information security managers. The second problem is the flip side to the first, i.e. the negative perception of information security in the organization in the minds of the end-users. The cure for the problem of effective information security in the organization lies in correcting both the negative images. Information Security Service Management (ISSM) is based on a positive conception of end-users, i.e. information security managers believe that end-users want to practise secure behaviours; any non-compliance is the result of a vast variety of factors largely beyond the control of the individual. ISSM, thus, resolves the first problem. This friendlier version of information security needs to be both communicated to end-users and appreciated by them in order to resolve the second problem. This section identifies the desirable components of the positive image of information security in the organization.

The positive image of information security should undo the negative image. As discussed in the previous section, the negative image consists of the negative experiences of end-users with information security: as an obstacle or hindrance, as "not my responsibility" and as information security managers being uncaring and unapproachable. The positive image must therefore consist of: security is desirable, "it is my responsibility" and information security managers are there to help and support. Table 7.1 provides a comparison of the negative image of information security as it exists with the desirable positive image that needs to be created in the minds of end-users in the organization.

The image of information security in the organization undergoes a change – the change in perception is from "I don't need security; it is not my job; management doesn't care about me" to "I need to be secure and I want security; it is my responsibility to safeguard security; management is there to help and support me". As stated earlier and shown in Figure 7.2, the positive image of information security will offer several benefits to information security in the organization. A positive image is bound to lead to greater commitment to information security, greater acceptance of information security policies and controls and greater levels of effort towards compliance.

Negative image of information security in the minds of end-users in the organization (as it exists today)	Positive image of information security in the minds of end-users in the organization (as it is to be projected)
I don't need security; it is difficult; it is something that creates problems for me and prevents me from doing my work.	Security is something I need; it is simple and used by my colleagues; it helps me do my work while reducing risks; it helps me stay free of losses, problems and liability.
It is not my responsibility.	It is my responsibility to stay secure.
Information security management does not care for me; I don't know them.	Business management, IT management and information security management are all there to support me and help me stay secure. The information security policies and controls are designed around my practices and use of information.

Table 7.1: Comparison of the negative and positive image of information security in the minds of end-users in the organization

The previous section highlighted the point that information security conjures up a negative image in the minds of the end-users. This section has provided a desirable positive image of information security which is consistent with ISSM. The next section provides an overview of information security awareness and how it fails to create a positive image of information security in the minds of end-users in the organization.

7.5 Information security awareness

This section discusses information security awareness (ISA). ISA is a vital communication tool used by organizations to influence end-users to comply with information security policies and controls in the organization. ISA operates by improving the awareness of end-users on information security issues, giving them the requisite training and skills and also by enhancing their overall understanding of the principles of information security. However, ISA has tended to ignore the question of image of information security in the minds of end-users in the

organization. The following sub-sections discuss ISA, its importance in the organization and its lack of attention to image correction for information security.

7.6 Information security awareness – its role and importance

Various international information security standards and guidelines have emphasized the value of ISA to the effectiveness of information security policies and controls in the organization. According to ISO/IEC 27002:2005 (ISO/IEC 27002, 2005), if end-users are not made aware of their security responsibilities, they remain unmotivated and unreliable and can cause information security incidents leading to considerable damage to an organization.

ISO/IEC 27001:2005 (ISO/IEC 27001, 2005) states that the ISA control consists of ensuring that all end-users, whether employees or contractors or other third party end-users, receive *"appropriate awareness training and regular updates in organizational policies and procedures, as relevant for their job function"*. According to ISO/IEC 27002:2005, the ISA activities should also include information on known threats, who to contact for further security advice and the proper channels for reporting information security incidents.

ISO/IEC 27002:2005 (ISO/IEC 27002, 2005) states that information security awareness, education and training are common practices and that this control applies to most organizations and in most environments. According to the standard, ISA, along with the marketing of information security and the dissemination of guidance on information security policy and standards within the organization are some of the critical success factors for the implementation of information security in the organization. ISO/IEC 27002:2005 (ISO/IEC 27002, 2005) underlines the importance of ISA by stating the following:

- The information security policy document should mention the security education, training, and awareness requirements;
- Management of the organization should initiate plans and programs to maintain information security awareness;
- Various functions in the organization should cooperate and coordinate their efforts to ensure effective promotion of information security education, training and awareness throughout the organization;
- It is the responsibility of the management of the organization to ensure that all end-users, whether employees, contractors or third party users are properly briefed on their information security roles and responsibilities; are provided with guidelines to state security expectations of their role within the organization; are motivated to fulfill the security policies of the organization; and achieve a level of awareness on security relevant to their roles and responsibilities within the organization.

ISO/IEC 27002:2005 (ISO/IEC 27002, 2005) also provides implementation guidance for ISA. According to this standard, ISA should begin with a formal induction process that introduces the end-users to the organization's security policies and expectations before the end-users are granted access to information or services. This induction process should be complemented by an ongoing ISA program disseminating information regarding security requirements, legal responsibilities, business controls, and the disciplinary process as well as training in the correct use of information processing facilities.

According to another standard GAISP V3.0 (ISSA, 2003), the purpose of ISA is to inform end-users regarding the 'acceptable use' principles and practices that lead to the protection of the information assets of the organization. GAISP V3.0 lists the *"Awareness Principle"* as one of the *"Pervasive Principles"*. This principle states that all end-users in an organization should have *"access to applied or available principles, standards, conventions, or mechanisms for the security of information and information systems"*. Furthermore, these end-users should be *"informed of applicable threats to the security of information"*. GAISP V3.0 underlines the importance of ISA by stating that enhanced awareness leads to improved levels of acceptance of controls; otherwise end-users may be tempted to ignore, bypass or overcome the existing controls. GAISP V3.0 also lists *"Education and Training"* as one of its *"Broad Functional Principles"*. According to this principle, the management in an organization should ensure that all end-users are educated about *"standards, baselines, procedures, guidelines, responsibilities, related enforcement measures, and consequences of failure to comply"*. A failure to communicate effectively can lead to the following implications: unintentional and intentional breaches by end-users. Furthermore, this failure may limit the organization's ability for enforcement, prosecution of criminal activity and the opportunity to seek legal redress.

Thomson and Von Solms (1998) stated that ISA is a program to educate, and continually remind, end-users regarding information security issues. According to the authors, the ISA program should be designed to change both the attitudes and the behaviour of the end-users to ensure that their actions are security conscious. Thomson and Von Solms (1998) highlight the issue that rapid changes in business and information technology are reducing the effectiveness of physical and technical controls and that these controls alone are not sufficient. Thus, for effective information security, it is necessary to educate end-users and change their behaviour to such an extent that security actions become part of their sub-conscious. According to Thomson and Von Solms (1998), changes in attitude are more likely to result in long-term and durable behaviour change. Consequently, the ISA methodology should first use persuasion in an attempt to change attitudes before proceeding to attempt any direct changes in behaviour. Thomson and Von Solms (1998) proceeded to state that end-user 'acceptance' of the message is an antecedent for attitude change; and for this 'acceptance' to occur, the ISA program must be tailored to the characteristics of the audience.

Siponen (2000) states that 'information security awareness' refers to *"a state where users in an organization are aware of – ideally committed to – their security mission"*. According to the author, ISA is of *"crucial importance"*. Siponen (2000) elaborates on the point that awareness includes education and training. Education enhances end-users' insight into information security issues; training imparts them the skills and competence to perform in accordance with information security policies and controls in the organization.

Du Plessis and Von Solms (2002) state that the effectiveness of information security in the organization depends to a large extent upon end-users. Consequently, end-users need to be educated on the importance of their role and how to behave in order to fulfill this role, so as to protect the information assets of their organization. According to the authors, ISA consists of *"making users aware of their responsibilities in securing the information technology environment and motivating them to do so"*. The content of the ISA program should include topics on the *"importance of information and information security"*, *"threats to and vulnerabilities of computer systems"*, *"information security policy"* and *"specific procedures and how to implement them"* (Du Plessis & Von Solms, 2002).

According to Wipawayangkool (2009), organizations no longer focus on writing formal policies; rather, organizations today focus on applying these policies via the building of an informal culture. This is achieved through ISA, which is a fundamental and critical factor for the effectiveness of ISM in the organization. According to the author, ISA has two key dimensions, namely, *"to understand"* and *"to act"*. Trainee progression along these two dimensions ensures that: the trainee learns all the principles of key knowledge of information security (cognitive aspect); the trainee develops optimistic attitudes towards both specific content in training sessions and generic concepts of security (affective aspect); and the trainee ultimately learns to act in a secure manner (skills aspect). Thus, ISA equips the trainee both with knowledge and the capability to act in compliance with information security policies and controls in the organization.

ISA is accorded great importance by various international standards, guidelines and academic authors. These standards, guidelines and authors also delineate the content of ISA and the ways and means by which ISA programs provide their benefits to the organization. However, several authors have also mentioned the weaknesses in present ISA approaches and they have pointed out the failure of ISA in delivering its promised benefits to the organization. The next sub-section discusses this aspect of ISA.

7.6.1 Information security awareness – its weaknesses

Various authors have written about the weaknesses in present-day ISA approaches. These weaknesses stem mainly from the simplistic approach to the link between ISA and the improved information security behaviour of end-users in the organization.

According to Siponen (2000), most organizations treat ISA as consisting of *"passing around security guidelines in a factual manner"*. In this approach, it is futile to believe that *"after a security awareness lesson people will all follow the guidelines at once"*. The author further states that people may respond to ISA in a positive manner leading to *"readjustment, co-operation, acceptance and internalization"*; a negative response may result in *"repulsiveness or hate, even leading to different kinds of resistance"*. Siponen (2000) concludes that an ISA approach based on the mere dissemination of information is bound to fail.

Albrechtsen (2007) states that most organizations conduct ISA as *"expert-based one-way communication directed towards many receivers"*. This approach to ISA is futile and most end-users tend to remain unaffected. Sometimes, ISA programs include gifts as incentives. Such programs too tend to fail as end-users remember only the gift, while they forget the message. Albrechtsen (2007) further cites the poverty of such communication as it fails in motivating end-users to seek security related information even when they are aware of its availability.

Chipperfield and Furnell (2010) state that the most common approach to ISA in the organization is to provide documented security policy to end-users. The authors cite the failure of such methods of promotion. According to the authors, the SafeBoot survey (Grant, 2007) shows that nearly 80% of public sector employees ignore information security policies and exhibit insecure behaviour. The simplistic view towards ISA is that end-users simply need to be told, i.e. made aware of various facts and, in return, end-users will simply comply. This approach has a negative impact as it leads end-users to regard policies *"as an overhead in terms of being just another thing to be read and remembered"*.

To tide over the weaknesses of present-day ISA approaches, various authors have proposed using a 'promotion' or 'selling' or 'marketing' approach to ISA (Chipperfield & Furnell, 2010; Stewart, 2009). These approaches are inspired by the principles of marketing from the business domain. According to Stewart (2009), marketing approaches promise a holistic approach to ISA. This concept is not new and Siponen (2000) cites Perry (1985) as proposing an approach that makes information security an *"in topic (fashionable and everybody-wants-to-use-it) within an organization"*. Siponen (2000) also cites McLean (1992) as proposing a 'selling' approach in which campaigns are used to promote information security in the organization. According to Siponen (2000), such approaches need to be used with care and cannot be considered as achieving the commitment of end-users to information security in the organization.

Weaknesses in the present-day approaches to ISA have been highlighted in this section. The main weakness is the assumption of a simplistic link between end-users being told and then complying. The next sub-section takes this discussion further by indicating the lack of consideration of the image of information security in the minds of end-users in the organization.

7.6.2 Information security awareness – its lack of focus on image

The previous two sub-sections have discussed the role and importance of ISA in the organization and the inherent weaknesses in the present approaches to ISA. This sub-section takes this discussion further. This sub-section indicates the lack of focus of present ISA approaches on improving the image of information security in the minds of end-users in the organization.

As discussed earlier in previous sections, information security suffers from a negative image in the minds of end-users in the organization. Earlier sections have also discussed the importance of image as a perceptional filter that influences the effectiveness of all communication and operational efforts of the organization. Against this backdrop, it is vital to stress that communication efforts in the organization should first focus on creating, or correcting, a positive image for information security in the minds of end-users in the organization. Instead, ISA has tended to focus on educating end-users to make them capable of behaving in accordance with information security policies and controls in the organization. ISA approaches have continued to ignore the antecedent for their effectiveness, namely, the image aspect. Even the selling or marketing approaches have addressed ISA in terms of the benefits, incentives or rewards and direct one-to-one communication – such approaches have not yet addressed the image issue. Thus, the failure of ISA approaches to achieve behavioural change, and hence the criticism in the previous sub-section, is not entirely unexpected.

The role, importance and weaknesses of present ISA approaches have been discussed in this section. It is vital to recognize that while ISA is considered to have significant benefits for the organization, it continues to suffer from weaknesses that limit the benefits it delivers. This section has concluded by suggesting that the failure of present ISA approaches lies in the fact that they tend to ignore the image aspect. The discussion in this chapter has so far emphasized the critical role of image regarding information security in the organization. Hence, it can be argued, that ISA efforts need to be enhanced with efforts targeted at improving the image of information security in the minds of end-users. Towards this end, branding, from the domain of marketing in business, is a useful concept. Branding is focused on creating a favourable image in the minds of customers. Likewise, in the context of information security in the organization, branding holds promise for creating a positive image of information security in the minds the of end-users in the organization. These branding efforts constitute Information Security Service

Branding (ISSB) and they will complement the existing ISA efforts in the organization. The concept of branding is discussed in the next section.

7.7 Brands and Branding

The American Marketing Association defines a brand as *"a name, term, design, symbol, or any other feature that identifies one seller's good or service as distinct from those of other sellers. The legal term for brand is trademark. A brand may identify one item, a family of items, or all items of that seller. If used for the firm as a whole, the preferred term is trade name"* (AMA, 2010a). AMA (2010a) also provides an associated definition of a brand as a *"customer experience represented by a collection of images and ideas; often, it refers to a symbol such as a name, logo, slogan, and design scheme"*. According to these definitions, the brand operates by identifying a seller's good or service, and by helping consumers discern between goods or services from different sellers. Hence the brand operates by identification and differentiation. However, these definitions emphasize brand attributes such as logos, colour and design. But, a brand is much more than its representative logo or symbol and, according to De Chernatony (2009) such an emphasis betrays a lack of branding sophistication. Further, in the context of services, Grönroos (2007) posits two objections to the AMA (2009) definition of brand. According to Grönroos (2007), the definition ignores the process characteristics of service and it also excludes the vital role of customers in branding.

The next sub-section will discuss the image aspect of a brand. As an image, a brand always exists in the minds of consumers, whether an organization/firm explicitly attempts to create one or not. The subsequent sub-section discusses branding as a process used by organizations/firms to create a brand.

7.7.1 The image aspect of a brand

Various authors have elucidated the image aspect of a brand through defining associated terms such as 'brand image', 'brand meaning' and 'brand personality'. Understanding a brand as an image, Keller (1993) defines 'brand image' as *"perceptions about a brand as reflected by the brand associations held in consumer memory"*. The image is shaped by both product-related and non-product related attributes, where the non-product related attributes result from a consumer's own experience with the brand and his/her contact with other brand users. Chiaravalle and Schenk (2007) also define 'brand image' as *"the set of beliefs about what your brand is and what it stands for that exist in the customer's mind as a result of associations with you and your name"*. Berry (2000) defines 'brand meaning' as *"what comes immediately to consumers'*

minds" when the brand is mentioned. Aaker (1997) associates human characteristics with a brand under the term 'brand personality'. Brand personality shows what kind of person the brand would be if it were human (Kapferer, 2008). These human traits are sincerity, excitement, competence, sophistication and ruggedness (Aaker, 1997). Keller (1993) says that customer-based brand equity results when the customer holds favourable, unique and strong brand associations in memory. This brand equity may be positive or negative and it reflects the marketing advantage the brand holds over an unnamed or fictitiously named competitor (Berry, 2000). A brand can also be described as a *"cluster of values"* (De Chernatony, 2009), and as a promise to the customer regarding future performance, satisfaction, benefits, value etc. (Berry, 2000; Chiaravalle & Schenk 2007; Mintz & Chan, 2009).

From the above discussion, it becomes evident that a brand is much more than the logo, colour and design of the symbols that represent it. A brand is an image that comes to the mind of a customer when he/she sees or hears about a product or service. This image is built upon the customer's own experiences and communications from the organization or from other customers. The next sub-section discusses how a brand is created.

7.7.2 Branding – creating a brand

Grönroos (2007) says that *"if anybody builds a brand, it is the customer"*. According to Grönroos (2007), customers play a critical role in the creation of a brand – since it is an image in their minds, it is the customer's perception of experiences, communications, word-of-mouth etc. that creates the image and thus, the brand. This brand creation happens as customers interpret brand messages consciously or unconsciously on a continuous basis. Thus, it can be said that the brand exists at the interface between the firm's activities and the customer's interpretations and perceptions of those activities.

The relationship between a firm's activities and the creation of brand as an image in the minds of the consumers is shown in Figure 7.3 (based on De Chernatony & Dall'Olmo Riley, 1998a). The firm's activities are performed by its employees and these are in the form of promises regarding functional and emotional attributes of the product or service. Consumers interpret these promises based on their own experiences with the product or service, together with other communications; and an image or personality for the brand is, thus, created in their minds. This image, then, serves as shorthand for referring to the brand and drives the consumer's purchase decisions.

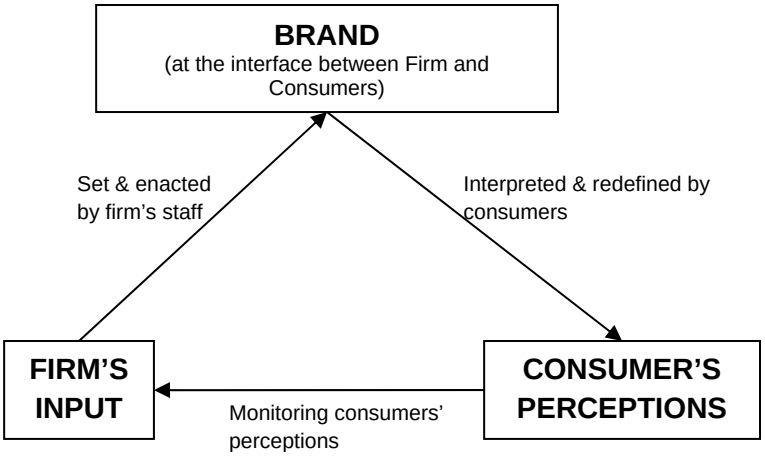


Figure 7.3: The BRAND Construct (based on de Chernatony and Dall'Olmo Riley, 1998a)

While it can be said that a brand is ultimately created by customers, an organization too may make a more deliberate effort to create a brand. However, this is, at best, only an attempt. Grönroos (2007) uses the term 'brand identity' to denote the image that the organization/firm wants to create – it is the target to be achieved. Grönroos (2007) further defines branding as the process of creating the image or brand. Keller (1998), states that branding involves attaching a 'label' (for identification) and a 'meaning' to a product, service, person, idea, etc. In this sense, branding involves first creating a label and a meaning and then communicating that to the consumers.

Service-branding model of Berry (2000). Berry (2000) presents a model for the branding of services, as shown in Figure 7.4 (from Berry, 2000). In Berry's (2000) model, several components of a service brand are involved. The inputs to the branding process are: the presented brand, external brand communications and customer experiences with the service.

The first input to the branding process is the presented brand. This refers to the organization's purposeful communication of its identity through various means such as advertising, service facilities and the appearance of service providers. This input makes use of brand attributes such as colour, logo, design etc. which establish the label attached to the brand. The next input is external brand communications. These refer to the messages customers receive regarding the organization and its service. These messages are not controlled by the organization and originate from external sources such as word-of-mouth from other customers. The final input to the branding process is the direct experience that customers have with the organization and the service. This input too is not controlled by the organization.

The combined inputs lead to the creation of 'brand awareness' and 'brand meaning' in the minds of the customers. Brand awareness refers to the customer's awareness of the brand and their ability to both recognize and recall the brand. Brand meaning refers to the image aspect of the brand and is the *"snapshot impression"* that comes to mind when the customer is reminded of the brand. In the service-branding model of Berry (2000), the inputs relate to brand awareness and brand meaning as follows:

- Brand awareness: the presented brand has a primary influence on brand awareness; external brand communications also influence brand awareness.
- Brand meaning: customer experience with the organization or service have a primary influence on brand meaning; external brand communications also influence brand meaning.

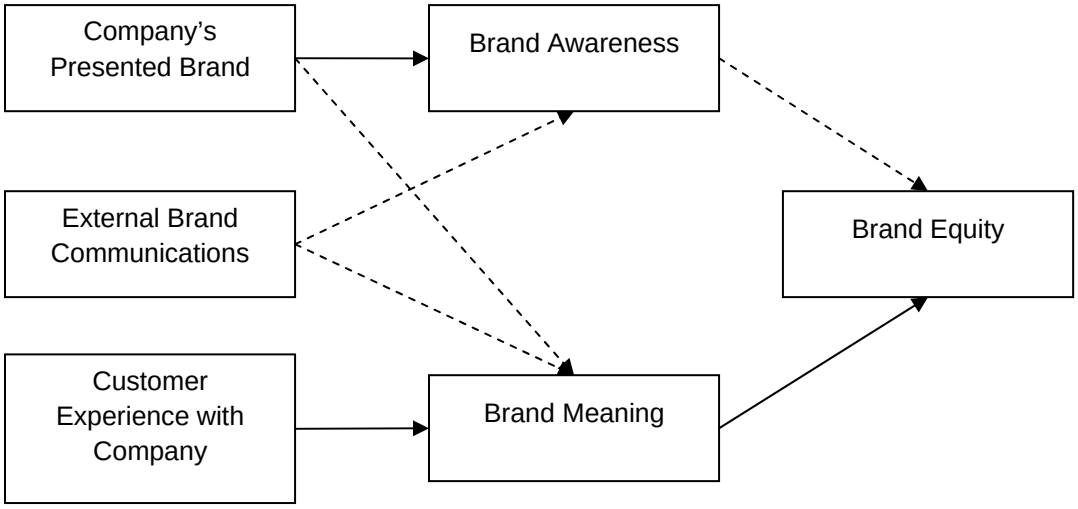


Figure 7.4: Service Branding Model (from Berry, 2000)

Brand awareness and meaning combine to create brand equity. Brand equity is the advantage that an organization gains because of the brand. Brand equity can be positive or negative. Positive brand equity results in an advantage. Negative brand equity results in a disadvantage for the organization. Brand equity is more influenced by brand meaning than by brand awareness.

Berry (2000) states that strong brands are built by brand distinctiveness and message consistency, by delivering on the core service, by connecting emotionally with customers and by creating trust in the brand. The four steps that the branding process follows are: dare to be different, determine your own fame, make an emotional connection and internalize the brand. In

this model, employees of the company play a vital role making or breaking the service brand as they deliver service to the customers. Positive service experiences lead to the creation of a strong brand whereas negative service experience erodes the brand.

Customer based brand equity (CBBE) from Keller (1993, 2001, 2008). Keller's model is based on building brand equity by taking customers over the rungs of the 'branding ladder'. Progression up the branding ladder represents increasing levels of customer commitment to the brand. The branding process is shown in Figure 7.5 (from Keller, 2001). Moving up the rungs on the 'branding ladder' takes the branding process from identity to meaning to responses to relationships. Each rung builds on top of the lower rung. These rungs are constructed from six brand-building blocks, namely, salience, performance, imagery, judgments, feelings and resonance. At the first rung, the branding process creates brand salience which refers to creating deep and broad brand awareness. Brand salience affects how customers recognize and recall the brand. The next rung is of brand meaning. Brand meaning refers to establishing an image in the minds of customers regarding the brand's characteristics. These characteristics are in terms of functional, performance-related considerations, as well as more abstract, image-related considerations. The brand image is created through customers' own experiences with the brand and through various forms of communication (e.g. advertising, word-of-mouth etc.). An important aspect of the image is the 'brand personality' that becomes associated with the brand in the customers' minds. At the third rung, brand responses refer to the judgments and feelings that customers develop towards the brand. Judgments are driven by the 'head' whereas feelings are driven by the 'heart'. At the top of the branding ladder, brand resonance refers to the deep, psychological bond customers develop with the brand. Brand resonance consists of four categories, namely, behavioural loyalty, attitudinal attachment, sense of community and active engagement. Keller's (2001) branding process results in creating strong customer brand equity whereby firms achieve resonance with their customers and reap the benefits that branding offers.

The concept of branding from the domain of marketing has been discussed in this section. A brand refers not just to the logo, colour and design of symbols representing it; the brand refers to the image that is formed in the minds of its customers regarding the products or services represented by the brand. In view of the importance of their brand, organizations need to work consciously towards creating their brand. Two models for branding were also discussed, namely, the service-branding model of Berry (2000) and the CBBE model of Keller (2001). Both models demonstrate that simple brand awareness is not sufficient to lead to customer loyalty. Brand image, brand meaning, customer feelings towards the brand etc. are all important antecedents of customer loyalty – in the absence of these factors, awareness alone seldom works. This reinforces the discussion in the previous section in which it was stated that the weaknesses of present ISA efforts in the organization have resulted from their focus only on the awareness of the end-users. Present ISA efforts continue to ignore the image issues much to the detriment of information security in the organization. The next section discusses Information Security Service

Branding (ISSB). ISSB seeks to address this shortcoming and provides a framework for branding information security in the organization.

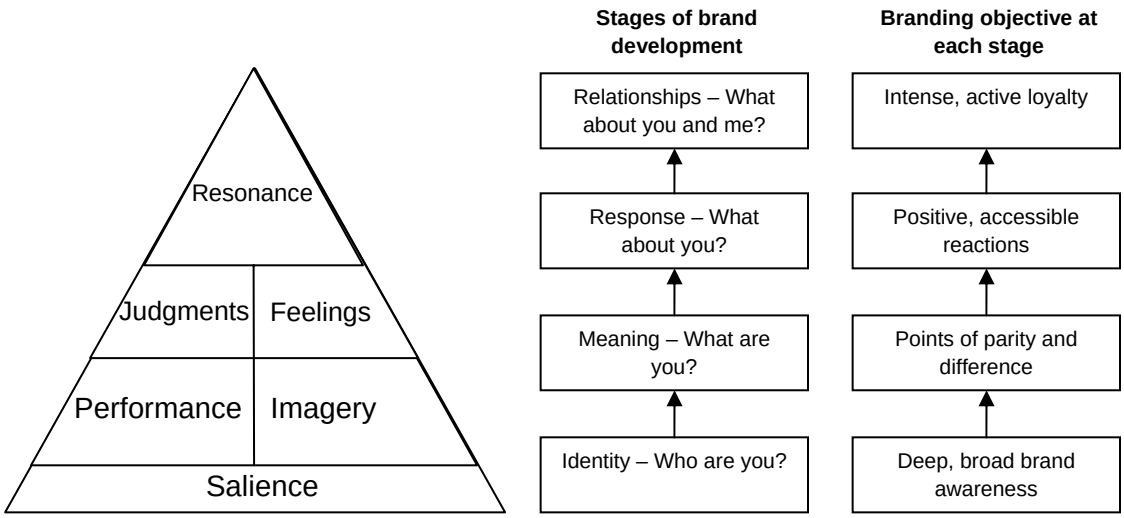


Figure 7.5: Customer Based Brand Equity Pyramid (from Keller, 2001 & 2008)

7.8 Information Security Service Branding in the Organization

In the previous section, it was mentioned that a brand always exists in the minds of its customers, whether the organization does any branding or not. In a similar vein, in the context of information security in the organization, it may be said that end-users always carry an image of information security in their mind. This is the brand image or brand meaning of information security in the organization; this image exists regardless of whether the organization attempts deliberate branding or not.

Previous sections have already discussed the negative image of information security in the organization. Information security in an organization typically evokes contempt from the end-users, particularly when it is juxtaposed against IT and information. Whereas end-users credit information and IT with providing them various benefits, they often see information security as a hindrance to their work and as not being their responsibility. End-users further have a negative opinion about information security management. Thus, it would not be inaccurate to say that information security has a negative brand image amongst the end-users in almost any

organization. This negative image reduces the effectiveness of all communications and of operational efforts in the organization to achieve effective information security. Information Security Service Branding (ISSB) represents a deliberate attempt by ISSM to reverse these negative perceptions and to create a positive brand image for information security. The remainder of this section describes the Information Security Service Branding process.

In the service-branding model of Berry (2000), brand equity is built through the company's communication of the presented brand, through publicity and word-of-mouth communication to customers, and through customer experiences of the service. ISSB applies this branding process to information security. Thus, the ISSB process proceeds as follows:

(1) Define the information security service brand.
(2) Communicate the brand to end-users, including using word-of-mouth communication to strengthen the information security service brand.
(3) Internalize the brand and organize to deliver security service consistent with the information security service brand.
(4) Monitor end-user characteristics and their perception of the information security service brand and use this information to modify the branding efforts

The ISSB process is depicted in Figure 7.6. Each of the above steps is discussed in greater detail below. In the organization, Information Security Service Management executes the ISSB process. This process culminates in the creation of the information security service brand as an image in the minds of the end-users. This image is influenced by the definition and communication of the brand as well as by the delivery of the service. The image that is created in the minds of end-users may not be the one promoted. Hence, it is necessary that the image of the information security service brand be regularly monitored to gauge the success of the ISSB process as well to serve as feedback for suitably modifying brand definition, communication and service delivery.

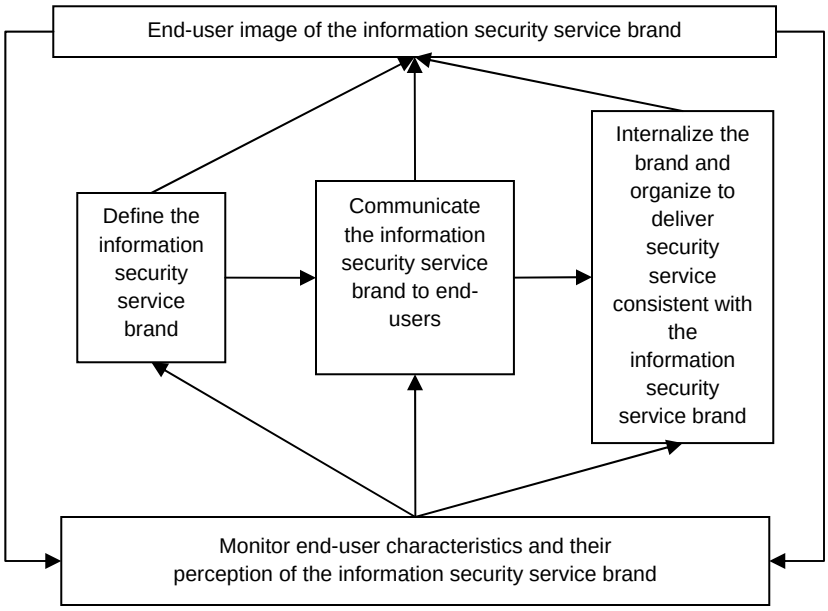


Figure 7.6: Information Security Service Branding process

7.8.1 Defining the Information Security Service Brand

Defining the brand is the first step in the ISSB process. It refers to identifying how ISSM wants to be perceived by end-users in the organization i.e. what snapshot impression, image, meaning or personality should come to the mind of end-users when they are reminded of information security.

Information Security Service Management is an approach focused on end-users and it is based on the CARE principles. The brand image or meaning should be consistent with the end-user focus of ISSM. As discussed in an earlier section, end-users tend to have a negative image of information security in which they see information security as an obstacle or hindrance; as not their responsibility and in which they find information security management as being invisible and coercive. To reverse this image, the information security brand should be defined so that it evokes a feeling of trust and confidence in information security management; so that end-users feel that security is in their own interests and, consequently, their responsibility too.

Traditionally, information security has focused on the technical aspects of information security. In terms of branding it may be said, that the traditional focus has been on the functional characteristics or brand performance rather than on any emotional characteristics or brand

imagery. Since the very nature of information security is that it is neither permanent nor perfect, functional characteristics can only be emphasized to a limited extent. Focusing on the emotional characteristics or imagery of information security may be more worthwhile. In this context, the emphasis could be on the extent of top management commitment, investments and resource allocations towards information security in the organization. The information security service brand could also emphasize the caring and concern that the organization shows for the information security needs and issues of end-users. The brand could project a personality of warmth, friendliness, sincerity, competence, responsiveness, etc. In conclusion, the end-users' snapshot impression of the information security service brand should be one of competence, sincerity and care.

7.8.2 Communicating the brand to end-users

Communicating the brand to end-users requires the creation of deep and broad brand awareness. Keller (2001) calls this brand salience. The depth of brand awareness refers to how easily customers can recall or recognize the brand. Breadth refers to the variety of situations which the customers are able to relate to the brand. In the context of information security in the organization, it may be said that information security must be in the top of the mind of end-users and end-users must be able to recall or recognize information security issues, policies and controls. Furthermore, end-users should be able to relate to information security issues whenever they deal with information or information technology or other potentially risky situations, e.g. while handling finances in the organization.

Communicating the brand requires:

- Identifying labels to be attached to the brand i.e. populating the logo, colour, design etc. attributes of the brand. This could also include using a slogan for the brand.
- Communicating the brand through a variety of channels and media to the target end-user audience.
- Communicating in a way so as to achieve both depth and breadth of awareness.

Keller (2001) mentions that the communications should include 'sub-brands' or specific behaviours, e.g. not sharing passwords, and linking them to the overall goals of information security in the organization. In this way these specific behaviours gain salience and they may be readily adopted by end-users. Another aspect of this communication is to establish an emotional connection with the end-users. This may be done by not just restricting the communication to organizational information security policies and controls, but by associating with other security concerns of end-users e.g. safe Internet use at home, safe credit-card usage or keeping children safe on the Internet. Word-of-mouth from other end-users may also be used to strengthen other end-users' beliefs in their own capabilities when dealing with information security policies and

controls in the organization. Such communication will transmit the message that it is possible, and indeed popular to exercise good security practices. Communications may also be used to reward and honor good security behaviours while at the same time discrediting improper security practices. Posters, emails, slogans, videos, information security weeks, screen-savers, etc. could all be used as the media for communication.

7.8.3 Internalizing the brand and organizing to deliver security service

The brand image in the minds of customers is created primarily by their experiences with the organization or service. The experiences of customers are largely dependent on the internal organization, culture and training of the service provider. In the context of information security in the organization, end-users' experiences with information security management employees and information security policies and controls have a large impact on the perceptions that end-users will develop regarding the information security service brand. All the efforts at defining the brand and communicating it will come to naught if the actual service is not consistent with the messages. As Berry (2000) says, *"customer's experience-based beliefs are powerful" and branding cannot "rescue a weak service"*. Internalization is related to the organization of Information Security Service Management and the design of information security policies and controls. These aspects form part of the Information Security Service Support (ISSS) and Information Security Service Culture (ISSC) components of ISSM. These issue will be discussed further in subsequent chapters.

7.8.4 Monitoring end-user characteristics and their perception of the information security service brand

In the ISSB process, it is vital to monitor the characteristics of end-users in the organization and their perception of the information security brand. This information is used in a two fold manner: to tune the brand definition and communication to the needs and characteristics of the end-users and also to measure the success of the branding process.

Chipperfield and Furnell (2010) state that different people receive the same message differently depending upon their personality. This indicates that to be successful, any communication program must tailor itself to the characteristics of its audience otherwise it loses its effectiveness. Segmentation is the concept of dividing a heterogeneous group into smaller, homogeneous segments. These homogeneous segments have similar characteristics and needs. Consequently, a communication approach tailored to individual segments will probably be more effective than a blanket communication approach. According to Keller (2008), segmentation requires a trade-off

between costs and effectiveness. A finely grained segmentation will lead to more effective communication but at increased cost. Keller (2008) has suggested the following segmentation bases: descriptive or customer-oriented (based on what kind of person the customer is) and behavioural or product-oriented (based on how the customer thinks or uses the product). Keller (2008) has also suggested other segmentation bases that build on brand loyalty. Other segmentation bases include demographic, psychographic and geographic attributes.

In the context of information security in the organization, end-users can be segmented in various ways. The segmentation of end-users will yield segments with different requirements and therefore requiring different treatment. Furnell and Thomson (2009a) state that end-users in an organization can be differentiated on the basis of their level of commitment to information security. These levels range from 'disobedience' at the most negative level to 'culture' at the most positive or committed level. Between these two extremes lie the levels of 'resistance', 'apathy' and 'ignorance' on the non-compliance side; 'commitment', 'obedience' and 'awareness' lie on the compliance side. These levels indicate differing levels of intensity of communication required for branding and hence they can be used for segmentation. These segments could then be used for tuning the branding process. Tsohou, Karyda and Kokolakis (2006) have indicated that different people have different cultural biases and this affects their risk perceptions and approaches to information system risk management. Segmentation can also be performed based upon a variety of different characteristics, such as psychographic factors (e.g. risk perceptions), working groups in the organization, the nature of information use by end-users (e.g. mobile end-users versus non-mobile end-users), the level of skill of end-users (e.g. technically skilled end-users versus technically naïve or not-so-well-skilled end-users). Segmentation requires an ongoing analysis of the characteristics of end-users and their working practices. Thus, segmentation is accompanied by costs; however, this cost can be recovered through improved targeting and effectiveness of communication efforts.

Monitoring of the brand image in the minds of end-users is also important to the branding process. The information security service brand lives in the minds of the end-users. This image or perception, however, may be different from what the organization tries to project through its communications and service delivery. This is most likely when the internalization and service delivery efforts are inconsistent with the information security service brand. Monitoring is also important to understand whether the brand is in sync with what end-users actually desire. End-users may be regularly surveyed to understand how they perceive the information security service brand as against the projected brand. This information may then be used to tailor the brand as well as the communication efforts in the branding process.

Various authors have suggested different metrics for measuring brand performance. There are generally three classes of measurement – perception metrics, performance metrics and financial metrics (Munoz & Kumar, 2004; Rajagopal, 2008). Perception metrics focus on the functional,

emotional and latent connections that customers use to form an opinion of the brand. These include awareness, familiarity, relevance, consideration and preference (Munoz & Kumar, 2004; Rajagopal, 2008). Performance metrics and financial metrics help to assess the impact branding efforts on overall business and economic performance. For the purpose of ISSB and ISSM, perception metrics are probably the most important. Lehmann, Keller and Farley (2008) suggest the following core dimensions of brand performance: comprehension (how much the brand is seen and thought of), comparative advantage (how favourably regarded and differentiated the brand is), interpersonal relations (interpersonal, social aspects related to how the customer feels or is treated by the brand), history (past brand-related events and emotions), preference (customer attitudes towards the brand) and attachment (how strongly customers connect to and interact with the brand).

In the context of information security in the organization, ISSB performance can be monitored by using the metrics as discussed above. From Munoz and Kumar (2004) and Rajagopal (2008), these metrics are the perception metrics that measure the levels of awareness, familiarity and consideration of the information security brand in the minds of end-users. Some questions or statements that can be put to end-users, as part of a survey, for assessing ISSB performance are (from Lehmann et al., 2008):

- I am aware of information security policies and controls;
- I am aware of information security managers and support employees;
- I talk about information security with my friends and colleagues;
- There are a lot of posters, advertisements and other information on information security;
- I often encounter information security tasks at work;
- I often encounter information security tasks away from work;
- I often perform information security tasks;
- I have experience using information security policies and controls;
- I have experience interacting with information security managers and support employees;
- Most of my colleagues are aware of information security policies and controls;
- Most of my colleagues use information security policies and controls;
- Information security is held in high esteem in the organization;
- Following good information security practices improves my standing amongst my colleagues;
- The organization, the information security managers and the support employees care about me;
- The organization and information security managers and support employees are committed to solving my problems and they have my interests at heart;
- I can count on competent and timely response from information security managers and support employees;
- Information security is: Bad – Good; etc.

A process for developing the information security service brand in the organization has been discussed in this section. The primary objective of ISSB is to reverse the negative perceptions of information security in the organization and, instead, to create a positive image in the minds of the end-users.

7.9 Conclusion

This chapter began with two quotes. The quote from Grönroos (2007) elaborated the importance of image for the communication and operational effectiveness of organizations. The quote from Chipperfield and Furnell (2010) indicated the negative image of information security in the minds of end-users in the organization. The chapter progressed from these two quotes and explored the importance of image, the negative image of information security and the failure of ISA approaches in tackling this short-coming. The chapter then discussed branding as a solution for overcoming the negative image of information security in the organization. Finally, the chapter proposed the ISSB process for branding information security, and for creating a positive image for it, in the minds of end-users in the organization.

Branding is ultimately based upon customer experiences with the organization and the service. Hence, branding requires that all activities of an organization should be integrated and consistent with the espoused brand. In this sense, branding is dependent upon all the activities of the organization, both internal as well as customer-facing. Thus, it may be said that ISSB depends upon the ISSS and ISSC components of ISSM. These components will be discussed in the following chapters.

CHAPTER 8

Information Security Service Support – helping end-users cope with security

"In short, when it comes to attracting and keeping buyers, the ability to deliver a satisfying service experience is the most powerful source of sustainable competitive edge. No other factor gets closer to the core of what customers care about most".

- Wollan (2008)

8.1 Introduction

As shown in Chapter 2, according to the Theory of Planned Behaviour, the behaviour of humans is influenced by their perceived behavioural control over a given task. Consequently, end-users' willingness to undertake their information security tasks and their ability to complete these tasks, both are influenced by their perception of the level of difficulty of the tasks. Further, this perception is moderated by past experience of difficulty in undertaking or completing the task. Combined together, the forces of perception and past experience may prompt the end-users to ignore their information security tasks. It thus becomes important to provide adequate support and assistance to ensure that end-users have good perceptions of control over their information security behaviours.

In Chapter 6, the CARE principles were elucidated providing the foundation for Information Security Service Management (ISSM). The CARE principles provide the essence of a human-centric approach to information security in the organization. The CARE principles consist of 'Communicate', 'Accommodate' and 'Respond' elements. The 'Respond' element of the CARE principles embodies the need of end-users for help and support as they interact with information security policies and controls in the organization during the course of their day-to-day work.

In ISSM, the support function is implemented by Information Security Service Support (ISSS). End-users seek help, and ISSS support employees provide help to the end-users in coping with

information security policies and controls in the organization. This support eases the interactions between end-users and the policies and controls; and it allows end-users to successfully undertake and complete their information security tasks. Satisfactory encounters between end-users and support employees lead to improved compliance by end-users, which in turn should lead to an improved state of information security in the organization (see Figure 8.1).

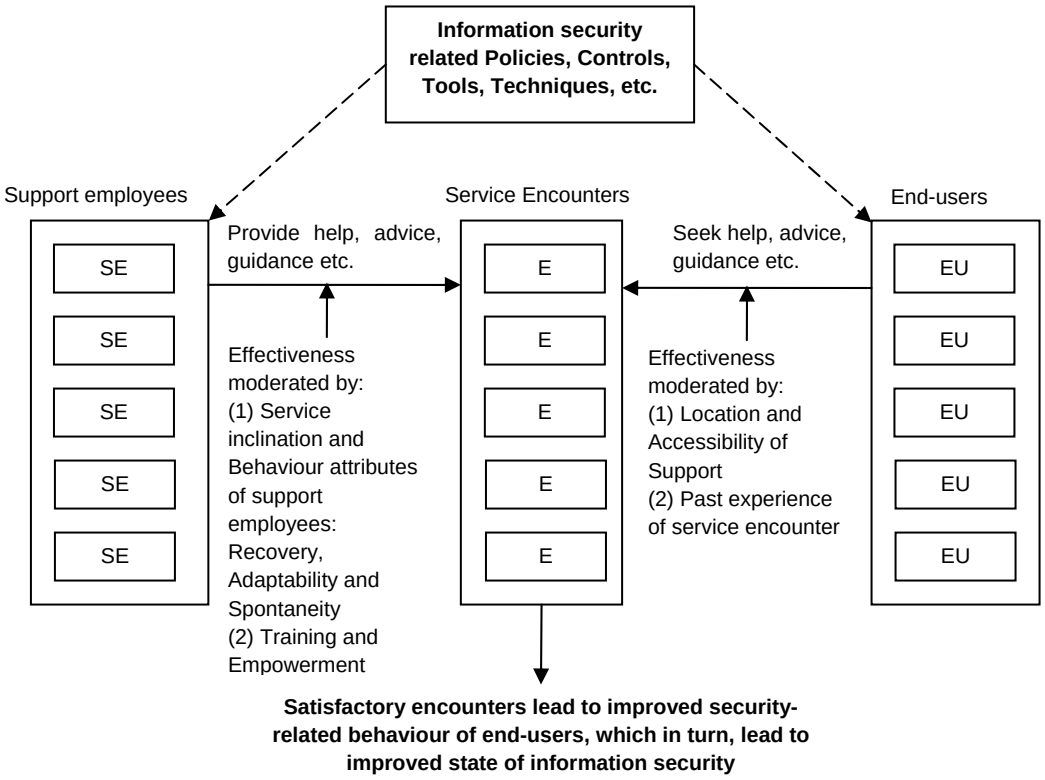


Figure 8.1: ISSS Framework

This chapter is organized as follows. Firstly, the need of end-users for support is discussed in the next section. It is suggested that end-users need help so as to enable them to comply with information security policies and controls in the organization. The next section highlights the need of end-users for support regarding information security policies and controls. The subsequent section then discusses the general concept of service encounters and their role in customer perceptions of service quality. This discussion prepares the grounds for the description of Information Security Service Support (ISSS). Finally, the chapter describes ISSS and provides guidelines for the management of ISSS employees.

8.2 The need of end-users for support

In the context of information security policies and controls in the organization, the information security behaviours of end-users are compromised by two problems. The first problem to plague end-users is a lack of awareness and skills in information security. The second problem is the apparent lack of interaction between end-users and information security support services; so, end-users do not know where to go to for help and assistance. This section discusses these problems and posits that the solution lies in establishing an information security support function in the organization.

Chapter 2 discussed a wide range of issues that affect the information security behaviours of end-users. The Theory of Planned Behaviour (TPB) (Ajzen, 1991, 2005), discussed in Chapter 2, indicates that perceived behavioural control (PBC) is an important determinant of an end-user's intention to undertake information security behaviours. PBC itself is determined by past experiences. In the context of information security, PBC can be understood as follows. If an end-user has a past of successfully undertaking information security behaviours, then this end-user will have a positive intention to undertake such behaviours in the future. If, however, the past is one of unsuccessful or dissatisfying experiences, then the end-user will have a negative intention to undertake information security behaviour in the future.

Typically, end-users face significant difficulties when undertaking information security behaviours in the organization. These difficulties arise from various factors including a lack of awareness (Albrechtsen, 2007; Albrechtsen & Hovden, 2009; Furnell et al., 2006; Sasse et al., 2001), a lack of intention (Adams & Sasse, 1999; Beautement, Sasse & Wonham, 2008; Dhillon, 2001b; Dourish et al., 2004) and a lack of skill (Adams & Sasse, 1999; Furnell et al., 2006; Furnell, 2010; Schultz et al., 2001). In this situation, end-users usually have a history of unsuccessful attempts at undertaking information security behaviours. In the absence of any support or assistance, end-users will feel diffident and they will attempt to avoid or bypass information security behaviours, as predicted by the TPB.

Regarding the lack of interaction between end-users and information security managers, Albrechtsen and Hovden (2009) have reported on the results of their surveys and interviews with information security managers and end-users in various Norwegian organizations. Some useful results from Albrechtsen and Hovden (2009), relevant to this aspect, are discussed below.

Albrechtsen and Hovden (2009) report that while end-users actually desire contact with the information security managers, there is actually very little contact. The end-users find the information security managers "*invisible*" and do not know who to turn to for reporting problems and seeking guidance. The end-users also reported that greater involvement with the

information security managers would lead to greater interest amongst the end-users with regard to information security. Furthermore, end-users believe that greater interaction with information security managers would lead to improved behaviour and knowledge. In summary, the findings of Albrechtsen and Hovden (2009) are that there is a definite digital divide between information security managers and end-users; that both groups underlined the need and importance of greater interaction amongst them for improving end-user awareness and behaviour; and that unfortunately there is a near complete absence of this interaction in the organization.

As discussed above, there is both theoretical and empirical evidence pointing towards the need for enhanced support for end-users. However, paradoxically, present-day approaches to ISM have largely neglected this aspect of information security as is evident from the discussion in Chapter 4. Information Security Service Support (ISSS), the objective of this chapter, aims at bridging this divide by providing a framework for possible day-to-day interactions between Information Security Service Support support-employees and end-users. The purpose of ISSS is to help end-users cope with the demands of information security policies and controls, thereby improving their level of compliance. ISSS operates by creating a chain of successful and satisfying past experiences which, in turn, lead to a successful present and future.

Before this chapter proceeds to describe Information Security Service Support, it is important to understand the concept of service encounters. Service encounters refer to the interaction between customers and service providers. In the context of ISSS, encounters will occur between end-users and support employees. The next section will discuss the concept of service encounters and it will also prepare the ground for the subsequent discussion of ISSS.

8.3 Service encounters and service quality

Findings from the ‘Accenture Global Customer Survey’ (Wollan, 2008) indicate customers’ preferences regarding service experiences. According to the study, service experience is a vital determinant of customers’ buying decisions, long-term loyalty and customer recommendations regarding companies, products and services (Wollan, 2008). A key finding of the survey is that service quality is the dominant reason for customers staying or leaving a provider. In this sense, the service experience of the customer is vital for the service provider. As the opening quotation to the chapter shows, customers care most about service quality and satisfying service experiences. Wollan (2008) presents the factors critical to a satisfying service experience, as follows: factors related to problem resolution (single service representative, fast resolution, speed of response, high-quality response) and the customer agent’s manner and approach. Grönroos (2007) has reported similar findings from a much older study: customers care most for care and concern, spontaneity, problem solving and recovery efforts of service providers.

Berry, Carbone and Haeckel (2002) and Berry, Wall and Carbone (2006) also highlight the role of service experience in the customer evaluation of service quality. According to Berry et al. (2002), service experiences are a major source of value for customers. These experiences consist of clues that influence how customers evaluate the service and whether they will choose to use the service again (Berry et al., 2006). Such clues are 'experience clues' and customers filter and organize these clues into impressions – rational and emotional – regarding the service. Experience clues are important as they influence customers' thoughts, feelings and behaviours. According to Berry et al. (2006), there are three kinds of experience clues – functional, mechanic and humanic clues. Functional clues refer to the technical aspects of the offering and the reliability of the offering; mechanic clues refer to the sensory presentation of the service; humanic clues arise from the behaviour and manner of service providers and these are embedded in the human interactions between customers and service providers. Functional clues influence the cognitive evaluation of service quality. Mechanic and humanic clues influence the emotional or affective perception of service quality. Berry et al. (2006) exhort managers to recognize that technical competence is insufficient for customer loyalty. Customers are wooed by how the service is performed as this performance affects their emotional perceptions of service quality.

As shown above, customer perceptions and loyalty are driven by customers' service experiences. These service experiences are expressed in terms of 'service encounters' which refer to the interactions between customers and service providers. Hence, to understand service experiences, it is important to understand service encounters. The next sub-section provides an overview of service encounters. The subsequent sub-section provides an overview of service quality and the role of service encounters in determining such service quality.

8.3.1 Service encounters

Service encounters represent the interaction between customers and service providers. There are various definitions of the term 'service encounter'. Some definitions are wide and include the physical facilities, technological tools etc. along with interpersonal interactions between customers and service providers (Shostack, 1985; Bitner, Booms & Tetrault, 1990); other definitions focus only on the interpersonal element (Surprenant & Solomon, 1987; Bitner et al., 1990). Shostack (1985) defines the service encounter as *"a period of time during which a consumer directly interacts with a service"* (Bitner et al., 1990). This definition indicates that the encounter encompasses the interpersonal interactions between the consumer and the service provider, and also the various other components like physical facilities, technological tools, etc. (Bitner et al., 1990). Surprenant and Solomon (1987) provide a narrower definition – they define the service encounter as *"the dyadic interaction between a customer and a service provider"*. This definition focuses on the interpersonal element of service firm performance (Bitner et al., 1990). Grönroos (2007) and Zeithaml et al. (2008) describe these interactions as 'moments of

truth' where *"promises are kept or broken"* (Zeithaml et al., 2008). Service encounters or interactions occur in the visible or interactive part of the organization where the customer meets the service provider (Grönroos, 2007). Gremler et al. (1995) apply the same concepts to 'internal service encounters' that occur in an organization. Internal service encounters are service encounters that occur between internal service providers and internal customers in an organization. These encounters occur within the organization, and internal customers include anyone in the organization who utilizes the services of others in the same organization.

Bitner et al. (1990) identified three major groups of behaviours of customer contact employees. These groups of behaviours are:

- Employee response to service delivery system failures – Recovery
- Employee response to customer needs and requests – Adaptability
- Unprompted and unsolicited employee actions – Spontaneity

Recovery refers to the situation when the service delivery system fails. In such a situation, customers are agitated and customer contact employees are required to respond to their complaints. Though the service failure represents a disappointing situation for the customer, it is ultimately the contact employee's manner and behaviour that determines whether the incident is remembered favourably or unfavourably.

Adaptability refers to the situation when a customer presents special needs or preferences. Such a situation requires the customer contact employee to adapt the service delivery system. From the customer's perspective, the customer requires flexibility and adaptability of the service delivery system. Customers feel pleased when the service provider attempts to meet their special needs.

Spontaneity refers to the situation when a customer contact employee takes an initiative that is unexpected and surprises the customer. Satisfactory incidents represent pleasant surprises for the customer. Unpleasant surprises can lead to dissatisfaction.

Zeithaml et al. (2008) have added a fourth category of behaviours, namely, coping. Coping refers to the response of customer contact employees to problem customers. Problem customers are those who are unreasonable and unwilling to cooperate with the service provider. In such situations, customers themselves are the source of their dissatisfaction and no actions of the customer contact employees would please them.

As seen above, the behaviour of customer contact employees is at the fulcrum of the service encounter. This has implications for service managers. Service managers need to ensure that customer contact employees can continue to provide satisfactory service encounters to customers, while operating under the policies and procedures of the organization. Key antecedents of the satisfactory behaviour of customer contact employees are their knowledge and

empowerment (Bitner et al., 1990). Customer contact employees need to have knowledge about all aspects of the service and its delivery. This knowledge enables them to satisfy the information needs of the customers and provide appropriate responses or assistance. Customer contact employees also need to be empowered through the delegation of control. Since customers detest having to talk to multiple employees to resolve an issue (Wollan, 2008), empowerment is important as it enables these employees to resolve customer issues effectively and efficiently.

A brief overview of service encounters and associated issues has been discussed in this sub-section. Service encounters are 'moments of truth' and they are highly dependent upon the behaviour of customer contact employees. The next sub-section discusses the role of service encounters in customer perception of service quality and how customer contact behaviour shapes customer perceptions of service quality.

8.3.2 The role of service encounters in customer perception of service quality

The service encounters or the interactions or 'moments of truth' are of critical importance as they form the basis for the customer's perception of service quality (Zeithaml et al., 2008). Service quality is perceived by customers in terms of two dimensions: the technical or outcome dimension and the functional or process-related dimension (Grönroos, 2007). The technical dimension relates to the 'what' whereas the functional dimension relates to the 'how' of the service. As discussed earlier, the importance of the 'how', and thus the service encounter, is underlined by customers' preference for satisfying customer experiences during service encounters (Grönroos, 2007 and Wollan, 2008). Berry et al. (2006) exhort managers in organizations to pay attention to not only the technical part of service provision but also to the interaction part.

The previous sub-section discussed the grouping of customer contact employee behaviours as stated by Bitner et al. (1990). The behaviour of customer contact employees during service encounters affects customer perception of service quality. When service failures occur, customers perceive the service quality favourably if the customer contact employees acknowledge the problem and accept it as their problem. Customers perceive the quality to be low if the failure remains unaddressed and unexplained. Some customers may have special needs or preferences. Such customers feel satisfied if their needs or preferences are accommodated. Customers feel dissatisfied if the seriousness of their needs is not understood or no sincere effort is made to accommodate their preferences. A particular situation is when a customer has made an error. At such times, the customer contact employee needs to adapt to the new situation. Such situations become highly satisfactory if the employee takes ownership of the problem and assists the customer. On the other hand, if the employee avoids any responsibility for resolving the problem or embarrasses the customer, the situation becomes highly dissatisfactory for the

customer. Often, a satisfactory encounter for customers is when they are treated with care and concern and they are paid attention to. Customers feel dissatisfied if they are ignored or treated impersonally. Customer contact employees can further lead to satisfactory experiences through their spontaneity towards customers. Employees can make their customers feel *"unique"* or *"pampered"*. Customers feel dissatisfied if contact employees demonstrate poor attitudes towards them. Similarly, customers feel satisfied and show empathy for the contact employees if these employees are able to deftly handle stressful situations. Bitner et al. (1990) stated the following sources of satisfaction in service encounters: the behaviour of employees as they respond to core service delivery failures; the behaviour of contact employees as they accommodate customer needs for customized service; and customer delight with unprompted and unsolicited service actions by customer contact employees. Bitner et al. (1990) also stated the following sources of dissatisfaction in service encounters: the unwillingness or inability of employees to respond to customers in the eventuality of service failure; failures to accommodate the need for customized service; and the customer assessments of the character and attitude of contact employees based upon their behaviour.

Service encounters between customers and customer contact employees play a vital role in customer perceptions of service quality. Depending upon how customer contact employees behave during service encounters, customers may perceive the service quality positively or negatively. Such perceptions affect the long term loyalty of customers to the service provider. Service encounters and their role in service quality have been discussed in this section.

The next section on ISSS applies the lessons learned in this section. In the context of information security in the organization, interactions can be said to occur between end-users and the providers of information security service. Firstly, the previous section highlighted the fact that the interactions between information security managers and end-users are minimal and that the interactions that do take place between the two parties are not necessarily experienced by all the end-users as positive. Secondly, as of the present, information security management tends to ignore the aspect of support to end-users; and thus, it may be said, that this aspect of the interaction is completely missing. It could be argued that the interactions of end-users with information security, and therefore also their experiences of the information security service, are not pleasant. In this scenario of unpleasantness, it seems that it may be worthwhile to apply the lessons of service encounters and perceived service quality to information security. Just as customers in a service setting value interpersonal interaction with their service provider, end-users in the context of information security too might be positively influenced by their interactions with ISS support employees. The next section will describe ISSS as a framework for managing the interactions between end-users and the information security service in the organization.

8.4 Information Security Service Support

The previous two sections highlighted some important aspects related to information security in organizations as well as general service management. In the domain of information security, it is noted firstly, that there is a poverty of interactions between end-users and information security service providers; and secondly, that improved interaction is expected to lead to better end-user awareness and behaviour. In the domain of service management, the interaction between customers and service providers, also called 'service encounter', is an important determinant of customer perceptions of service quality. Combining these aspects, it may be concluded that end-users in an organization, as customers of the information security service, have often had dissatisfying service experiences and that these negative experiences lead them to have negative perceptions of the quality of the information security service. Hence there is a definite need for 'bridging the gap' between end-users and information security service providers in an organization. This gap can bridged by Information Security Service Support (ISSS), based on the principles of general service management. ISSS fills another gap too – by providing timely support to end-users it allows end-users to successfully undertake information security behaviours; further, it enhances their perceptions of behavioural control over information security behaviours, thus, improving their motivation towards undertaking such behaviours. This chapter focuses on the 'service encounter' aspect of ISSS and provides guidelines that can be used to successfully introduce ISSS in the organization.

The previous section discussed two kinds of definitions of 'service encounter' – one which is quite broad and does not limit itself to the interpersonal interactions between customers and customer contact employees; the other which is narrow and focuses on the interpersonal element only. Applying the broad definition to ISSS, service encounter in the context of ISSS would include interactions of end-users with information security related policies, controls, tools and technologies on the one hand, and interpersonal interactions with support employees on the other hand. Interactions of end-users with information security policies, controls, tools and technologies lie in the domain of usability and they are beyond the scope of ISSS – these issues will be touched upon in the next chapter. For the purpose of ISSS, this chapter adopts the narrow definition of service encounter, focusing only on the interpersonal interactions between end-users (customers) and ISS support employees. The ISS support employees perform the role of 'customer contact employees' which is the term used in the literature on service encounters.

The sub-sections below discuss various issues associated with providing support to end-users. Ease of accessing support employees is the first step in obtaining support. Accessibility is discussed in the next sub-section. The subsequent sub-section discusses the behaviours of support employees that lead to satisfying service experiences for end-users. The final sub-section

discusses the managerial actions required to ensure that support employees are able to undertake the identified behaviours.

8.4.1 The accessibility of support employees

According to Grönroos (2007), service management requires the development of the service concept. The service concept consists of the basic service package, the augmented service offering and the management of image and communication. The service concept is important, as it eventually determines the intentions of the organization. The basic service package focuses on the technical outcomes, i.e. the 'what' of the service offering. However, as noted earlier, customers base their perceptions of service quality on the functional aspects, i.e. the 'how' of the service offering. Hence, the basic service package needs to be complemented by an augmented service offering. This augmented service offering focuses on the functional aspects of the service provided and attempts to satisfy customers on the 'how' aspect. Finally, the management of image and communication enhance the customer perception of the service offering.

Considering only the basic service package and the augmented service, the Information Security Service provided to end-users can be equated to the basic service package offered by the organization to the end-users; while the Information Security Service Support (ISSS) is the augmented service offering that complements the basic service package. For augmented service offerings, accessibility is a core issue (Grönroos, 2007), i.e. how easy is it for customers to search, locate and interact with the augmented service offering? In the context of ISSS, accessibility means how easy it is for end-users to seek help, support and guidance from the support employees. Accessibility of the support employees consists of the following (based on Grönroos, 2007):

- 'Location': Support employees should be available at a known 'location' and information of this location should be readily available to end-users. The 'location' could consist of a physical location or even a telephone number or a software helpdesk, etc. The support must also be available at times that match the working hours of the end-users. Further, the various tools, technologies and procedures for seeking support must be user-friendly and not overly complicated.
- 'Approachability': When end-users seek to get hold of support employees, the support employees should be approachable and readily accessible. Small things such as the response time to answer a telephone call have an important bearing on the end-user's perception of accessibility. Further, a negative attitude or unfriendly tone on answering a call can have negative repercussions on the end-user's perception of accessibility.

Accessibility is a key issue as it is the first step in the interaction between end-users and support employees. Accessibility is determined not only by the 'locatability' of support employees but

also their ‘approachability’. Once end-users are able to access the support employees, the behaviour of support employees determines the success or failure of the ensuing service encounter. The following sub-section discusses the desirable and undesirable behaviours of support employees in service encounters.

8.4.2 The behaviours of support employees

Apart from accessibility, the general behaviour of support employees is critical in all situations involving end-users with problems or queries related to information security policies and controls. Following Bitner et al. (1990) and Zeithaml et al. (2008), these behaviours can be classified into the following groups:

- Recovery – support employee response to failures of the information security service e.g. security breaches or failures and difficulty experienced by end-users in working with security policies and controls.
- Adaptability – support employee response to special needs, preferences or requests of end-user.
- Spontaneity – unprompted and unsolicited actions by support employees towards end-user.
- Coping – support employee coping with uncooperative or unreasonable end-user.

Security can never be perfect and incidents or breaches are a regular part of information security. Such situations, such as virus outbreaks, can be treated as service failures. In addition, an end-user may find it difficult to work with certain controls e.g. choosing a strong password. Such situations call for the ‘recovery’ capabilities of the support employees. Often, it may not be possible to make it easier for the end-user, e.g. by diluting the password strength. Thus, there is a need for the support employees to engage the end-user and initiate service recovery. Components of the recovery strategy could include acknowledging the problem, explaining the nature of the problem and its cause, explaining the rationale for the control and its importance for effective information security and apologizing for the failure or inconvenience. For example, in the case of an end-user facing a problem with strong passwords, the support employee should accept the difficulties posed by strong passwords, explain the need for strong passwords, apologize for the uncomfortable situation and finally guide the end-user in the creation of a strong password.

Often, end-users in an organization need some flexibility regarding the enforcement of information security policies and controls. For example, in an organization where Internet browsing is restricted, a particular end-user may need access, perhaps for personal reasons. In this situation, a strict enforcement of the security control will result in denying the access to the end-user, resulting in a dissatisfactory encounter for the end-user. Alternatively, the ‘adaptability’ of the support employee to the situation, by appreciating the innocuous and

temporary nature of the request and arranging the required access for the end-user, would result in a satisfactory encounter for the end-user.

Another frequent situation that takes place in an organization is when an end-user makes a mistake and calls the support employee for help. For example, the end-user has forgotten a password. In this situation, the support employee may criticize the end-user and even deplore end-users in general as a source of regular problems. This will lead to a highly unsatisfactory encounter for the end-user. Alternatively, the support employee may take ownership of the resolution of the problem by getting a new password reissued to the end-user and also guiding the end-user in resetting the password according to the organizational policy. This will result in a satisfactory encounter for the user. Personalization and 'spontaneity' towards end-users result in satisfactory encounters. End-users will feel dignified if the support employee refers to them by name and exhibits familiarity. Support employees may even adopt a relational approach towards end-users in which they establish personal rapport or friendships with end-users. This relational approach results in benefits for end-users and also gains end-user loyalty and positive word-of-mouth for the information security service (Hennig-Thurau, Gwinner & Gremler, 2002). Support employees should actively solicit feedback, suggestions and complaints from end-users and then feed this information to information security service managers. This escalates concerns of end-users to the managers and allows for end-user concerns to be addressed.

A summary of support employee behaviours and specific dos and don'ts is presented in Table 8.1.

The eventual objective of the ISSS, and therefore the support employees, is to assist end-users in the organization in navigating through the information security policies and controls and behaving in a compliant manner. This assistance should help end-users cope with the difficulties posed by information security policies and controls and ensure that end-users have a satisfying security service experience. Consequently, support employees are crucial to the success of ISSS as their interaction with end-users determines their perception of the overall quality of the security service. This sub-section has highlighted the importance of service encounters and support employee behaviours that lead to satisfactory encounters. The next sub-section discusses how information security managers need to manage and empower the support employees.

Theme	Behaviour categories	Do	Don't
Recovery e.g. virus attack; inability to choose strong password etc.	• Response to unavailable service • Response to unreasonably slow service • Response to other core service failures	• Acknowledge problem • Explain causes • Apologize • Compensate / upgrade • Lay out options • Take responsibility	• Ignore the end-user • Blame end-user • Leave end-user to fend for himself or herself • Downgrade • Act as if nothing is wrong • "Pass the buck"
Adaptability e.g. request for temporary Internet access; end-user forgetting password.	• Response to "special needs" of end-users • Response to end-user preferences • Response to admitted end-user error • Response to potentially disruptive others	• Recognize the seriousness of the need • Acknowledge • Anticipate • Attempt to accommodate • Adjust the system • Explain rules / policies • Take responsibility	• Ignore • Promise but fail to follow through • Show willingness to try • Embarrass the end-user • Laugh at the end-user • Avoid responsibility • "Pass the buck"
Spontaneity e.g. getting a new password reissued to end-user.	• Attention paid to end-user • Truly out-of-the-ordinary employee behaviour • Employee behaviours in the context of cultural norms • Gestalt evaluation • Performance under adverse circumstances	• Take time • Be attentive • Anticipate needs • Listen • Provide information • Show empathy	• Exhibit impatience • Ignore • Yell / laugh / swear • Steal from end-user • Discriminate
Coping e.g. an end-user may turn uncooperative or abusive if request is not accepted.	• Response to unreasonable or uncooperative end-user	• Listen • Try to accommodate • Explain • Let go of the end-user	• Take customer's dissatisfaction personally • Let end-user's dissatisfaction affect others

Table 8.1: ISS support employee service behaviours – Dos and Don'ts (based on Bitner et al., 1990 and Zeithaml et al., 2008)

8.4.3 Management of ISS support employees

Service encounters, or interpersonal interactions, occur between end-users and ISS support employees. In these service encounters, the service employees play a crucial role as their

behaviour determines the level of satisfaction of end-users. To enable support employees to undertake these behaviours requires specific managerial actions. Consequently, the management of the support employees gains prominence in a service setting. This sub-section provides some guidelines towards the management of ISS support employees so that they can interact effectively with end-users.

In a typical service setting, customer contact employees are the first, and, often, the only representative of the organization with whom customers are dealing with (Hartline & Farrell, 1996 and Hartline, Maxham III & McKee, 2000). Zeithaml et al. (2008) emphasize the importance of these employees: they are the service; they are the organization in the customer's eyes; they are the brand and they are the marketers. Likewise, in the context of ISSS, the support employees are the 'visible' face of ISSM with whom end-users associate any problem or query related to information security policies and controls in the organization.

Due to the nature of service encounters and the varied demands that are placed on ISS support employees, the effective management of support employees is crucial to ensure that they are able to exhibit appropriate attitudes and behaviours. The key enablers of attitudes and behaviours of support employees are: knowledge, empowerment and behaviour-based evaluation (Grönroos, 2007 and Hartline & Ferrell, 1996). According to Lewis and Entwistle (1990), the following characteristics are required for support employees to perform effectively in service encounters:

- Process, procedural and technical skills,
- Interpersonal or 'people' skills,
- Behavioural flexibility and adaptability, and
- Empathy to be able to perceive the customer's perception of service.

Zeithaml et al. (2008) mention a four-step strategy in this regard: hire the right people; develop the people to deliver service quality; provide them with needed support systems and retain the best people. The four-step strategy, as applicable to ISSS, is shown in Fig. 8.2 and discussed below.

Hiring the right people for ISSS. This is the necessary first step. Service employees should possess service inclination (Zeithaml et al., 2008). 'Service inclination' reflects the employee's orientation towards helping, guiding and supporting the end-users. Personality characteristics associated with this attribute are helpfulness, thoughtfulness and sociability (Zeithaml et al., 2008).

Developing the people to deliver service quality. ISS managers need to provide training and empowerment to support employees. ISS support employees need both technical and interaction skills to perform their job effectively. The technical skills include knowledge of the information security policies and controls in the organization, as well as the rationale behind these policies

and controls. Support employees must also be aware of the various procedures or processes enforced in the organization. This knowledge-base of the support employees needs to be regularly updated to match the actual situation in the organization. Thus, appropriate training must be regularly imparted to support employees.

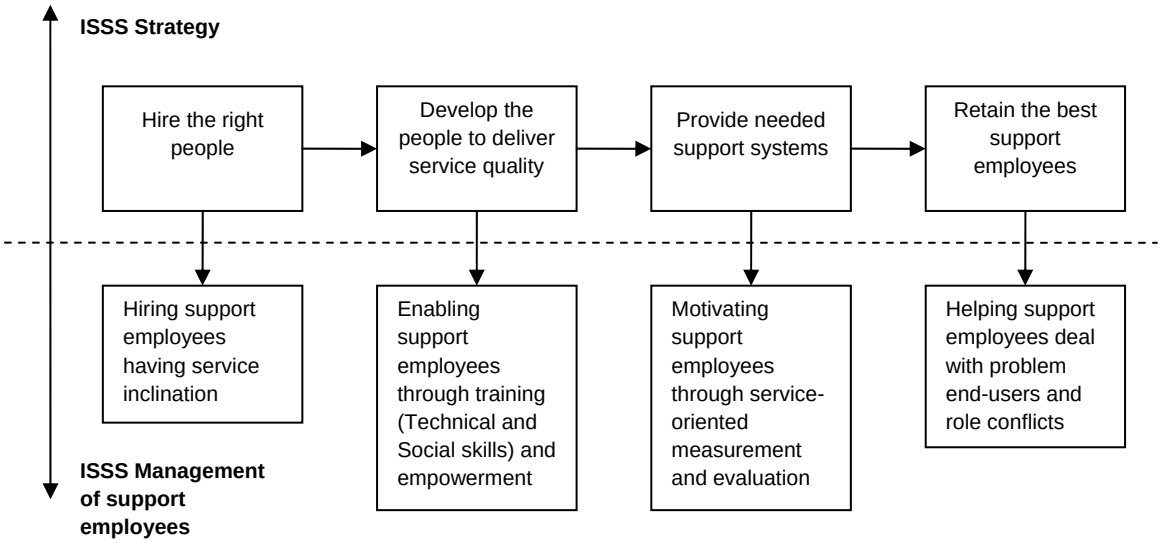


Figure 8.2: Four-step strategy for ISSS and Management of support employees

Support employees should also be trained for people skills, or social, or interactive skills. Since, interaction with end-users is the main function of their jobs, such skills become the differentiator between positive and negative customer service experiences. Thus, such skills acquire great importance. Social, or interactive, or people, skills, refer to the ability of the support employee to understand the end-user's perspective during interactions (Mead, 1934, cited in Hennig-Thurau, 2004) and showing care, concern and empathy towards end-users (Zeithaml et al., 2008).

Empowerment of support employees is another important aspect of enabling them (Bitner et al., 1990 and Zeithaml et al., 2008). Empowerment refers to giving the support employees the authority to respond and adapt to the needs of the end-users. In an example in the previous section, when an end-user needed temporary Internet access, the support employee could help the end-user only because he/she was empowered to take the decision on his/her own. Empowerment is particularly important as end-users desire single-window resolution of issues (Wollan, 2008). However, empowerment has the potential to become a security risk in itself.

Consequently, managers must set and inform support employees of the boundaries to their authority. Empowerment needs to be supported by appropriate training and knowledge.

Providing needed support systems. Measurement and evaluation of the support employees is an important tool in motivating them towards a service mindset. As stated in Rastogi and Von Solms (2009), supervisory focus, reward systems and measurement focus in ISSM must be tuned towards ensuring that support employees are supported, measured and rewarded for their interactions with end-users. Behaviour-based support employee evaluation involves measuring the performance of service employees in satisfying end-user needs rather than work related outputs (Hartline et al., 2000).

Another aspect of enabling support employees is to provide them with the appropriate internal processes and equipment. Internal processes should be aligned with the service inclination of employees. Bureaucratic processes driven by cost-efficiency can impede the adaptability and flexibility of support employees.

Retaining the best support employees. According to Lewis and Entwistle (1990), people are the highest cost element as well as the biggest assets for service organizations in view of their impact on customer perceptions of service quality. Thus, retaining the best people becomes a core requirement. Retaining the best people involves several HR-related strategies. However, the problem and its solution are not unique to the context of ISS and hence will not be discussed any further. Rather, this section takes an alternative approach – that of identifying the problems faced by support employees and the managerial solutions to those problems. Managerial actions to solve the problems of support employees should support the retention of good employees.

ISS support employees face many problems while performing their job. Some end-users may be non-cooperative or even unreasonable and their service encounter will be unsatisfactory in spite of the best efforts of the support employee. It is important that support employees be provided with the appropriate training to deal with such ‘problem’ end-users (Bitner et al., 1994). It is also important that support employees be provided management support in dealing sternly with such ‘problem’ end-users. Zeithaml et al. (2008) describe this as ‘coping’.

Another problem that afflicts support employees is role conflict. Role conflict represents the *“incompatibility between one or more roles within an employee’s role set, such that fulfilling one role makes fulfilling the others more difficult”* (Weatherly & Tansik, 1993, cited in Hartline & Ferrell, 1996). In the context of ISSS, such role conflicts might arise when the support employee’s responsibility for satisfactory encounters is pitted against an end-user who is making a demand which is clearly in violation of organizational information security policies and controls. In such situations, support employees need to know their boundaries. Support

employees should also possess the knowledge to understand the negative impact of meeting end-user's demands.

Support employees are a key resource and they need to be provided managerial support so as to be able to deliver satisfactory encounters with end-users. This sub-section has provided some of the issues related to the management of support employees. A strong service attitude, appropriate knowledge, training and empowerment coupled with organizational support for service are the pre-requisites for support employees to function. Thus, the success of the ISS is hugely dependent on the quality of the support employees as well as the manner in which they are managed.

8.5 Conclusion

The main objective of ISSS is to help end-users cope with the demands of information security policies and controls in the organization. Adequate and appropriate support to end-users ensures that they are able to successfully undertake their information security behaviours. Further, satisfying encounters between end-users and support employees ensures that end-users will have positive perception of the information security service. ISSS, if introduced and managed appropriately, can contribute positively towards enhancing the compliance of end-users with organizational information security policies and controls to the eventual benefit of the organization. This chapter has provided guidelines for the implementation of ISSS in the organization in terms of support accessibility, positive support employee behaviours and managerial actions required for enabling support employees.

The previous chapter discussed Information Security Service Branding (ISSB) which implements the 'Communicate' element of the CARE principles. This chapter has discussed the 'Respond' element. The next chapter discusses Information Security Service Culture (ISSC) which is the final component of ISSM and implements the 'Accommodate' element of the CARE principles.

CHAPTER 9

Information Security Service Culture – information security for the end-users

"Democracy is the government of the people, by the people, for the people."

- Abraham Lincoln (1863)

9.1 Introduction

In their paper, *"The Protection of Information in Computer Systems"* (Saltzer & Schroeder, 1975), the authors presented eight principles applicable to the mechanisms for the protection of information. One of these eight principles is the principle of psychological acceptability. According to this principle, ease of use of the human interface is crucial for protection mechanisms. If the protection mechanism is easy to use, then end-users will use it routinely and without errors; otherwise, end-users will make errors (Saltzer & Schroeder, 1975). Likewise, Bishop (2003) has expounded a similar principle. According to Bishop (2003) security or protection mechanisms place an extra burden on end-users. The principle of psychological acceptability can then be interpreted to mean that "*security mechanisms should not make the resource more difficult to access than if the security mechanisms were not present"* (Bishop, 2003). Apparently, these principles have not found much favour with information security managers and developers. In spite of the early origins of the principles of psychological acceptability, one of the most severe problems of information security continues to be the difficulties end-users face as they try to interact with information security policies and controls in the organization (Furnell, 2010; Schultz et al., 2001). Zurko and Simon (1996) go to the extent of stating that "*secure systems have a particularly rich tradition of indifference to the user"*.

The above problem of 'indifference to the user' arises from the present-day approaches to the formulation of information security policies and controls in the organization. These approaches are typically technically oriented and work in isolation from the end-users, their needs and requirements. The needs and requirements of end-users are treated in a post-facto manner by

providing them with awareness and training programs. Compliance is sought to be achieved through culture, incentives and punitive measures. This approach leads to information security policies and controls that lack usability. Such poor usability evokes end-user resistance and the subsequent rejection of these policies and controls (Schultz et al., 2001). Schultz et al. (2001) further state that end-user resistance manifests itself as *"passive resistance, negative verbal behaviour, reluctance to perform tasks, failure to pay sustained attention to tasks, actions that cause damage to system components and many others"*. This seriously weakens the effectiveness of information security policies and controls in the organization.

The CARE principles (discussed in Chapter 6) recognize this problem, namely, lack of consideration to end-user needs leads to unfriendly policies and controls which in turn lead to end-user resistance; this resistance finally leads to weakened information security (this is analogous to the vicious circle of Figure 6.1). These principles serve as the foundation of Information Security Service Management (ISSM). The CARE principles embody the essence of a human-centric approach to information security in the organization and consist of the 'Communicate', 'Accommodate' and 'Respond' elements. The 'Accommodate' element of the care principles attempts to resolve this chain of unfortunate circumstances: to accommodate is to accept the role of end-users in information security and formulate information security policies and controls in the organization in an end-user centric manner. The 'Accommodate' element of the CARE principles embodies the need for formulating end-user centric information security policies and controls in the organization, thereby minimizing the conflict between information security and the day-to-day working practices of end-users. The opening quote to this chapter by Abraham Lincoln puts people at the centre of democracy; so does the 'Accommodate' element put end-users at the centre of information security in the organization.

Information Security Service Management (ISSM) is an information security management approach that is based on, and implements, the CARE principles. In contrast to the technology driven approaches, ISSM is an end-user centric approach to the formulation of information security policies and controls in the organization. ISSM incorporates the needs and requirements of end-users from the start. The ISSM approach, however, requires a mental shift in the minds of information security managers and developers – away from the firmly entrenched technical approach towards the end-user centric approach. Information Security Service Culture (ISSC) is a tool to achieve this shift and to implement the 'Accommodate' element of the CARE principles.

This chapter presents the concept of Information Security Service Culture (ISSC). The chapter is organized as follows. It first examines the view of end-users in the perception of information security managers and developers. In an attempt to understand how these perceptions of developers affect the formulation and use of information security policies and controls, the chapter next discusses the values and beliefs of information systems developers and how these

affect the systems they develop. The chapter takes this discussion further by examining how the present-day functionalist paradigm of information systems development leads to a 'technology trap'; the section then goes on to suggest the use of the interpretivist paradigm to break out of the 'technology trap'. But before the functionalist paradigm can be replaced by the interpretivist paradigm, developers need to change in their approach to the development of systems and the end-users of these systems. This change can be wrought through ISSC, as culture drives behaviour through values and beliefs at both the conscious and unconscious levels (Schein, 2004). Hence, the chapter first puts culture, service culture, information security culture and Information Security Service Culture in perspective. The chapter concludes by discussing the Information Security Service Culture and its constituent elements.

A note of caution here; many of the concepts presented later in the chapter come from the streams of information systems and information systems development. These concepts are subsequently applied to information security. It may be said that the streams of information systems or IT and information security are closely related (Albrechtsen & Hovden, 2009; Frangopoulos, 2007) and hence the concepts or results from the former fields can be validly applied to the latter. Furthermore, it should be noted that the chapter treats the terms engineer, technologist and developer as synonyms. In the subsequent discussions, different authors have used one term or the other; this chapter uses the term 'developer' and refers to the role of people who develop and manage the systems (including information systems and information security policies and controls) that underlie the work of other people in the organization.

9.2 The end-user in the perception of information security managers and developers

Ashenden (2008) and Albrechtsen and Hovden (2009) have discussed the difficulties arising from the mismatch between the highly technical information security managers and developers and the technically naive end-users. This section is based on these two papers and discusses the negative image of end-users in the perception of information security managers and developers in the organization.

According to Ashenden (2008), in most organizations, information security is still a purely technical subject and is best managed by technical staff. Information security managers and developers approach their subject in a 'command and control' manner and remain isolated and disengaged from the end-users of their creation. The managers and developers do not make any attempts to understand or negotiate with their end-users and continue to rely on *"how they think end-users see information security"* (Ashenden, 2008).

Albrechtsen and Hovden (2009) state that a divide exists between end-users and information security managers with respect to skills, knowledge and responsibilities. This situation leads to information security policies and controls being designed with a duty-oriented or *"policing"* approach. In this approach, the policies and controls focus on allowing or disallowing end-users to perform specific activities. There is also an emphasis on surveillance and monitoring. Albrechtsen and Hovden (2009) further state that information security managers regard end-users both as a resource and as a problem. Managers feel that end-users lack motivation, knowledge and the skills required for safe and secure behaviour and hence the end-users cause adverse incidents. Managers also have negative assessments of end-users. Consequently, information security policies and controls rely on *"technological tools that seek to control and monitor user behaviour"* because *"technology is also believed to be more sound and reliable than users"*. Though user participation and involvement are rated highly, most information security managers remain aloof and distant from end-users while formulating information security policies and controls. Information security managers typically do not have detailed information regarding the information security behaviours of end-users – they continue to design information security policies and controls based on their own perceptions of end-users. There is a trust deficit – information security managers do not trust end-users.

The preceding discussion has presented the view of end-users in the perception of information security managers and developers in the organization. The discussion has also indicated how this view impacts the nature of information security policies and controls in the organization. In the present-day approach to information security in the organization, information security policies and controls are based on the functionalist assumption that end-users are rational actors who will readily comply with information security policies and controls. Further, information security managers and developers have an antagonistic view towards the end-users in the organization. These factors conspire to ensure information security managers and developers in the organization continue to neglect the principle of psychological acceptability and the ease of use of information security policies and controls. It may be said that this inadequacy of present-day information security policies and controls results from the unrealistic models and expectations of the developers regarding the end-users of these policies and controls. The unrealistic models and expectations, in turn, arise from the lack of knowledge regarding the everyday work and information security behaviours of end-users. The absence of this information sets up a dysfunctional vicious circle. In this vicious circle, information security developers rely upon their already incorrect perceptions of end-users (the vicious circle was shown earlier in Figure 6.1).

Various authors have explored the link between developer's perceptions of end-users and the nature of systems that results from these perceptions. The next section discusses this link further in an attempt to understand how the image of end-users in the perceptions of information

security developers influences the nature of information security policies and controls in the organization.

9.3 The end-user in the perception of information systems developers

The developers in the organization have an implicit perception regarding the end-users in the organization. As these developers develop systems for the use of end-users, their perceptions of end-users have an impact on the nature and the success or failure of the developed systems (Bostrom & Heinen, 1977; Orlikowski & Gash, 1994). This section discusses these perceptions and their role in an organization.

9.3.1 The role of image

In the field of information systems development (ISD), Bostrom and Heinen (1977) and Orlikowski and Gash (1994) have adopted a similar approach to understanding the interaction between developers of information systems and their end-users in the organization. According to Bostrom and Heinen (1977), the development of information systems is impacted significantly by the view that system designers and developers hold regarding the organization, end-users and the function of the information system within the organization. The ISD is not solely determined by the available technology, but it is also affected by the knowledge, skills and values of the designers, and the assumptions they hold about the organization and end-users. These factors act as 'frames of reference' and 'perceptual filters' that act to guide the designers and developers. The frames of reference of the designers and developers constrain their range of design alternatives and change strategies and, finally, they even determine the chosen design alternatives and change strategies. Bostrom and Heinen (1977) further state that these frames of reference act at the sub-conscious level and designers and developers may not always be aware of the content of their frame of reference.

Orlikowski and Gash (1994) use the concept of 'technological frames', or 'technology frames', to understand the development and use of information systems in organizations. Technological frames, or technology frames, are the *"understanding that members of a social group come to have of particular technological artifacts, and they include not only knowledge about the particular technology but also local understanding of specific uses in a given setting"* (Orlikowski & Gash, 1994). Further, these frames concern the *"assumptions, expectations and knowledge"* that people in an organization hold regarding technology in the organization. Thus, a technology frame consists of a technology dimension as well as a contextual use dimension. Frames operate in the background as implicit assumptions and have the potential of creating

"psychic prisons" (Bolman & Deal, 1991). These inhibit learning and creativity in problem solving. In a negative sense, frames are self-reinforcing and may even lead to the rejection of new knowledge; they may also manifest ideas that are *"ambiguous, obsolete, incomplete or incorrect"*. These inconsistencies are implicit and the group may frequently not even be aware of them. For example, in the context of information security in the organization, information security management may preach the need for end-user friendly policies and controls, and yet continue with formulating policies and controls that do not promote the secure behaviour of end-users.

According to Orlikowski and Gash (1994), technological frames have powerful effects as they influence the design and use of technologies in the organization. The design and development of an information system in the organization is determined implicitly by assumptions concerning the *"views of how work should be done, what the division of labor should be, how much autonomy employees should have, and how integrated or decoupled production units should be"* (Orlikowski & Gash, 1994). In this way, information systems embody the *"objectives, values, interests and knowledge"* of the designers and developers of the system.

9.3.2 The negative image of end-users in the perception of developers

Schein (1996 and 2004) states that any organization develops three dominant cultures, namely, the executive culture, the engineering culture and the operator culture. These are the three cultures of management. The executive culture represents the executive management, CEO and his/her immediate subordinates that manage the organization. The engineering culture represents the designers and technocrats who design and develop the systems that underlie the work of the organization. The operator culture consists of the workers who conduct the work of the organization. For the purpose of this chapter, only the engineering culture is relevant and will be discussed further. In the context of information security in the organization, the engineering culture would represent the information security managers and developers who formulate and implement the information security policies and controls in the organization. According to Schein (1996 and 2004), the developers prefer *"linear, simple cause-and-effect, quantitative thinking"*. They develop systems requiring standard responses from the end-users. The engineering culture expects the end-users to change and adapt to the system; any inadequacy is seen as *"resistance to change"*. In such thinking, the end-users are seen as costs or sources of error; the developers assume that they need to constrain the end-users and make them follow policies and guidelines. The engineering culture further seeks to develop systems *"working in perfect precision and harmony without human intervention"*.

According to Bostrom and Heinen (1977), Theory X and Theory Y may be used to explain the frames of reference of designers and developers. A design or system developed according to

Theory X assumptions will lead to a highly structured system with an emphasis on order, stability and efficiency. On the other hand, Theory Y will lead to a flexible system with both end-users and technology seen as precursors to effectiveness. System designers and developers typically hold a Theory X view (Bostrom & Heinen, 1977). In this approach, the designers and developers are the experts whereas end-users are treated as another *"operating unit"* holding their place *"alongside computers, display consoles, and other forms of system operating units"*. Problems arising from the use of the systems by end-users are solved by adjusting the end-users, e.g. through training and incentives, to make them compatible with the technical system. In the Theory X view, the focus is on the technical system; the Theory X view ignores the social system which consists of the attributes of people (e.g. attitudes, skills and values), the relationships between people, reward systems and authority structures. This approach leads to systems that suffer from problems such as *"non-usage"* to *"outright sabotage"* (Bostrom & Heinen, 1977).

According to Orlikowski and Gash (1994), technology frames develop and evolve as people interact with technology, and they are helpful in understanding the development and use of technologies. Technology frames are specific to different groups in organizations and these frames are shared by people in the group. The similarities and dissimilarities between the frames of different groups are labelled as 'congruence' and 'incongruence' by Orlikowski and Gash (1994). The congruence and incongruence are important as they are useful in understanding the issues associated with the implementation and use of a technology in an organization. According to Orlikowski and Gash (1994), congruence implies agreement between groups regarding *"the role of technology in business processes"*, *"the nature of technological use" and "the type and frequency of support and maintenance"*. Incongruence reflects disagreement regarding these issues related to the technology. Orlikowski and Gash (1994) report on the incongruence between the technology frames of developers in the organization and the users. The frames have the dimensions of 'nature of technology', 'technology strategy' and 'technology in use'. The incongruence between developers and users in the organization is as follows:

- Nature of technology: developers focus on technological capabilities in isolation from the context of use in the organization; users focus on the context of use and they frequently misunderstand the technology.
- Technology strategy: developers are enamoured of the sweeping changes that technology can bring in the organization; users tend to see technology as facilitating incremental change. In terms of measuring success, developers prefer technical measures whereas users prefer business measures.
- Technology in use: developers focus only on the technical implementation of the technology and do not realize the issues arising from the use of the technology; users focus on the issues arising from the use of the technology in the organization.

This section has examined the link between the image of end-users in the perception of the developers of information systems and the impact of this image on the nature of systems developed in the organization. This confirms the link between the image of end-users in the perception of information security managers and developers and the unfriendly nature of information security policies and controls in the organization. The next section attempts to provide a way out of this imbroglio.

9.4 A pathway to the development of end-user centric information security in the organization

Hirschheim and Klein (1989) define a paradigm as consisting of *"assumptions about knowledge and how to acquire it, and about the physical and social world"*. According to the authors, in a professional community, all members typically follow a common paradigm and hence share both perceptions and practices. As already discussed earlier, these perceptions and practices are particularly important in the context of system development. The perceptions and practices of developers have a significant impact on the nature of system development, the nature of the system that is developed and the nature of the use of the system. In their work, Hirschheim and Klein (1989) presented four paradigms of information systems development. These paradigms are based on the four paradigms proposed by Burrell and Morgan (1979). Various authors have applied the four paradigms of Burrell and Morgan (1979) and Hirshheim and Klein (1989) to the study of information security (Clarke & Drake, 2003; Dhillon, 1995; Dhillon & Backhouse, 2001; McFadzean, Ezingeard & Birchall, 2006; White & Dhillon, 2005). This section provides a brief overview of the four paradigms and how these paradigms have been applied to information security. The section also provides an overview of the functionalist paradigm of the present-day technology-dominant approach to information security. The section concludes by discussing the interpretivist paradigm as the way forward to a more holistic, end-user centric approach to information security in the organization.

Burrell and Morgan (1979) defined four paradigms for classifying research. According to them, a paradigm may be defined as *"very basic meta-theoretical assumptions which underwrite the frame of reference, mode of theorizing and modus operandi"* of the researchers who operate within each paradigm. The paradigms identified by Burrell and Morgan (1979) are: 'Functionalist', 'Interpretivist', 'Radical Structuralist' and 'Radical Humanist' (see Figure 9.1). A paradigm does not represent a *"complete unity of thought"*; rather each paradigm represents certain underlying assumptions that are considered to be 'taken for granted' by the researchers working within that paradigm. The four paradigms thus divide the world into four sets of meta-theoretical assumptions.

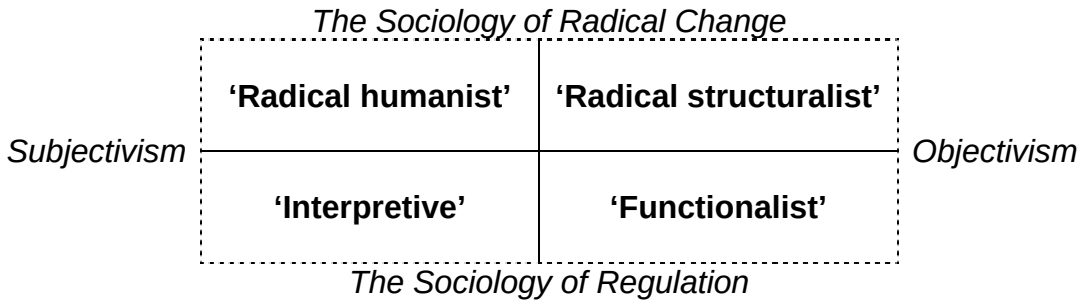


Figure 9.1: Four paradigms of Burrell & Morgan (1979)

As may be seen in Figure 9.1, the matrix of the four paradigms is composed of two axes, namely, the Subjectivism-Objectivism axis and the axis of the sociology of Radical change and Regulation. According to Burrell and Morgan (1979), objectivism is characterized by a positivistic and deterministic approach to the study of human affairs. In this approach, models and methods derived from the natural sciences are applied to the study of human affairs. Humans are treated as behaving mechanistically to their environment. Subjectivism, in contrast, brings in far more richness to the study of human affairs. Subjectivism is characterized by anti-positivism and voluntarism. In this approach, humans play a creative role and interpret and control their environment. Consequently, their affairs are studied in an anti-positivistic approach according to which the social world is relativistic, and understandable only from the perspective of the individuals involved in the activities being studied. The sociology of regulation in the other axis of the matrix represents the study of the unity and cohesiveness of society. It focuses on the need for regulation in human affairs. In contrast, the sociology of radical change is concerned with conflict, change, the deprivation of man and modes of domination. This approach is often *"visionary and Utopian"* (Burrell & Morgan, 1979).

Hirschheim and Klein (1989) applied the four paradigms of Burrell and Morgan (1979) to information systems development. They retained the subjective-objective dimension; however, instead of the regulation-radical change dimension of Burrrell and Morgan (1979), Hirschheim and Klien (1989) used the order-conflict dimension. Order emphasizes the integrationist view of the social world that is characterized by *"order, stability, integration, consensus, and functional coordination"* (Hirschheim & Klien, 1989) and *"commitment, cohesion, solidarity, consensus, reciprocity, cooperation, integration, stability and persistence"* (Burrell & Morgan, 1979). Conflict emphasizes the coercive view of the social world characterized by *"change, conflict, disintegration and coercion"* (Hirschheim & Klien, 1989) and *"coercion, division, hostility, dissensus, conflict, malintegration and change"* (Burrell & Morgan, 1979).

Using the subjective-objective and order-conflict axes, Hirschheim and Klein (1989) identified four paradigms as: 'Functionalism', 'Social Relativism', 'Radical Structuralism' and 'Neohumanism' (see Figure 9.2).

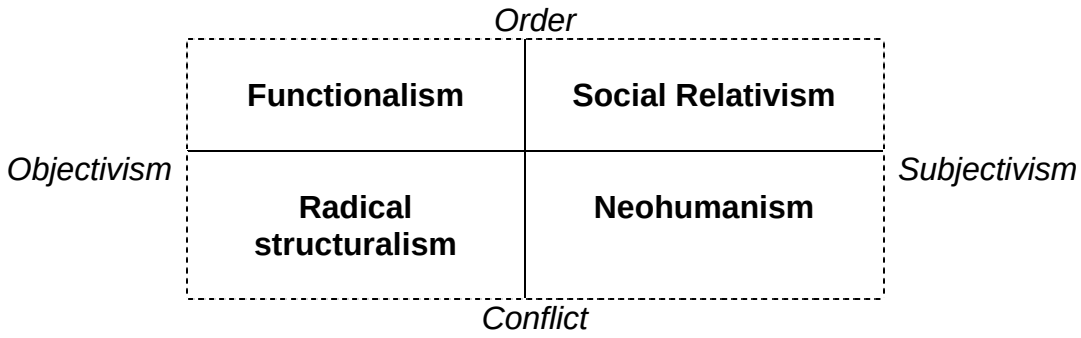


Figure 9.2: The Four paradigms of Hirschheim & Klein (1989)

The following description of the four paradigms of Hirschheim and Klein (1989) is based on Hussain and Taylor (2007):

- The functionalist paradigm: In this paradigm, the information systems developer acts as an expert. The expert takes a mechanistic approach, and uses tools and technologies to develop systems through rationalistic, procedural methodologies. In this approach, users are considered biased and hence not consulted.
- The social relativist paradigm: In this paradigm, the developer acts as a facilitator or catalyst and seeks to unravel and understand the needs and requirements of the users. The users are best placed to develop the system and they should be consulted throughout the development process. In this approach, the developer acts as a catalyst to facilitate users in reflecting and learning about the system.
- The radical structuralist paradigm: In this paradigm, the developer acts as a warrior, taking either the side of management or of users. The developer undertakes political action to change the IT environment rather than try to interpret it.
- The neohumanist paradigm: In this paradigm, the developer acts as an emancipator or social therapist. The developer seeks to gain consensus over needs and requirements amongst various stakeholders by creating an environment of debate free from any social constraints.

Dhillon (1995) and Dhillon and Backhouse (2001) have applied the four paradigms to information security. Dhillon (1995) observes that information systems researchers and developers have begun to move away from a purely technical approach to systems development;

the researchers and developers increasingly now consider the act of systems development as a social act. Unfortunately, information security researchers and developers have remained locked into their *"psychic prison"* of a *"mechanistic, technical vision"* (Dhillon, 1995). A similar view is echoed by Frangopoulos (2007), Ashenden (2008) and Albrechtsen and Hovden (2009). The present-day approach to the development of information security policies and controls lies in the functionalist paradigm. White and Dhillon (2005) have proposed using the 'interpretivist' or 'social relativist' paradigm for resolving the crisis of information security. This shift from functionalism to interpretivism is necessitated by the fact that information security relies heavily upon end-user interpretation and participation in compliance with information security policies and controls in the organization. In view of these facts, the further discussion in this section will consider only the functionalist and interpretivist approaches to information security.

In the present-day, functionalist approach to information security in the organization, the information security developer acts as an expert. The developer is focused on technology, tools and methods for controlling the access of end-users to information assets. The developer is unconcerned with the impact on end-users, their working practices, their needs and requirements. The end-users are expected to act mechanistically and according to the needs of the system. This approach satisfies the 'system ideal' and leads to a *"technology trap"*, in which technology is considered to provide the complete solution to a problem.

The interpretivist approach to information security stands in stark contrast to the functionalist approach. The interpretivist approach is a holistic approach and is based upon understanding how end-users interpret and comply with information security policies and controls in the organization. The information security developer acts as a catalyst or a facilitator who seeks to understand the working practices and needs and requirements of end-users. The emphasis is to ensure that end-users will be willing to learn, adapt and accept the information security policies and controls. This approach satisfies the 'contextualist ideal', in which the emphasis is on the social context and processes.

A comparison of the functionalist and interpretivist approaches to the formulation of information security policies and controls in the organization is given below in Tables 9.1 and 9.2.

Given the importance of end-user behaviour to the success of information security in the organization, it is to be expected that an end-user centric approach to information security is required. The present-day approach to information security is functionalistic and is therefore inappropriate. The way out, as suggested by White and Dhillon (2005) is to use an interpretivist approach. Such an approach emphasizes the 'contextualist ideal' and requires the study of the *"social context and associated processes"* of end-users, their work in the organization and their information security behaviours. The change from a functionalist to an interpretivist approach requires an antecedent change - that of changing the mind-set of the information security

developers towards recognizing and accepting a far more substantive and richer role for end-users. In the context of ISSM, this change can be brought about through the Information Security Service Culture (ISSC). Before discussing ISSC, the next section presents an overview of the related concepts of culture, service culture, information security culture and Information Security Service Culture.

Dimension	Functionalist	Social Relativist
Behavioural role	Technical expert	Change agent
Acts as an	Outsider	Insider
System requirements are	Objective	Socially constructed
Seeks to achieve	Rational analysis	Learning and system acceptance
Operates through	Tools, methods, procedures	Continual interaction
Behaviours involve users?	No	Yes, to reconcile views and gain consensus
Avoids difference and conflict?	Yes	Yes
Treats information requirements as	A product	A journey with an uncertain destination
Behaviours towards IS stakeholders	Detached, isolated, top down	Laissez-faire, interactive

Table 9.1: Behavioural dimensions for information security developers (adapted from Hussain & Taylor, 2007)

Core design ideal	Sociological paradigm	Security design ideal	Objective for design and use of information systems
Private enterprise ideal: Main objective is profitability; organization rationalization is considered fundamental	**Functionalist:** Objective is to gain competitive advantage through objective, structured and scientifically valid causal relationships.	**Systems ideal:** The primary goal is that systems should be elegant, well-organized, efficient and reliable. Security can be designed by systematically evaluating the functionalities. The designs are ahistorical and non-contextual.	**Functionalism:** Information systems development is concerned with fitting technology, i.e. it is a means to better realize pre-defined objectives. Information systems use is aimed at overcoming computation limits of man and improved productivity.
Neopopulist ideal: Practices of enterprises should be easily intelligible to ordinary citizens and be responsive to their needs.	**Interpretivist:** The endeavor is to comprehend subjectivity of experiences from the viewpoint of human actors rather than their own.	**Contextualist ideal:** System designs emphasize content, social context and the associated processes. Security designs are not imposed, but are based on an organization's communication patterns and the intentional acts of agents involved.	**Social relativism:** To elicit the design objectives and modes of use which are consistent with the prevailing conditions; to help others to understand and accept them. To develop systems which implement 'the prevailing Zeitgeist' (spirit of the times).

Table 9.2: Design ideals for developers of information security policies and controls in the organization (adapted from White & Dhillon, 2005)

9.5 Culture, service culture, information security culture and Information Security Service Culture

The concept of Information Security Service Culture is related to the three concepts of culture, service culture, and information security culture. Further, the concepts of service culture and information security culture are themselves related to the concept of culture. This section provides an overview of these concepts.

Davis (1985) defines culture as the *"pattern of shared values and beliefs that give the members of an organization meaning, and provide them with the rules for behaviour in the organization"* (Grönroos, 2007). Schein (2004) defines culture as *"a pattern of shared basic assumptions that was learned by a group as it solved its problems of external adaptation and internal integration, that has worked well enough to be considered valid and, therefore to be taught to new members as the correct way to perceive, think and feel in relation to those problems"*. Thus culture operates in an organization by shaping how people in an organization *"do certain things, think in common ways and appreciate similar goals, routines and even jokes"* (Grönroos, 2007). Culture acts as a patterning force and always exists. Researchers in the fields of service management and information security have cited the importance of culture to their respective fields.

Culture is critically important for service organizations (Grönroos, 2007; Zeithaml et al., 2008). Zeithaml et al. (2008) defines service culture as *"a culture where an appreciation for good service exists, and where good service to internal as well as ultimate, external customers is considered a natural way of life and one of the most important norms by everyone"*. Grönroos (2007) states that *"a functioning service culture requires that providing good service is second nature to everyone within that organization"*. Further, service culture arises when all organizational components such as *"organizational routines, directions for action given by policies and management and reward systems"* converge together to emphasize good service to customers, whether internal or external. Culture, as the attitude of its employees, is particularly important for service organizations. Because delivering a service involves the coming together of the employees and their customers, employee attitudes and performance are visible to customers. Hence the attitude of employees, as a reflection of the service culture in the organization, becomes critically important.

According to Von Solms (2000), the idea of information security culture (ISC) emerged in the third wave of information security evolution. The idea of information security culture *"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"* (Von Solms, 2000). Martins and Eloff (2002) define ISC *"as the assumption about which type of information security behaviour is accepted and encouraged in order to incorporate information security characteristics as the way in which*

things are done in an organization". Ramachandran, Rao and Goles (2008) state that ISC involves *"identifying the security related ideas, beliefs and values of the group, which shape and guide security-related behaviours"*. The importance of ISC lies in the fact that it fosters an attitude in end-users whereby safe information security behaviours become a way of organizational life for these end-users (Van Nekerk & Von Solms, 2005; Von Solms, 2000). ISC shapes and guides the behaviour of end-users in the organization in regard to information security policies and controls.

Information Security Service Culture (ISSC) is based upon the concepts of culture and service culture. ISSC refers to the culture, and hence the patterns of shared values and beliefs, amongst the Information Security Service Management managers and employees in the organization. Just as culture and service culture apply to the employees of the organization, ISSC applies to the members of the ISSM function. ISSC consists of the patterning force of culture that drives the information security managers, the developers and other staff members to deliver 'good service' to their customers, namely, the end-users in the organization. ISSC becomes visible when end-users come in contact with information security service members and the information security policies and controls in the organization. Further, as stated above, ISSC can arise only when all the different organizational components come together to stress 'good service' to end-users. ISSC and 'good service' to end-users, however, do not imply that the security needs of the organization's information assets are to be completely ignored; it only means that while these classical security issues are also important, service to end-users should play the dominant role.

The inter-relationship between culture, service culture, information security culture and ISSC are shown in Figure 9.3. According to this figure, both concepts of Information Security Service Culture and information security culture are based upon the concept of culture; ISSC is also based upon the concept of service culture. ISSC differs from information security culture in that ISSC applies to the employees of the ISSM function, particularly the developers, whereas information security culture applies to the customers of the ISSM function i.e. the end-users in the organization. Furthermore, while ISSC seeks to promote an end-user centric approach to information security, ISC seeks to promote the compliance of end-users with information security policies and controls in the organization. It is also pertinent to note that both ISSC and ISC contribute to the state of information security in the organization.

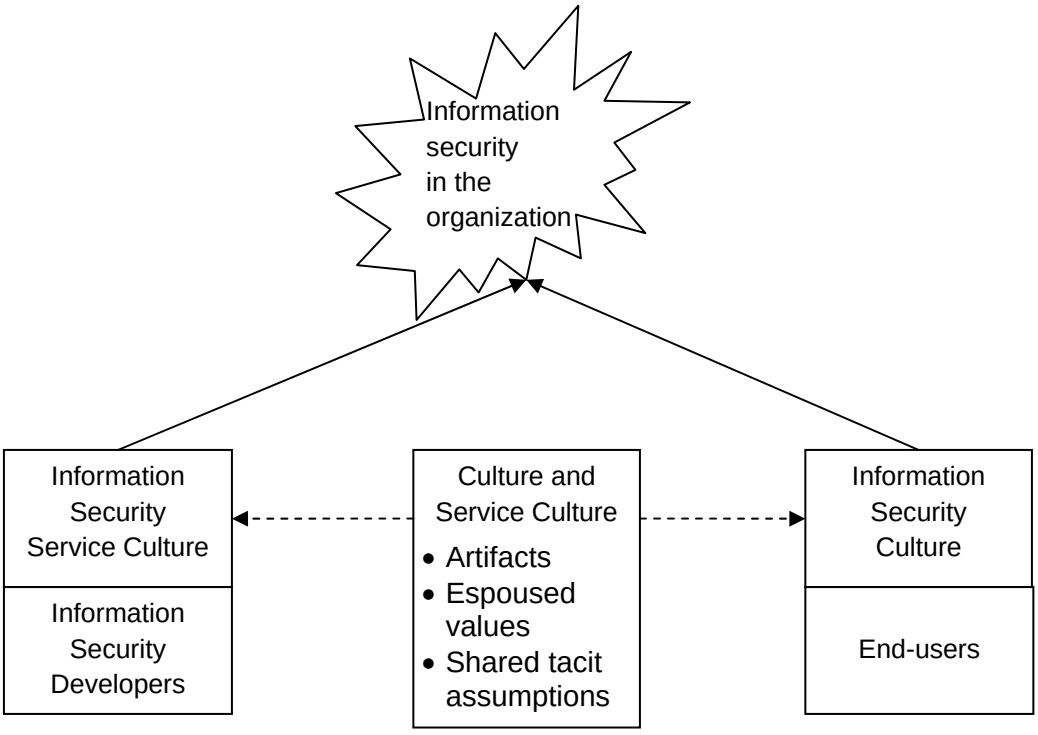


Figure 9.3: Information Security Service Culture and Information Security Culture leading to effective information security in the organization

Having discussed the meaning and the role of various types of cultures, it is important to understand the constituent parts of culture. According to Schein (2004), culture exists at three levels – 'artifacts', 'espoused values and beliefs' and 'underlying assumptions' (see Figure 9.4). The topmost level is that of artifacts. Artifacts are the observable phenomena that reflect a particular culture. In the context of a group, artifacts are the visible behaviour of the group. In an organization, artifacts refer to the organizational processes and structural elements that lead to the behaviour of the constituent groups. Espoused values and beliefs are psychological or attitudinal in nature, and exist at the conscious level. They reflect the strategies, goals and philosophies of the group. While artifacts are the visible manifestations of behaviour, espoused values and beliefs are the invisible determinants of behaviour. Below the beliefs and values at the conscious level, lie the shared tacit assumptions. Shared tacit assumptions operate at the unconscious level and are deeply ingrained. These assumptions are 'taken-for-granted' and are strongly held by a group.

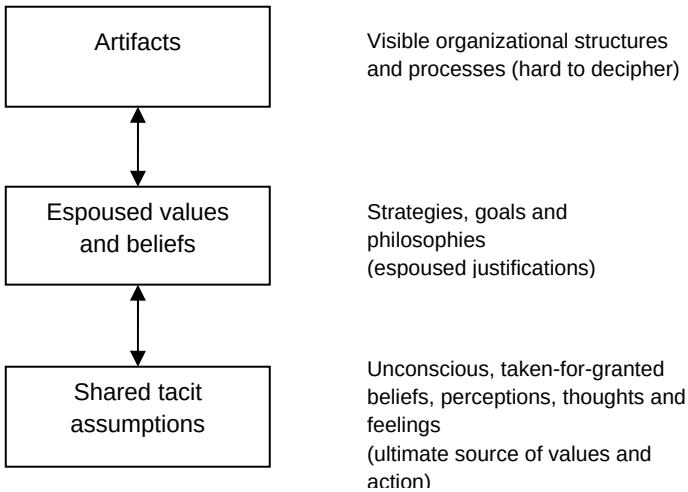


Figure 9.4: Levels of Culture (from Schein, 2004)

The role of culture as a patterning force is extremely important for organization, particularly in a service context. The above discussion has provided an overview of the related concepts of culture, service culture, information security culture and Information Security Service Culture. ISSC differs from information security culture in that ISSC applies to the employees of the ISSM function whereas information security culture applies to the customers, i.e. the end-users, of the ISSM function. The influence of ISSC over information security support employees has already been discussed in Chapter 8. The next section discusses in greater detail the influence of ISSC over information security managers and developers who formulate information security policies and controls in the organization.

9.6 Information Security Service Culture

The previous sections have highlighted the crucial role of the attitude of the developers of systems towards the end-users of those systems. This attitude plays an important role in shaping how the system is developed, how the developers incorporate human issues and, finally, how the system is accepted and used by the end-users. These attitudes have been variously labelled as the 'engineering culture' (Schein, 1996 and 2004), 'frames of reference' (Bostrom & Heinen, 1977), 'technology frames' (Orlikowski & Gash, 1994) and 'paradigms' (Burrell & Morgan, 1979; Hirshheim & Klein, 1989). These concepts are applicable in the development of information security policies and controls in the organization (Clarke & Drake, 2003; Dhillon, 1995; Dhillon & Backhouse, 2001; McFadzean et al., 2006; White & Dhillon, 2005). The traditional approach to information security has been technology oriented, or functionalist, and therefore it has failed

to garner support from end-users; the way out of this imbroglio is to use an interpretivist approach to information security (White & Dhillon, 2005). This section proposes and discusses Information Security Service Culture (ISSC) as a means of moving developers of information security policies and controls from the functionalist to the interpretivist paradigm.

A key aspect of Schein's model of culture, as discussed in the previous section, is the disconnect that can occur between the three levels of culture in a group or organization. Espoused beliefs and values at the conscious level may be said to predict behaviours at the artifacts level. However, if the beliefs and values are incongruent with the assumptions at the unconscious level, then there can be a misalignment between what people 'say' they will do in a situation and what they actually 'do'. Thus as Schein (2004) says, *"a company may say that it values people and that it has high quality standards for its products, but its record in that regard may contradict what it says"*. If the espoused beliefs and values are congruent with the underlying assumptions, then there is alignment between what people 'say' and what they 'do'. In the context of information security, it may be said that information security developers and managers suffer from an incongruence between their underlying assumptions and their espoused beliefs and behaviours – there is misalignment between what they say and what they do in respect of end-users – they profess the importance of end-users to information security and yet, they continue to formulate information security policies and controls with scant regard for the needs and requirements of the end-users.

Information Security Service Culture is an attempt to align what information security developers and mangers say with what they actually do, i.e. to align the espoused with the enacted. In terms of information security, this means that developers and managers adopt the interpretivist paradigm and that the organization provides them with the encouragement and resources to enable them to formulate end-user centric information policies and controls. The three levels of culture can thus be mapped as follows:

- **Shared tacit assumptions**
  At the unconscious level, developers and managers of information security should hold the beliefs that end-users are not their 'enemy', rather the end-users are an 'asset'. They should also believe that the end-users want to comply with information security policies and controls; and that there often is no malicious intent behind their non-compliance. End-users want to work in the interest of their organization. Any non-compliance is largely a result of the cognitive limitations of end-users or because the information security policies and controls are incompatible with their work practices. The information security developers and managers should also believe that end-users are their customers and that they are there for providing the information security service to the end-users. In this frame of mind, the end-users become the raison d'être of the information security developers and managers.

- **Espoused values and beliefs**

  This is the conscious level at which the strategies, goals and philosophies exist. At this level, the information security developers and managers should utilize technologies, tools and methods that lead to end-user centric information security policies and controls in the organization. End-user acceptance and the ease of use of policies and controls should be important determinants of the security measures. Further, formulation of information security policies and controls must not happen in isolation from end-users; but rather, in keeping with the interpretivist paradigm, policies and controls should be formulated with the active involvement of the end-users. ISO/IEC 9241-210:2010 is an international standard titled *"Human-centred design for interactive systems"* (ISO/IEC 9241-210, 2010). Information security policies and controls are 'interactive systems' and this standard, with its focus on designing human-centred interactive systems, can provide useful guidance for their formulation. According to this standard, formulation of end-user centric information security policies and controls would require *"an approach to interactive systems development that aims to make systems usable and useful by focusing on the users, their needs and requirements, and by applying human factors and ergonomics, and usability knowledge and techniques"* (ISO/IEC 9241-210, 2010). This standard wwould enable information security developers and managers to *"design and redesign processes to identify and plan effective and timely human-centre design activities"*. According to ISO/IEC 9241-210:2010, the principles of human-centred design are:

  a. The design is based upon an explicit understanding of users, tasks and environments.
  b. Users are involved throughout design and development.
  c. The design is driven and refined by user-centred evaluation.
  d. The process is iterative.
  e. The design addresses the whole user experience.
  f. The design team includes multidisciplinary skills and perspectives.

- **Artifacts**

  The artifacts level is populated by organizational processes and structures, as well as the behaviours of information security developers and managers. The artifacts level is also populated by the end-user centric information security policies and controls. These end-user centric policies and controls will be acceptable to end-users, be usable by them and will earn the commitment of end-users to information security. ISO/IEC 9241-210:2010 provides guidance on the activites that need to be performed for the development of human-centred interactive systems. These activities are:

  a. Understanding and specifying the context of use.
  b. Specifying the user requirements.
  c. Producing design solutions.
  d. Evaluating the design.

  The artifacts level is also populated by the behaviours of business managers and IT managers – their behaviours create an end-user centric environment for the day-to-day work that

promotes safe information security behaviours of end-users. Adequate encouragement, knowledge and resources must be provided to ISSM managers and developers to enable them to undertake the formulation of end-user centric information security policies and controls in the organization. Leadership is a key aspect of building a service culture (Bartley, Gomibuchi & Mann, 2007; Grönroos, 2007; Mather, 2008). The behaviour of managers in supporting the developers in their end-user centric endevaours removes any incongruence between what is said and what is actually done. According to Grönroos (2007), any incongruity in the stance of managers will be detrimental to establishing an Information Security Service Culture – if managers do not walk their talk, then developers too will be unable to deliver end-user centricity.

The three levels of the Information Security Service Culture are shown in Figure 9.5.

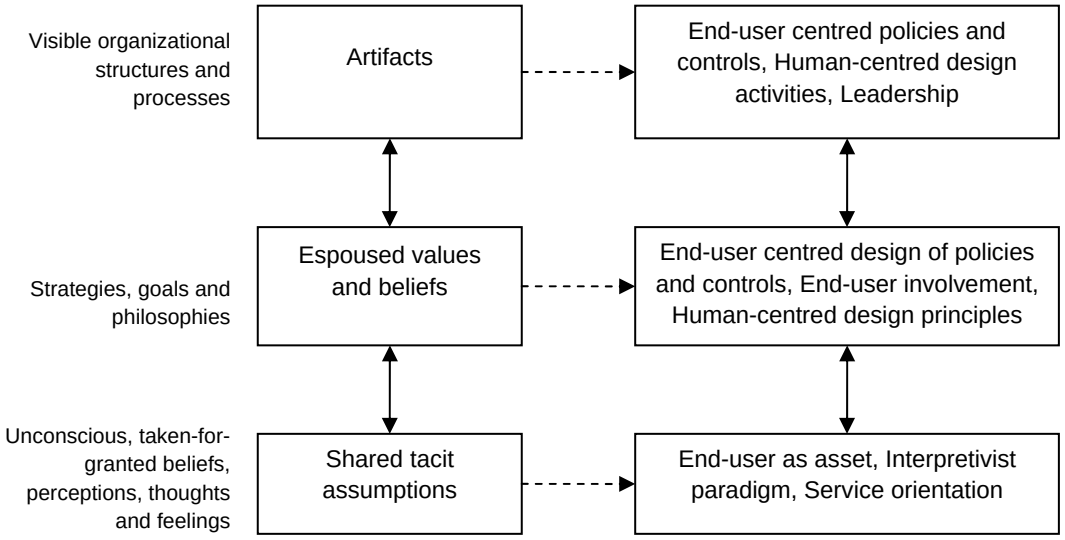


Figure 9.5: The three levels of Information Security Service Culture (ISSC)

9.7 Conclusion

This chapter began with a quote from Abraham Lincoln. The quote depicts the importance of people to the democratic form of government. Likewise, the end-users are of vital importance to information security in the organization. This fact is acknowledged by the end-user centric focus

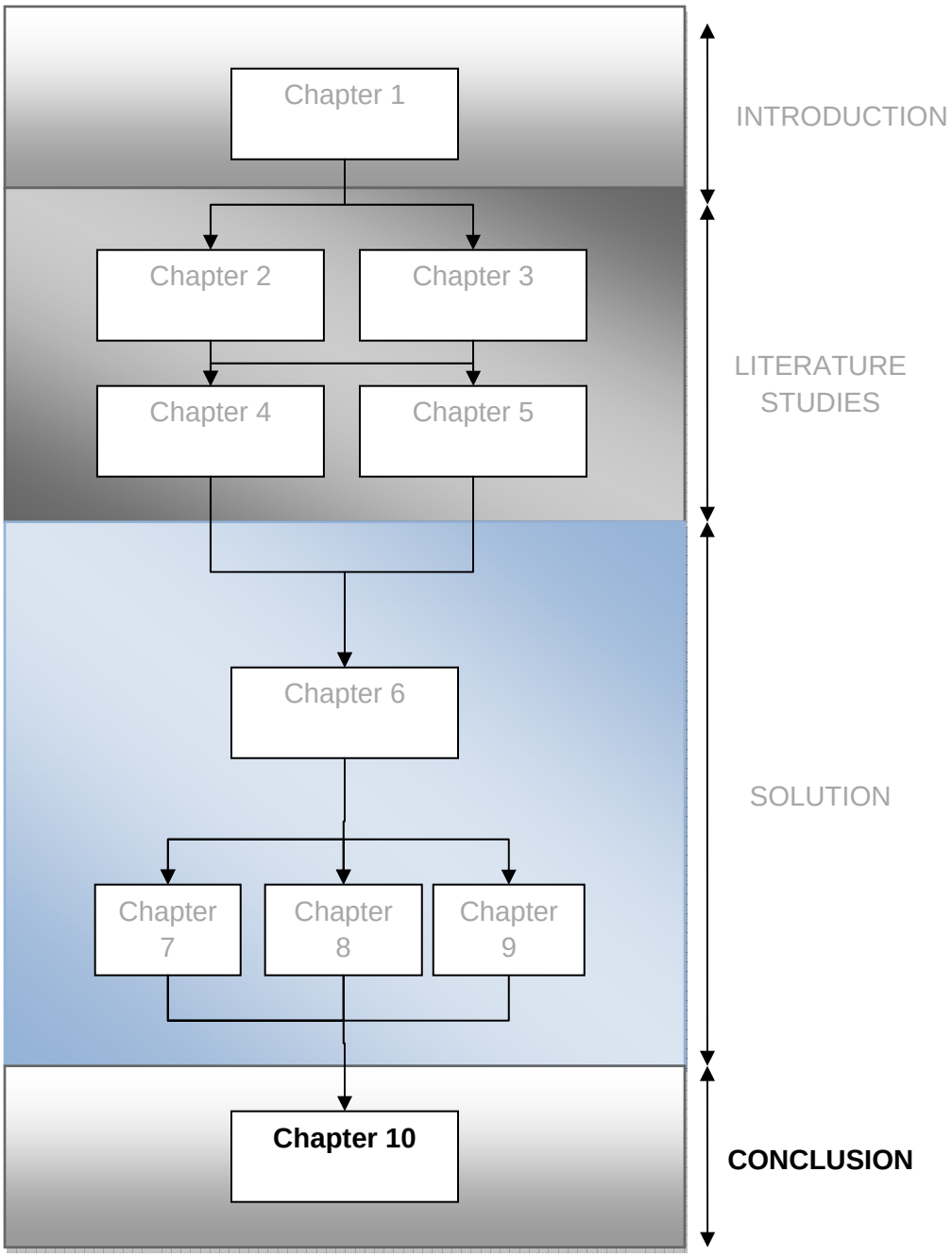
of the CARE principles and ISSM. However, before ISSM can be adopted and implemented in an organization, it is essential that the information security managers and developers develop an appropriate mind-set towards end-users and a culture of service towards the end-users. This chapter has discussed Information Security Service Culture and identified the components of this culture in terms of shared tacit assumptions, espoused values and beliefs and artifacts. ISSC underpins the ISSM approach and serves as the foundation of an end-user centred approach to information security in the organization.

This chapter brings to a close the discussion of ISSM that began in Chapter 6. The ISSM approach has three components, namely, Information Security Service Branding, Information Security Service Support and Information Security Service Culture. This chapter on Information Security Service Culture completes the presentation of the components of ISSM.

The next chapter is a cumulative conclusion to this thesis. It provides an evaluation of the research in meeting its research objective and also includes suggestions for further research.

SECTION IV

CONCLUSION



CHAPTER 10

Conclusion

"Nothing is more difficult, and therefore more precious, than to be able to decide."

- Napoleon Bonaparte

10.1 Introduction

This thesis is a report of the research undertaken in an attempt to improve the effectiveness of information security management in tackling the general problem of end-user non-compliance with information security policies and controls in the organization. To accomplish this aim, the following topics, inter alia, were examined: the information security behaviours of end-users; studies of human behaviour in various other disciplines; the management of people in the organization and the effect of managerial style on the behaviour of people in the organization; the nature of present-day approach to information security management; service management approach; and various other related topics such as service branding, service encounters and service culture.

In this research project, it has been argued that the general behaviour of end-users in an organization is not entirely under their control, but is actually determined by various conditions existing in the organization. These conditions are created by the managerial style prevailing in the organization, which in turn, is determined by the managerial assumptions regarding human nature. In the context of information security in the organization, this argument can be re-stated as follows: the information security behaviours of end-users, particularly their non-compliance, result from the underlying assumptions that information security managers in the organization hold regarding the nature of end-users. Currently, these assumptions treat end-users in an antagonistic manner and the present-day approaches to information security management are based on the principles of scientific management and bureaucracy. These facts set up the vicious circle of bureaucratic information security management (shown earlier in Figure 6.1) and lead to non-compliance by end-users. In an attempt to tackle this problem, it was argued that

information security management needed to adopt a more friendly approach towards end-users and become end-user centric. This research has suggested a solution in the form of the CARE principles and Information Security Service Management (ISSM). ISSM, based upon the CARE principles, sets up the virtuous circle of Information Security Service Management (shown earlier in Figure 6.2). This leads to end-user centric information security in the organization which aims to obtain the commitment and compliance of end-users to information security policies and controls in the organization.

This thesis began as a journey of both discovery and invention. This chapter is the concluding chapter of this thesis and evaluates whether the research objectives of this thesis have been met, or not. The evaluation forms the next section. The subsequent section identifies certain areas for future research.

10.2 Evaluation of research outcomes

The primary objective of this research was to develop an understanding as to how information security management in an organization can be improved. The purpose of these improvements is to bridge the divide between information security managers and end-users leading to improved compliance by end-users to the information security policies and controls in the organization. This objective was stated in section 1.4 as the following problem:

To identify an improved approach to ISM that can assist in resolving the end-user crisis and lead to improved compliance of end-users with the information security policies and controls in the organization.

To achieve this primary objective, a number of secondary objectives need, initially, to be addressed. These secondary objectives provide a road-map for this research and are:

- To understand the information security behaviours of end-users and the reasons behind non-compliance.
- To understand the link between managerial styles and the behaviours of employees in the organization.
- To study the dominant managerial style inherent in present-day ISM and how it leads to the end-user crisis.
- To identify a management approach that has the potential to resolve the end-user crisis.
- To apply this identified approach to formulate an alternative approach to ISM and to identify the components of this approach so it can be applied in organizations for the management of information security.

The secondary objectives are vital as they help in providing a pathway to the successful resolution of the problem studied in this research. The remainder of this section addresses the secondary objectives.

- **Research Objective:** To understand the information security behaviours of end-users and the reasons behind non-compliance.

This objective helped understand the information security behaviours of end-users, particularly their non-compliance with information security policies and controls in the organization. This issue was taken up in Chapter 2 which also explored the study of human behaviour in various other disciplines. The investigation was based upon the works of several other authors and researchers in the field of information security and other disciplines.

Chapter 2 began with an investigation into the kinds of non-compliances that end-users exhibit as they interact with information security policies and controls in the organization. These non-compliant behaviours occur at all levels of this interaction, i.e. at the awareness, attitude and skill levels. The difficulties faced by end-users were the hurdles of perception failings, priority or responsibility failings and the capability or usability failings. It was also discussed that a difficulty in any of the stages could force the end-users away from compliance towards non-compliance.

Chapter 2 then undertook the study of human behaviour in the domains of 'thinking under risk' and 'human error'. The research in the domain of 'thinking under risk' indicated that end-users in the organization are often faced with a trade-off as they come across information security policies and controls during their day-to-day work in the organization. This trade-off is between non-compliance versus productivity or of compliance versus lost productivity. In the presence of various factors, this trade-off is frequently decided in favour of productivity and non-compliance. The studies in the domain of 'human error' also underline this fact. According to this domain, humans are intrinsically error-prone and this leads to unintended consequences for organizations. There are two approaches that organizations can adopt in dealing with this issue – these are the 'person' approach or the 'old view' and the 'system' approach or the 'new view'. In the person approach or the old view, the end-user is the sole cause of the error and remediation is targeted at him/her. In the system approach or the new view, the end-user is only the immediate cause of the error; however, the error is believed to originate in the organization. Consequently, the remediation has to target not only the end-user but also the organization.

The discussion then turns to the study of loyalty and commitment as determinants of human action. Loyalty and commitment exist as psychological bonds that bind people to a course of action. The discussion also distinguishes between true and spurious loyalty. In true loyalty, behavioural consistency is built upon underlying psychological commitment; in spurious loyalty,

behavioural consistency exists but without the psychological commitment. In the context of business, the loyalty and commitment of customers comprise a cherished goal, since loyal and committed customers lead to repeat purchases and to improved profitability for the business. However, while 'true loyalty' customers are unlikely to switch to competitors, 'spurious loyalty' customers are likely to shift at the slightest opportunity.

The chapter finally discussed the Theory of Planned Behaviour (TPB). TPB explains the factors that drive human behaviour in any given situation. According to the TPB, behaviour is determined by personal and social factors as well as the information available with the person; further, behaviour is also determined by the person's beliefs about the difficulty or ease of performing the behaviour.

The research objective was satisfied as the discussion in Chapter 2 uncovered the complexity of the information security behaviours of end-users in the organization. The discussion also emphasized that it may not be entirely justified to blame end-users solely for any non-compliance; the non-compliance likely results from various other factors prevailing in the organization.

- **Research Objective:** To understand the link between managerial styles and the behaviours of employees in the organization.

This objective helped understand how the managerial style in an organization creates the conditions that influence how end-users will behave in the organization. This issue was explored in Chapter 3 based upon the works of several management researchers.

Chapter 3 explored various organizational typologies and management theories. The typologies discussed include those proposed by Davis (1968), Etzioni (1975), Pheysey (1993) and Schein (2004). Pertinent to this research, all the typologies identify a defining characteristic of organizations. This defining characteristic of an organization relates to the understanding of human motivation and behaviour in the perception of its managers. This perception is vital as it determines the amount of democratization and the participation of employees in management. This further influences the kinds of behaviours exhibited by employees in the organization.

Subsequently, the chapter provided an overview of different management theories, including Taylor's scientific management, Weber's bureaucracy, Mayo's human relations model and finally, McGregor's Theory X and Theory Y. Each management theory has its underlying perception of employees and concepts of dealing with these employees. Theories X and Y explain two competing conceptions of employees. In Theory X, employees are considered as inherently uncommitted and unwilling to work. In this setting, management is responsible for organizing the elements of production, and motivating, directing, controlling people for the

completion of work through incentives and coercion. In Theory Y, employees are committed and willing to work and management only needs to arrange organizational conditions and methods of operation in order to enable employees to achieve their goals.

The investigation in Chapter 3 also included a discussion of the dysfunctional effects of a managerial style based on the principles of scientific management and bureaucracy. In this management style, as in Theory X, employees are motivated by using the carrot and stick approach; however this leads to indolence, passivity, resistance to change, lack of responsibility, willingness to follow any demagogue and unreasonable demands for economic benefits.

The discussion in Chapter 3 firmly established the link between managerial perceptions and style and the behaviour of employees in the organization. This achieved the research objective.

- **Research Objective:** To study the dominant managerial style inherent in present-day ISM and how it leads to the end-user crisis.

This objective helped understand how the managerial style of information security management in an organization creates the conditions that influence the information security behaviours of end-users in the organization. Chapter 4 explored information security management (ISM) and its embodiment, namely, the information security management system (ISMS), based upon the works of several researchers and the ISO/IEC 27000 family of international standards. Chapter 4 treated the terms ISM and ISMS synonymously.

Chapter 4 provided an overview of present-day ISM in the organization. ISM is essential to the success of information security in the organization. ISM, operating through an ISMS, establishes an environment of information security in the organization through its constitutive structures, processes and procedures. ISO/IEC 27001:2005 (ISO/IEC 27001, 2005) adopts a ‘process approach’ for implementing an ISMS in the organization. The chapter also discussed the evolution of information security through four waves. This discussion established the dominance of the technical aspects of information security and the rather simplistic approach to the issue of end-users.

The discussion in Chapter 4 also explored the nature of the present-day ISM. According to the discussion, present-day ISM is based upon the principles of scientific management and bureaucracy. Under this approach, information security managers adopt the position of technical specialists and then proceed to apply a ‘command and control’ style to information security management. This style treats end-users antagonistically and largely ignores their needs and requirements.

The discussion in Chapter 4 firmly established the bureaucratic nature of present-day ISM. This, combined with the earlier discussions, established the link between the non-compliance of end-users and the bureaucratic nature of information security management in the organization. The end-user crisis is stated in section 1.2 as:

Knowing the important role that end-users play in information security, ISM concerns itself with achieving end-user compliance with information security policies and controls; however, on the contrary, present-day ISM is leading to the creation of a digital divide between information security managers and end-users; this failure of ISM constitutes its end-user crisis.

This paradox of information security management, in which it achieves exactly the opposite of its stated objective, is confirmed. A bureaucratic managerial style establishes dysfunctional organizational conditions which lead to uncommitted employees. By analogy, bureaucratic information security management leads to end-users who are uncommitted to information security and exhibit non-compliance with information security policies and controls in the organization. By establishing this link, the discussion culminated the problem discovery phase of this research.

- **Research Objective:** To identify a management approach that has the potential to resolve the end-user crisis.

The task of identifying an appropriate management approach signaled the commencement of the solution invention phase of the research. This objective led to the identification of a management approach that could be applied to resolve the paradox of the end-user crisis of information security management in the organization. The approach identified was the service management approach.

Chapter 5 provided an overview of the concepts of services and service management. Service management is a mind-set that enables organizations to focus on their customers. Further, since it is a mind-set, the concept of service management is applicable to all types of businesses and activities. The discussion distinguished between the three management paradigms, namely, the manufacturing paradigm, the bureaucratic-legal paradigm and the service paradigm. The service paradigm differs from the other two in the intensity of its focus on its customers. In the service paradigm or service management approach, the focus is on the customer and the customer's interactions with the service provider. Furthermore, the quality of service is not just about conforming to technical standards and specifications, but it revolves primarily around customer satisfaction.

Chapter 5 also discussed the application of service management to internal services and to IT management in the organization. Internal services consist of employees of the organization who become customers, and thus, service providers to each other in the organization. The same logic is applied to IT management in which the end-users are the customers and the IT function becomes the service provider. The service management approach helps both internal services and IT management in achieving customer orientation.

In the context of information security, the service management approach provides a pathway to an end-user centric managerial style. In this style, information security management is focused not on the technical standards and specifications, but on the needs of end-users and how end-users can be assisted in coping with the requirements of information security.

The discussion in Chapter 5 established service management as a suitable approach for an alternative and improved style of information security management in the organization. This achieved the research objective.

- **Research Objective:** To apply this identified approach to formulate an alternative approach to ISM and to identify the components of this approach so it can be applied in organizations for the management of information security.

The research objective was achieved with the formulation of the CARE principles, Information Security Service Management (ISSM) and the ISSMCube model. Further, the delineation of the components of ISSM – ISS Branding, ISS Support and ISS Culture, completed the solution invention phase of this research, achieving the overall objective of this research.

Chapter 6 laid the foundation of the ISSM approach in terms of the CARE principles and the shifts in management approach. The CARE principles consist of the 'Communicate', 'Accommodate' and 'Respond' elements that serve as the foundation of an end-user centric approach to information security management.

The ISSM approach is based on the concepts of service management and is structured to deliver information security management based on the CARE principles. This means that ISSM moves information security management away from its bureaucratic roots. ISSM utilizes the customer focus of service management to achieve end-user centricity for information security management. In this approach, the focus of information security management shifts away from the compliance of end-users to their commitment. The CARE principles provide the required guidance to enable this shift.

Identification of the CARE principles and ISSM satisfied the first part of this research objective, namely, that of formulating an alternative, improved approach to ISM in the organization. The

second part of the research objective was to provide guidance on how ISSM could be applied in organizations. The ISSMCube and the delineation of the components of ISSM in subsequent chapters (Chapters 7, 8 and 9) completed this aspect as well.

The ISSMCube shows the inter-relationships between the issues related to implementing ISSM in the organization. These issues constitute the six faces of the ISSMCube. An organization can implement ISSM by incorporating these issues. The issues (as depicted by the six faces of the ISSMCube) are:

(1) The CARE Principles.
(2) The position of ISSM in the organization in the midst of Business Management, IT Management and end-users in the organization.
(3) The internal organization of ISSM so as to be able to deliver information security as a service.
(4) Information Security Service Branding (ISSB).
(5) Information Security Service Culture (ISSC).
(6) Information Security Service Support (ISSS).

Chapters 7, 8 and 9 provided guidance on the three components of ISSM as they implement the CARE principles. ISS Branding applies the concepts of brands and branding to implement the 'communicate' element of the CARE principles (Chapter 7); ISS culture implements the 'accommodate' element by identifying the components of an end-user centric culture for information security managers and developers (Chapter 9); and ISS Support utilizes the concept of service encounters to implement the 'respond' element of the CARE principles (Chapter 8). This achieves the second part of the research objective.

This research project began with the objective of identifying an approach to information security management that could resolve the paradox of the end-user crisis of information security in the organization. In order to achieve this objective, the research proceeded in two phases – the problem discovery phase and the solution invention phase. Both phases relied upon an extensive review of the works of various researchers in the disciplines of information security and several other disciplines pertinent to this research. The problem discovery phase was completed by the discussions in Chapters 2, 3 and 4. This phase culminated in the identification of the bureaucratic nature of present-day information security management as being the underlying cause of the non-compliance of end-users. The solution invention phase of this research began in Chapter 5 and proceeded through Chapters 6, 7, 8, and 9. This phase culminated in the invention of the CARE principles, the ISSM approach, the ISSMCube and the components of ISSM – ISS Branding, ISS Culture and ISS Support – as the vehicles for resolving the end-user crisis. The research, it may be asserted, has achieved its objective.

This research project has relied upon peer review for the validation of its research results. During the course of this research, a number of papers were prepared and submitted to various conferences and journals. The papers covered the problem discovery and the solution invention phases. The papers discuss the genesis of the problem of end-user non-compliance, the failure of present-day information security management in tackling this challenge and the solution in the form of an alternative, improved approach to information security management. The papers also present the details of the proposed solution. The details of the papers are as follows:

- Rastogi, R., & von Solms, R. (2009). A service-oriented approach to information security management.
  This paper discusses the problem of end-user non-compliance with information security policies and controls in the organization. It establishes the failure of present-day information security management in tackling the end-user crisis. The paper provides a solution to the problem in the form of an alternative approach to information security management. This solution is Information Security Service Management (ISSM) based upon the principles of service management. The paper explores the concept of service management and presents ISSM to the information security community. The paper was presented at the 7th Annual Conference on Information Science, Technology & Management (CISTM) *"Sustaining a Knowledge Economy"* and published in its proceedings. A modified version has also been submitted to the Journal of Information System Security (JISSec).
- Three papers were prepared discussing the individual components of ISSM, namely, Information Security Service Branding, Information Security Service Support and Information Security Service Culture. These papers have been submitted to various conferences and journals for peer review. The details of the papers are:
  - "Information Security Service Branding – beyond information security awareness".
    This paper has been accepted for presentation at the 9th International Conference on Education and Information Systems, Technologies and Applications: EISTA 2011, USA. The paper discusses the negative image of information security in the perception of end-users and how this leads to non-compliance by end-users. Present-day information security management relies upon information security awareness programs to obtain end-user compliance. However, as the paper shows, this approach fails to achieve its objective as it neglects the issue of image. The paper presents Information Security Service Branding (ISSB) to create a positive brand image for information security in the perception of end-users.
  - "Information Security Service Support – helping end-users cope with security".
    This paper has been accepted for publication by the Journal of Computer Technology and Application. The paper discusses the problems faced by end-users as they interact with information security policies and controls in the organization. It establishes that end-users are unable to navigate and comprehend various policies, controls and associated issues and hence need support. According to the paper, the solution lies in

Information Security Service Support (ISSS) which is based upon the concept of service encounter in the service industry.

- "Information Security Service Culture – information security for end-users".
  This paper has been submitted to the Human Aspects in Information Security and Assurance (HAISA 2011) conference. The paper establishes that information security managers and developers demonstrate indifference to the needs of end-users in the organization. This indifference leads to the formulation of information security policies and controls that violate the principles of usability and psychological acceptability, and which, in turn, lead to non-compliance by end-users. The paper posits that the root cause of the non-compliance of end-users lies in this indifference. The paper presents a solution in the form of Information Security Service Culture (ISSC) which seeks to transform information security managers and developers from being technology-focused to becoming end-user focused in their approach.

10.3 Directions for future research

The research began with an attempt at understanding the non-compliance of end-users with information security policies and controls in the organization. It proceeded through establishing the bureaucratic nature of present-day information security management as the cause. Finally, the research culminated in the identification of ISSM as an alternative, improved approach to information security management that has the promise of achieving the commitment and compliance of end-users. The research established the theoretical basis of ISSM based upon an analysis of present-day information security management and the concept of service management.

This research has developed the concept of ISSM. Guidance is also provided for the implementation of ISSM in the organization. This guidance is in the form of the details of the components of ISSM, namely, Information Security Service Branding, Support and Culture. This research presents ISSM to the information security community as a promising alternative approach to information security management. It is now up to the information security community to adopt ISSM and to implement its various components in the organization. This would allow for the concept to be tested in the real world.

A further issue that needs to be understood is how the information security function itself changes under the influence of ISSM. To support ISSM, the traditional structures, processes and procedures of present-day information security management will have to undergo changes. This research has identified the shifts necessitated by ISSM; however, much detailing still needs to be done. Some possible locales for these changes are the educational and skill requirements of information security managers and developers in the organization; the structural and resource

requirements of ISSM; and, the integration of ISSM in the governance of the organization. A crucial issue is how ISSM will be adopted in an organization that otherwise adopts a bureaucratic stance towards the general management of its employees. Here it can be stated that the structure of ISSM lends itself to piecewise implementation. ISSB, ISSS and ISSC can be implemented either alone or in any other combination. This allows ISSM to be gradually adopted into the organization.

These areas of further research point towards the study of issues related to the implementation of ISSM in the organization. They do not undermine the value of ISSM as a concept. As stated earlier in section 5.3, in the present times, all types of organizations are adopting the service paradigm and this paradigm will be the management style of most businesses in the future. It can be safely stated that most organizations will be able to adopt ISSM and resolve their problem of end-user compliance.

10.4 Epilogue

Information, and IT, are critical assets for most organizations in the 21st century. The rising value of these assets to organizations has created a new problem – that of protecting these assets. This problem has given birth to the disciplines of information security and its management in organizations.

Through its evolution over several decades, information security has now come to realize the value of end-users to the protection of information assets in the organization. End-users have the potential to be the ‘human firewall’, but they also have the vulnerability of being the ‘weakest link’. End-users often find it difficult to comply with information security policies and controls in the organization. This non-compliance jeopardizes the effectiveness of information security in the organization. Information security management has responded through ever more stringent policies and controls and feeble attempts at training and awareness programs aimed at end-users. This has established the paradox of the end-user crisis and the vicious circle of bureaucratic information security management. The solution lies in reconceptualizing end-users as committed individuals willing to participate in the protection of the information assets of the organization. This reconceptualization paves the way forward to an end-user centric approach to information security. This research proposes Information Security Service Management (ISSM) as this approach – an approach based on the principles of service management. ISSM promises to resolve the end-user crisis and to achieve the commitment and compliance of end-users. ISSM is the 21st century solution to a 21st century problem.

References

Aaker, J. L. (1997). Dimensions of brand personality. *Journal of Marketing Research*, 34(3), 347-356.

Adams, A., & Sasse, M. A. (1999). Users are not the enemy. *Communications of the ACM*, 42(12), 40-46.

Ajzen, I. (1991). The theory of planned behavior. *Organizational Behavior and Human Decision Processes*, 50(2), 179-211.

Ajzen, I. (2001). Nature and operation of attitudes. *Annual Review of Psychology*, 52, 27-58.

Ajzen, I. (2005). *Attitudes, personality, and behavior* (2nd Ed.). Milton-Keynes, England: Open University Press / McGraw- Hill.

Ajzen, I., & Fishbein, M. (2005). The influence of attitudes on behavior. In D. Albarracín, B. T. Johnson, & M. P. Zanna (Eds.), *The handbook of attitudes* (pp. 173-221). Mahwah, NJ: Erlbaum.

Albrechtsen, E. (2007). A qualitative study of users' view on information security. *Computers & Security*, 26(4), 276-289.

Albrechtsen, E. (2008). *Friend or foe? Information security management of employees*. Doctoral Thesis, Norwegian University of Science and Technology, Faculty of Social Sciences and Technology Management, Department of Industrial Economics and Technology Management. Retrieved June 20, 2010, from http://ntnu.diva-portal.org/smash/record.jsf?searchId=1&pid=diva2:231438.

Albrechtsen, E., & Hovden, J. (2009). The information security digital divide between information security managers and users. *Computers & Security*, 28(6), 476-490.

AMA (2010a). Dictionary. *Marketing Power - American Marketing Association*. Retrieved June 20, 2010, from http://www.marketingpower.com/_layouts/Dictionary.aspx?dLetter=B

AMA (2010b). Dictionary. *Marketing Power - American Marketing Association*. Retrieved June 20, 2010, from http://www.marketingpower.com/_layouts/Dictionary.aspx?dLetter=S

Ashenden, D. (2008). Information security management: A human challenge? *Information Security Technical Report*, 13(4), 195-201.

Bakos, J. Y., & Treacy, M. E. (1986). Information technology and corporate strategy: A research perspective. *MIS Quarterly*, 10(2), 107-119.

Bansal, H. S., Irving, G. P., & Taylor, S. F. (2004). A three-component model of customer commitment to service providers. *Journal of the Academy of Marketing Science*, 32(3), 234-250.

Bartley, B., Gomibuchi, S., & Mann, R. (2007). Best practices in achieving a customer-focused culture. *Benchmarking: An International Journal*, 14(4), 482-496.

Baskerville, R. (1993). Information systems security: Adapting to survive. *Information Systems Security*, 2(1), 40-47.

Beautement, A., Sasse, M. A., & Wonham, M. (2008). The compliance budget: Managing security behaviour in organisations. New Security Paradigms Workshop 2008 22-25 September, 2008, Lake Tahoe, California, USA.

Berry, L. L. (2000). Cultivating service brand equity. *Journal of the Academy of Marketing Science*, 28(1), 128-137.

Berry, L. L., Carbone, L. P., & Haeckel, S. H. (2002, Spring). Managing the total customer experience. *MIT Sloan Management Review*, 43, 85-89.

Berry, L. L., Wall, E. A., & Carbone, L. P. (2006). Service clues and customer assessment of the service experience: Lessons from Marketing. *Academy of Management Perspectives*, 20(2), 43-57.

Bishop, M. (2003). *Computer security: Art and science*. New Delhi: Pearson.

Bitner, M. J., Booms, B. H., & Mohr, L. A. (1994). Critical service encounters: The employee's viewpoint. *Journal of Marketing*, 58(October), 95-106.

Bitner, M. J., Booms, B. H., & Tetrault, M. S. (1990). The service encounter: Diagnosing favorable and unfavorable incidents. Journal of Marketing, 54(January), 71-84.

Bolman, L. G., & Deal, T. E. (2003). *Reframing organizations*. San Francisco: Jossey-Bass.

Bostrom, R. P., & Heinen, J. S. (1977). MIS Problems and Failures: A Socio-Technical Perspective. Part I: The Causes. *MIS Quarterly*, 1(3), 17-32.

Bowen, J. T., & Shoemaker, S. (1998). Loyalty: A strategic commitment. *The Cornell Hotel and Restaurant Administration Quarterly*, 39(1), 12-25.

Braun, C., & Winter, R. (2007). Integration of IT service management into enterprise architecture. In 2007 ACM symposium on Applied computing, 1215-1219.

Brostoff, S., & Sasse, M. A. (2001). Safe and sound: A safety-critical approach to security. Proceedings of the 2001 Workshop on New Security Paradigms (Cloudcroft, New Mexico, September 10 - 13, 2001). New York: ACM, pp. 41-50. DOI= http://doi.acm.org/10.1145/508171.508178

Burrell, G., & Morgan, G. (1979). *Sociological paradigms and organisational analysis*. London: Heinemann Educational Books Ltd.

Cater-Steel, A., Toleman, M., & Tan, W. (2006). Transforming IT Service Management – the ITIL Impact. 17th Australasian Conference on Information Systems 6-8 Dec 2006, Adelaide.

ChangingMinds (2002). Toulmin's argument model. *ChangingMinds*. Retrieved June 20, 2010, from http://changingminds.org/disciplines/argument/making_argument/toulmin.htm

Chiaravalle, B., & Schenk, B. F. (2007). *Branding for dummies*. Hoboken, New Jersey: Wiley Publishing.

Chipperfield, C., & Furnell, S. (2010). From security policy to practice: Sending the right messages. *Computer Fraud & Security*, 2010(3), 13-19.

Christopher, M., Payne, A., & Ballantyne, D. (1991). *Relationship marketing: Bringing quality, customer service and marketing together*. Oxford:Butterworth Heinemann.

Chua, W.F. (1986). Radical developments in accounting thought. *The Accounting Review*, LXI(4), 601-632.

Clarke, S., & Drake, P. (2003). A social perspective on information security: theoretically grounding the domain. In S. Clarke, E. Coakes, M. G. Hunter & A. Wenn (Eds.), Socio-Technical and Human Cognition Elements of Information Systems (pp. 249-265). London: Information Science Publishing.

Clemens, E. K., & Row, M. C. (1991). Sustaining IT advantage: The role of structural differences. *MIS Quarterly*, 15(3), 275-292.

Corley, K. G., & Gioia, D. A. (2011). Building theory about theory: What constitutes a theoretical contribution? *Academy of Management Review*, 36(1), 12-32.

Davis, K. (1968). Evolving Models of Organizational Behavior. *The Academy of Management Journal*, 11(1), 27-38.

Davis, S. M. (1985). *Managing Corporate Culture*. Cambridge, MA: Ballinger.

Day, G. S. (1969). A two-dimensional concept of brand loyalty. *Journal of Advertising Research*, 9(3), 29-34.

Dayal, I. (1981). Concept of Man in Management. *Economic and Political Weekly*, 16(22).

De Chernatony, L. (2009). Towards the holy grail of defining 'brand'. *Marketing Theory*, 9(1), 101-105.

De Chernatony, L., & Dall'Olmo Riley, F. (1998a). Defining a "brand": Beyond the literature with experts' interpretations. *Journal of Marketing Management*, 14(5), 417-443.

De Chernatony, L., & Dall'Olmo Riley, F. (1998b). Modelling the components of the brand. *European Journal of Marketing*, 32(11/12), 1074-1090.

De Chernatony, L., Drury, S., & Segal-Horn, S. (2003). Building a services brand: Stages, people and orientations. *The Service Industries Journal*, 23(3), 1-21.

De Chernatony, L., & Segal-Horn, S. (2001). Building on services' characteristics to develop successful services brands. *Journal of Marketing Management*, 17(7/8), 645-669.

De Chernatony, L., & Segal-Horn, S. (2003). The criteria for successful services brands. *European Journal of Marketing*, 37(7/8), 1095-1118.

Dekker, S. W. A. (2002). The re-invention of human error. Technical Report 2002-01, Ljungbyhed, Sweden: School of Aviation, Lund University.

Desouza, K. C., & Vanapalli, G. K. (2005). Securing knowledge assets and processes: Lessons from the defense and intelligence sectors. *Proceedings of the 38th Hawaii Intrenational Conference on System Sciences.*

Dewett, T., & Jones, G. R. (2001). The role of information technology in the organization: A review, model and assessment. *Journal of Management*, 27(3), 313-346.

Dhillon, G. (1995). *Interpreting the management of information systems security*. Doctoral Thesis, Information Systems Group, London School of Economics. Retrieved June 20, 2010, from http://www.lse.ac.uk/collections/informationSystems/pdf/theses/dhillon.pdf.

Dhillon, G. (2001a). Principles for managing information security in the new millennium. In G. Dhillon, *Information security management: Global challenges in the new millennium* (pp. 173-177). London: Idea Group Publishing. ISBN: 1878289780.

Dhillon, G. (2001b). Violation of safeguards by trusted personnel and understanding related information security concerns. *Computers & Security*, 20(2), 165-172.

Dhillon, G., & Backhouse, J. (2001). Current directions in IS security research: Toward socio-organizational perspectives. *Information Systems Journal*, 11(2), 127-153.

Dourish, P., Grinter, R., Delgado de la Flor, J., & Joseph, M. (2004). Security in the wild: User strategies for managing security as an everyday, practical problem. *Personal and Ubiquitous Computing*, 8(6), 391-401.

Drucker, P. (1954). *The Practice of Management.* New York: Harper & Row.

Du Plessis, L., & von Solms, R. (2002). Information Security Awareness: Baseline Education and Certification. In Proceedings of ISSA2002, Muldersdrift, 10-12 July 2002.

Edvardsson, B. (2005). Service quality: beyond cognitive assessment. *Managing Service Quality*, 15(2), 127-131.

Eloff, J., & Eloff, M. (2003, September). Information security management - a new paradigm. Paper presented at the SAICSIT South African Institute for Computer Scientists and Information Technologists, South Africa.

Etzioni, A. (1975). *A comparative analysis of complex organizations*. New York: Free Press.

Evanschitzky, H., Iyer, G. R., Plassmann, H., Niessing, J., & Meffert, H. (2006). The relative strength of affective commitment in securing loyalty in service relationships. *Journal of Business Research*, 59(12), 1207-1213.

Fazio, R. H., & Towles-Schwen, T. (1999). The MODE model of attitude-behavior processes. In S. Chaiken & Y. Trope (Eds.), *Dual-process theories in social psychology*. (pp. 97-116). New York: Guilford Press.

Fishbein, M., & Ajzen, I. (1975). *Belief, attitude, intention, and behavior: An introduction to theory and research*. Reading, MA: Addison-Wesley.

Frangopoulos, E. (2007). *Social engineering and the ISO/IEC 17799:2005 security standard: a study on effectiveness*. Master of Science Thesis, School of Computing, University of South Africa. Retrieved June 20, 2010, from http://uir.unisa.ac.za/bitstream/10500/2142/1/dissertation.pdf.

French, D. P., Sutton, S., Hennings, S. J., Mitchell, J., Wareham, N. J., Griffin, S., Hardeman, W., & Kinmonth, A. L. (2005). The importance of affective beliefs and attitudes in the Theory of Planned Behavior: Predicting intention to increase physical activity. *Journal of Applied Social Psychology*, 35, 1824-1848.

Furnell, S. (2005). Why users cannot use security. *Computers & Security*, 24(4), 274-279.

Furnell, S. (2010). Jumping security hurdles. *Computer Fraud & Security*, 2010(6), 10-14.

Furnell, S., Jusoh, A., & Katsabas, D. (2006). The challenges of understanding and using security: A survey of end-users. *Computers & Security*, 25(1), 27-35.

Furnell, S., & Thomson, K. L. (2009a). From culture to disobedience: Recognising the varying user acceptance of IT security. *Computer Fraud & Security*, 2009(2), 5-10.

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

Galloway, R.L., & White, G. (1993). The internal information systems function as a service operation. *International Journal of Operations & Production Management*, 9(4), 19-27.

Geyskens, I., Steenkamp J. B. E. M., Scheer L. K., & Kumar, N. (1996). The effects of trust and interdependence on relationship commitment: A trans-Atlantic study. *International Journal of Research in Marketing*, 13(4), 303-17.

Gibbons, M. T. (1987). Introduction: the Politics of Interpretation. In M. T. Gibbons (Ed.), *Interpreting politics* (pp. 1-31), New York: New York University Press.

Gioia, D. A., & Pitre, E. (1990). Multiparadigm perspectives on theory building. *Academy of Management Review*, 15(4), 584-602.

Given, L. M. (2008) (Ed.). The SAGE encyclopedia of qualitative research methods (Vol. 1 & 2). New Delhi, India: SAGE Publications India Pvt. Ltd.

Goles, T., & Hirschheim, R. (2000). The paradigm is dead, the paradigm is dead ... long live the paradigm: The legacy of Burrell and Morgan. *Omega, International Journal of Management Sciences*, 28(3), 249-268.

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.

Govier, T. (2010). *A Practical Study of Argument*. Belmont: Wadsworth Publishing.

Grant, I. (2007, December 6). Public sector staff 'ignore IT security'. In *ComputerWeekly.com*. Retrieved October 20, 2010, from

http://www.computerweekly.com/Articles/2007/12/06/228513/Public-sector-staff-ignore-IT-security.htm.

Gremler, D. D., Bitner, M. J., & Evans, K. R. (1995). The internal service encounter. *Logistics Information Management*, 8(4), 28-34.

Grönroos, C. (1990). Service management: A management focus for service competition. *International Journal of Service Industry Management*, 1(1), 6-14.

Grönroos, C. (1994). From scientific management to service management. *International Journal of Service Industry Management*, 5(1), 5-20.

Grönroos, C. (1997). From Marketing Mix to Relationship Marketing – towards a paradigm shift in Marketing. *Management Decision*, 35(4), 322-339.

Gronroos, C. (2007). Service management and Marketing: Customer management in service competition (3rd ed.). Delhi, India: John Wiley & Sons Ltd.

Guba, G., & Lincoln, Y. S. (1994). Competing paradigms in qualitative research. In N. K. Denzin, & Y. S. Lincoln (Eds.), Handbook of qualitative research (pp. 105-117). Thousand Oaks, CA: SAGE.

Gummesson, E. (1993). *Quality management in service organizations*. New York: International Service Quality Association (ISQA).

Gummesson, E. (1994). Service management: An evaluation and the future. *International Journal of Service Industry Management*, 5(1), 77-96.

Gurbaxani, V., & Whang, S. (1991). The impact of information systems on organizations and markets. *Communications of the ACM*, 34(1), 59-73.

Ha, J. H. (2005). A conceptual model of psychological commitment based on the concept of attitude strength. Doctoral Dissertation, Department of Sport Management, Recreation Management, and Physical Education, The Florida State University, College of Education, Retrieved October 5, 2008 from http://etd.lib.fsu.edu/theses/available/etd-11222005-002013/unrestricted/DissertationJaeHyunHa.pdf.

Harrison, R. (1972, May-June). Understanding your organization's character. *Harvard Business Review*, 119-128.

Hartline, M. D., & Ferrell, O. C. (1996). The management of customer-contact service employees: An empirical investigation. *Journal of Marketing*, 60(4), 52-70.

Hartline, M. D., Maxham III, J. G., & McKee, D. O. (2000). Corridors of influence in the dissemination of customer-oriented strategy to customer contact service employees. *Journal of Marketing*, 64(2), 35-50.

Hennig-Thurau, T. (2004). Customer orientation of service employees – Its impact on customer satisfaction, commitment, and retention. *International Journal of Service Industry Management*, 15(5), 460-478.

Hennig-Thurau, T., Gwinner, K. P., & Gremler, D. D. (2002). Understanding Relationship Marketing outcomes: An integration of relational benefits and relationship quality. *Journal of Service Research*, 4(3), 230-247.

Herath, T., & Rao, H. R. (2009). Encouraging information security behaviours in organizations: Role of penalties, pressures and perceived effectiveness. *Decision Support Systems*, 47(2), 154-165.

Hevner, A. R., Salvatore, March, T., Park, J., & Ram, S. (2004). Design Science in Information Systems Research. *MIS Quarterly*, 28(1), 75-105.

Hillson, D., & Murray-Webster, R. (2005). *Understanding and managing risk attitude*. Aldershot, UK: Gower Publishing Limited. ISBN 0566086271.

Hirschheim, R. & Klein, H. (1989). Four Paradigms of Information Systems Development. C*ommunications of the ACM*, 32(1989), 1199-1216.

Hirschheim, R., Schwarz, A., & Todd, P.A. (2006, March). Marketing maturity model for IT: Building a customer-centric IT organization. *IBM Systems Journal*.

Hochstein, A., Tamm, G., & Brenner, W. (2005). Service oriented IT management: Benefit, cost and success factors. In ECIS 2005 Proceedings.

Hudson, P. T. W., Verschuur, W. L. G., Parker, D., & Lawton, R. (2000). Bending the Rules: Managing Violation in the Workplace. Retrieved June 20, 2010, from http://www.energyinst.org.uk/heartsandminds/docs/bending.pdf.

Hussain, Z., & Taylor, W. A. (2007). Evaluating the behaviour of information systems developers: The relevance and utility of paradigms. *Behaviour and Information Technology*, 26(3), 221-236.

Iden, J. (2009). Implementing IT service management: Lessons learned from a university IT department. In A. Cater-Steel (Ed.) *Information Technology Governance and Service Management: Frameworks and Adaptations* (pp. 333-349), Hershey: Information Science Reference.

IEP (2003, January 27). Argument. *Internet Encyclopedia of Philosophy*. Retrieved June 20, 2010, from http://www.iep.utm.edu/argument/

IEP (2006, July 7). Omniscience and Divine Foreknowledge. *Internet Encyclopedia of Philosophy*. Retrieved June 20, 2010, from http://www.iep.utm.edu/omnisci/

IIA (2000). Information security management and assurance - a call to action for corporate governance - guidance for Boards of Directors. The Institute of Internal Auditors. Retreived October 5, 2008 from http://www.theiia.org/download.cfm?file=22398

Imperva (2010). Consumer password worst practices. Retrieved June 20, 2010, from http://www.imperva.com/docs/WP_Consumer_Password_Worst_Practices.pdf.

ISO/IEC 9241-210 (2010). Ergonomics of human-system interaction - Part 210: Human-centred design for interactive systems. ISO/IEC 9241-210:2010, International Organization for Standardization and International Electrotechnical Commission.

ISO/IEC 27000 (2009). Information technology - Security techniques - Information security management systems - Overview and vocabulary. ISO/IEC 27000:2009, International Organization for Standardization and International Electrotechnical Commission.

ISO/IEC 27001 (2005). Information technology - Security techniques - Information security management systems - Requirements. *ISO/IEC 27001:2005*, International Organization for Standardization and International Electrotechnical Commission.

ISO/IEC 27002 (2005). Information technology - Security techniques - Code of practice for information security management. *ISO/IEC 27002:2005*, International Organization for Standardization and International Electrotechnical Commission.

ISSA (2003). Generally Accepted Information Security Principles (GAISP v3.0). Information Systems Security Association.

Jacoby, J., & Chestnut, R. W. (1978). *Brand loyalty measurement and management*. New York: John Wiley & Sons, Inc.

Johnston, K. (1993). *Busting bureaucracy: how to conquer your organization's worst enemy*.

Johnston, J., Eloff, J. P. H., & Labuschagne, L. (2003). Security and human computer interfaces. *Computers & Security*, 22(8), 675-684.

Jonker, J., & Pennink, B. (2010). *The essence of research methodology - a concise guide for master and phd students in management science*. Springer.

Kahneman, D., & Tversky, A. (1979). Prospect theory: An analysis of decision under risk. *Econometrica*, 47(2), 263-292.

Kapferer, J. N. (2008). *The new strategic brand management: Creating and sustaining brand equity long term*. London:Kogan Page.

Keel, A. J., Orr, M. A., Hernandez, R. R., Patrocinio, E. A., & Bouchard, J. (2007). From a technology oriented to a service oriented approach to IT managennent. *IBM Systems Journal*, 46(3), 549-564.

Keir, M. (1918). Scientific management simplified. *The Scientific Monthly*, 7(7), 525-529.

Keller, K. L. (1993). Conceptualizing, measuring, and managing customer-based brand equity. *Journal of Marketing*, 57(1), 1-22.

Keller, K. L. (1998). Branding perspectives on Social Marketing. In Alba, J. W., & Hutchinson, J. W. (Eds.). (1998). *Advances in Consumer Research*, 25, 299-302. Provo, Utah: Association for Consumer Research.

Keller, K. L. (2001). Building customer-based brand equity. *Marketing Management*, 10(2), 14-19.

Keller, K. L. (2008). *Strategic brand management (3rd ed.)*. Delhi, India: Prentice Hall of India.

Khatri, N., Baveja, A, Boren, S. A., & Mammo, A. (2006). Medical errors and quality of care: From control to commitment. *California Management Review*, 48(3), 115-141.

Kotler, P., & Keller, K. L. (2006). *Marketing Management (12th ed.)*. Upper Saddle River, NJ, USA: Prentice Hall. ISBN 0-13-145757-8.

Kumar, N., Hibbard, J. D., & Stern, L. W. (1994). The nature and consequences of marketing channel intermediary commitment. MSI Working Paper, Report No. 94-115.

Lambert, C. (2006, March-April). The marketplace of perceptions. *Harvard Magazine*. Retrieved June 20, 2010, from http://harvardmagazine.com/2006/03/the-marketplace-of-perce.html

Lehmann, D. R., Keller, K. L., & Farley, J. U. (2008). The Structure of Survey-Based Brand Metrics. *Journal of International Marketing*, 16(4), 29-56.

Lehtinen, U., & Lehtinen, J. R. (1991). Two approaches to service quality dimensions. *The Service Industries Journal*, 11(3), 287-303.

Lewis, B.R., & Entwistle, T.W. (1990). Managing the service encounter: a focus on the employee. *International Journal of Services Industry Management*, 1(3), 41-52.

Lineberry, S. (2007, November). The Human Element: The Weakest Link in Information Security. *Journal of Accountancy*. Retrieved October 22, 2010, from http://www.journalofaccountancy.com/Issues/2007/Nov/TheHumanElementTheWeakestLinkInInformationSecurity.htm

Lovelock, C., & Gummesson, E. (2004). Whither services marketing? In search of a new paradigm and fresh perspective. *Journal of Service Research*, 7(1), 20-41.

Lynham, S. A. (2000). Theory building in the human resource development profession. *Human Resource Development Quarterly*, 11(2), 159-178.

Lynham, S. A. (2002). The general method of theory-building research in applied disciplines. *Advances in Developing Human Resources*, 4(3), 221-241.

March, S. T., & Smith, G. F. (1995). Design and natural science research on information technology. *Decision Support Systems*. 15, 251-266.

Martins, A., & Eloff, J. P. H. (2002). Promoting information security culture through an information security culture model. In Proceedings of ISSA2002, Johannesburg, South Africa.

Mather, J. (2008). Creating the service culture. *Human Resources*,18-19.

Mauwa, H., & von Solms, R. (2007). Information security awareness: Towards a genertic programme. In S. M. Furnell, & N. L. Clarke (Eds.), Proceedings of the international symposium on human aspects of information security & assurance (HAISA 2007) (pp. 37-43). ISBN: 978-1-84102-174-4.

McBride, N. (2009). A model for IT service strategy. In A. Cater-Steel (Ed.) *Information Technology Governance and Service Management: Frameworks and Adaptations* (pp. 350-363), Hershey: Information Science Reference.

McFadzean, E., Ezingeard, J.-N., & Birchall, D. (2006). Anchoring information security governance research: Sociological groundings and future directions. Journal of Information System Security, 2(3).

McGregor, D. M. (1957, November). The human side of enterprise. *Management Review*, 41-49.

McGregor, D. M. (1960). *The human side of enterprise*. New York: McGraw-Hill.

McKay, J., Marshall, P., & Heath, G. (2008). An exploration of the concept of design in Information Systems. The 4th Information Systems Foundation Workshop: Answering the Unanswered Questions about Design Research, The Australian National University, Canberra, Australia, 2nd-3rd October 2008.

McLean, K. (1992). Information security awareness - selling the cause. In Proceedings of the IFIP TC11/Sec'92, 27-29 May, Singapore.

McNaughton, B., Ray, P., & Lewis, L. (2010). Designing an evaluation framework for IT service management. *Information and Management*, 47(4), 219-225.

Mead, G. H. (1934). *Mind, self and society: From the standpoint of a social behaviorist*. Chicago, IL: University Press.

Meyer, J P., & Allen, N. J. (1991). A three-component conceptualization of organizational commitment. *Human Resource Management Review*, 1(1), 61-89.

Meyer, J. P., & Herscovitch, L. (2001). Commitment in the workplace: Toward a general model. *Human Resource Management Review*, 11(3), 299-326.

Mintz, J. H., & Chan, J. (2009). Guide to branding in the public and not-for-profit sectors. Centre of Excellence for Public Sector Marketing, April (http://www.publicsectormarketing.ca).

Mintzberg, H. (1980). Structure in 5's: A synthesis of the research on organization design. *Management Science*, 26(3), 322-341.

Moorthi, Y. L. R. (2002). An approach to branding services. *Journal of Services Marketing*, 16(3), 259-274.

Morgan, G. (1996). *Images of organization*. Thousand Oaks, CA: Sage Publications.

Morgan, R. M., & Hunt, S. D. (1994). The commitment-trust theory of Relationship Marketing. *Journal of Marketing*, 58(3), 20-38.

Mullins, L. J. (2004). *Management and organizational behavior* (7th Ed.). Harlow, England: Pearson Education Limited. ISBN 0273688766.

Munoz, T., & Kumar, S. (2004). Brand metrics: Gauging and linking brands with business performance. *The Journal of Brand Management*, 11(5), 381-387.

Niehaves, B., & Stahl, B. C. (2006). Criticality, epistemology, and behavior vs. design – information systems research across different sets of paradigms.

Olson, J. M., & Maio, G. R. (2003). Attitudes in social behavior. In T. Millon & M. J. Lerner (Eds.), *Comprehensive handbook of psychology:* Vol. 5. Personality and Social Psychology (pp. 299-325). Hoboken, NJ: Wiley.

Orlikowski, W. J., & Baroudi, J. J. (1991). Studying information technology in organizations: Research approaches and assumptions. *Information Systems Research*, (2), 1-28.

Orlikowski, W. J., & Gash, D. C. (1994). Technological frames: Making sense of information technology in organizations. *ACM Transactions on Information Systems*, 2(2), 174–207.

Oxford Dictionaries (2010). Argumentation. *Oxford Dictionaries*. Retrieved June 20, 2010, from http://www.oxforddictionaries.com/definition/argumentation?view=uk

Parasuraman, A., Zeithaml, V. A., & Berry, L. L. (1985). A conceptual model of service quality and it's implications for future research. *Journal of Marketing*, 49(), 41-50.

Payne, A., Ballantyne, D., & Christopher, M. (2005). A stakeholder approach to relationship marketing strategy: The development and use of the "six markets" model. *European Journal of Marketing*, 39(7/8), 855-871.

Peppard, (2003). Managing IT as a Portfolio of Services. *European Management Journal*, 21(4), 467-483.

Perry, W.E. (1985). *Management Strategies for Computer Security*, Boston, MA: Butterworth Publisher.

Pheysey, D. C. (1993). Organizational cultures – Types and transformations. London: Routledge.

Porter, M. E., & Millar, V. E. (1985, July-August). How information gives you competitive advantage. *Harvard Business Review*.

Post, G. V., & Kagan, A. (2007). Evaluating information security tradeoffs: Restricting access can interfere with user tasks. *Computers & Security*, 26(3), 229-237.

Posthumus, S. & von Solms, R. (2005). A responsibility framework for information security. In Security Management, Integrity, and Internal Control in Information Systems (volume

193/2006, pp. 205-221), Proceedings of the IFIP 11.1&11.5 Working Conference, Fairfax, Virginia, USA, December 2005.

Potgieter, B., Botha, J., & Lew, C. (2005). Evidence that use of the ITIL framework is effective. In Proceedings of the 18th Annual Conference of the National Advisory Committee on Computing Qualifications, Tauranga, New Zeland, July 10-13.

Rajagopal (2008). Measuring brand performance through metrics application. *Measuring Business Excellence*, 12(1), 29-38.

Ramachandran, S., Rao, S.V., & Goles, T. (2008). Information security cultures of four professions: A comparative study. In Proceedings of the 41st Annual Hawaii International Conference on System Sciences. ISBN: 978-0-7695-3075-8.

Rasmussen, J. (1997). Risk management in a dynamic society: a modelling problem. *Safety Science*, 27(2-3), 183-213.

Rastogi, R., & von Solms, R. (2005). Information Security Goverance – a re-definition. In P. Downland, S. Furnell, B. Thuraisingham & X. S. Wang (Ed.), *Security Management, Integrity, and Internal Control in Information Systems* (pp. 223-236), Proceedings IFIP International Federation for Information Processing, Volume 193/2006, New York: Springer. ISBN: 0387298266.

Rastogi, R., & von Solms, R. (2009). A service-oriented approach to information security management. In G. Dhillon (Ed.), Proceedings of the 7th Annual Conference on Information Science, Technology & Management (CISTM) "Sustaining a Knowledge Economy". July 13-15. DC: Information Institute Publishing. ISBN: 978-1-935160-06-9.

Ravald, A., & Grönroos, C. (1996). The value concept and relationship marketing. *European Journal of Marketing*, 30(2), 19-30.

Reason, J. (1990). *Human Error*. New York, NY: Cambridge University Press.

Reason, J. (2000). Human error: models and management. *British Medical Journal*, 320(7237), 768-70.

Rowan, J. (1973). *The social individual*. London: Davis-Poynter.

Rusbult, C. E. (1980). Commitment and satisfaction in romantic relationships. *Journal of Experimental Social Psychology*, 16(2), 172-186.

Saltzer, J. H., & Schroeder, M. D. (1975). The protection of information in computer systems. *Communications of the ACM*, 17(7),

Sandrone, V. (n.d.). F. W. Taylor & Scientific Management : Efficiency or Dehumanization. In *Skymark*. Retrieved June 20, 2010, from http://www.skymark.com/resources/leaders/taylor.asp.

Santiago, A. (2007). Why employees do not follow procedures. *Inter Metro Business Journal*, 3(2), 15-49.

Sasse, M. A., Brostoff, S., & Weirich, D. (2001). Transforming the 'weakest lnk' — a Human/Computer interaction approach to usable and effective security. *BT Technology Journal*, 19(3), 122-131.

Saunders, M.N.K., Thornhill, A., & Lewis, P. (2003). *Research methods for business students* (3rd Ed.). Delhi: Pearson Education. ISBN: 9788131701157.

Schein, E. H. (1980). *Organizational psychology* (3rd Ed.). Englewood Cliffs, NJ: Prentice Hall.

Schein, E. H. (1996). Three cultures of management: The key to organizational learning. *Sloan Management Review*, 38(1), 9-20.

Schein, E. H. (2004). *Organizational culture and leadership* (3rd Ed.). San Francisco: Jossey-Bass.

Schlienger, T., & Teufel, S. (2002). Information security culture - The socio-cultural dimension in information security management. In Proceedings of IFIP TC11 International Conference on Information Security (Sec2002): Security in the information society: visions and perspectives.

Schneberger, S., Pollard, C., & Watson, H. (2009). Theories: For academics and practitioners. *Information Systems Management*, 26(1), 52-60.

Schneier, B. (2000). *Secrets and lies: Digital security in a networked world*. New York: John Wiley & Sons, Inc.

Schneier, B. (2008). The psychology of security. Retrieved June 20, 2010, from http://www.schneier.com/essay-155.html.

Schultz, E. E., Proctor, R. W., Lien, M., & Salvendy, G. (2001). Usability and security: An appraisal of usability issues in information security methods. *Computers & Security*, 20(7), 620-634.

Shostack, G. L. (1985). Planning the service encounter. In Czepiel, J. A., Solomon, M. R., & Surprenant, C. F. (Eds.). *The Service Encounter*. Lexington Books.

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

Siponen, M. T. (2001). Five dimensions of information security awareness. *Computers & Society*, 31(2), 24-29.

Sirota, D., Mischkind, L. A., & Meltzer, M. I. (2008). Stop demotivating your employees! *Harvard Management Update*, 13(7).

Spafford, E. H., The Mole in the Machine, The New York times, 25 July 1999.

Stanovich, K. E., & West, R. F. (2003). Evolutionary versus instrumental goals: How evolutionary psychology misconceives human rationality. In D. Over (Ed.), *Evolution and the psychology of thinking: The debate* (pp. 171-230). Hove, England: Psychology Press.

Stanton, J. M., Stam, K. R., Guzman, I., & Caldera, C. (2003). Examining the linkage between organizational commitment and information security. In Proceedings of IEEE International Conference on Systems, Man & Cybernetics (Vol. 3, pp. 2501-2506). October 5-8. ISBN: 0-7803-7952-7.

Stanton, J. M., Stam, K. R., Mastrangelo, P., & Jolton, J. (2005). Analysis of end user security behaviours. *Computers & Security*, 24(2), 124-133.

Stewart, G. (2009). Maximizing the Effectiveness of Information Security Awareness Using Marketing and Psychology Principles. Egham, England: Department of Mathematics, Royal Holloway, University of London. Technical Report RHUL-MA-2009-02 16th February 2009, available online at http://www.ma.rhul.ac.uk/static/techrep/2009/RHUL-MA-2009-02.pdf.

Surprenant, C. F., & Solomon, M. R. (1987). Predictability and personalization in the service encounter. *Journal of Marketing*, 51(2), 86-96.

Tan, W., Cater-Steel, A., & Toleman, M. (2009). Implementing IT service management: A case study focussing on critical success factors. *The Journal of Computer Information Systems*, Winter.

Taylor, F. W. (1911). *Scientific Management*. London: Harper & Row.

Thomson, M. E., & von Solms, R. (1998). Information security awareness: Educating your users effectively. *Information Management & Computer Security*, 6(4), 167-173.

Thomson, K. L., & von Solms, R. (2004). Information security obedience: A definition. *Computers & Security*, 24(1), 69-75.

Thomson, K. L., von Solms, R., & Louw, L. (2006). Cultivating an organizational information security culture. *Computer Fraud & Security*, 2006(10), 7-11.

Thomson, M. E. & von Solms, R. (1998). Information security awareness: educating your users effectively. *Information Management & Computer Security*, 6(4), 167-173.

Trafimow, D., Sheeran, P., Lombardo, B., Finlay, K. A., Brown, J., & Armitage, C. J. (2004). Affective and cognitive control of persons and behaviours. *British Journal of Social Psychology*, 43(2), 207-224.

Transactional Leadership. (n.d.). Retrieved October 22, 2010, from http://changingminds.org/disciplines/leadership/styles/transactional_leadership.htm

Toulmin, S. E. (1958). *The uses of argument*. Cambridge, UK: Cambridge University Press.

Tsohou, A., Karyda, M., Kokolakis, S., & Kiountouzis, E. A. (2006). Formulating information systems risk management strategies through cultural theory. *Information Management & Computer Security*, 14(3), 198-217.

Ugboaja, P. C. (2006). Management's assumptions about people in organizations and implications of these assumptions on management strategies. *Inter-world Journal of Management and Development Studies*, 2(1), 268-274.

UNL (1998, May 1). The Toulmin project home page. *Univeristy of Nebraska-Lincoln*. Retrieved June 20, 2010, from http://www.unl.edu/speech/comm109/Toulmin/

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.

Vandermerwe, S., & Gilbert, D. (1989). Making internal services market driven. *Business Horizons*, 32(6), 83-89.

Vargo, S. L., & Akaka, A. (2009). Service-Dominant logic as a foundation for service science: Clarifications. Service Science, 1(1), 32-41.

Vargo, S. L., & Lusch, R. F. (2004). Evolving to a new dominant logic for marketing. *Journal of Marketing*, 68(1), 1-17.

Vargo, S., & Lusch, R. F. (2008). Why "service"? *Journal of the Academy of Marketing Science*, 36(1), 25-38.

Ven De Ven, A. H., & Johnson, P. E. (2006). Knowledge for theory and practice. *Academy of Management Review*, 31(4), 802-821.

Verplanken, B., & Aarts, H. (1999). Habit, attitude, and planned behaviour: Is habit an empty construct or an interesting case of goal-directed automaticity? *European Review of Social Psychology*, 10, 101-134.

Verplanken, B., & Orbell, S. (2003). Reflections on past behavior: A self-report index of habit strength. *Journal of Applied Social Psychology*, 33, 1313-1330.

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

von Solms, B. (2001). Information Security — A multidimensional discipline. *Computers & Security*, 20(6), 504-508.

von Solms, B. (2006). Information Security – the Fourth Wave. *Computers & Security*, 25(3), 165-168.

von Solms, B., & von Solms, R. (2004). The 10 deadly sins of information security management. *Computers & Security*, 23(5), 371-376.

Walton, R. E. (1985). From control to commitment in the workplace. *Harvard Business Review*, March-April.

Weatherly, K. A., & Tansik, D. A. (1993). Managing multiple demands: A Role-Theory examination of the behaviours of customer contact service workers. In Swartz, T. A., Bowen, D. E., & Brown, S. W. (Eds.). *Advances in Services Marketing and Management* (Vol. 2, 279-300), Greenwich. CT: JAI Press.

Weber, M. (1947). *The theory of social and economic organization*. Translated by A. M. Henderson & Talcott Parsons, The Free Press.

Wetzels, M., de Ruyter, K., & von Birgelen, M. (1998). Marketing service relationships: The role of commitment. *Journal of Business & Industrial Marketing*, 13(4/5), 406-423.

White, E. F. R., & Dhillon, G. (2005). Synthesizing information system design ideals to overcome developmental duality in securing information systems. In Proceedings of the 38th Annual Hawaii International Conference on System Sciences (HICSS'05) - Track 7. ISBN: 0-7695-2268-8.

Whitten, A., & Tygar, J. D. (1999). Why Johnny can't encrypt: A usability evaluation of PGP 5.0. Proceedings of the 8th conference on USENIX Security Symposium. Berkeley, CA, USA: USENIX Association.

Whittingham, R.B. (2004). *The blame machine: Why human error causes accidents*. Elsevier/ Butterworth-Heinemann.

Whyte, G., & Bytheway, A. (1996). Factors affecting information systems' success. *International Journal of Service Industry Management*, 7(1), 74-93.

Wipawayangkool, K. (2009). Security Awareness and Security Training: An Attitudinal Perspective. In M. Rao (Ed.), Proceedings of Southwest Decision Sciences Institute (2009 SWDSI). Retrieved October 22, 2010, from http://www.swdsi.org/swdsi2009/Papers/9J01.pdf.

Wohnlich, T. (2006, October 27). *Building a human firewall: Raising awareness to protect against social engineering*. Retrieved October 22, 2010, from http://www.ciscopress.com/articles/article.asp?p=663084.

Wollan, R. (2008, January). The new rules for customer service: Findings from the Accenture Global Customer Satisfaction Survey. *Outlook Point of View*. Retrieved October 22, 2010, from http://www.accenture.com/Global/Research_and_Insights/Outlook/By_Subject/Customer_Relationship_Mgmt/SatisfactionSurvey.htm

Zeithaml, V. A., Bitner, M. J., Gremler, D. D., & Pandit, A. (2008). Service marketing – integrating customer focus across the firm (4th ed.). Delhi, India: Tata McGraw-Hill Publishing Company Ltd.

Zurko, M. E., & Simon, R. T. (1996). User-centered security. New Security Paradigms Workshop.

Appendices: Papers Presented and Published

The following papers were presented and published whilst conducting research towards this thesis:

Appendix A:

Paper 1: Rastogi, R., & von Solms, R. (2005). Information Security Goverance – a re-definition. In P. Downland, S. Furnell, B. Thuraisingham & X. S. Wang (Ed.), *Security Management, Integrity, and Internal Control in Information Systems* (pp. 223-236), Proceedings IFIP International Federation for Information Processing, Volume 193/2006, New York: Springer. ISBN: 0387298266.

Appendix B:

Paper 2: Rastogi, R., & von Solms, R. (2009). A service-oriented approach to information security management. In G. Dhillon (Ed.), *Sustaining a knowledge* economy, Proceedings of the 7th Annual Conference on Information Science, Technology & Management (CISTM), Washington D.C.: Information Institute Publishing. ISBN: 978-1-935160-06-9.

Appendix C:

Paper 3: Rastogi, R., & von Solms, R. (forthcoming). Information Security Service Branding – beyond information security awareness. Submitted to the 9th International Conference on Education and Information Systems, Technologies and Applications: EISTA 2011, USA.

Appendix D:

Paper 4: Rastogi, R., & von Solms, R. (forthcoming). Information Security Service Support – helping end-users cope with security. To be published by the Journal of Computer Technology and Application.

Appendix E:

Paper 5: Rastogi, R., & von Solms, R. (forthcoming). Information Security Service Culture – information security for end-users. Submitted to the Human Aspects in Information Security and Assurance (HAISA 2011) conference.

Appendix A:

Information Security Governance - a Re-definition

Rahul Rastogi[a] and Rossouw von Solms[b]

[a] *Nelson Mandela Metropolitan University, rahul.rastogi@eil.co.in,*

[b] *Nelson Mandela Metropolitan University, rossouw.vonsolms@nmmu.ac.za*

Abstract: Information is a fundamental asset of any organization and needs protection. Consequently, Information Security Governance has emerged as a new discipline, requiring the attention of Boards of Directors and Executive Management for effective information security. This paper investigates the literature on Corporate Governance, IT Governance and Information Security Governance to identify the components towards a definition of Information Security Governance. The paper concludes by defining Information Security Governance and discussing the definition, identifying and addressing all important issues that need to be taken into account to properly govern information security in an organization.

Keywords: Corporate Governance, IT Governance, Information Security Governance, Information Security

1. INTRODUCTION

Much has been said in recent literature about bringing Information Security into the fold of Corporate Governance, thereby making it a crucial responsibility of the Board of Directors and Executive Management. Information Security Governance has, thus, emerged as a new discipline and responsibility for Board of Directors and Executive Management. But, before Board of Directors and Executive Management can discharge this new responsibility, the term Information Security Governance needs to be defined and understood.

Existing literature provides some guidance on Information Security Governance. However, in the opinion of the authors, this guidance is insufficient. The guidance is prescriptive and does not clearly bring out the meaning of Information Security Governance. In a recent article, the plight of Executive Management with respect to IT Governance is stated as most C-level executives responding to IT Governance with a “frustrated roll of their eyes” (Melnicoff, Shearer & Goyal,

2005, p. 1). We feel that the existing guidance on Information Security Governance will elicit similar reactions.

The objective of this paper is to propose a 'new' definition of Information Security Governance, identifying and addressing all important issues that need to be taken into account to properly govern information security in an organization. The definition answers the following questions:

- What is to be understood from Information Security Governance?
- Who formulates the framework to implement Information Security Governance in an organization?
- Where in the organization is Information Security Governance implemented?
- What are the benefits that Information Security Governance should deliver to the organization?

In proposing the definition of Information Security Governance, this paper first reviews how Information Security is evolving and how it is being brought under the purview of Corporate Governance. It then investigates the existing literature on Corporate Governance, IT Governance and Information Security Governance to identify the components of the proposed definition. The paper concludes by proposing the definition and discussing its various components.

2. THE EVOLUTION OF INFORMATION SECURITY AND THE EMERGENCE OF INFORMATION SECURITY GOVERNANCE

Over the years, IT has penetrated every aspect of modern business and today businesses are critically dependent on IT and information. This has led to the evolution of the role of Information Security. Further, because of the wide impact of information security breaches on organizations, Information Security is increasingly being brought under the fold of Corporate Governance. However, Board of Directors and executive management have very little guidance on what Information Security and Information Security Governance mean for their organization.

Regarding the evolution of Information Security and the emergence of Information Security Governance, two trends emerge from the current literature:

- The role of Information Security is changing – it is no longer about only protecting information assets, but also about assurance and trust (BSA, 2003, p. 3). Information Security is now a competitive weapon.
- Increasingly, Information Security is being linked to Corporate Governance. Many researchers in the field have motivated the need for integrating Corporate Governance and Information Security (Von Solms and Thomson, 2003). Further, various regulations and legislation are formalizing this requirement (FISMA, 2002).

Information Security is thus evolving and leading to the emergence of Information Security Governance as a new discipline. Through this evolution and change, Boards of Directors and Executive Management need to understand the value that Information Security delivers for their organization and what they need to do to discharge their responsibility towards Information Security Governance.

This paper attempts to bring the required clarity and understanding by providing a definition of Information Security Governance for Boards of Directors and Executive Management. The following sections investigate the existing literature on Corporate Governance, IT Governance and Information Security Governance to identify the possible components of this definition.

3. CORPORATE GOVERNANCE

Corporate Governance emerged as a discipline when the ownership of an organization was separated from its management. Governance, then, means protection of owners' interests through oversight, direction and control of management by owners, the owners being represented by the Board of Directors. Thus one of the main aspects of governance is to assure the suppliers of finance that they would get a return on their investments (Shleifer and Vishny, 1996, p. 3). Corporate Governance provides this assurance by providing incentives to the board and management to "pursue objectives that are in the interests of the company and its shareholders" (OECD, 2004, p. 13).

Moving forward from these philosophical underpinnings, guidance is available on the operational and implementation aspects of Corporate Governance. Corporate Governance is implemented through structures such as an organization's management, board, shareholders and other stakeholders that are bound by relationships. These structures and relationships are then utilized to set objectives and to determine the means of attaining those objectives and monitoring performance (OECD, 2004, p. 13).

A recent trend in the literature on governance of corporations or enterprises is towards taking a wider view of governance, i.e. Enterprise Governance with Corporate Governance being a part of it, or being synonymous with it. Figure 1 shows the Enterprise Governance Framework consisting of the conformance and performance dimensions (CIMA, 2004, p. 2).

The conformance dimension consists of the organization using its "governance arrangements to ensure it meets the requirements of the law, regulations, published standards and community expectations of probity, accountability and openness" (ANAO, 2003, p. 13). The conformance dimension includes Corporate Governance (CIMA, 2004, p. 2). The performance dimension consists of the organization using its "governance arrangements to contribute to its overall

performance and the delivery of its goods, services or programs" (ANAO, 2003, p. 13). Operationally, Governance is "basically concerned with structures and processes for decision-making and with the controls and behaviour that support effective accountability for performance outcomes" (ANAO, 2003, p. 13).

Together, the conformance and performance structures and processes implement governance through "providing strategic direction, ensuring that objectives are achieved, ascertaining that risks are managed appropriately and verifying that the organization's resources are used responsibly" (Hamaker, 2003, p. 1).

From the above discussion, Governance can be understood to consist of the following aspects:

- It involves the Board of Directors and Executive Management.
- It makes the Board of Directors and Executive Management responsible towards all stakeholders including shareholders and suppliers of finance.
- It involves the creation of an organizational structure specifying the distribution of rights and responsibilities among the various participants in the organization.
- Governance includes the specification of processes for directing, controlling and monitoring performance of the organization towards attaining its objectives.
- Governance has conformance and performance aspects.
- The conformance dimension of Governance involves the formation of decision-making guidelines and structures and the clear identification and articulation of responsibilities.
- The performance dimension of Governance involves performance measurement and accountability for performance.

This section has investigated the meaning of governance. The following section investigates the definitions of IT Governance. Since, today, information largely exists in the IT devices deployed in organizations, it is instructive to look at what Governance means to IT to understand how it can be applied to Information Security.

4. IT GOVERNANCE

Information today is largely manifest in the electronic form. Also, today Information Security is largely about controls applicable to IT. This section investigates some definitions of IT Governance to understand what governance means to IT, in an attempt to understand what it can mean to cover Information Security. This paper does not see Information Security Governance as a subset of IT Governance as the drivers for IT Governance are very different from those for Information Security Governance.

The IT Governance Institute (ITGI) defines IT Governance as follows :

“IT Governance is the responsibility of the board of directors and executive management. It is an integral part of enterprise governance and consists of the leadership and organizational structures and processes that ensure that the organization's IT sustains and extends the organization's strategies and objectives” (ITGI, 2003, p. 18).

Weill and Woodham (2002, p. 4) defines IT Governance as:

> “specifying the decision rights and accountability framework to encourage desirable behaviour in the use of IT”.

Van Grembergen (2002, p. 1) defines IT Governance as:

> “the organizational capacity exercised by the Board, executive management and IT management to control the formulation and implementation of IT strategy and in this way ensuring the fusion of business and IT”.

The key point of the above definitions of IT Governance is that they see governance as a mechanism for fusing or aligning business and IT and getting value out of IT implementation. The definitions focus on the 'performance' outcomes of value creation and resource utilization. Likewise, the proposed definition of Information Security Governance should focus on the 'performance' outcomes of Information Security Governance and the value delivered by Information Security to the organization. However, the 'performance' outcomes and value delivered by Information Security Governance would be different from that of IT Governance.

5. EXISTING GUIDANCE ON INFORMATION SECURITY GOVERNANCE

This section investigates the guidance on Information Security Governance provided in the existing literature. This will help put in perspective the definition proposed in this paper.

The existing guidance on Information Security Guidance has two main themes:

- Motivating that Information Security must be governed and
- Defining Information Security Governance and providing guidance for implementation of governance.

The motivation for Information Security Governance is derived from the fiduciary responsibility of Board of Directors and Executive Management towards corporate governance and protection of stakeholder interests. It is motivated that not only are the Board of Directors and Executive Management responsible for maintaining information security, but also that they are liable for legal action for breaches in information security at their organization (Von Solms, 2001) (Von Solms and Thomson, 2003).

Since Governance consists of structures, relationships and processes, the existing guidance (ISACF, 2001) (CGTF, 2004) (BSA, 2003) (FISMA, 2002) provides frameworks for implementing Information Security Governance. The implementation proceeds mainly by mapping Information Security Governance responsibilities to the organizational hierarchy. A summary is provided in Table 1 – Information Security Governance and Organizational Hierarchy.
The existing guidance represents the beginning of a trend towards providing frameworks for Information Security Governance. The frameworks are therefore not sufficiently detailed and, in our opinion, would lead to a 'frustrated roll of eyes', as stated earlier. Further, the frameworks do not explicate a model or definition of Information Security Governance and are prescriptive in nature.

We attempt to remedy this shortcoming partially by proposing a definition of Information Security Governance in the next section.

6. PROPOSED DEFINITION OF INFORMATION SECURITY GOVERNANCE

This section proposes the following definition of Information Security Governance:
"Information Security Governance consists of the frameworks for decision-making and performance measurement that Board of Directors and Executive Management implement to fulfill their responsibility of providing oversight, as part of their overall responsibility for protecting stakeholder value, for effective implementation of Information Security in their Organization, to ensure that:

a. The Organization practices due care and due diligence in its use of Information and IT Systems and that this care and diligence is extended to its partners and customers.
b. The Organization manages the risks associated with its use of Information and IT Systems and that the process for Information Security is effective, efficient and responsive to security incidents and existing or emerging vulnerabilities, threats and risks.
c. The Organization's Information and IT Systems can be trusted by all stakeholders, including, customers, partners and regulators.
d. There is alignment between the needs and strategies of Business, IT and Information Security.
e. The Organization complies with laws and regulations applicable to its use of Information and IT Systems.
f. There is visibility into the state of Information Security in the Organization, providing relevant details to concerned stakeholders."

Figure 2 depicts a model of Information Security Governance, based on this definition. The following sections provide a brief discussion of the various components and characteristics of this definition.

7. THE 'GOVERNANCE' ASPECT OF INFORMATION SECURITY GOVERNANCE

This section discusses the 'Governance' aspect of the definition of Information Security Governance, i.e., what is meant by Governance, as it is applied to Information Security.
The definition states that Information Security Governance is a part of Enterprise or Corporate Governance and that the responsibility of Boards of Directors and Executive Management for providing oversight for protecting stakeholder interests includes providing oversight for implementation of Information Security.

The mechanisms for providing governance include creating the decision-making and performance measurement frameworks. These frameworks are formulated by the Board of Directors and Executive Management, but they are to be applied across all the layers of the organization. For the purpose of this discussion, an organization is modeled as consisting of the following layers :

- Corporate Governance Layer
- Executive Management Layer
- Operational Management Layer
- Technical Execution Layer

Thus, according to the definition, the decision-making and performance measurement frameworks are formulated by the top two layers, whereas the frameworks are applied across all 4 layers i.e. throughout the organization. Each of the four layers will, however, have its own requirements for what decisions are to be taken and what performance measures are to be monitored and reported.
As stated earlier in section 3 on Corporate Governance, the two frameworks will indeed be implemented through organizational structures. These structures will be related by their decision rights, responsibilities and accountabilities and the structures will operate as per the defined processes. These details will form the two frameworks.

The formulation of the Decision-making framework will be guided by questions such as:

- What are the decisions to be taken?
- Who takes which decision?
- What process is to be followed?
- What are the standards, policies, guidelines etc. that are needed to guide decision-making?

- What are the checks, controls and balances for ensuring proper decision-making?

The formulation of the Performance-Measurement framework will be guided by questions such as:

- Who are the stakeholders and what value do they expect from Information Security?
- Are our decisions being implemented and to what extent?
- What metrics do we need to monitor and report?

The approach to applying governance to information security would then mean asking and answering the above questions, and many more such questions, as they apply to information security e.g.

- What does information security mean for us?
- How much security do we need ? What is our risk appetite?
- Who will decide information security project prioritization and budgeting?
- How do we ensure alignment between Business, IT and Information Security?
- What support do Information Security projects need from the organization?
- What is our security architecture?
- Etc.

In the next section, the value that governance will enable information security to deliver to the organization gets discussed.

8. THE 'PERFORMANCE' OUTCOMES ASPECT OF INFORMATION SECURITY GOVERNANCE

This section discusses the 'performance' outcomes aspect of the definition of Information Security Governance i.e., the value that governance allows Information Security to deliver to the organization. The value ranges from being an effective protective mechanism to strategic alignment between the needs of business and information security.

The first three 'performance' outcomes of Information Security Governance can be seen as a hierarchy:

a. Due care and due diligence in the use of Information and IT Systems i.e. a healthy control environment which is the base foundation,
b. An effective and efficient process with due commitment and allocation of resources which leads to … (the next higher layer mentioned below),
c. Internal and external trust in the organization’s information and IT systems.

Information Security Governance has to ensure that appropriate entities are responsible for decision-making and accountable for performance measurement for delivering on the above objectives.

Another important aspect of information security implementation in organizations is the alignment that must be achieved between business, IT and information security. Information Security Governance has a crucial role in ensuring this alignment – not only must information security satisfy business and IT needs, but business and IT must conform to security guidelines. Information Security Governance delivers on alignment by ensuring that business, IT and information security participate in relevant decision-making and that appropriate performance metrics are defined.

Information Security is increasingly being regulated with many legislations and regulations being applicable. Information Security Governance has to ensure that the compliance posture of the organization is identified and that the appropriate regulations are complied with accordingly.
A major requirement for governance is to ensure reporting of relevant details to stakeholders. The purpose of this reporting is to ensure that stakeholders have visibility into the health of the organization. Information Security Governance has to ensure that the stakeholders are identified and their information needs are satisfied.

In this section, the elements of the value that information security delivers to the organization has been identified. Information Security Governance has a vital role in enabling this value delivery.

9. CONCLUSION

In this paper, a definition of Information Security Governance, based on a review of the current literature on Corporate Governance, IT Governance and Information Security Governance, was provided. This definition has two parts namely, the governance aspect and the value aspect. The definition links these two aspects together to show how governance can enable information security to deliver value to the organization.

The proposed definition is comparable to the definition of 'Internal Control' as proposed by (COSO, 1992) which define 'Internal Control' as the responsibility of Board of Directors and Executive Management. The objectives of 'Internal Control' are effectiveness of operations, reliability of financial reporting and compliance with applicable laws and regulations (COSO, 1992). Likewise, the proposed definition is comparable to the 'Security Organization' control contained in ISO 17799 (ISO 17799). This control envisages a management framework consisting of allocation of responsibilities, co-ordination and approval processes. However, ISO 17799 does not provide any detailed framework for the implementation of this control.

The definition can serve as a foundation for developing a framework for Information Security Governance in organizations. This framework can then be used by Board of Directors and Executive Management to implement effective Information Security within their organization.

10. REFERENCES

ANAO (2003). Public Sector Governance Volume 1 Better Practice Guide Framework, Process and Practices. *Australian National Audit Office*. (online) (cited 05 May 2005). Available from Internet: URL http://www.anao.gov.au/WebSite.nsf/0/957e55a69b1050724a256d73001dfd1c/$FILE/Volume%201,%20Framework,%20Processes.pdf

BSA (2003). Information Security Governance: Toward a Framework for Action. Business Software Alliance. (online) (cited 05 May 2005). Available from Internet: URL http://www.bsa.org/resources/loader.cfm?url=/commonspot/security/getfile.cfm&pageid=5841&hitboxdone=yes

CGTF (2004). Information Security Governance: A Call To Action. Corporate Governance Task Force. (online) (cited 05 May 2005). Available from Internet: URL http://www.cyberpartnership.org/InfoSecGov4_04.pdf

CIMA (2004). Enterprise Governance Getting the Balance Right Executive Summary. Chartered Institute of Management Accountants. (online). (cited 05 May 2005). Available on Internet: URL http://www.cimaglobal.com/cps/rde/xbcr/SID-0AAAC564-30AB5F4F/live/enterprise_governance_summary_2004.pdf

COSO (1992). Internal Control - Integrated Framework Executive Summary. The Committee of Sponsoring Organizations of the Treadway Commission. (online). (cited 05 May 2005). Available from Internet: URL http://www.coso.org/publications/executive_summary_integrated_framework.htm

FISMA (2002). Federal Information Security Management Act of 2002. U.S. Congress. (online). (cited 05 May 2005). Available from Internet: URL http://csrc.nist.gov/policies/FISMA-final.pdf

Hamaker, S. (2003). Spotlight on Governance. Information Systems Control Journal, Volume 1, 2003. (online). (cited 05 May 2005). Available on Internet: URL http://www.shamrock-technologies.com/Journal_article2.pdf

ISACF (2001). Information Security Governance: Guidance for Boards of Directors and Executive Management. Information Systems Audit and Control Foundation. (online). (cited 05 May 2005). Available on Internet: URL http://www.isaca.org/Content/ContentGroups/ITGI3/Resources1/Information_Security_Governance_Guidance_for_Boards_of_Directors_and_Executive_Management/infosecurity.pdf

ISO 17799. ISO / IEC 17799:Code of Practice for Information Security Management. International Standards Organisation, Geneva, Switzerland.

IT Governance Institute (ITGI) (2003). Board Briefing on IT Governance, 2nd Edition. IT Governance Institute. (online). (cited 05 May 2005). Available on Internet: URL http://www.itgi.org/Template_ITGI.cfm?Section=ITGI&Template=/ContentManagement/ContentDisplay.cfm&ContentFileID=4667

Melnicoff, Richard M., Shearer, Sandy G. & Goyal, Deepak K. (2005). Is There a Smarter Way to Approach IT Governance ? (online). (cited 05 May 2005). Available from Internet: URL http://www.accenture.com/xdoc/en/ideas/outlook/1_2005/pdf/it_gov.pdf

OECD (2004). OECD Principles of Corporate Governance. Organisation For Economic Co-operation and Development. (online). (cited 05 May 2005). Available on Internet: URL http://www.oecd.org/dataoecd/32/18/31557724.pdf

Shleifer, Andrei and Vishny, Robert W. (1996). A Survey of Corporate Governance. NBER Working Paper No. W5554. (online). (cited 05 May 2005). Available on Internet: URL http://papers.nber.org/papers/w5554.pdf

Van Grembergen, W. (2002). Introduction to the Minitrack: IT governance and its mechanisms. Proceedings of the 35th Hawaii International Conference on System

Sciences (HICCS), IEEE. (online). (cited 05 May 2005). Available on Internet: URL http://www.hicss.hawaii.edu/HICSS39/foscfp.htm

von Solms, Basie (2001). Corporate Governance and Information Security. Computers & Security 20(3): 215-218 (2001).

von Solms, R., & Thomson, Kerry-Lynn (2003). Integrating Information Security into Corporate Governance. IFIP TC11, 18th International Conference on Information Security (SEC2003), Athens, Greece. Kluwer Academic Publishers Group, Netherlands : pp. 169-180.

Weill, Peter & Woodham, Richard (2002). Don’t Just Lead, Govern: Implementing Effective IT Governance. MIT Sloan Working Paper No. 4237-02. (online). (cited 05 May 2005). Available from Internet: URL http://ssrn.com/abstract=317319

Table 1. **Information Security Governance and Organizational Hierarchy**

(ISACF, 2001)	(CGTF, 2004)	(BSA, 2003)	(FISMA, 2002)
• Board • Management	• Board of Directors / Trustees • Senior Executive • Executive Team Members • Senior Managers • All Employees and Users	• Corporate Executives • Business Unit Heads • Senior Managers • CIOs / CISOs	• CEO • Business Unit Heads • Senior Managers • CIO / CISO

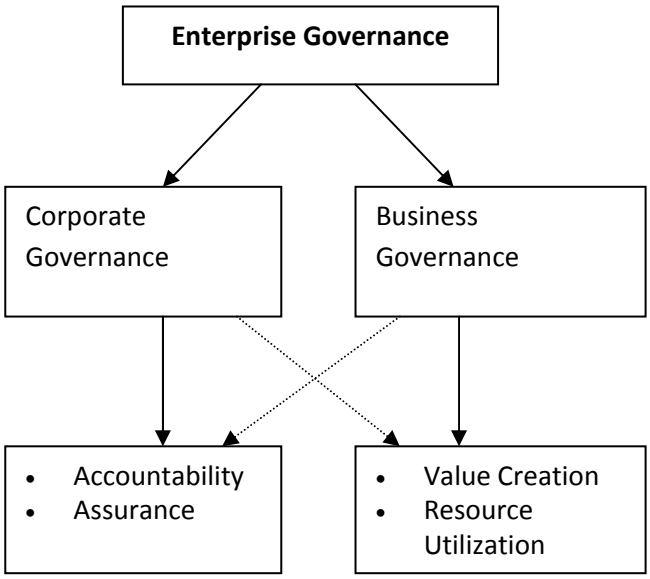


Figure 1. **The enterprise governance framework (CIMA, 2004)**

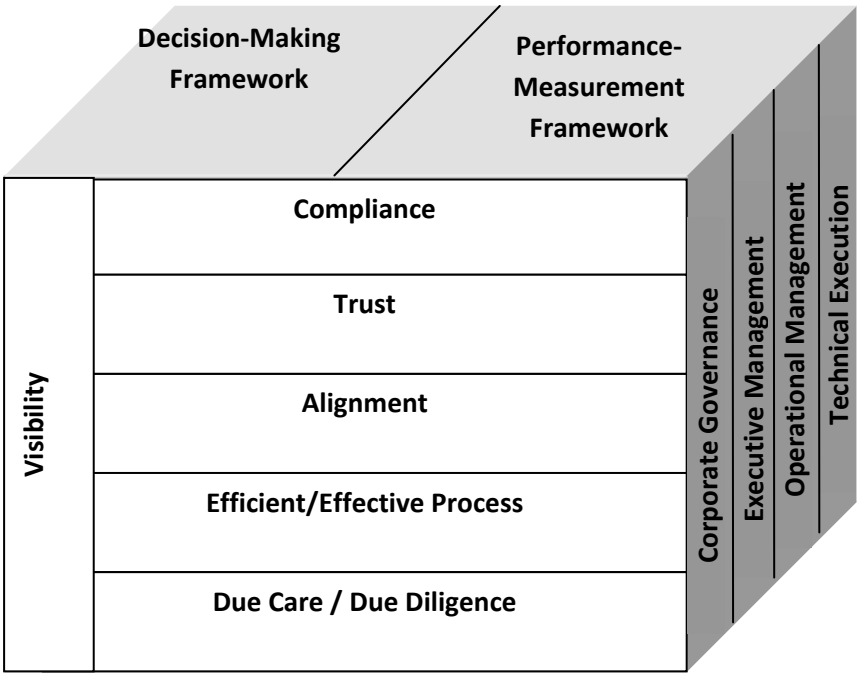


Figure 2. **Information Security Governance Model**

Appendix B:

A Service-oriented Approach to Information Security Management

Rahul Rastogi[a] **and Rossouw von Solms**[b]

Institute for ICT Advancement,
Nelson Mandela Metropolitan University, South Africa

[a]rahul.rastogi@eil.co.in
[b]rossouw.vonsolms@nmmu.ac.za

Abstract

People, whether as decision-makers or as end-users, are central to the effectiveness of Information Security Management in organizations. Successive waves in the evolution of Information Security Management have attempted to address this issue. However, the prevailing approaches to Information Security Management have a "control-based management" orientation, which does not promote people's commitment and loyalty to Information Security. In this paper, an alternative approach is proposed – the service management approach, i.e. Information Security Service Management, having "commitment-based management" orientation. It is hoped that this approach will foster true loyalty amongst people towards the organization's Information Security policies and controls.

Keywords: Information Security Management, Information Security Service Management, ISSM, service management.

1. Introduction

"The only system that is truly secure is one that is switched off and unplugged, locked in a titanium safe, buried in a concrete vault on the bottom of the sea and surrounded by very highly paid armed guards. Even then I wouldn't bet on it." (Spafford, E.H., 1999)

The quote above epitomizes the dilemma that the process of Information Security Management faces. In a world where collaboration, flexibility, speed of response, borderless organizations etc. are the mantras for business success, Information Security is often perceived as a hindrance and irritant. There is a constant tension between the free

flow and use of information assets and the need to secure these assets, often at the peril of restricting this freedom (Baskerville, 1993). This tension exists at both the organizational level as well as at the individual level, and at both levels the tension leads to the emergence of several trade-offs. At the organizational level, there are two constituencies that make the trade-off namely, Business Management and IT Management. At the individual level, it is the employees or end-users that make the trade-off.

At the organizational level, people in senior management positions have to understand how information has become a key asset to their organization and how they have a distinct role in its protection. As the Institute of Internal Auditors notes, "An organization's information is amongst its most valuable assets and is critical to its success. The board of directors, which is ultimately accountable for the organization's success, is therefore responsible for the protection of its information" (IIA, 2000). The trade-off that exists for business management then is whether they invest in protecting existing stakeholder value through securing information assets or whether they invest in creating new stakeholder value through new business initiatives making innovative use of information assets.

People in IT Management also have to make trade-offs related to Information Security. Information Security made modest beginnings as technical or IT-based protection controls and IT was the custodian entrusted with the responsibility of Information Security. But, today, this role of custodian puts IT Management against its other role of strategic partner of business management. This creates a conflict of interest for IT Management. The dynamic business environment compels IT Management to focus on ease-of-use, flexibility, adaptation, open IT environments, new collaboration applications, anytime-anywhere access to information etc. Further, IT Management is often under constraints of resources and time for meeting the constant flow of new demands. In this scenario, it becomes difficult, if not entirely impossible, for IT Management to continue to serve as the sole custodian of information related assets.

End-users, the employees, are perhaps the most beleaguered constituency having to deal with Information Security in a fast changing world. They are recognized as the "human firewall" (Wohnlich, 2006), but they are also maligned as the "weakest link" (Lineberry, 2007). End-users have to deal with the conflicting demands of information use and Information Security. They have to undergo this dilemma several times everyday. Should they trust their colleagues or should they be paranoid – how do they decide? Should they share their password with a colleague or secretary and get going with the job at hand? Or insist on the sanctity of passwords at the cost of losing their colleague's confidence or perhaps even preventing the organization from achieving its goals? In this scenario, end-users are often tempted to take the course of expediency, even if at the expense of

Information Security control objectives, and they sacrifice security in the pursuit of work (Desouza and Vanapalli, 2005). So, even though they do so for bonafide reasons, they end up putting the organization and its information assets at increased risk (Stanton et al., 2005).

People, whether as decision-makers in Business and IT Management or as end-users, are central to the effectiveness of Information Security Management at large. However, it may be argued that current approaches to Information Security Management have not focused adequately on the people-aspect of Information Security. In the view of the authors of this paper, the inadequacy of this focus is a consequence of the "control-based management" orientation of prevailing Information Security Management. This paper proposes a new "service management" approach to Information Security Management, namely, the Information Security Service Management (ISSM) approach. In ISSM, people are placed at the centre of Information Security Management and a "commitment-based management" orientation is adopted. It is hoped that this approach may be more advantageous to the effectiveness of Information Security Management in organizations.

The next section explores the evolution of Information Security Management and identifies the importance of people's loyalty and commitment to Information Security in an organization. The following two sections provide a brief overview of the literature on commitment and service management. The subsequent section applies the principles of service management to Information Security Management leading to the development of the Information Security Service Management (ISSM) approach. The final section concludes by providing areas for further research.

2. The Evolution of Information Security Management

At all levels, Business Management, IT Management or end-users, it is people that are involved in making the trade-offs between information use and security. Recognizing this fact, Information Security Management has continued to evolve. Though it began as technical IT-controls, the domain of Information Security has expanded to include people, processes, policies and technologies. Von Solms (2000, 2006) have identified four waves of development: the Technical Wave, the Management Wave, the Institutional Wave and the Information Security Governance Wave. In the first Technical wave, controls were IT-based, that means most controls were physical and technical in nature. This wave was enhanced by the introduction of "management" to security controls to lead to the second or the Management wave. In this wave, security controls were "managed" and policies and management involvement gained prominence. In the third Institutional wave, standards, guidelines, best practices and checklists began to appear to guide the implementation of Information Security within organizations. The

fourth wave is the wave of Information Security Governance which relates to the legal and regulatory obligations of Top Management and Boards of Directors towards the state of Information Security in their organizations.

A common thread that runs through these four waves is that the process of implementation of Information Security within an organization has remained largely unchanged. Information Security controls are designed to protect information assets and formulated on the basis of risk assessments. As Baskerville (1993) states, "the common purpose (of all security controls) is to constrain the information system to legitimate, allowed behaviour". In this philosophy, Information Security Management follows the "control" mindset in which a top-down organizational structure formulates the rules and policies that are to be obeyed by the rest of the organization. This is the "control-based management" or "transactional leadership" style, in which "the prime purpose of a subordinate is to do what their manager tells them to do" (Transactional Leadership, n.d.). Information Security Management also establishes a regime of rewards and punishments to obtain compliance. Training is provided to employees to ensure they can perform security-related activities. Business Management creates a tone-at-the-top to encourage an organizational culture of Information Security compliance. However, as already discussed earlier, this approach to Information Security Management has not been entirely successful. As a consequence, employees continue to indulge in opportunistic behaviour and side-step security policies and controls, exhibiting low levels of commitment to Information Security. As noted by Sirota et al. (2008) in the context of workforce management, such behaviour can be attributed to the prevailing orientation of Information Security Management.

A brief review of the literature on Information Security reveals attempts to mitigate this short-coming by accommodating the "people-aspect". Human error models and usability guidelines are being adopted to guide the design of security controls to make them more people-friendly (Brostoff and Sasse, 2001 and Whitten and Tygar, 1999). Security tools and technologies are being designed to obviate the need for end-user action. Training and awareness campaigns are being studied and designed to motivate people and enable them to successfully execute security-related activities (Siponen, 2000 and Thomson and Von Solms, 1998). Ethics and culture-issues are being targeted to create an organizational culture of Information Security compliance or obedience (Siponen, 2001, Thomson et al., 2006, and Thomson and Von Solms, 2004). Organizational commitment of employees is also seen as a predictor of employees' secure behaviour (Stanton et al., 2003). All these research efforts attempt to ensure that users of information will comply with the Information Security policies and controls. It is the view, however, of the authors of this paper that these efforts still represent the prevailing "control" or "transactional" style of Information Security Management, albeit with some amount of democratization.

It can be argued that an alternative approach to Information Security Management is needed as the prevailing approach is proving inadequate to deal effectively with the issues of Information Security in organizations, particularly with respect to the 'people-aspect'. In order to propose an alternative, this paper studies the concept of "loyalty" as in marketing theory.

Businesses often strive to obtain customer loyalty. Customer loyalty results in greater repeat purchases by existing customers. Further, loyal customers are less likely to switch to competitors solely because of price (Bowen and Shoemaker, 1998). Jacoby and Chestnut (1978, cited in Ha, 2005) state that loyalty is represented by a set of six conditions:
"Loyalty is (1) the biased (i.e. nonrandom), (2) behavioural response (i.e. purchase), (3) expressed over time, (4) by some decision-making unit, (5) with respect to one or more alternative brands out of a set of brands, and (6) is a function of psychological (decision-making evaluative) processes."

Thus, a loyal individual exhibits the behavioural consistency of repeat purchase driven by psychological evaluative processes. Loyalty is a construct that combines both behavioural consistency and psychological commitment. Behavioral consistency combined with psychological commitment leads to "true loyalty", whereas behavioural consistency without psychological commitment leads to "spurious loyalty" (Day, 1969, cited in Ha, 2005). "True loyalty" customers exhibit a strong psychological commitment and will exhibit repeat purchasing behaviour. Such customers are also unlikely to switch to competing brands. "Spurious loyalty" customers exhibit a lack of psychological commitment to the brand. Though such customers exhibit behavioural consistency, such customers are likely to shift to competing brands at the slightest opportunity. This combined construct of loyalty is useful in not only understanding past behaviour, but also predicting future patronage (Evanschitzky et al., 2006).

Returning to the previous discussion of the prevailing "control" or "transactional" style of Information Security Management, it is evident that the current approach concerns itself only with behavioural consistency of employees towards Information Security policies and controls. Following the discussion above, this leads only to "spurious loyalty" under which employees are often tempted to switch to more convenient solutions, flouting security policies and controls. The present approach to Information Security Management does not give due importance to psychological commitment, which is the precursor to "true loyalty" of employees towards Information Security. Thus, an approach to Information Security Management that promotes psychological commitment of employees to Information Security policies and controls will lead to a more effective

state of Information Security in an organization. (Since commitment is regarded as psychological in nature, from hereon, this paper will refer to “psychological commitment” as only “commitment”.)

In “commitment-based” management strategy, employees are fully committed to the well-being of the organization (Walton, 1985 and Khatri et al., 2006). Further, from Walton (1985) and Khatri et al. (2006), individual performance is not monitored and controlled closely, rather employees are trusted and allowed to work autonomously. Coordination and control are based more on shared goals, values and traditions. Employee participation in decision-making is encouraged. Employees take pride in the organization and are willing to go beyond the call of duty and role definitions.

From the previous discussions it can be concluded that a “commitment-based” approach to Information Security Management will be more advantageous to the organization as compared to the “control-based” approach. This paper proposes that a “commitment-based” approach to Information Security Management can be achieved using a “service management” approach. In the service management approach, Information Security will become an internal service. Business Management, IT Management and end-users will become the customers of the internal Information Security Service. Information Security Management will attempt to identify and meet the evolving needs of its customers, “sell” Information Security to its customers and obtain on-going and long-term commitment to Information Security in the organization. The role of Business Management will be to establish the strategic importance of Information Security for the organization. The role of Information Security Management will be to establish and maintain the relationships with Business Management, IT Management and end-users. Table 1 summarizes the benefits that accrue on account of this approach. Figure 1 indicates the relationships between Business Management, IT Management, End-users and Information Security Management.

Customer of Information Security Service	Information Security Service Provider	
	What does Information Security Service Management deliver to its Customer i.e. What is the Customer Value Proposition?	**What does Information Security Service Management obtain from its Customer in return?**
End-users	Deliver a user-centric approach to Information Security leading to a friendly and satisfying user-experience.	Obtain ongoing end-user loyalty and long-term commitment to compliance with policies and controls.
Business Management	Deliver effective Information Security to the organization, aligned to the needs and directives of the Business Management.	Obtain greater credibility for the Information Security Service Management and long-term commitment to Information Security efforts.
IT Management	Partner with IT and provide directives / guidelines / support to IT in the area of Information Security.	Obtain IT Management's long-term commitment to comply with Information Security directives and policies.

Table 1: Benefits of Information Security Service Management - the "service management" approach to Information Security Management.

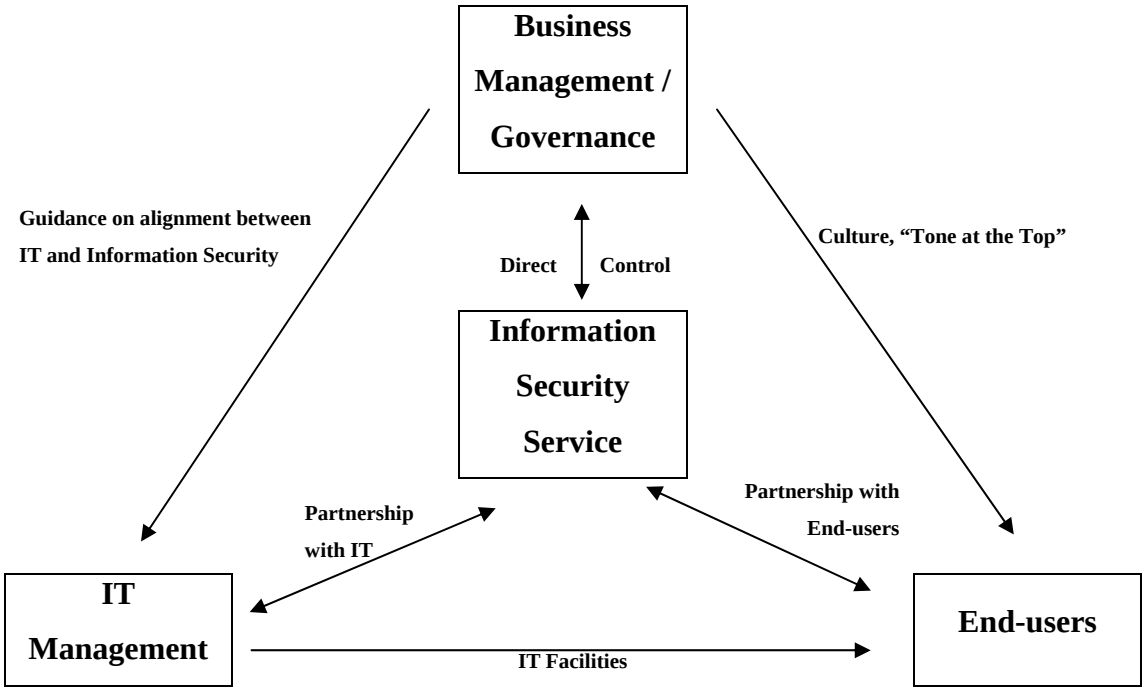


Fig. 1: Relationships between Business Management, IT, End-users and Information Security Service

Commitment, relationships and service management are inter-related concepts. Commitment and relationships are mutually reinforcing – commitment leads to stronger relationships, stronger relationships lead to increased commitment. Service management is inherently relational (Gronroos, 2007). Thus, service management initiates a causal chain linking service management, relationships and commitment. Finally, as commitment leads to "true loyalty", service management may open a path leading to "true loyalty".

The next two sections look at these inter-related concepts. The next section provides an overview of Commitment and Relationships and the subsequent section provides an overview of Service Management.

3. Commitment and Relationships

Meyer and Herscovitch (2001, cited in Bansal, Irving and Taylor, 2004) define commitment as the force of a psychological bond that causes the individual to continue with a relationship:

"a force that binds an individual to a course of action of relevance to one or more targets. As such, commitment is distinguishable from exchange based forms of motivation and from target-relevant attitudes and can influence behaviour even in the absence of intrinsic motivation or positive attitudes."

Meyer and Allen (1991) presented the "Three-component" model of commitment of employees to their organization. They state that organizational commitment is a mind-set or psychological state concerning the employee's relationship with the organization and has implications for the decision to continue or discontinue membership in the organization. Commitment is conceptualized as composed of three components – affective, continuance and normative commitment. Affective commitment refers to the employee's emotional attachment to, identification with, and involvement in the organization. Affective commitment reflects a desire to continue. Employees continue with the relationship because they want to continue. Continuance commitment refers to an awareness of the costs associated with discontinuing the relationship. Employees under continuance commitment, continue because they need to. Normative commitment reflects a feeling of obligation to continue the relationship. Employees under normative commitment, continue because they feel that they ought to.

In the three-component model, an employee can experience all three forms of commitment to varying degrees. The three components interact to influence behaviour. Meyer and Allen (1991) state that employees' willingness to contribute to organizational effectiveness will be influenced by the nature of commitment they experience. Employees under affective commitment might be more likely to exert effort on behalf of the organization. Such employees exert more effort because they want to, rather than because they need to (continual commitment) or because they feel obligated to (normative commitment). Individuals under affective commitment may be more inclined to engage in behaviours that benefit the organization than those under normative or continuance commitment. Morgan and Hunt (1994) state that affective commitment is created when an individual internalizes, the values of the organization. Affective commitment reflects a sense of liking and emotional attachment to the partnership. Calculative commitment (i.e. normative and continuance components) is based on gains / losses, rewards / punishments or plusses / minuses. Kumar et al. (1994, cited in Wetzels et al., 1998) state that affective commitment contributes most to the establishment and continuation of mutually beneficial relationships between partners. Affective commitment has strong positive influence on the intention to stay in a relationship, the desire to stay in a relationship, performance and the willingness to invest in a relationship. Affective commitment contributes further to the relationship by discouraging development of alternatives for a relationship and opportunistic behaviour.

Evanschitzky et al. (2006) cite various researchers to show that the three-component conceptualization of commitment is equally applicable to other kinds of relationships – employee-employer relationship (Meyer and Allen, 1991), manufacturer-distributor relationship (Geyskens et al., 1996) and romantic relationships (Rusbult, 1980). Bansal et al. (2004) also cite various researchers to show that the three-component model is equally applicable to the domains of relationship marketing, organizational behaviour, marital commitment etc. Evanschitzky et al. (2006), Bansal et al. (2004) and Wetzels et al. (1998) apply this model to the relationship between service consumers and service providers. Thus, the three-component model of commitment has broad applicability and can be used to model commitment in a wide variety of relationships, including the relationships of Business Management, IT Management and end-users with Information Security Management.

The notion of relationship is central to the concept of commitment. Relationship and commitment are mutually reinforcing. Grönroos (2007) provides an attitude-oriented description of relationship: “a relationship has developed when a customer perceives that a mutual way of thinking exists between customer and supplier or service provider”. The “mutual way of thinking” reflects bidirectional commitment i.e. not only is the customer to be committed to the business, but the business must in turn be committed to the customer. The business should understand its customer and the customer’s needs and continuously strive to meet those needs.

Ravald and Grönroos (1996) state that the relationship between a business and its customers influences how customers perceive the total value of a business’s offering. The difference between a business and its competitors and the reason why a customer chooses to patronize a business over its competitors may be the relationship the business establishes with the customer and the value the customer attaches to the relationship. In this case, the customer shifts the focus from evaluating separate offerings to evaluating the relationship as a whole (Ravald and Grönroos, 1996). This relationship is valuable to the business because it makes the customer tolerant to occasional inferior performance (Ravald and Grönroos, 1996). So, the focus for the business shifts from the “offerings it provides to the customers” to the “kinds of relationships the business can maintain with the customers” (Ravald and Grönroos, 1996).

Commitment has multiple components, affective commitment being the most enduring component. Further, relationships and commitment are mutually reinforcing. There is a causal link between relationships and commitment. Thus, if a business adopts a relational strategy, customer commitment will be achieved, leading to “true loyalty”. The next section is an overview of the service management strategy, which is inherently relational.

4. Service Management

This section provides an overview of the service management approach and identifies the main components thereof. Researchers like Christian Gronroos, Evert Gummesson, Stephen L. Vargo, and Robert F. Lusch have made significant contributions to the concepts of “service”, “service management” and “service-dominant logic”. This section is heavily influenced by the thinking of these researchers and quotes extensively from their works.

At the outset, it is worth stating that the service management approach is as applicable to internal services as it is to the provisioning of a service by a firm for its external customer. “Service” is a philosophical perspective and “service management” is not one discipline or coherent area of its own (Gronroos, 1994). It is a logic that is philosophically grounded in a commitment to collaborative processes with customers, partners and employees (Lusch et al., 2007). Being a mind-set, service management is applicable to all kinds of organizations and businesses. Service management is also applicable to internal services, the basic premise being that if the internal services are aligned to the needs and usage by internal users, the overall effectiveness of the corporation will be enhanced (Vandermerwe and Gilbert, 1989). Vandermerwe and Gilbert (1989) delineate the market-driven approach to internal services. In this approach, providers and receivers become sellers and buyers. Sellers attempt to know about their buyers’ business, why they want the service and how it will be used. The priority for all is value added to the buyer, and thus to the corporation. The internal service function becomes the “flexible service factory” wherein systems and processes are engineered for productivity and cost effectiveness while at the same time meeting specific buyer needs.

Having thus established the applicability of service management to management of internal services, and, therefore, to Information Security Management in an organization, the remainder of this section provides an overview of service management and its implications for firms adopting it.

In the realm of management of organizations, different management paradigms or perspectives have been identified. Three paradigms identified by Gummesson (1993, cited in Gummesson, 1994) are, viz:

- The manufacturing paradigm – the focus is on goods. Productivity and cost are important parameters to be controlled. Quality is only about technical standards and specifications.
- The bureaucratic-legal paradigm – the focus is on compliance to regulations and rituals than on end results.
- The service paradigm – the focus is on the customer and the customer’s interactions with the provider. Process thinking is the core of service delivery. Quality is not just

about conforming to technical standards and specifications, it revolves around customer satisfaction.

Grönroos (2007) identifies four different strategic perspectives, namely:

- Core-product perspective – this is the traditional scientific management-based approach, where the quality of the core solution is considered to be the main source of competitive advantage. The firm focuses on the development of the core solution, whether product or service. This strategy is not sustainable in the long run.
- Price perspective – the firm takes the view that price is the dominating purchasing criterion for its customers. The firm focuses on being the cheapest, or one of the cheapest, alternatives available to the customer.
- Image perspective – the firm focuses on creating a brand image through advertising and marketing. This brand image is considered to be the major contributor to the customer's value-creating processes.
- Service perspective – the firm focuses on providing a total service offering to the customer. This service offering consists of the physical product component, the service component, information, personal attention and other elements of customer relationships. Developing the total service package is seen to be of strategic importance and given highest priority. Price is considered less important for customers in comparison to long-term costs.

The firm's choice of the "service paradigm" or "service perspective" as its strategic management perspective is motivated by what customers demand today. As Grönroos (2007) says, customers are looking for solutions or packages which they can use so that value is created for them. They need support for their everyday lives and activities. In the words of Gummesson (1994), "Customers do not buy goods or services in the traditional sense; they buy an offering which renders services which create value for the customer". This focus on meeting customer needs through a total service package is again emphasised by the definition of "service" by Vargo and Lusch (2008) "as the application of specialized competences (operant resources – knowledge and skills) through deeds, processes and performances for the benefit of another entity or the entity itself". Regarding quality of the service package, Gronroos (2007) notes that customers perceive quality of a service in terms of both technical and functional aspects. The technical aspects refer to "what" the customer receives; the functional aspects refer to "how" the customer receives it. The functional aspects are determined by the quality of interactions between the firm and the customer. Lehtinen and Lehtinen (1991) call this "interactive quality" which is "the dimension of quality originating in interaction between the customer and the interactive elements of the service organization". Gronroos (2007) also states that the customer perceives the quality of the solution in terms of the "service experience". The service encounter creates the customer's "service experience" in terms

of the cognitive, emotional and behavioural “mental mark”. This mental mark may be positive (or favourable), negative (or unfavourable) or neutral. The experience has a strong impact on the customer’s quality perception, commitment and loyalty. Wollan (2008), reviewing Accenture’s Global Customer Satisfaction Survey of 2008, notes that a “satisfying service experience” is the “core of what customers care about most”. At this backdrop, Wollan (2008) further notes that “consumer expectations are rising with no ceiling in sight” and that “the gap is widening between the service consumers expect and the service they experience”. Thus, customers demand that firms focus more and more on providing a total service package to the customer and ensure excellence in the service experience.

Consequently, firms have a need to re-orient themselves, move away from traditional, scientific management and adopt the service management approach. Gronroos (1990) defines service management as:
“Service Management is:

- To understand the utility customers receive by consuming or using the offerings of the organization and how services alone or together with physical goods or other kinds of tangibles contribute to this utility that is, to understand how total quality is perceived in customer relationships and how it changes over time;
- To understand how the organization (personnel, technology and physical resources, systems and customers) will be able to produce and deliver this utility or quality;
- To understand how the organization should be developed and managed so that the intended utility or quality is achieved; and
- To make the organization function so that this utility or quality is achieved and the objectives of the parties involved (the organization, the customers, other partners, society, etc.) are met”.

Making service to customer a strategic imperative requires a shift in organizational focus. Customer satisfaction and external efficiency become critical, internal efficiency and cost operations become secondary (Gronroos, 1990).

Gronroos (1990) identified six principles of service management:

- The business logic: managing customer relationships and customer perceived quality are critically important to success. Interest in cost and productivity become secondary.
- Decision-making authority: employees are empowered, encouraged, and trained, to solve problems following from deviations from standard procedures so that customer satisfaction is created.
- Organizational Focus: focus shifts away from structure and control procedures to process and customer perceived quality.

- Supervisory Control (or rather Supervisory Support): supervisory focus has to be on encouragement and enablement of employees so they can deliver quality service.
- Reward Systems: efforts at producing customer perceived excellence are rewarded rather than compliance to predetermined standards.
- Measurement Focus: the primary variable to be measured becomes customer satisfaction with service quality.

Service management is seen as an alternative to scientific management. Gronroos (1994) stated the problems associated with traditional, scientific management as deteriorating quality of service and internal workforce environment, which in turn lead to deterioration of customer relationships, eventually causing profitability problems. Service management promises to mitigate these problems through teamwork, inter-functional collaboration, inter-organizational partnership, and a long-term perspective. This approach requires the development of a different set of competences and resources for meeting the needs of customers by offering them the "total service package". Service management is inherently relational, and customer requirements and relationships become the driving force. In service management, customer loyalty is the pivot of success.

This section outlined the service management paradigm. This paradigm is not just another alternative to scientific management, but is necessitated by the rising demands that customers place on businesses or organizations. It is imperative that this change in customer-needs will also apply to employees of these businesses or organizations, as these employees relate to the internal services being provided by different departments within the organization. The next section applies the principles of service management to Information Security Management, which really is an internal service.

5. Information Security Service Management (ISSM)

The famous Harvard Professor, Theodore Levitt has remarked, "People don't buy quarter inch drills, they buy quarter-inch holes". In the context of Information Security, people and organizations do not buy controls, policies, patches, firewalls etc. but they buy a sense of security and protection. Encapsulating the Information Security function as a service hides all the technical details and surfaces only the service delivery / service encounter aspect that provides value to the organization and the end-users. Vandermerwe and Gilbert (1989) delineated a market-driven approach to internal services. Proceeding from this, Information Security Service Management (ISSM) function should position itself as an internal service provider. The Information Security Service Management function then becomes the provider or seller of Information Security Service, whereas the organization becomes the customer. The key customer segments are Business Management, IT Management and end-users. In this scenario, the Information Security

Service Management function should attempt to understand the needs of its customers and what they expect from the service.

The previous section identified the implications of the service management approach. This approach is characterized by the "total service offering" for the customer and strategic importance of customer satisfaction. In this approach, internal efficiency becomes secondary to the customer experience. Information Security Service Management is derived by applying the principles of service management (Gronroos, 1990) to traditional Information Security Management (ISM). Table 2 provides a summary.

In traditional Information Security Management, the business logic is considered only through the lens of protecting the information assets of the organization. The confidentiality, integrity and availability properties of information assets become of prime importance. Various kinds of security policies and controls are formulated and implemented. End-users are expected to comply at the risk of punitive measures for non-compliance. The business logic is very much a top-down and "control-based" approach. In contrast, the business logic of ISSM is "commitment-based". It is focused not just on formulating security policies and controls, but the ISSM function sees itself as providing a complete support system to its customers, namely, the people who are involved as decision-makers or as end-users of Information Security. The ISSM approach is based on the belief that satisfied and loyal users will lead to a more effective state of Information Security in the organization and that the user satisfaction is derived from the service experience or the users' encounters with the Information Security Service. In the ISSM approach, factors such as costs, strength of security architecture, efficiency of operations etc. become secondary to the user experience.

Dimension	Principle of Service Management	Principle applied to Information Security Service Management (ISSM)
The business logic	Managing customer relationships and customer perceived quality are critically important to success. Interest in cost and productivity become secondary.	ISSM realizes that formulation and enforcement of security policies and controls are insufficient for effective security. Managing relationships and obtaining long-term commitment of Business Management, IT Management and end-users are seen as critical to success.
Decision-making authority	Employees are empowered, encouraged, and trained, to solve problems following from deviations from standard procedures so that customer satisfaction is created.	Maintaining a state of "lock-down" is not the sole purpose of Information Security staff. Staff must understand that their responsibility is to provide support to the users to enable them to understand and work with security policies and controls.
Organizational Focus	Focus shifts away from structure and control procedures to process and customer perceived quality.	ISSM realizes that customer perceives quality not by the technical strength of security controls and technical competence of staff. ISSM realizes that customer perceives quality on the basis of his/her experience in dealing with security policies and controls and the behaviour of the security support staff.
Supervisory Control (or rather Supervisory Support)	Supervisory focus has to be on encouragement and enablement of employees so they can deliver quality service.	ISSM has to encourage not just its own staff but also end-users to practice secure behaviour. Regular training and feedback sessions are crucial. Both staff and end-users must understand and appreciate each other's compulsions.
Reward Systems	Efforts at producing customer perceived excellence are rewarded rather than compliance to predetermined standards.	User satisfaction rating of security and security staff is considered more important than the traditional security metrics such as number of patched systems, number of viruses stopped etc.
Measurement Focus	The primary variable to be measured becomes customer satisfaction with service quality.	The primary variable to be measured is user satisfaction. Metrics, such as number of patched systems, number of viruses stopped etc., become secondary.

Table 2: Principles of Service Management applied to Information Security Service Management (Information Security Service Management)

In conjunction with the new business logic, the organizational focus of ISSM shifts from formulating security policies and controls to establishing, maintaining and continuously enhancing the relationships with its customer segments namely, Business Management, IT Management and end-users. ISSM must also initiate a feedback loop between all these

segments ensuring that each segment understands and appreciates each others' views on Information Security. With the IT Management and end-users, understanding their needs and converting them to the Business Management's view on Information Security become crucial. At the same time, Business Management's views on Information Security must be informed by the IT Management and end-user perspectives. For ISSM, obtaining end-user commitment to organization's policies and controls becomes top priority. This necessitates not just communication of organization's policies to end-users but also communicating and incorporating the end-users' needs and perspective into the security policies and controls.

The shifts in business logic and organization focus lead to a shift in decision making. In the ISSM approach, the Information Security function no longer just consists of security architects and experts, but also end-user facing support personnel. These personnel must not only be trained to understand the Information Security policies and controls, but must also be empowered to use their discretion in helping end-users navigate through these policies and controls. These personnel also understand the crucial role of their behaviour while dealing with the end-users. Appropriate technology may also be used to make it easy for end-users to seek help and enable the support personnel to provide friendly and efficient service.

The supervisory control, reward system and measurement focus are all geared to ensure that the ISSM function delivers on the directions provided by the business logic and the organizational focus. In the ISSM approach, the role of supervisors is not so much to control the support personnel, as to enable and empower them in maintaining relationships with the end-users. The reward system and the measurement focus should also reflect this focus on end-user relationships and satisfaction. The reward system does not reward maintaining an adequate level of "lock-down", but it rewards excellence in end-user service. Measurement focus is then on customer perceived quality based on their experiences with the security policies, controls, support personnel and the rest of the ISSM function.

The service management approach to Information Security Management entails a shift in focus from the formulation and enforcement of security policies and controls towards the satisfaction of the customers of the Information Security service. This shift is aimed at obtaining long-term commitment and loyalty of people to the organizational security policies and controls. This section discussed the implications of the service management approach for Information Security Service Management in terms of six service management principles namely, business logic, organizational focus, decision-making authority, supervisory control, reward systems and measurement focus.

6. Conclusion

This paper began by highlighting the centrality of people to the effectiveness of Information Security Management in organizations. People are important as decision-makers in Business Management and IT Management positions. People are also important as end-users who have to comply with the organization's Information Security policies and controls. Information Security Management has recognized this "people-aspect" and has evolved to meet this challenge. However, the "control-based management" orientation of prevailing approaches to Information Security Management has certain shortcomings in that it only promotes "spurious loyalty". This paper proposes that the "commitment-based management" orientation of Information Security Service Management may be more advantageous for organizations and it may lead to "true loyalty".

Gronroos (1990) identified six principles of service management. This paper developed the Information Security Service Management approach by applying these principles to Information Security Management. These principles are wide-ranging and cover the dimensions of business logic, organizational focus, decision making authority, supervisory control, reward systems and measurement focus.

The main contribution of this paper is in proposing an alternative management orientation for Information Security Management. In the view of the authors of this paper, the shifts in business logic and organizational focus to Information Security Service Management represent a significant reorientation of security practitioners' view of people, as decision-makers or as end-users. In this "relational" approach, Information Security Service Management could, perhaps, be re-defined as the management of the relationships between the four constituencies of Information Security, the end-users, Business Management and IT Management.

This paper represents a work in progress. Considerable work remains to be done in creating an actionable framework by exploring the various issues related to the creation, establishment and maintenance of the various relationships and how these could be leveraged to ensure "true loyalty" of people to the organization's Information Security policies and controls.

7. References

Adams, Anne and Sasse, Martina Angela (1999), Users are not the Enemy. Communications of the ACM, December, Vol. 42, No. 12.

Bansal, Harvir S., Irving, Gregory P. and Taylor, Shirley F. (2004), A Three-Component Model of Customer Commitment to Service Providers. Journal of the Academy of Marketing Science, Vol. 32, No. 3, pp. 234-250.

Baskerville, Richard (1993), Information Systems Security: Adapting to Survive. Information Systems Security, Vol. 2, No. 1, pp. 40-47.

Bowen, John T. and Shoemaker, Stowe (1998), Loyalty: A Strategic Commitment. The Cornell Hotel and Restaurant Administration Quarterly, February, pp. 12-25.

Brostoff, S. and Sasse, M. Angela. (2001), Safe and sound: a safety-critical approach to security. Proceedings of the 2001 Workshop on New Security Paradigms (Cloudcroft, New Mexico, September 10 - 13, 2001). New York: ACM, pp. 41-50. DOI= http://doi.acm.org/10.1145/508171.508178.

Desouza, Kevin C. and Vanapalli, Ganesh K. (2005), Securing Knowledge Assets and Processes: Lessons from the Defense and Intelligence Sectors. Proceedings of the 38th Hawaii Intrenational Conference on System Sciences.

Edvardsson, Bo (2005), Service quality: beyond cognitive assessment. Managing Service Quality, Vol. 15, No. 2, pp. 127-131.

Evanschitzky, Heiner, Iyer, Gopalkrishnan R., Plassmann, Hilke, Niessing, Joerg and Meffert, Heribert (2006), The relative strength of affective commitment in securing loyalty in service relationships. Journal of Business Research, Vol. 59, pp. 1207-1213.

Geyskens, I., Steenkamp J. B. E. M., Scheer L. K. and Kumar, N. (1996), The effects of trust and interdependence on relationship commitment: a trans-atlantic study. International Journal of Research in Marketing, October, Vol. 13, pp. 303–17.

Grönroos, Christian (1994), From Scientific Management to Service Management. International Journal of Service Industry Management, Vol. 5, No. 1, pp. 5-20.

Grönroos, Christian (1997), From Marketing Mix to Relationship Marketing – towards a Paradigm Shift in Marketing. Management Decision, Vol. 35, No. 4, pp. 322-339.

Grönroos, Christian (2007), *Service Management and Marketing - Customer Management in Service Competition.* (3rd ed.), New Delhi: John Wiley & Sons Ltd.

Gummesson, E. (1993), *Quality Management in Service Organizations.* New York: International Service Quality Association (ISQA).

Gummesson, E. (1994), Service Management: An Evaluation and the Future. International Journal of Service Industry Management, Vol. 5, No. 1, pp. 77-96.

Ha, Jae-Hyun (2005), A Conceptual Model of Psychological Commitment Based On The Concept of Attitude Strength. Doctoral Dissertation, Department of Sport Management, Recreation Management, and Physical Education, The Florida State University, College of Education, Retrieved October 5, 2008 from http://etd.lib.fsu.edu/theses/available/etd-11222005-002013/unrestricted/DissertationJaeHyunHa.pdf.

IIA (2000), *Information Security Management and Assurance - A Call to Action for Corporate Governance – Guidance for Boards of Directors*, The Institute of Internal Auditors. Retreived October 5, 2008 from http://www.theiia.org/download.cfm?file=22398.

Jacoby, J., & Chestnut, R. W. (1978). *Brand loyalty measurement and management.* New York: John Wiley & Sons, Inc.

Khatri, Naresh, Baveja, Alok, Boren, Suzanne A. and Mammo, Abate (2006), Medical Errors and Quality of Care: From Control to Commitment. University of California, Berkeley, vol. 48, No.3, Spring.

Kumar, N., Hibbard, J. D. and Stern, L. W. (1994), The Nature and Consequences of Marketing Channel Intermediary Commitment. MSI Working Paper, Report No. 94-115.

Lehtinen, Uolevi and Lehtinen, Jarmo R. (1991), Two Approaches to Service Quality Dimensions. The Service Industries Journal, Vol. 11, No. 3, July, pp. 287-303.

Lineberry, Stephen (2007), The Human Element: The Weakest Link in Information Security. Retrieved October 5, 2008 from http://www.aicpa.org/PUBS/jofa/nov2007/human_element.htm

Meyer, John P. and Allen, Natalie J. (1991), A Three-Component Conceptualization of Organizational Commitment. Human Resource Management Review, Vol. 1, No. 1, pp. 61-89.

Meyer, John P. and Herscovitch, Lynne (2001), Commitment in the workplace: Toward a General Model. Human Resource Management Review, Vol. 11, No. 3, pp. 299-326.

Morgan, Robert M. and Hunt, Shelby D. (1994), The Commitment-Trust Theory of Relationship Marketing. Journal of Marketing, Vol. 58, July, pp. 20-38.

Ravald, Annika and Grönroos, Christian (1996), The value concept and relationship marketing. European Journal of Marketing, Vol. 30, No. 2, pp. 19-30.

Rusbult, C. E. (1980), Commitment and satisfaction in romantic relationships. Journal of Experimental Social Psychology, Vol. 16, pp. 172-186.

Siponen, Mikko T. (2000), A conceptual foundation for organizational Information Security awareness. Information Management & Computer Security, Vol. 8, No. 1, pp. 31-41.

Siponen, Mikko T. (2001), Five Dimensions of Information Security Awareness. Computers & Society, June, Vol. 31, No. 2, pp. 24-29.

Sirota, David, Mischkind, Louis A. and Meltzer, Michael Irwin (2008), Stop Demotivating Your Employees! Harvard Management Update, July, Vol. 13, No. 7.

Spafford, E. H., The Mole in the Machine, The New York times, 25 July 1999.

Stanton, Jeffrey M., Stam, Kathryn R., Mastrangelo, Paul and Jolton, Jeffrey (2005), Analysis of end user security behaviours. Computers & Security, Vol. 24, No. 2, pp. 124-133.

Thomson, Kerry-Lynn and von Solms, Rossouw (2004), Information Security Obedience: a definition. Computers & Security, February, Volume 24, No. 1, pp. 69-75.

Thomson, Kerry-Lynn, von Solms, Rossouw and Louw, Lynette (2006), Cultivating an organizational Information Security culture. Computer Fraud & Security, October, Vol. 2006, No. 10, pp. 7-11.

Thomson, M. E. and von Solms, R. (1998), Information security awareness: educating your users effectively. Information Management & Computer Security, Vol. 6, No. 4, pp. 167-173.

Transactional Leadership, Retrieved October 5, 2008 from http://changingminds.org/disciplines/leadership/styles/transactional_leadership.htm.

Vandermerwe, Sandra and Gilbert, Douglas (1989), Making Internal Services Market Driven. Business Horizons, November-December, pp. 83-89.

Vargo, Stephen and Lusch, Robert F. (2008), Why “service”? Journal of the Academy of Marketing Science, Vol. 36, pp. 25-38.

von Solms, Basie (2006), Information Security – the Fourth Wave. Computers & Security, Vol. 25, pp. 165-168.

von Solms, Basie (2000), Information Security – the Third Wave? Computers & Security, Vol. 19, pp. 615-620.

Walton, Richard E. (1985), From control to commitment in the workplace. Harvard Business Review, March-April.

Wetzels, Martin, de Ruyter, Ko and von Birgelen, Marcel (1998), Marketing service relationships: the role of commitment. Journal of Business & Industrial Marketing, Vol. 13, No. 4/5, pp. 406-423.

Whitten, A. & Tygar, J. D. (1999), Why Johnny can't encrypt: A usability evaluation of PGP 5.0. Proceedings of the 8th USENIX Security Symposium, August 1999, Washington.

Wohnlich, Thierry (2006), Building a Human Firewall: Raising Awareness to Protect Against Social Engineering. Retrieved October 5, 2008 from http://www.ciscopress.com/articles/article.asp?p=663084.

Wollan, Robert (2008), The new rules for customer service: Findings from the Accenture Global Customer Satisfaction Survey. Outlook Point of View, No. 1, January.

Appendix C:

Information Security Service Branding – beyond information security awareness

Rahul Rastogi[a] **and Rossouw von Solms**[b]

Institute for ICT Advancement,

Nelson Mandela Metropolitan University, South Africa

[a]rahul.rastogi@eil.co.in

[b]rossouw.vonsolms@nmmu.ac.za

Abstract

End-users play a critical role in the effective implementation and running of an information security program in any organization. The success of such a program depends primarily on the effective implementation and execution of associated information security policies and controls and the resultant behaviour and actions of end-users. However, end-users often have negative perception of information security in the organization and exhibit non-compliance. In order to improve compliance levels, it is vital to improve the image of information security in the minds of end-users. This paper borrows the concepts of brands and branding from the domain of marketing to achieve this objective and applies these concepts to information security. The paper also describes a process for creating the information security service brand in the organization.

Keywords: Information Security Management, Information Security Service Management, ISSM, service management, Information Security Service Branding, ISSB, service branding.

1. Introduction

In any organization, information security management faces the daunting challenge of managing end-users to ensure their compliance to information security policies and controls. While organizations may deploy a wide variety of policies and controls for securing their information assets, the success of many of these measures hinges on the

actions of end-users. For example, having a policy of strong passwords is futile if end-users willingly share their passwords. End-users, thus, play a crucial role in the security of information assets of any organization.

End-users face a variety of obstacles in complying with the information security policies and controls. These obstacles are both behavioural as well as attitudinal. Often, end-users find it difficult to take actions as per security policies and controls – various cognitive and usability factors impinge on their capability to successfully navigate the security policies and controls. However, attitudinal issues lead to more serious problems. Inappropriate attitude towards information security prevents end-users from even intending or initiating behaviours to comply with the security policies and controls. Attitudinal issues manifest themselves as low levels of commitment of end-users which makes them prone to sacrificing security in the pursuit of their work (Desouza & Vanapalli, 2005). So, even though they do so for bonafide reasons, end-users put the organization and its information assets at increased risk (Stanton et al., 2005). Attitudinal issues related to information security pose a significant challenge to organizations. As Chipperfield and Furnell (2010) state, “one significant challenge is the image of security, in the sense that no one ever really encounters it for a good reason”.

This paper proposes the use of Information Security Service Branding (ISSB) for improving the attitudinal compliance of end-users to information security policies and controls in the organization. ISSB is positioned as a component of the overall ISSM approach of Rastogi and Von Solms (2009) and achieves its objective by gaining commitment of end-users to information security through successful branding of information security in the organization. Also, it is important to note here that information security awareness (ISA) is already an important communication tool used by information security management in organizations to influence end-users. However, as discussed later in section 3, ISA limits itself to a concentration on raising awareness, knowledge and skill levels of end-users; ISA does not focus on repairing the problems caused by the negative image of information security. In this sense, ISSB is complementary to ISA and can be said to exist in addition to, and as a complement of, ISA efforts in the organization.

This paper is organized as follows. The next section discusses the negative image of information security in the organization. This discussion is followed by an overview of the literature on traditional approaches to ISA. The subsequent section provides an overview of branding in the business domain. Finally, the paper describes ISSB as an application of the concepts of brand and branding to information security in the organization and provides a process for its implementation in the organization.

2. The negative image of information security in the organization

Information and information technology (IT) are believed to accord numerous advantages to organizations. The advantages relate to flexibility, collaboration, information sharing, just-in-time, sense-and-respond, etc. In this backdrop, information security, with its policies, controls and restrictions, comes as a poor second in the organization (Baskerville, 1993; Chipperfield and Furnell, 2010). In this context, end-users, more often than not, develop a negative image of information security (Chipperfield and Furnell, 2010). This leads to a resistance towards information security and an inclination to readily switch from compliance to non-compliance (Adams & Sasse, 1999; Whitten & Tygar, 1999; Dourish, Grinter et al., 2004; Albrechtsen, 2007; Chipperfield & Furnell, 2010).

Albrechtsen (2007) states that the negative image of information security in the perception of end-users is shaped by various organizational, technological and individual factors. These factors include the trade-offs made during day-to-day work; the existence of social norms and interactions between individuals; the quality of information security management; the technological solutions implemented; and individual factors such as knowledge, attitudes, values, risk perceptions, etc. (Albrechtsen, 2007). Under these influences, the negative image of information security in the organization develops along the axes of: security as an obstacle or hindrance to work; delegation of security responsibility or "security is not my responsibility"; and negative views on information security management (or managers) discussed below.

The first and foremost problem that information security creates for users is that it gets in their way towards completing their day-to-day activities. Post and Kagan (2007) state that restricting access to information and IT systems can lead to interference in the completion of end-user activities. These "security hindrances" (Post & Kagan, 2007) represent the problems faced by end-users as security procedures and controls interfere with their work. In such situations, security is often sacrificed in the pursuit of work (Desouza & Vanapalli, 2005).

According to Dourish and Grinter et al. (2004), end-users, in the course of their day-to-day activities, may abdicate their security responsibilities and delegate them to other entities such as technology or the organization. After the abdication and delegation of security responsibility, end-users continue with their day-to-day work without caring about information security and without making any additional effort required for information security.

The final aspect of the negative image of information security in the organization is the "digital divide" between end-users and information security managers in the organization. End-users perceive information security managers as invisible and unapproachable and this made it difficult to report problems or ask questions (Albrechtsen & Hovden, 2009). Albrechtsen and Hovden (2009) also state that the negative image of information security is further reinforced by the overly technical and admonitory nature of the information security communication such as documentation. Because of these difficulties, end-users often give up on reading the security documentation and continue with low levels of awareness.

This section discussed the negative image of information security in the minds of end-users in the organization. The image is shaped by how end-users experience information security and its management in the organization. End-users view information security as an obstacle, as a low priority activity, as unnecessary, as intrusive, as unapproachable, etc. Because of this, end-users continue to remain indifferent to information security in the organization. The focus of this paper is to use the concept of branding to counter this negativity. But before ISSB is discussed, the next section discusses the weakness of present-day ISA programs in tackling the question of image of information security. The subsequent sections then discuss branding and its application to information security as ISSB.

3. Information security awareness

Information security awareness (ISA) is a vital communication tool used by organizations to influence end-users towards compliance with information security policies and controls in the organization. ISA operates by improving the awareness of end-users about information security issues, giving them the requisite training and skills and by enhancing their overall understanding of the principles of information security. However, ISA has tended to ignore the question of image of information security in the minds of end-users in the organization. This section discusses ISA, its importance in the organization and its lack of attention to image correction for information security.

ISO/IEC 27001:2005 (ISO/IEC 27001, 2005) and ISO/IEC 27002:2005 (ISO/IEC 27002, 2005) emphasize the value of ISA to the effectiveness of information security policies and controls in the organization. According to ISO 27002:2005 (ISO 27002, 2005), if end-users are not made aware of their security responsibilities, they remain unmotivated and unreliable and can cause information security incidents leading to considerable damage to an organization. ISO/IEC 27001:2005 (ISO/IEC 27001, 2005) states that the ISA control consists of ensuring that all end-users, whether employees or contractors or

other third party end-users, receive “appropriate awareness training and regular updates in organizational policies and procedures, as relevant for their job function”. ISO/IEC 27002:2005 (ISO/IEC 27002, 2005) states that information security awareness, education and training is a common practice and that this control applies to most organizations and in most environments.

However, various authors have pointed out weaknesses in the present-day approach of ISA in the organization. These weaknesses stem mainly from the simplistic approach to the link between ISA and improved information security behaviour of end-users in the organization. According to Siponen (2000), most organizations treat ISA as consisting of “passing around security guidelines in a factual manner”. Albrechtsen (2007) terms this present-day ISA approach as “expert-based one-way communication directed towards many receivers”. Chipperfield and Furnell (2010) concur and state that the most common approach to ISA in the organization is to provide documented security policy to end-users.

This present-day approach to ISA in the organization is based on documentation and dissemination of information related to policies and controls. However, this approach fails to address the issue of image. In this approach, it is futile to believe that “after a security awareness lesson people will all follow the guidelines at once” (Siponen, 2000). Albrechtsen (2007) also states that this approach fails as most end-users remain unaffected. Siponen (2000) concludes that an ISA approach based on mere dissemination of information is bound to fail. According to Chipperfield and Furnell (2010), the simplistic approach of ISA has a negative impact on end-users. In this approach, it is believed that end-users simply need to be told and they will comply. This approach leads end-users to regard policies “as an overhead in terms of being just another thing to be read and remembered”.

The importance of ISA in the organization has been highlighted in this section. However, the present-day approach to ISA suffers from weaknesses. The main weakness is the assumption of a simplistic link between end-users being told and then complying. ISA tends to ignore the issue of image of information security in the organization. ISSB corrects this short-coming and focuses on the image aspect. The next section discusses the concept of branding. The final section then discusses ISSB.

4. Brands and Branding

The American Marketing Association (AMA, 2009) defines a brand as *“a name, term, design, symbol, or any other feature that identifies one seller's good or service as distinct*

from those of other sellers. The legal term for brand is trademark. A brand may identify one item, a family of items, or all items of that seller. If used for the firm as a whole, the preferred term is trade name". AMA (2009) also provides an associated definition of a brand as a *"customer experience represented by a collection of images and ideas; often, it refers to a symbol such as a name, logo, slogan, and design scheme"*. According to these definitions, the brand operates by identifying a seller's good or service, and by helping consumers discern between goods or services from different sellers. Hence the brand operates by identification and differentiation. However, these definitions emphasize brand attributes such as logos, color and design. But, a brand is much more than its representative logo or symbol and, according to De Chernatony (2009) such emphasis betrays a lack of branding sophistication.

Various authors have highlighted the image aspect of a brand through defining associated terms such as "brand image", "brand meaning" and "brand personality". Keller (1993) defines "brand image" as "perceptions about a brand as reflected by the brand associations held in consumer memory". The image is shaped by both product-related and non-product related attributes, where the non-product related attributes result from a consumer's own experience with the brand and contact with other brand users. Berry (2000) defines "brand meaning" as "what comes immediately to consumers' minds" when the brand is mentioned. Keller (1993) says that customer-based brand equity results when the customer holds favorable, unique and strong brand associations in memory. This brand equity may be positive or negative and reflects the marketing advantage the brand holds over an unnamed or fictitiously named competitor (Berry, 2000). Hence a brand is much more than the logo, color and design of the symbols that represent it. A brand is an image that comes to the mind of a customer when he/she sees or hears about a product or service. This image is built from the customer's own experiences and communications from the organization or other customers. The remainder of this section discusses how this image or brand can be created by an organization.

Berry (2000) presents a model for branding of services, as shown in Figure 1 (from Berry, 2000). In Berry's (2000) model, several components of a service brand are involved. The inputs to the branding process are: the presented brand, external brand communications and customer experiences with the service.

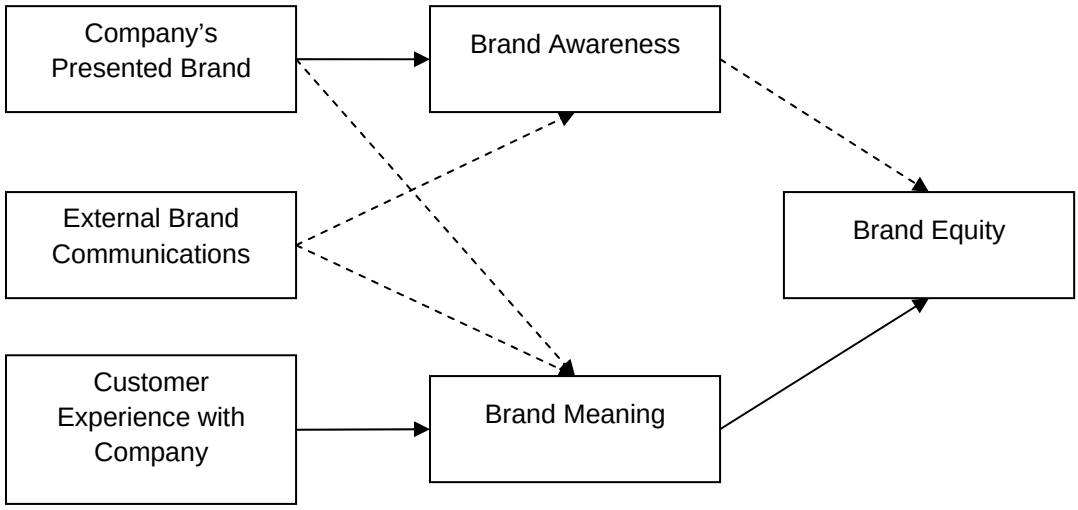


Figure 1: Service Branding Model (from Berry, 2000)

The first input to the branding process is the presented brand. This refers to the organization's purposeful communication of its identity through various means such as advertising, service facilities and the appearance of service providers. This input makes use of brand attributes such as color, logo, design etc. which establish the label attached to the brand. The next input is external brand communications that refers to the messages customers receive regarding the organization and its service. These messages are not controlled by the organization and originate from external sources such as word-of-mouth from other customers. The final input to the branding process is the direct experience that customers have with the organization and the service. This input too is not controlled by the organization.

The combined inputs lead to the creation of "brand awareness" and "brand meaning" in the minds of customers. Brand awareness refers to the customer's awareness of the brand and their ability to both recognize and recall the brand. Brand meaning refers to the image aspect of the brand and is the "snapshot impression" that comes to mind when the customers is reminded of the brand. Brand awareness and meaning combine to create brand equity. Brand equity is the advantage that an organization gains because of the brand. Brand equity can be positive or negative. Positive brand equity results in an advantage. Negative brand equity results in a disadvantage for the organization. Brand equity is more influenced by brand meaning than by brand awareness.

This section discussed the concept of branding from the domain of marketing. A brand refers not just to the logo, color and design of symbols representing it; the brand refers to the image that is formed in the minds of its customers regarding the products or services

represented by the brand. In view of the importance of the brand, organizations need to work consciously towards creating their brand. A model for branding was also discussed, namely, the service-branding model of Berry (2000). This model demonstrates that simple brand awareness is not sufficient to lead to customer loyalty. Brand image, brand meaning, customer feelings towards the brand etc. are important antecedents of customer loyalty – in the absence of these factors, awareness alone seldom works. This reinforces the discussion in the previous section wherein it was stated that the weaknesses of present ISA efforts in the organization emerge from their focus only on awareness of end-users. Present ISA efforts continue to ignore the image issues much to the detriment of information security in the organization. The next section discusses ISSB seeking to address this shortcoming and provides a framework for branding information security in the organization.

5. Information Security Service Branding (ISSB) in the Organization

In the previous section, it was mentioned that a brand always exists in the minds of customers, whether the organization does any branding or not. In a similar vein, in the context of information security in the organization, it can be said that end-users always carry an image of information security in their mind. This is the brand image or brand meaning of information security in the organization; this image exists irrespective of whether the organization attempts deliberate branding of information security or not.

Previous sections have already discussed the negative image of information security in the organization. Information security in an organization typically evokes contempt from end-users, particularly when it is juxtaposed with IT and information. Whereas end-users credit information and IT with providing them various benefits, they often see information security as a hindrance in their work and as not their responsibility. End-users further have a negative opinion about information security management. Thus, it would not be too wrong to say that information security has a negative brand image amongst the end-users in any organization. This negative image reduces the effectiveness of all communication and operational efforts of the organization to achieve information security. Information Security Service Branding (ISSB) represents a deliberate attempt to reverse these negative perceptions and create a positive brand image for information security. The remainder of this section describes the ISSB process.

In the service-branding model of Berry (2000), brand equity is built through company's communication of the presented brand, through publicity and word-of-mouth communication to customers, and through customer experiences of the service. ISSB applies this branding process to information security. Thus, the ISSB process proceeds as follows:

(1) Define the information security service brand.
(2) Communicate the brand to end-users, including using word-of-mouth communication to strengthen the information security service brand.
(3) Internalize the brand and organize to deliver security service consistent with the information security service brand.
(4) Monitor end-user characteristics and their perception of the information security service brand and use this information to modify the branding efforts.

The ISSB process is depicted in Figure 2. Each of the above steps is discussed in greater detail below. In the organization, Information Security Service Management executes the ISSB process. This process culminates in the creation of the Information Security Service Brand as an image in the minds of end-users. This image is influenced by the definition and communication of the brand as well as by the delivery of the service. The image that is created in the minds of end-users may not be the one promoted. Hence, it is necessary that the image of the Information Security Service Brand is regularly monitored to gauge the success of the ISSB process as well to serve as feedback for suitably modifying brand definition, communication and service delivery.

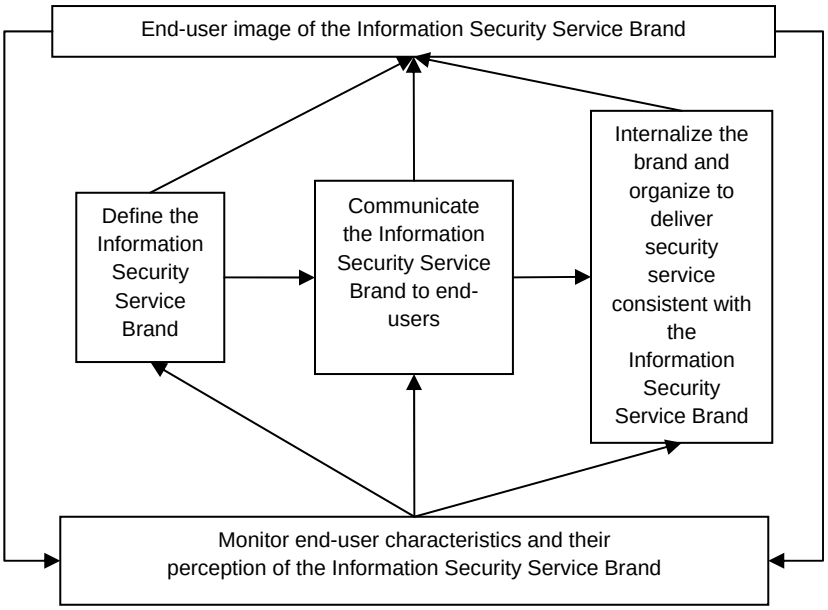


Figure 2: Information Security Service Branding process

5.1 Defining the Information Security Service Brand

Defining the brand is the first step in the ISSB process. It refers to identifying how the organization wishes information security to be perceived by end-users in the organization i.e. what snapshot impression, image, meaning or personality should come to the mind of end-users when they are reminded of information security. As discussed in section 2, end-users tend to have a negative image of information security in which they see information security as an obstacle or hindrance; as not their responsibility and in which they find information security management as invisible and coercive. To reverse this image, the information security brand should be defined so that it evokes a feeling of trust and confidence in information security management; so that end-users feel that security is in their interest and their responsibility.

Traditionally, information security has focused on the technical aspects of information security. In terms of branding it can be said, that the traditional focus has been on the functional characteristics or brand performance rather than on emotional characteristics or brand imagery. Since the very nature of information security is that it is neither permanent nor perfect, functional characteristics can only be emphasized to a limited extent. Focusing on the emotional characteristics or imagery of information security may be more worthwhile. In this context, the emphasis could be on the extent of top management commitment, investments and resource allocations towards information security in the organization. The information security service brand could also emphasize the caring and concern that the organization shows for the information security needs and issues of end-users. In conclusion, the end-users' snapshot impression of the information security service brand should be that of competence, sincerity and care.

5.2 Communicating the brand to end-users

Communicating the brand to end-users requires creation of deep and broad brand awareness. Keller (2001) calls this brand salience. Depth of brand awareness refers to how easily customers can recall or recognize the brand. Breadth refers to the variety of situations which the customers are able to relate to the brand. In the context of information security in the organization, it can be said that information security, must always to be at the top of the mind of end-users and they must be able to recall or recognize information security issues, policies and controls. In terms of depth, end-users should be able to relate to information security issues whenever they deal with information or information technology or other potentially risky situations, e.g. while handling finances in the organization.

Communicating the brand requires:

- Identifying labels to be attached to the brand i.e. populating the logo, color, design etc. attributes of the brand. This could also include using a slogan for the brand.
- Communicating the brand through a variety of channels and media to the target end-user audience.
- Communicating in a way so as to achieve both depth and breadth of awareness.

Keller (2001) mentions that the communications should include "sub-brands" or specific behaviours e.g. not sharing passwords, and linking them to the overall goals of information security in the organization. This way these specific behaviours gain salience and they may be readily adopted by end-users. Another aspect of this communication is to establish an emotional connection with end-users. This may be done by not just restricting the communication to organizational information security policies and controls, but by associating with other security concerns of end-users e.g. safe Internet use at home, safe credit-card usage or keeping children safe on the Internet. Word-of-mouth from other end-users may also be used to strengthen other end-users' beliefs in their own capabilities in dealing with information security policies and controls in the organization. Such communication will transmit the message that it is possible, and indeed popular to exercise good security practices. Communications may also be used to reward and honor good security behaviours while discrediting improper security practices. Posters, emails, slogans, videos, information security weeks, screen-savers, etc. could be used as the media for communication.

5.3 Internalizing the brand and organizing to deliver security service

The brand image in the minds of customers is created primarily by their experiences with the organization or service. The experiences of customers are largely dependent on the internal organization, culture and training of the service provider. In the context of information security in the organization, end-users' experiences with information security management employees and information security policies and controls have a large impact on the perceptions that end-users develop regarding the information security service brand. All the efforts at defining the brand and communicating it will come to naught if the actual service is not consistent with the messages. Internalization is related to the overall organization of information security in the organization and lies beyond the communicative aspect of branding. Further discussion of this aspect is beyond the scope of this paper.

5.4 Monitoring end-user characteristics and their perception of the information security service brand

In the ISSB process, it is vital to monitor the characteristics of end-users in the organization and their perception of the information security brand. This information is used in a twofold manner: to tune the brand definition and communication to the needs and characteristics of end-users and also to measure the success of the branding process.

Chipperfield and Furnell (2010) state that different people receive the same message differently depending upon their personality. This indicates that to be successful, any communication program must tailor itself to the characteristics of its audience otherwise it loses its effectiveness. Segmentation is the concept of dividing a heterogeneous group into smaller, homogeneous segments. These homogeneous segments have similar characteristics and needs. Consequently, a communication approach tailored to individual segments will likely be more effective than a blanket communication approach. According to Keller (2008), segmentation requires a trade-off between costs and effectiveness. A finely grained segmentation will lead to more effective communication but at increased cost. Keller (2008) has suggested the following segmentation bases: descriptive or customer-oriented (based on what kind of person the customer is) and behavioural or product-oriented (based on how the customer thinks or uses the product). Keller (2008) has also suggested other segmentation bases that build on brand loyalty. Other segmentation bases include demographic, psychographic and geographic attributes.

In the context of information security in the organization, end-users can be segmented in various ways. Segmentation of end-users will yield segments with different requirements and therefore requiring different treatment. Furnell and Thomson (2009) state that end-users in an organization can be differentiated on the basis of their level of commitment to information security. These levels range from “disobedience” at the most negative level to “culture” at the most positive or committed level. Between these two extremes lie the levels of “resistance”, “apathy” and “ignorance” on the non-compliance side; “commitment”, “obedience” and “awareness” lie on the compliance side. These levels indicate differing levels of intensity of communication required for branding and hence can be used for segmentation. These segments could then be used for tuning the branding process. Tsohou, Karyda & Kokolakis (2006) have indicated that different people have different cultural biases and this affects their risk perceptions and approaches to information system risk management. Segmentation can also be based upon psychographic factors (e.g. risk perceptions), based upon working groups in the organization, the nature of information use by end-users (e.g. mobile end-users versus non-mobile end-users), the level of skill of end-users (e.g. technically skilled end-users versus technically naïve or not-so-well-skilled end-users). Segmentation requires ongoing

analysis of the characteristics of end-users and their working practices. This cost will however lead to improved targeting and effectiveness of communication efforts.

Monitoring of the brand image in the minds of end-users is also important to the branding process. The information security service brand lives in the minds of end-users. This image or perception, however, may be different from what the organization tries to project through its communications and service delivery. This is most likely when the internalization and service delivery efforts are inconsistent with the information security service brand. Monitoring is also important to understand whether the brand is in sync with what end-users actually desire. End-users may be regularly surveyed to understand how they perceive the information security service brand as against the projected brand. This information may then be used to tailor the brand as well as the communication efforts in the branding process.

A process for developing the information security service brand in the organization has been discussed in this section. The primary objective of ISSB is to reverse the negative perceptions of information security in the organization and, instead, create a positive image in the minds of end-users.

6. Conclusion

This paper has discussed the negative image of information security in the perception of end-users in the organization. It is stated that this negative image is a major cause of non-compliance of end-users to information security policies and controls in the organization. The paper also highlighted the importance and weakness of information security awareness (ISA) programs in tackling this issue. Finally, Information Security Service Branding (ISSB) is proposed as a solution to this problem. ISSB utilizes the concepts of brands and branding and operates by attempting to create a positive image of information security in the minds of end-users. The paper also provided a process for developing the Information Security Service Brand in the organization.

References

Adams, A. & Sasse, M. A. (1999). Users are not the enemy. *Communications of the ACM*, Volume 42, No. 12, pp. 40-46.

Albrechtsen, E. (2007). A qualitative study of users' view on information security. *Computers & Security*, Volume 26, Issue 4, pp. 276-289.

Albrechtsen, E. & Hovden, J. (2009). The information security digital divide between information security managers and users. *Computers & Security*, Volume 28, Issue 6, pp. 476-490.

American Marketing Association (2009). Dictionary [online]. [cited 20 June 2010] Available from Internet:
URL http://www.marketingpower.com/_layouts/Dictionary.aspx?dLetter=B

Berry, L.L. (2000). Cultivating Service Brand Equity. *Journal of the Academy of Marketing Science*, Volume 28, No. 1, pp. 128-137.

Chipperfield, C. & Furnell, S. (2010). From security policy to practice: Sending the right messages. *Computer Fraud & Security*, Volume 2010, Issue 3, pp. 13-19.

De Chernatony, L. (2009). Towards the holy grail of defining 'brand'. *Marketing Theory*, Volume 9, Issue 1, pp. 101-105.

Desouza, K.C. & Vanapalli, G.K. (2005). Securing Knowledge Assets and Processes: Lessons from the Defense and Intelligence Sectors. *Proceedings of the 38th Hawaii Intrenational Conference on System Sciences*.

Dourish, P., Grinter, R., Delgado de la Flor, J., & Joseph, M. (2004). Security in the Wild: User Strategies for Managing Security as an Everyday, Practical Problem. *Personal and Ubiquitous Computing*, Volume 8, No. 6, pp. 391-401.

Furnell, S. & Thomson, K.L. (2009). From culture to disobedience: Recognising the varying user acceptance of IT security. *Computer Fraud & Security*, Volume 2009, Issue 2, pp. 5-10.

ISO/IEC 27001 (2005). Information technology -- Security techniques -- Information security management systems – Requirements. *ISO/IEC 27001:2005*, International Organization for Standardization and International Electrotechnical Commission.

ISO/IEC 27002 (2005). Information technology -- Security techniques -- Code of practice for information security management. *ISO/IEC 27002:2005*, International Organization for Standardization and International Electrotechnical Commission.

Keller, K.L. (1993). Conceptualizing, Measuring, and Managing Customer-Based Brand Equity. *Journal of Marketing*, Volume 57, January, pp. 1-22.

Keller, K.L. (2001). Building Customer-Based Brand Equity. *Marketing Management*, July/August, pp. 14-19.

Keller, K.L. (2008). Strategic brand management, 3/e. Prentice Hall of India, ISBN:9788131719770.

Post, G.V. & Kagan, A. (2007). Evaluating information security tradeoffs: Restricting access can interfere with user tasks. *Computers & Security*, Volume 26, Issue 3, pp. 229-237.

Rastogi, R. & von Solms, R. (2009). A Service-oriented Approach to Information Security Management. *Proceedings of the 7th Annual Conference on Information Science, Technology & Management (CISTM).*

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

Stanton, J.M., Stam, K.R., Mastrangelo, P. & Jolton, J. (2005). Analysis of end user security behaviours. *Computers & Security*, Volume 24, No. 2, pp. 124-133.

Whitten, A. & Tygar, J.D. (1999). Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0. *Proceedings of the 8th USENIX Security Symposium*.

Appendix D:

Information Security Service Support - helping end-users cope with security

Rahul Rastogi[a] and Rossouw von Solms[b]

Institute for ICT Advancement, Nelson Mandela Metropolitan University, South Africa.
[a]rahul.rastogi@eil.co.in
[b]rossouw.vonsolms@nmmu.ac.za

Abstract: Organizations implement an information security program for the protection of their information assets. The success of such a program depends primarily on the effective implementation and execution of associated information security policies and controls. These policies and controls depend directly upon the resultant behaviour and actions of end-users. Hence, end-users play a critical role in the effective implementation and running of an information security program in any organization. However, end-users are often unable to navigate and comprehend the various policies, controls and associated issues. Support to end-users is therefore a vital element, but is often neglected by present information security management systems. In the service industry, support to customers is established as an important determinant of customer perceived service quality. This paper applies the same philosophy to provide support to end-users, who are the customers of the Information Security Service.

Keywords: Information Security Management, Information Security Service Management, ISSM, service management, Information Security Service Support, ISSS, service encounter.

1. Introduction

In any organization, end-users are crucial to maintaining information security in the organization. While organizations may establish an elaborate infrastructure of information security policies and controls, if end-users fail to comply with these policies and controls, the effectiveness of these measures is diminished. Thus, the success of end-users, in complying with information security policies and controls in the organization, is vital for obtaining an effective state of information security in the organization.

End-users face numerous difficulties in dealing and complying with the information security policies and controls. Firstly, end-users may not be aware or knowledgeable of the organizational information security policies and controls, and security principles in general, and consequently do not know right and wrong [1, 2]. Even if end-users are aware, the daily work pressures and surrounding culture in the organization may dissuade end-users from exercising the correct behaviour [3]. Finally, a lack of skill and the complexity of security policies and controls may often prevent end-users from following on their intentions to undertake the correct action in a given situation [4, 5]. Combined together, the importance of end-users and the difficulties they encounter in complying with information security policies and controls, signify the 'end-user crisis' in information security.

In response, the information security community has focused on a variety of measures to resolve this 'end-user crisis'. These measures include running training and awareness programs for end-users [1], addressing the socio-cultural influences on information security behaviour of end-users in organizations [6], and improving the usability of security controls [5, 7].

Amongst all these varied efforts, the information security community has tended to neglect the area of providing support to end-users in their day-to-day interactions with information security policies and controls. This support can play an important role in helping end-users cope with the complexity of information security policies and controls in the organization. The present paper, thus, proposes that organizations provide a support system, namely, Information Security Service Support (or ISSS), to end-users thereby improving their security-related behaviours to the benefit of the organization. It must be noted that ISSS is proposed in addition to, and not in place of, usual information security practices.

The remainder of this paper is structured as follows. The next section explores the need of end-users for support in coping with information security. The subsequent section provides some contextual information related to ISSS and its position in the service management approach to information security management. Having thus set the scene, the paper proceeds to discuss the concept of service encounter between customers and service providers. The next two sections then proceed to lay out the guidelines for ISSS and the management of support employees.

2. The need of end-users for support

In the context of information security policies and controls in the organization, the information security behaviours of end-users are afflicted by two problems. The first problem to plague end-users is a lack of awareness and skills about information security. The second problem is the apparent lack of interaction between end-users and information security support services; so, end-users do not know where to go to for help and assistance. This section discusses these problems and posits that the solution lies in establishing an information security support function in the organization.

Behaviour may be defined as the "observed overt acts" undertaken by individual end-users [8]. The Theory of Planned Behaviour of Ajzen [9, 10] provides an explanation of the underlying causes of human behaviour. In the context of information security, this theory can be used to understand the behaviour of end-users related to information security policies and controls in the organization. In the Theory of Planned Behaviour (TPB), one of the important determinants of people's behaviour is perceived behavioural control (or PBC). PBC refers to "people's perception of the ease or difficulty of performing the behaviour of interest" [9]. Thus, it is an individual's perception of his or her ability to successfully undertake the behaviour, given the availability of opportunity, skills and resources. These control beliefs are based upon the individual's past experience as well as the second-hand information obtained from sources such as acquaintances and friends. In the context of information security in an organization, perceived behavioural control refers to an end-user's beliefs about his or her ability to undertake a security behaviour as mandated by the organization's information security policies and controls. These beliefs are shaped, in part, by the end-user's past success or failure with respect to information security policies and controls. If an end-user has a past of successfully undertaking information security behaviours, then this end-user will have a positive intention to undertake such behaviours in the future. If, however, the past is one of unsuccessful or dissatisfying experiences, then the end-user will have negative intention to undertake information security behaviour in the future.

Typically, end-users face significant difficulties when undertaking information security behaviours in the organization. These difficulties arise from various factors including lack of awareness [3, 11, 12, 13], lack of intention [7, 14, 15, 16] and lack of skill [7, 12, 17, 18]. In this situation, end-users usually have a history of unsuccessful attempts at undertaking information security behaviours. In the absence of any support or assistance, end-users will feel diffident and will attempt to avoid or bypass information security behaviours, as predicted by the TPB.

The problem discussed above is compounded by the reported lack of interaction between end-users and information security managers. Albrechtsen and Hovden [11] report that while end-users actually desire contact with the information security managers, there is actually very little contact. The end-users find the information security managers "invisible" and do not know who to turn to for reporting problems and seeking guidance. The end-users also reported that greater involvement with the information security managers would lead to greater interest amongst the end-users with regard to information security. Further, end-users believe that greater interaction with information security managers would lead to improved behaviour and knowledge. In summary, the findings of Albrechtsen and Hovden [11] are that there is a definite digital divide between information security managers and end-users; that both groups underlined the need and importance of greater interaction amongst them for improving end-user awareness and behaviour; and that unfortunately there is a near complete absence of this interaction in the organization.

As discussed above, there is both theoretical and empirical evidence pointing towards the need for enhanced support for end-users. However, paradoxically, present-day approaches to information security management have largely neglected this aspect of information security. Information Security Service Support (ISSS), the objective of this paper, aims at bridging this divide by providing a framework for possible day-to-day interactions between ISSS support-employees and end-users. The purpose of ISSS is to help end-users cope with the demands of information security policies and controls, thereby improving their level of compliance. ISSS operates by creating a chain of successful and satisfying past experiences which, in turn, lead to a successful present and future.

Before this paper proceeds to describe ISSS, it is important to understand the concept of service encounters. Service encounters refer to the interaction between customers and service providers. In the context of ISSS, encounters will occur between end-users and support employees. The next section discusses the concept of service encounters and prepares the ground for the subsequent discussion of ISSS.

3. Information Security Service Support and end-users as customers

In their paper, 'A service-oriented approach to information security management', Rastogi and Von Solms [19] proposed Information Security Service Management (ISSM) as a service-oriented approach to information security management. Through this approach, information security becomes an internal service, the end-users become its customers and information security management becomes the service provider. To offer

information security as a service, it is important to implement the following three components that are integral to the service-oriented approach; i.e. the *design* of the service, the *marketing* of the service and the *support* of the service. Thus, the support system, i.e. Information Security Service Support (ISSS), as proposed in this paper, is a component of the overall information security service. The other components, the design and the marketing, will not be addressed in this paper.

ISSS consists of support employees that provide information security support to end-users, who are the customers of ISSS. The delivery of support normally happens during interpersonal, or one-to-one, interactions between customers and support employees. Since these interactions are crucial for providing support, as well as creating a good working relationship between the customer and the support employee, the concept of interactions needs to be discussed in more detail. This is done in the next two sections. The next section explores the critical nature of these interactions in the context of information security managers and end-users in an organization. The subsequent section explores interactions in the context of general service management.

A word of caution is provided here. It is to be noted that there is some diversity in the use of terms in this paper. The service management literature uses terms like customer / client / consumer. In the context of this paper, the end-user is the customer of the service. Again, service management literature uses the term “customer contact employee” – in the context of ISSS, this paper uses the term “support employee”. The term “support employee” seems more appropriate as it refers to the specific “support” function of the employee rather than to the generic “customer contact” function. Further, these support employees are most likely not directly involved with the framing of information security policies and controls in the organization; they may provide feedback about the experiences of end-users and this feedback may be used to tailor the information security policies and controls. Another clarification is with regard to the term “information security manager”. In the context of service-oriented approach to information security management, it can be said that “information security managers” are the “information security service providers” or “information security service managers” (or ISS managers).

4. Service encounter – the interaction between customers and service provider

Various authors have provided definitions for the term “service encounter”. Shostack [20] defines the service encounter as “a period of time during which a consumer directly interacts with a service” [21]. As per this definition, the encounter encompasses not just the interpersonal interactions between the consumer and the service provider, but also the

various other components like physical facilities, technological tools, etc. [21]. Surprenant and Solomon [22] define the service encounter as “the dyadic interaction between a customer and a service provider”. This definition focuses on the interpersonal element of service firm performance [21]. Grönroos [23] and Zeithaml, Bitner, Gremler and Pandit [24] call these interactions as “moments of truth” where “promises are kept or broken”. Service encounters or interactions occur in the visible or interactive part of the organization where the customer meets the service provider [23].

The service encounters or interactions or “moments of truth” are of critical importance as they form the basis for the customer’s perception of service quality [24]. Customers perceive the quality of service in terms of the technical or outcome dimension and the functional or process-related dimension [23]. The technical dimension relates to the “what” whereas the functional dimension relates to the “how” of the service. The importance of the “how”, and thus the service encounter, is underlined by customers’ preference for satisfying customer expectations during service encounters [25]. Berry, Wall and Carbone [26] exhort the managers in organizations to pay attention to not just the technical part of providing service but also to the interaction part. According to them, “humanic clues” are embedded in the behaviour and appearance of service providers and exhibit the organization’s commitment towards customers.

As stated above, an important determinant of customer perception of service quality is the behaviour of the employees of the organization directly interacting with the customers namely, customer contact employees. Bitner, Booms and Tetrault [21] identified three major groups of behaviours of these customer contact employees that have significant impact on the customer’s perception of service quality. These groups of behaviours are:

- Employee response to service delivery system failures – Recovery
- Employee response to customer needs and requests – Adaptability
- Unprompted and unsolicited employee actions – Spontaneity

In the case of service failures, customers perceive the service quality favorably if the customer contact employees acknowledge the problem and accept it as their problem. Customers perceive the quality to be low if the failure remains unaddressed and unexplained. Many times, customers have special needs or preferences. Customers feel satisfied if their needs or preferences are accommodated. Customers feel dissatisfied if the seriousness of their needs is not understood or no sincere effort is made to accommodate their preferences. A particular situation is when a customer has made an error. At such times, the customer contact employee needs to adapt to the new situation. Such situations become highly satisfactory if the employee takes ownership of the problem and assists the customer. On the other hand, if the employee avoids responsibility for resolving the problem or embarrasses the customer, the situation

becomes highly dissatisfactory for customer. Often, a satisfactory encounter for customers is when they are treated with care and concern and they are paid attention to. Customers feel dissatisfied if they are ignored or treated impersonally.

Since customer contact employees are the fulcrum of the service encounter, they need special attention to ensure that they can provide satisfactory service encounters to customers. Knowledge and empowerment of customer contact employees are critical elements [21]. Customer contact employees need to have knowledge about all aspects of the service and its delivery. This knowledge enables them to satisfy the information needs of the customers and provide appropriate responses or assistance. Customer contact employees also need to be empowered through delegation of control. Empowerment enables these employees to resolve customer issues effectively and efficiently. Customers detest having to talk to multiple employees to resolve an issue [25].

This section highlighted the role of the service encounter and the customer contact employees in customer perceptions of service quality. Thus, in this section some criteria were addressed to ensure that a service encounter between the customer contact employee and the customer can result in a very positive encounter for both parties. On the contrary, section 3 highlighted that the contact between information security managers and end-users are firstly, minimal and secondly, that the interaction that do take place between the two parties are not necessarily experienced as positive. In the next section, the principles of service encounters, as explained in this section, are extrapolated onto the scenario described in section 3 between information security managers and end-users. As customers in a service setting value interpersonal interaction, end-users in the context of information security too might be positively influenced by their interactions with Information Security Service support employees.

5. Information Security Service Support

The previous two sections highlighted some important aspects related to information security in organizations as well as general service management. These aspects are; firstly, that there is very little interaction between end-users and information security service providers; secondly, that this interaction can lead to better end-user awareness and behaviour; and thirdly, that this interaction, also called “service encounter” in the service literature, is an important determinant of customer perceptions of service quality. Combining these aspects, it can be concluded that there is a definite need for ‘bridging the gap’ between end-users and information security service providers in an organization and further, that this bridging function can be provided by Information Security Service

Support (ISSS), based on the principles of general service management. The rest of this section will provide a typical framework that can be used to successfully introduce ISSS.

The previous two sections highlighted some important aspects related to information security in organizations as well as general service management. In the domain of information security, it is noted firstly, that there is a poverty of interactions between end-users and information security service providers; and secondly, that improved interaction is expected to lead to better end-user awareness and behaviour. In the domain of service management, the interaction between customers and service providers, also called "service encounter", is an important determinant of customer perceptions of service quality. Combining these aspects, it can be concluded that end-users in an organization, as customers of the information security service, have dissatisfying service experiences and that these poor experiences lead them to have negative perceptions of the quality of the information security service. Hence there is a definite need for 'bridging the gap' between end-users and information security service providers in an organization. This gap can be bridged by Information Security Service Support (ISSS), based on the principles of general service management. ISSS fills another gap too – by providing timely support to end-users it allows end-users to successfully undertake information security behaviours; further, it enhances their perceptions of behavioural control over information security behaviours, thus, improving their motivation towards undertaking such behaviours. This paper focuses on the "service encounter" aspect of ISSS and provides guidelines that can be used to successfully introduce ISSS in the organization. Figure 1 shows the ISSS framework wherein service encounters link ISSS support employees with end-users. During these encounters, the need of end-users for help, support and guidance with policies and controls is satisfied by the support employees.

According to Bitner et al. [21], Shostack [20] provided an early definition of exactly what a service encounter entails. This definition, discussed in the previous section, is quite broad and does not limit itself to the interpersonal interactions between customers and customer contact employees. Applying this definition to ISSS, it can be said that a service encounter in the context of ISSS, consists of interactions of end-users with information security related policies, controls, tools and technologies on one hand and interpersonal interactions with support employees on the other. Another definition of service encounter focused on the interpersonal element only [22]. Following Bitner et al. [21] and the literature on "moments of truth" [23-24], this paper too focuses on the interpersonal element of service encounters. Thus, for the purpose of this paper, a service encounter, or moment of truth, in the context of ISSS, refers to the interpersonal interactions between end-users (customer) and support employees (customer contact employees).

Grönroos [23] states that managing a service offering requires the careful development of the service concept by; firstly, the development of a basic service package; secondly, the development of an augmented service offering and finally, the management of image and communication. This service concept eventually determines the intentions of the organization. The basic service package focuses on the technical outcomes. However, as noted earlier, customers base their perceptions of service quality on the functional aspects of the service. Hence, the basic service package needs to be complemented by an augmented service offering. This augmented service offering focuses on the functional aspects of the service provided. Finally, the management of image and communication enhance the customer perception of the service offering.

Similarly, the Information Security Service to be provided can be equated to the basic service package offered by the organization to the end-users. This basic service package is complemented by the support provided, i.e. Information Security Service Support (ISSS), which functions as the augmented service offering. An important aspect of the augmented service offering is the accessibility of the service [23] i.e. how easy is it for customers to search, locate and interact with the service. In the context of ISSS, accessibility means how easy it is for end-users to seek help, support and guidance from the support employees. Accessibility of the support employees consists of the following (based on [23]):

- "Location": Support employees should be available at a known "location" and that information of this location is readily available to end-users. The "location" could consist of a physical location or even a telephone number or a software helpdesk, etc. The support must also be available at times that match the working hours of the end-users. Further, the various tools, technologies and procedures for seeking support must be user-friendly and not overly complicated.
- "Accessibility": When end-users seek to get hold of support employees, the support employees should create an impression of being readily accessible. Small things such as the response time to answer a telephone call have an important bearing on the end-user's perception of accessibility. Further, a negative attitude or unfriendly tone on answering a call can have negative repercussions on the end-user's perception of accessibility.

Apart from accessibility, the general behaviour of support employees is critical in all situations involving end-users with problems or queries related to information security policies and controls. Following Bitner et al. [21], these behaviours can be classified into the following groups:

- Recovery - support employee response to security breaches or failures and difficulty experienced by end-users in working with security policies and controls
- Adaptability - support employee response to end-user needs and requests

- Spontaneity - unprompted and unsolicited support employee actions towards end-users

Security can never be perfect and incidents or breaches are a regular part of information security. Such situations, such as virus outbreaks, can be treated as service failures. In addition, an end-user may find it difficult to work with certain controls e.g. choosing a strong password. Such situations call for the "recovery" capabilities of the support employees. Often, it may not be possible to make it easier for the end-user, e.g. by diluting the password strength. Thus, there is a need for the support employees to engage the end-user and initiate service recovery. Components of the recovery strategy could include acknowledging the problem, explaining the nature of the problem and its cause, explaining the rationale for the control and its importance for effective information security and apologizing for the failure or inconvenience.

In an organization, end-users may sometimes need some flexibility regarding the enforcement of information security policies and controls. As an example, in an organization where Internet browsing is not freely available to end-users, a particular end-user may need access, perhaps for personal reasons. In this situation, a strict enforcement of the security control will result in denying the access to the end-user, resulting in a dissatisfactory encounter for the end-user. Alternatively, the "adaptability" of the support employee to the situation, by appreciating the innocuous and temporary nature of the request and arranging the required access for the end-user, will result in a satisfactory encounter for the end-user.

Another frequent situation the takes place in an in organization is when an end-user makes a mistake and calls the support employee for help. For example, the end-user has forgotten a password. In this situation, the support employee may criticize the end-user and even deplore end-users in general as a source of regular problems. This will lead to a highly dissatisfactory encounter for the end-user. Alternatively, the support employee may take ownership of the resolution of the problem by getting a new password reissued to the end-user and also guiding the end-user in resetting the password as per organizational policy. This will result in a satisfactory encounter for the user. Personalization and "spontaneity" towards end-users result in satisfactory encounters. End-users will feel dignified if the support employee refers to them by name and exhibits familiarity. Support employees may even adopt a relational approach towards end-users wherein they establish personal rapport or friendships with end-users. This relational approach results in benefits for end-users and also gains end-user loyalty and positive word-of-mouth for information security in the organization [27]. Support employees should actively solicit feedback, suggestions and complaints from end-users and feed

these information to information security service managers. This escalates concerns of end-users to the managers and allows for end-user concerns to be addressed.

The eventual objective of the ISSS, and therefore the support employees, is to make it easier for the end-users in the organization to navigate through the information security policies and controls and behave in a compliant manner. Support employees are crucial to the success of ISSS as their interaction with end-users determines the overall quality of the security service. This section highlighted the importance of service encounters and support employee behaviours that lead to satisfactory encounters. The next section looks at how information security managers need to manage and empower the support employees.

6. Management of ISSS support employees

The previous section has highlighted the role of service encounters, or interpersonal interactions, between end-users and ISSS support employees. These encounters act as "moments-of-truth" and have a definite influence on the end-user perception of quality of the information security service. In service encounters, the service employees play a crucial role as the satisfaction of end-users depends to a large extent on the behaviour of the service employees. Consequently, the management of the support employees gains prominence in a service setting. This section provides some guidelines towards the management of ISSS support employees so they can interact effectively with end-users.

In a typical service setting, customer contact employees are the first, and, often, the only representation of the organization that customers are dealing with [28, 29]. Zeithaml et al. [24] emphasize the importance of these employees: they are the service; they are the organization in the customer's eyes; they are the brand and they are the marketers. Likewise, in the context of ISSS, the support employees are the "visible" face of information security management with whom end-users associate any problem or query related to information security policies and controls in the organization.

Due to the nature of service encounters and the varied demands that are placed on ISSS support employees, effective management of support employees is crucial to ensure that they are able to exhibit appropriate attitudes and behaviours. The key enablers of attitudes and behaviours of support employees are: knowledge, empowerment and behaviour-based evaluation [23, 28]. Zeithaml et al. [24] mention a four-step strategy in this regard: hire the right people; develop the people to deliver service quality; provide them with needed support systems and retain the best people (see Figure 2).

Hiring the right people for ISSS is the necessary first step. Service inclination is an important attribute of support employees [24]. This attribute reflects the employee's orientation towards helping, guiding and supporting the end-users. Personality characteristics associated with this attribute are helpfulness, thoughtfulness and sociability [24].

Information security managers need to provide training and empowerment to support employees. ISSS support employees need both technical and interaction skills to perform their job effectively. The technical skills include knowledge about the security policies and controls in the organization and the rationale behind these policies and controls. Support employees must also be aware of the various procedures or processes enforced in the organization. This knowledge-base of the support employees needs to be regularly updated to match the actual situation in the organization. Thus, appropriate training must be regularly imparted to support employees.

Social, or interactive, skills training is also required by support employees. Since, interaction with end-users is their main task, social skills acquire great importance in the repertoire of support employees. According to Mead [30], social, or interactive skills, refer to the ability of the support employee in understanding the end-user's perspective during interactions [31]. These social, or interactive skills, also include showing care, concern and empathy towards end-users [24].

Empowerment of support employees is another important aspect of enabling them [21, 24]. Empowerment refers to giving the support employees the authority to respond and adapt to the needs of the end-users. In an example in the previous section, when an end-user needed temporary Internet access, the support employee could help the end-user only because he/she was empowered to take the decision on his/her own. Empowerment is particularly important as end-users desire single-window resolution of issues [25]. However, for empowerment to not become a security risk in itself, managers must set and inform support employees of the boundaries of their authority. Empowerment needs to be supported by appropriate training and knowledge.

Measurement and evaluation of the support employees is an important tool to motivate them towards a service mindset. As stated in Rastogi and Von Solms [19], supervisory focus, reward systems and measurement focus in ISSM must be tuned towards ensuring that support employees are supported, measured and rewarded for their interactions with end-users. Behaviour-based support employee evaluation involves measuring the performance of service employees in satisfying end-user needs rather than work related outputs [29].

Retaining the best people involves several HR-related strategies. However, the problem and its solution are not unique to the context of ISSS and hence are not discussed further. Rather, this paper takes an alternate approach – that of identifying the problems faced by support employees and the managerial solutions to those problems. Managerial actions to solve the problems of support employees should support retention of good employees at all cost.

ISSS support employees face many problems while performing their job. Some end-users may be non-cooperative or even unreasonable and their service encounter will be dissatisfactory in spite of the best efforts of the support employee. It is important that support employees are provided appropriate training to deal with such "problem" end-users [32]. It is also important that support employees are provided management support in dealing sternly with such "problem" end-users.

Another problem that afflicts support employees is role conflict. According to Weatherly and Tansik [33], role conflict represents the "incompatibility between one or more roles within an employee's role set, such that fulfilling one role makes fulfilling the others more difficult" [28]. In the context of ISSS, such role conflicts might arise when the support employee's responsibility of satisfactory encounters is pitted against an end-user who is making a demand which is clearly in violation of organizational security policies and controls. In such situations, support employees need to know their boundaries. Support employees should also possess the knowledge to understand the negative impact of meeting end-user's demands.

Support employees are a key resource and they need to be provided managerial support so as to be able to deliver satisfactory encounters with end-users. This section has provided some of the issues related to the management of support employees. A strong service attitude, appropriate knowledge, training and empowerment coupled with organizational support for service are the pre-requisites for support employees to function. Thus, the success of information security in the organization is hugely dependent on the quality of the support employees as well as the manner in which they are managed.

ISSS, if introduced and managed in a proper manner, can contribute positively towards end-users complying with organizational information security policies and controls to the eventual benefit of the organization.

7. Conclusion

The information security community has explored various approaches for improving end-user information security behaviours in an organization. Various approaches to end-user education and awareness have been tried and tested, but end-users are still dubbed as the weakest link in information security. This paper has proposed another approach in the same direction, that of Information Security Service Support (ISSS). This approach should not be seen as a total alternative to previous approaches, but rather as an important supplement to any information security program. ISSS consists of providing support to end-users in their day-to-day interactions to effectively comply with information security policies and controls through interactions with the support employees. The paper has provided a framework for understanding the interactions between end-users and support employees. Further, the paper also provided some guidelines for the effective management of support employees so as to enable them to deliver quality support to end-users, their customers.

8. References

[1] Thomson, M. E. and von Solms, R. (1998), Information security awareness: educating your users effectively. Information Management & Computer Security, Vol. 6, No. 4, pp. 167–173.

[2] von Solms, B., & von Solms, R. (2004). The 10 deadly sins of information security management. *Computers & Security*, 23(5), 371-376.

[3] Albrechtsen, E. (2007). A qualitative study of users' view on information security. *Computers & Security*, 26(4), 276-289.

[4] Furnell, S. (2005). Why users cannot use security. *Computers & Security*, 24(4), 274-279.

[5] Whitten, A., & Tygar, J. D. (1999). Why Johnny can't encrypt: A usability evaluation of PGP 5.0. Proceedings of the 8th conference on USENIX Security Symposium. Berkeley, CA, USA: USENIX Association.

[6] Thomson, K. L., von Solms, R., & Louw, L. (2006). Cultivating an organizational information security culture. *Computer Fraud & Security*, 2006(10), 7-11.

[7] Adams, A., & Sasse, M. A. (1999). Users are not the enemy. *Communications of the ACM*, 42(12), 40-46.

[8] Fishbein, M., & Ajzen, I. (1975). *Belief, attitude, intention, and behavior: An introduction to theory and research*. Reading, MA: Addison-Wesley.

[9] Ajzen, I. (1991). The theory of planned behavior. *Organizational Behavior and Human Decision Processes*, 50(2), 179-211.

[10] Ajzen, I. (2005). *Attitudes, personality, and behavior* (2nd Ed.). Milton-Keynes, England: Open University Press / McGraw- Hill.

[11] Albrechtsen, E., & Hovden, J. (2009). The information security digital divide between information security managers and users. *Computers & Security*, 28(6), 476-490.

[12] Furnell, S., Jusoh, A., & Katsabas, D. (2006). The challenges of understanding and using security: A survey of end-users. *Computers & Security*, 25(1), 27-35.

[13] Sasse, M. A., Brostoff, S., & Weirich, D. (2001). Transforming the 'weakest lnk' — a Human/Computer interaction approach to usable and effective security. *BT Technology Journal*, 19(3), 122-131.

[14] Beautement, A., Sasse, M. A., & Wonham, M. (2008). The compliance budget: Managing security behaviour in organisations. New Security Paradigms Workshop 2008 22-25 September, 2008, Lake Tahoe, California, USA.

[15] Dhillon, G. (2001). Violation of safeguards by trusted personnel and understanding related information security concerns. *Computers & Security*, 20(2), 165-172.

[16] Dourish, P., Grinter, R., Delgado de la Flor, J., & Joseph, M. (2004). Security in the wild: User strategies for managing security as an everyday, practical problem. *Personal and Ubiquitous Computing*, 8(6), 391-401.

[17] Furnell, S. (2010). Jumping security hurdles. *Computer Fraud & Security*, 2010(6), 10-14.

[18] Schultz, E. E., Proctor, R. W., Lien, M., & Salvendy, G. (2001). Usability and security: An appraisal of usability issues in information security methods. *Computers & Security*, 20(7), 620-634.

[19] Rastogi, R., & von Solms, R. (2009). A service-oriented approach to information security management. In G. Dhillon (Ed.), Proceedings of the 7th Annual Conference on Information Science, Technology & Management (CISTM) “Sustaining a

Knowledge Economy". July 13-15. DC: Information Institute Publishing. ISBN: 978-1-935160-06-9.

[20] Shostack, G. L. (1985). Planning the service encounter. In Czepiel, J. A., Solomon, M. R., & Surprenant, C. F. (Eds.). *The Service Encounter*. Lexington Books.

[21] Bitner, M. J., Booms, B. H., & Tetrault, M. S. (1990). The service encounter: Diagnosing favorable and unfavorable incidents. Journal of Marketing, 54(January), 71-84.

[22] Surprenant, C. F., & Solomon, M. R. (1987). Predictability and personalization in the service encounter. *Journal of Marketing*, 51(2), 86-96.

[23] Grönroos, C. (2007). Service management and Marketing: Customer management in service competition (3rd ed.). Delhi, India: John Wiley & Sons Ltd.

[24] Zeithaml, V. A., Bitner, M. J., Gremler, D. D., & Pandit, A. (2008). Service marketing – integrating customer focus across the firm (4th ed.). Delhi, India: Tata McGraw-Hill Publishing Company Ltd.

[25] Wollan, R. (2008, January). The new rules for customer service: Findings from the Accenture Global Customer Satisfaction Survey. *Outlook Point of View*. Retrieved October 22, 2010, from http://www.accenture.com/Global/Research_and_Insights/Outlook/By_Subject/Customer_Relationship_Mgmt/SatisfactionSurvey.htm.

[26] Berry, L. L., Wall, E. A., & Carbone, L. P. (2006). Service clues and customer assessment of the service experience: Lessons from Marketing. *Academy of Management Perspectives*, 20(2), 43-57.

[27] Hennig-Thurau, T., Gwinner, K. P., & Gremler, D. D. (2002). Understanding Relationship Marketing outcomes: An integration of relational benefits and relationship quality. *Journal of Service Research*, 4(3), 230-247.

[28] Hartline, M. D., & Ferrell, O. C. (1996). The management of customer-contact service employees: An empirical investigation. Journal of Marketing, 60(4), 52-70.

[29] Hartline, M. D., Maxham III, J. G., & McKee, D. O. (2000). Corridors of influence in the dissemination of customer-oriented strategy to customer contact service employees. Journal of Marketing, 64(2), 35-50.

[30] Mead, G. H. (1934). Mind, self and society: From the standpoint of a social behaviorist. Chicago, IL: University Press.

[31] Hennig-Thurau, T. (2004), Customer orientation of service employees – Its impact on customer satisfaction, commitment, and retention. International Journal of Service Industry Management, Vol. 15, No. 5, pp. 460-478.

[32] Bitner, M. J., Booms, B. H., & Mohr, L. A. (1994). Critical service encounters: The employee's viewpoint. Journal of Marketing, 58(October), 95-106.

[33] Weatherly, K. A., & Tansik, D. A. (1993). Managing multiple demands: A Role-Theory examination of the behaviours of customer contact service workers. In Swartz, T. A., Bowen, D. E., & Brown, S. W. (Eds.). Advances in Services Marketing and Management (Vol. 2, 279-300), Greenwich. CT: JAI Press.

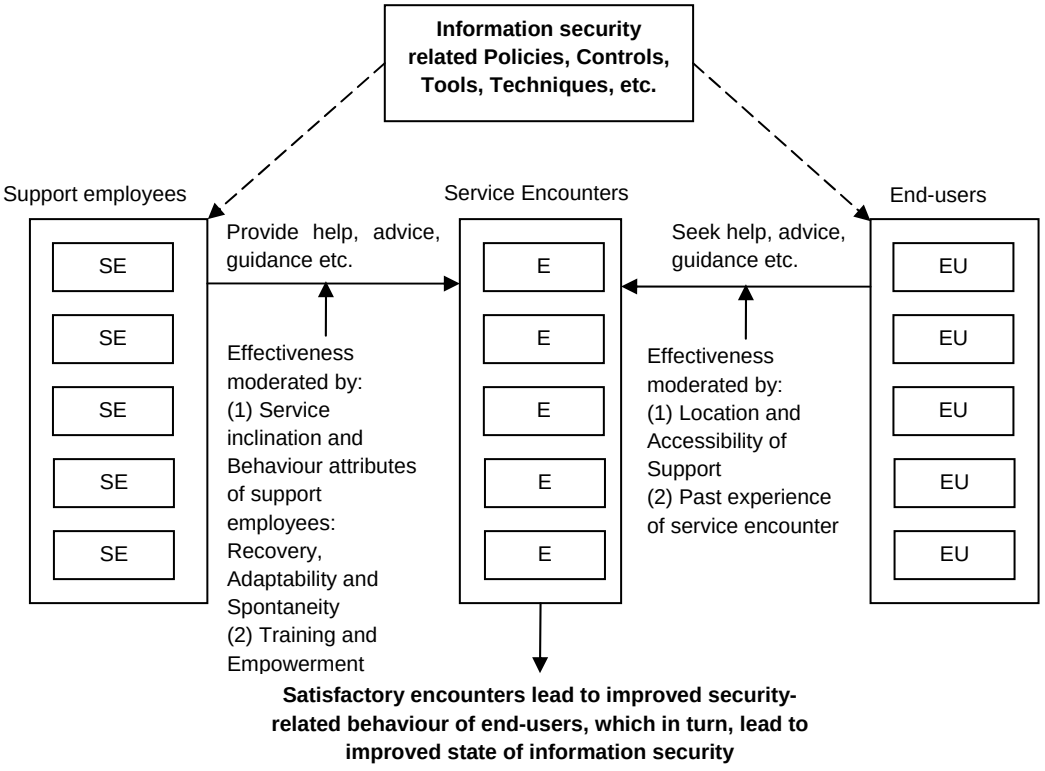


Figure 1: ISSS Framework

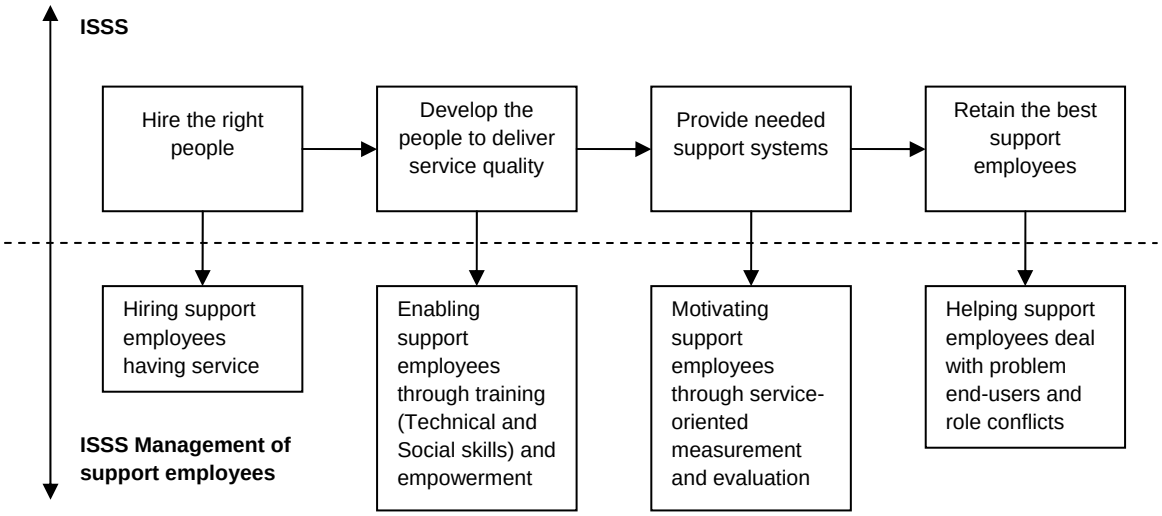


Figure 2: Four-step strategy for ISSS and Management of support employees

Appendix E:

Information Security Service Culture – information security for end-users

Rahul Rastogi[a] **and Rossouw von Solms**[b]

Institute for ICT Advancement,

Nelson Mandela Metropolitan University, South Africa

[a]rahul.rastogi@eil.co.in

[b]rossouw.vonsolms@nmmu.ac.za

Abstract

Usability of information security policies and controls is vital to the effectiveness of information security in the organization. This fact has been known since long, however, information security managers and developers have continued to display indifference to the needs of end-users. This indifference has manifested itself in bureaucratic and technology focused approach to information security. This paper posits that the root cause of this indifference is the negative image of end-users in the perception of information security developers and managers. The paper goes on to provide a solution in the form of Information Security Service Culture (ISSC). ISSC refers to the culture of the information security managers and developers in the organization. ISSC is useful in transforming information security managers and developers from technology-focused to end-user centric in approach.

Keywords: Information Security Management, Information Security Service Management, ISSM, service management, Information Security Service Culture, ISSC.

1. Introduction

In an early paper on information security, “The Protection of Information in Computer Systems” (Saltzer & Schroeder, 1975), the authors J.H. Saltzer and M.D. Schroeder presented eight principles applicable to the mechanisms for protection of information. One of these eight principles is the principle of psychological acceptability. According to this principle, ease of use of the human interface is crucial for protection mechanisms. If the protection mechanism is easy to use, then end-users will use it routinely and without

errors; otherwise, end-users will make errors (Saltzer & Schroeder, 1975). More recently, Bishop (2003) has expounded a similar principle. According to Bishop (2003), security or protection mechanisms place an extra burden on end-users. The principle of psychological acceptability can then be interpreted to mean that *"security mechanisms should not make the resource more difficult to access than if the security mechanisms were not present"* (Bishop, 2003). Apparently, these principles have not found much favor with information security managers and developers. Zurko and Simon (1996) go to the extent of stating that *"secure systems have a particularly rich tradition of indifference to the user"*.

The indifference of information security managers and developers towards the needs of end-users is a critical issue. Information security policies and controls based on this indifference exhibit a lack of usability. In spite of the early origins of the principles of psychological acceptability, one of the most severe problems of information security continues to be the difficulties end-users face as they try to interact with information security policies and controls in the organization (Furnell, 2010; Schultz et al., 2001). This poor usability is an issue of concern as it evokes end-user resistance and rejection of these policies and controls (Schultz et al., 2001). According to Schultz et al. (2001), end-user resistance manifests itself as *"passive resistance, negative verbal behaviour, reluctance to perform tasks, failure to pay sustained attention to tasks, actions that cause damage to system components and many others"*. This leads to non-compliance and severely weakens the effectiveness of information security policies and controls in the organization.

Based on the above discussion, it can be stated that to improve end-user compliance to information security policies and controls, the discipline of information security must first tackle the "rich tradition of indifference" of its practitioners towards end-users. This paper is a step in this direction. The paper posits that the indifference of information security managers and developers is rooted in the negative image of end-users in their perception. This paper provides a solution out of this imbroglio in the form of Information Security Service Culture (ISSC) which is discussed later in the paper.

An important aspect of ISSC is its service orientation. ISSC is a component of the overall framework of Information Security Service Management (ISSM) proposed by Rastogi and Von Solms (2009). ISSM is an alternative information security management approach which promises to mitigate the "rich tradition of indifference to the user" through its end-user centric approach to the formulation of information security policies and controls in the organization. In ISSM, information security becomes an internal service, the end-users become its customers and information security management becomes the service provider. To offer information security as a service, it is important to

implement the following three components that are integral to the service-oriented approach; i.e. the *design* of the service, the *marketing* of the service and the *support* of the service. To successfully offer information security as a service to end-users, ISSM requires a mental shift amongst the information security managers and developers – away from the firmly entrenched, present-day technical approach towards the end-user centric approach of ISSM. In ISSM, ISSC is a tool to achieve this shift. This paper discusses ISSC; the other components of ISSM, namely, marketing and support, are not addressed in this paper. ISSC can be said to rest on the pillar of a mind-set of service to the end-user.

The paper is organized as follows. It first examines, in the next section, the link between the image of end-users in the perception of developers and the resultant nature of the developed systems. The section also demonstrates that a negative image of end-users in the perception of information security managers and developers leads to bureaucratic and technology-focused information security polices and controls in the organization. The subsequent section examines different paradigms of information system development in order to identify an alternative approach to information security in the organization. Later the paper discusses the related concepts of culture, service culture and information security culture. Finally, the paper discusses ISSC.

A note of caution is provided here. Some of the concepts presented later in the paper come from the streams of information systems and information systems development. These concepts are subsequently applied to information security. It can be said that the streams of information systems or IT and information security are closely related (Albrechtsen & Hovden, 2009; Frangopoulos, 2007) and, hence, the concepts or results from the former fields can be validly applied to the latter. Further, it is to be noted that the paper treats the terms ‘engineer’, ‘technologist’ and ‘developer’ as synonyms. In the subsequent discussions, different authors have used one term or the other; this chapter uses the term ‘developer’ and refers to the role of people who develop the systems (including information systems and information security policies and controls) that underlie the work of other people in the organization.

2. The end-user in the perception of information security managers and developers

Various authors have explored the link between developers’ perceptions of end-users and the nature of systems that result from these perceptions. This section discusses this link in an attempt to understand the image of end-users in the perception of information security managers and developers and how this image influences the nature of information

security policies and controls in the organization. The section further discusses the resultant bureaucratic nature of present-day information security management.

2.1 The role of image

The developers in the organization have an implicit perception regarding the end-users in the organization. As these developers develop systems for the use of end-users, their perceptions of end-users have an impact on nature and the success or failure of the developed systems (Bostrom & Heinen, 1977; Orlikowski & Gash, 1994). In the field of information systems development (ISD), Bostrom and Heinen (1977) and Orlikowski and Gash (1994) have adopted a similar approach to understand the interaction between developers of information systems and their end-users in the organization. According to Bostrom and Heinen (1977), the development of information systems is impacted significantly by the view that system designers and developers hold regarding the organization, end-users and the function of the information system within the organization. The design of the information system is not solely determined by the available technology, but affected also by the knowledge, skills and values of the designers and the assumptions they hold about the organization and end-users. These factors act as "frames of reference" and "perceptual filters" that act to guide the designers and developers. The frames of reference of the designers and developers constrain their range of design alternatives and change strategies and, finally, even determine the chosen design alternatives and change strategies. Bostrom and Heinen (1977) further state that these frames of reference act at the sub-conscious level and designers and developers may not always be aware of the content of their frame of reference.

Orlikowski and Gash (1994) use the concept of "technological frames", or "technology frames", to understand the development and use of information systems in organizations. Technological frames, or technology frames, are the "*understanding that members of a social group come to have of particular technological artifacts, and they include not only knowledge about the particular technology but also local understanding of specific uses in a given setting"* (Orlikowski & Gash, 1994). Further, these frames concern the "assumptions, expectations and knowledge" that people in an organization hold regarding technology in the organization. Thus, a technology frame consists of a technology dimension as well as a contextual use dimension. Frames operate in the background as implicit assumptions and have the potential of creating "psychic prisons" (Bolman & Deal, 2003) which inhibit learning and creativity in problem solving. In a negative sense, frames are self-reinforcing and may lead to rejection of new knowledge; they may also manifest ideas that are "ambiguous, obsolete, incomplete or incorrect". These inconsistencies are implicit and the group often may not be aware. For example, in the context of information security in the organization, information security management

may preach the need for end-user friendly policies and controls, and yet continue with formulating policies and controls that do not promote secure behaviour by end-users.

According to Orlikowski and Gash (1994), technological frames have powerful effects as they influence the design and use of technologies in the organization. The design and development of an information system in the organization is determined implicitly by assumptions concerning the *"views of how work should be done, what the division of labor should be, how much autonomy employees should have, and how integrated or decoupled production units should be"* (Orlikowski & Gash, 1994). In this way, information systems reflect the "objectives, values, interests and knowledge" of the designers and developers of the system.

2.2 The image of end-users

Ashenden (2008) and Albrechtsen and Hovden (2009) have discussed the difficulties arising from the mismatch between the highly technical information security managers and developers and the technically naive end-users. This section is based on these two papers and discusses the negative image of end-users in the perception of information security managers and developers in the organization.

According to Ashenden (2008), in most organizations, information security is still a purely technical subject and best managed by technical staff. Information security managers and developers approach their subject in a "command and control" manner and remain isolated and disengaged from the end-users of their creation. The managers and developers do not make any attempts to understand or negotiate with their end-users and continue to rely on "how they think end-users see information security" (Ashenden, 2008).

Albrechtsen and Hovden (2009) state that a divide exists between end-users and information security managers with respect to skills, knowledge and responsibilities. This situation leads to information security policies and controls being designed with a duty-oriented or "policing" approach. In this approach, the policies and controls focus on allowing or disallowing end-users from performing specific activities. There is also an emphasis on surveillance and monitoring. Albrechtsen and Hovden (2009) further state that information security managers regard end-users both as a resource and as a problem. Managers feel that end-users lack motivation, knowledge and skills required for safe and secure behaviour and hence cause adverse incidents. Managers also have negative assessments of end-users. Consequently, information security policies and controls rely on "technological tools that seek to control and monitor user behaviour" because

"technology is also believed to be more sound and reliable than users". Though user participation and involvement is rated highly, most information security managers remain aloof and distant from end-users while formulating information security policies and controls. Information security managers typically do not have detailed information regarding the information security behaviours of end-users – they continue to design information security policies and controls based on their perceptions of end-users. There is a trust deficit wherein information security managers do not trust end-users. It can be said that the relationship of information security managers and developers with their end-users is marred by incorrect perceptions, distrust and antagonism.

2.3 The resultant approach to information security management

The preceding discussion in this section has presented the link between the image of end-users in the perception of information systems developers and the nature of information systems developed in the organization. The discussion has also covered the negative image of end-users in the perception of information security managers and developers in the organization. This section now discusses how this negative image influences the nature of information security policies and controls in the organization.

According to Frangopoulos (2007), present-day information security management is bureaucratic in nature and while it is "complete from a technical viewpoint", it falls short on the treatment of the "idiosyncratic nature of the human element, especially within a social context" (Frangopoulos, 2007). Frangopoulos (2007) further states that present-day information security management ignores the inherent variability of humans and their impact on the information security in the organization. Echoing Frangopoulos (2007), Albrechtsen (2008) too states that present-day information security management represents a paradox in that it attempts to manage the security of modern and dynamic IT through traditionally structured approaches and perspectives.

It can now be said that end-users and information security managers and developers are linked by two factors. Firstly, information security managers and developers formulate information security policies and controls based on technological considerations only and ignore the needs of end-users. The assumption underlying this approach is that end-users are rational actors who will readily comply with information security policies and controls. This assumption ignores the inherent variability of end-users and is thus flawed. Secondly, as end-users exhibit resistance and rejection of information security policies and controls built upon a flawed assumption, information security managers and developers come to have an antagonistic view towards the end-users in the organization. These two factors conspire to ensure information security managers and developers in the

organization continue to neglect the principle of psychological acceptability and the ease of use of information security policies and controls. It can be said that this inadequacy of present-day information security policies and controls results from the unrealistic models and expectations of the developers regarding the end-users of these policies and controls. The unrealistic models and expectations, in turn, arise from the lack of knowledge regarding the everyday work and information security behaviours of end-users.

This section has established the importance of image of end-users in the perception of information security managers and developers in determining the nature of information security management and policies and control in the organization. In the present-day, information security managers and developers hold a negative image of end-users and this leads to bureaucratic, technology-focused information security policies and controls in the organization; such an environment, in turn, leads to end-user resistance and non-compliance. The next section discusses a possible approach to resolve this imbroglio.

3. A pathway to the development of end-user centric information security in the organization

This section discusses the various paradigms that are adopted in the development of information systems in organizations. Each paradigm has its own set of assumptions regarding end-users and leads to systems of different natures. The section concludes by identifying a paradigm suitable to information security in the organization.

Hirschheim and Klein (1989) define a paradigm as consisting of "assumptions about knowledge and how to acquire it, and about the physical and social world". According to Hirschheim and Klein (1989), in a professional community, all members typically follow a common paradigm and hence share both perceptions and practices. As already discussed earlier, these perceptions and practices are particularly important in the context of system development. The perceptions and practices of developers have a significant impact on the nature of system development, the nature of the system that is developed and the nature of the use of the system. In their work, Hirschheim and Klein (1989) present four paradigms of information systems development. These paradigms are based on the four paradigms proposed by Burrell and Morgan (1979). Various authors have applied the four paradigms of Burrell & Morgan (1979) and Hirshheim and Klein (1989) to the study of information security (Clarke & Drake, 2003; Dhillon, 1995; Dhillon & Backhouse, 2001; McFadzean, Ezingeard & Birchall, 2006; White & Dhillon, 2005). This section provides a brief overview of the four paradigms and how these paradigms have been applied to information security. The section also provides an overview of the functionalist paradigm of present-day technology-dominant approach to information

security. The section concludes by discussing the interpretivist paradigm as the way forward to a more holistic, end-user centric approach to information security in the organization.

Hirschheim and Klein (1989) applied the four paradigms of Burrell and Morgan (1979) to information systems development. Hirschheim and Klein (1989) identified four paradigms as: "Functionalism", "Social Relativism", "Radical Structuralism" and "Neohumanism" (see Figure 9.1).

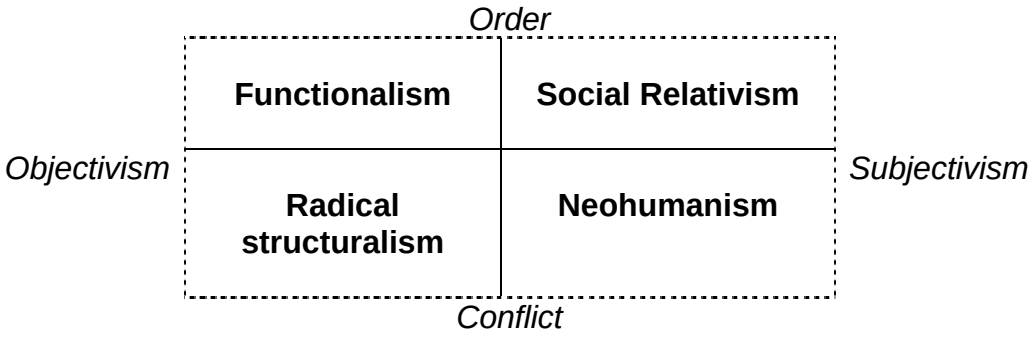


Figure 9.1: Four paradigms of Hirschheim & Klein (1989)

The following description of the four paradigms of Hirschheim and Klein (1989) is based on Hussain and Taylor (2007):

- The functionalist paradigm: In this paradigm, the information systems developer acts as an expert. The expert takes a mechanistic approach, and uses tools and technologies to develop systems through rationalistic, procedural methodologies. In this approach, users are considered biased and hence not consulted.
- The social relativist paradigm: In this paradigm, the developer acts as a facilitator or catalyst and seeks to unravel and understand the needs and requirements of the users. The users are best placed to develop the system and they should be consulted throughout the development process. In this approach, the developer acts as catalyst to facilitate users in reflecting and learning about the system.
- The radical structuralist paradigm: In this paradigm, the developer acts as a warrior, taking either the side of management or of users. The developer undertakes political action to change the IT environment rather than interpret it.
- The neohumanist paradigm: In this paradigm, the developer acts as an emancipator or social therapist. The developer seeks to gain consensus over needs and requirements

amongst various stakeholders by creating an environment of debate free from social constraints.

Dhillon (1995) and Dhillon and Backhouse (2001) have applied the four paradigms to information security. Dhillon (1995) observes that information systems researchers and developers have begun to move away from a purely technical approach to systems development; the researchers and developers consider the act of systems development as a social act. Unfortunately, information security researchers and developers have remained locked in their "psychic prison" (Bolman & Deal, 2003) of a "mechanistic, technical vision" (Dhillon, 1995). A similar view is echoed by Frangopoulos (2007), Ashenden (2008) and Albrechtsen and Hovden (2009). The present-day approach to the development of information security policies and controls lies in the functionalist paradigm. White and Dhillon (2005) have proposed using the "interpretivist" or "social relativist" paradigm for resolving the crisis of information security. This shift from functionalism to interpretivism is necessitated by the fact that information security relies heavily upon end-user interpretation and participation in compliance with information security policies and controls in the organization. In view of these facts, the further discussion in this section considers only the functionalist and interpretivist approaches to information security as outlined by White and Dhillon (2005).

In the present-day, functionalist approach to information security in the organization, the information security developer acts as an expert. The developer is focused on technology, tools and methods for controlling the access of end-users to information assets. The developer is unconcerned with the impact on end-users, their working practices, their needs and requirements. The end-users are expected to act mechanistically and according to the needs of the system. This approach satisfies the "system ideal" and leads to a "technology trap" wherein technology is considered to provide the complete solution to a problem.

The interpretivist approach to information security lies in stark contrast to the functionalist approach. The interpretivist approach is a holistic approach and is based upon understanding how end-users interpret and comply with information security policies and controls in the organization. The information security developer acts as a catalyst or facilitator that seeks to understand the working practices and needs and requirements of end-users. The emphasis is to ensure that end-users will be willing to learn, adapt and accept the information security policies and controls. This approach satisfies the "contextualist ideal" wherein the emphasis is on the social context and processes.

Given the importance of end-user behaviour to the success of information security in the organization, it is to be expected that an end-user centric approach to information security is required. The present-day approach to information security is functionalistic and is therefore inappropriate. The way out, as suggested by White and Dhillon (2005), is to use an interpretivist approach. Such an approach emphasizes the "contextualist ideal" and requires the study of the "social context and associated processes" of end-users, their work in the organization and their information security behaviours. The change from a functionalist to an interpretivist approach requires an antecedent change - that of changing the mind-set of the information security developers towards recognizing and accepting a far more substantive and richer role for end-users. In the context of ISSM, this change can be brought through Information Security Service Culture (ISSC). Before discussing ISSC, the next section presents an overview of the related concepts of culture, service culture, information security culture and Information Security Service Culture.

4. Culture, service culture, information security culture and Information Security Service Culture (ISSC)

The concept of Information Security Service Culture is related to the three concepts of culture, service culture and information security culture. Further, the concepts of service culture and information security culture themselves are related to the concept of culture. This section provides an overview of these concepts.

Davis (1985) defines culture as the "pattern of shared values and beliefs that give the members of an organization meaning, and provide them with the rules for behaviour in the organization" (Grönroos, 2007). Schein (2004) defines culture as *"a pattern of shared basic assumptions that was learned by a group as it solved its problems of external adaptation and internal integration, that has worked well enough to be considered valid and, therefore to be taught to new members as the correct way to perceive, think and feel in relation to those problems"*. Thus culture operates in an organization by shaping how people in an organization "do certain things, think in common ways and appreciate similar goals, routines and even jokes" (Grönroos, 2007). Culture acts as a patterning force and always exists. Researchers in the fields of service management and information security have cited the importance of culture to their respective fields.

Culture is critically important for service organizations (Grönroos, 2007; Zeithaml et al., 2008). Zeithaml et al. (2008) define service culture as "a culture where an appreciation for good service exists, and where good service to internal as well as ultimate, external customers is considered a natural way of life and one of the most important norms by everyone". Grönroos (2007) states that "a functioning service culture requires that

providing good service is second nature to everyone within that organization". Further, service culture arises when all organizational components such as "organizational routines, directions for action given by policies and management and reward systems" converge together to emphasize good service to customer, whether internal or external. Culture, as the attitude of its employees, is particularly important for service organizations. Because delivering a service involves the coming together of the employees and their customers, employee attitudes and performance are visible to customers. Hence the attitude of employees, a reflection of the service culture in the organization, is critically important.

According to Von Solms (2000), the idea of information security culture (ISC) emerged in the third wave of information security evolution. The idea of information security culture "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" (Von Solms, 2000). Martins and Eloff (2002) define ISC "as the assumption about which type of information security behaviour is accepted and encouraged in order to incorporate information security characteristics as the way in which things are done in an organization". Ramachandran, Rao and Goles (2008) state that ISC involves "identifying the security related ideas, beliefs and values of the group, which shape and guide security-related behaviours". The importance of ISC lies in the fact that it fosters an attitude in end-users whereby safe information security behaviours become a way of organizational life for these end-users (Van Niekerk & Von Solms, 2005; Von Solms, 2000). ISC shapes and guides the behaviour of end-users in the organization in regard to information security policies and controls.

Information Security Service Culture (ISSC) is based upon the concepts of culture and service culture. ISSC refers to the culture, and hence the patterns of shared values and beliefs, amongst the Information Security Service Management managers and employees in the organization. Just as culture and service culture apply to the employees of the organization, ISSC applies to the members of the ISSM function. ISSC consists of the patterning force of culture that drives the information security managers, developers and other staff members to deliver "good service" to their customers, namely, the end-users in the organization. ISSC is visible when end-users come in contact with information security service members and the information security policies and controls in the organization. Further, as stated above, ISSC can arise only when all the different organizational components come together to stress "good service" to end-users. ISSC and "good service" to end-users, however, do not imply that the security needs of the organization's information assets are completely ignored; it only means that while these classical security issues are also important, service to end-users should have a dominant role.

The inter-relationship between culture, service culture, information security culture and ISSC are shown in Figure 9.2. According to this figure, both concepts of Information Security Service Culture and information security culture are based upon the concept of culture; ISSC is also based upon the concept of service culture. ISSC differs from information security culture in that ISSC applies to the employees of the ISSM function, particularly the developers, whereas information security culture applies to the customers of the ISSM function i.e. the end-users in the organization. Further, while ISSC seeks to promote an end-user centric approach to information security, ISC seeks to promote the compliance of end-users to information security policies and controls in the organization. It is also pertinent to note that both ISSC and ISC contribute to the state of information security in the organization.

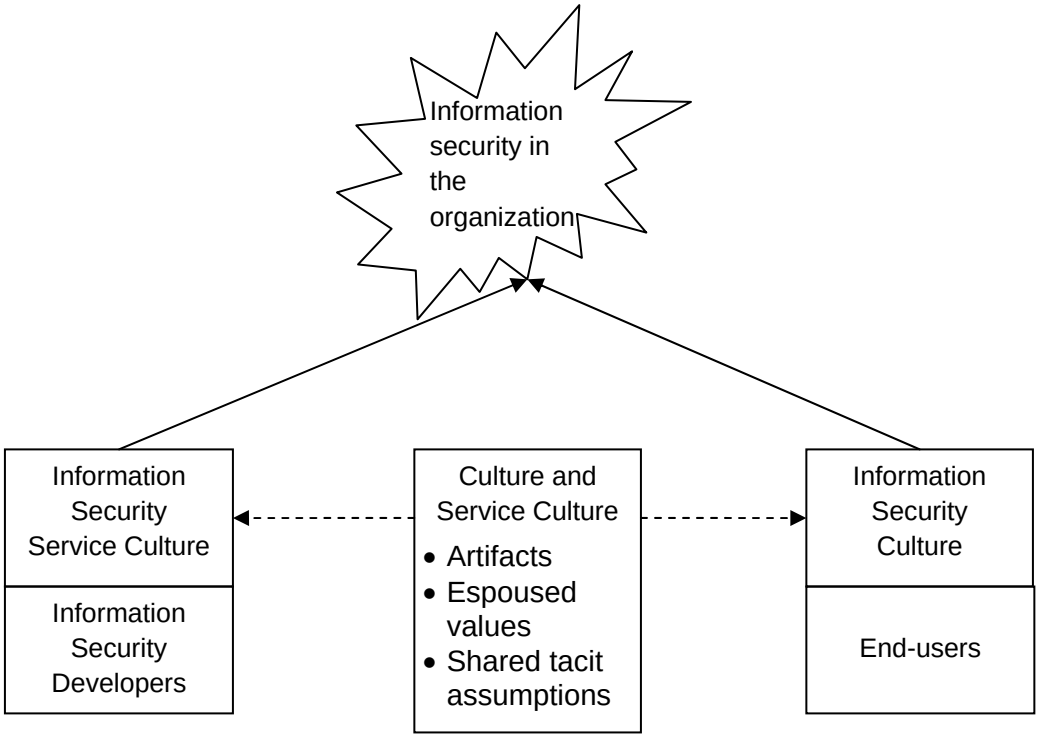


Figure 9.2: Information Security Service Culture and Information Security Culture leading to effective information security in the organization

Having discussed the meaning and role of various types of cultures, it is important to understand the constituent parts of culture. According to Schein (2004), culture exists at three levels – 'artifacts', 'espoused values and beliefs' and 'underlying assumptions' (see Figure 9.3). The topmost level is that of artifacts. Artifacts are the observable phenomena that reflect a particular culture. In the context of a group, artifacts are the visible behaviour of the group. In an organization, artifacts refer to the organizational processes and structural elements that lead to the behaviour of the constituent groups. Espoused values and beliefs are psychological or attitudinal in nature, and exist at the conscious level. They reflect the strategies, goals and philosophies of the group. Whereas artifacts are the visible manifestations of behaviour, espoused values and beliefs are the invisible determinants of behaviour. Below the beliefs and values at the conscious level, lie the shared tacit assumptions. Shared tacit assumptions operate at the unconscious level and are deeply ingrained. These assumptions are 'taken-for-granted' and are strongly held in a group.

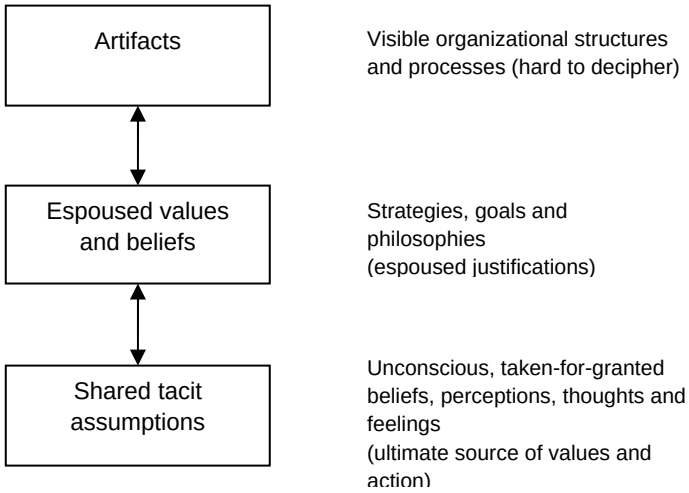


Figure 9.3: Levels of Culture (from Schein, 2004)

The role of culture as a patterning force is extremely important for organizations, particularly in a service context. The above discussion has provided an overview of the related concepts of culture, service culture, information security culture and Information Security Service Culture. ISSC differs from information security culture in that ISSC applies to the employees of the ISSM function whereas information security culture applies to the customers, i.e. the end-users, of the ISSM function. The next section discusses in greater detail the influence of ISSC over information security managers and developers who formulate information security policies and controls in the organization.

5. Information Security Service Culture (ISSC)

The previous sections have highlighted the crucial role of the attitude of the developers of systems towards the end-users of those systems. This attitude plays an important role in shaping how the system is developed, how the developers incorporate human issues and, finally, how the system is accepted and used by end-users. These attitudes have been variously called as the "engineering culture" (Schein, 1996 and 2004), "frames of reference" (Bostrom & Heinen, 1977), "technology frames" (Orlikowski & Gash, 1994) and "paradigms" (Burrell & Morgan, 1979; Hirshheim & Klein, 1989). These concepts are also applicable in the development of information security policies and controls in the organization (Clarke & Drake, 2003; Dhillon, 1995; Dhillon & Backhouse, 2001; McFadzean et al., 2006; White & Dhillon, 2005). The traditional approach to information security has been technology oriented, or functionalist, and therefore has failed to garner support from end-users; the way out of this imbroglio is to use an interpretivist approach to information security (White & Dhillon, 2005). This section proposes and discusses Information Security Service Culture (ISSC) as a means to migrate developers of information security policies and controls from the functionalist to the interpretivist paradigm.

A key aspect of Schein's model of culture, discussed in the previous section, is the disconnect that can occur between the three levels of culture in a group or organization. Espoused beliefs and values at the conscious level can be said to predict behaviours at the artifacts level. However, if the beliefs and values are incongruent with the assumptions at the unconscious level, then there can be a misalignment between what people 'say' they will do in a situation and what they actually 'do'. Thus as Schein (2004) says, *"a company may say that it values people and that it has high quality standards for its products, but its record in that regard may contradict what it says"*. If the espoused beliefs and values are congruent with the underlying assumptions, then there is alignment between what people 'say' and 'do'. In the context of information security, it can be said that information security developers and managers suffer from an incongruence between their underlying assumptions and their espoused beliefs and behaviours – there is misalignment between what they say and do in respect of end-users – they profess the importance of end-users to information security and yet, continue to formulate information security policies and controls with scant regard for the needs and requirements of end-users.

Information Security Service Culture is an attempt at aligning what information security developers and mangers say with what they do, i.e. the espoused and the enacted. In terms of information security, this means that developers and managers adopt the interpretivist paradigm and that the organization provides them with the encouragement

and resources to enable them to formulate end-user centric information policies and controls.

The three levels of culture can thus be mapped as follows:

- Shared tacit assumptions

  At the unconscious level, developers and managers of information security should hold the beliefs that end-users are not their "enemy", rather the end-users are an "asset". They should also believe that end-users want to comply with information security policies and controls; and that there often is not any malicious intent behind non-compliance. End-users want to work in the interest of their organization. Any non-compliance is largely a result of the cognitive limitations of end-users or because the information security policies and controls are incompatible with their work practices. The information security developers and managers should also believe that end-users are their customers and that they are there for providing the information security service to the end-users. In this frame of mind, the end-users become the raison d'être of the information security managers and developers.

- Espoused values and beliefs

  This is the conscious level at which the strategies, goals and philosophies exist. At this level, the information security developers and managers should utilize technologies, tools and methods that lead to end-user centric information security policies and controls in the organization. End-user acceptance and ease of use of policies and controls should be important determinants of the security measures. Further, formulation of information security policies and controls must not happen in isolation from end-users; rather, in keeping with the interpretivist paradigm, policies and controls must be formulated with the active involvement of end-users. ISO/IEC 9241-210:2010 is an international standard titled "Human-centred design for interactive systems" (ISO/IEC 9241-210, 2010). Information security policies and controls are "interactive systems" and this standard, with its focus on designing human-centred interactive systems, can provide useful guidance for their formulation. According to this standard, formulation of end-user centric information security policies and controls would require "an approach to interactive systems development that aims to make systems usable and useful by focusing on the users, their needs and requirements, and by applying human factors / ergonomics, and usability knowledge and techniques" (ISO/IEC 9241-210, 2010). This standard will enable information security developers and managers to "design and redesign processes to identify and plan effective and timely human-centre design activities". According to ISO/IEC 9241-210:2010, the principles of human-centred design are:

    a. The design is based upon an explicit understanding of users, tasks and environments.

b. Users are involved throughout design and development.
c. The design is driven and refined by user-centred evaluation.
d. The process is iterative.
e. The design addresses the whole user experience.
f. The design team includes multidisciplinary skills and perspectives.

- Artifacts

  The artifacts level is populated by organizational processes and structures and the behaviours of information security developers and manager. The artifacts level is also populated by the end-user centric information security policies and controls. These end-user centric policies and controls will be acceptable to end-users, be usable by them and will earn the commitment of end-users to information security. ISO/IEC 9241-210:2010 provides guidance on the activites that need to be performed for the development of human-centred interactive systems. These activities are:

  e. Understanding and specifying the context of use.
  f. Specifying the user requirements.
  g. Producing design solutions.
  h. Evaluating the design.

  The artifacts level is also populated by the behaviours of business managers and IT managers – their behaviours create an end-user centric environment for the day-to-day work that promotes safe information security behaviours of end-users. Adequate encouragement, knowledge and resources must be provided to ISSM managers and developers to enable them to undertake the formulation of end-user centric information security policies and controls in the organization. Leadership is a key aspect of building a service culture (Bartley, Gomibuchi & Mann, 2007; Grönroos, 2007; Mather, 2008). The behaviour of managers in supporting the developers in their end-user centric endevaours removes any incongruence between what is said and what is actually done. According to Grönroos (2007), any incongruity in the stance of managers will be detrimental to establishing the Information Security Service Culture – if managers do not walk their talk, then developers too will be unable to deliver end-user centricity.

The three levels of the Information Security Service Culture are shown in Figure 9.4.

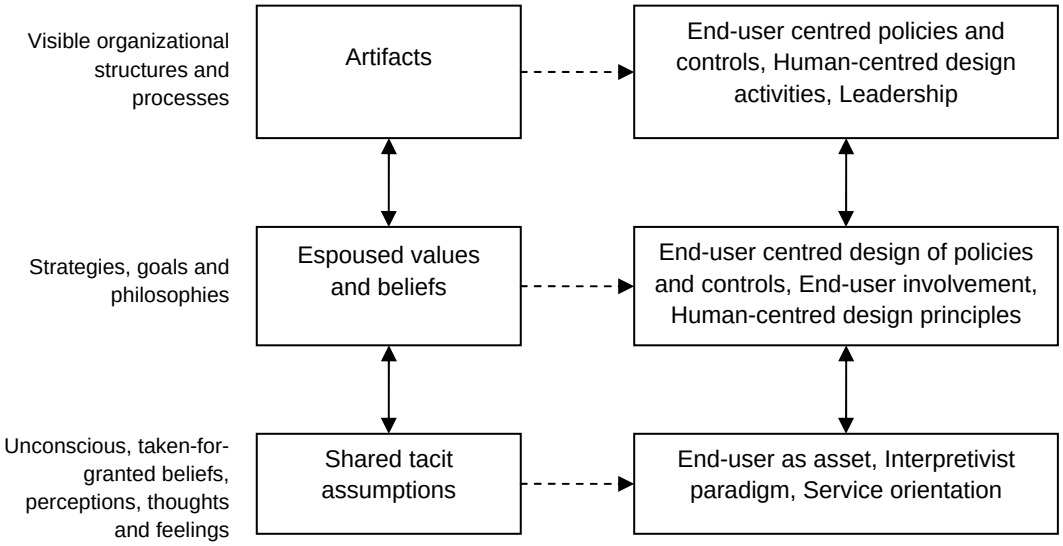


Figure 9.4: The three levels of Information Security Service Culture (ISSC)

6. Conclusion

This paper began with an elaboration of the importance of usability of information security policies and controls in the organization. The principle of psychological acceptability has been known for the last few decades; however, information security managers and developers have continued to display indifference to the needs of end-users. This has resulted in bureaucratic and technology-focused information security policies and controls which have not found favor with end-users. This paper identified the cause of this indifference as the negative image of end-users in the perception of information security managers and developers. The paper presented a solution in the form of Information Security Service Culture (ISSC). ISSC seeks to shift the mind-set of information security managers and developers towards an end-user centric approach to information security. The paper concluded by presenting the components of ISSC.

7. References

Albrechtsen, E. (2008). *Friend or foe? Information security management of employees*. Doctoral Thesis, Norwegian University of Science and Technology, Faculty of Social Sciences and Technology Management, Department of Industrial

Economics and Technology Management. Retrieved June 20, 2010, from http://ntnu.diva-portal.org/smash/record.jsf?searchId=1&pid=diva2:231438.

Albrechtsen, E., & Hovden, J. (2009). The information security digital divide between information security managers and users. *Computers & Security*, 28(6), 476-490.

Ashenden, D. (2008). Information security management: A human challenge? *Information Security Technical Report*, 13(4), 195-201.

Bartley, B., Gomibuchi, S., & Mann, R. (2007). Best practices in achieving a customer-focused culture. *Benchmarking: An International Journal*, 14(4), 482-496.

Bishop, M. (2003). *Computer security: Art and science*. New Delhi: Pearson.

Bolman, L. G., & Deal, T. E. (2003). *Reframing organizations*. San Francisco: Jossey-Bass.

Bostrom, R. P., & Heinen, J. S. (1977). MIS Problems and Failures: A Socio-Technical Perspective. Part I: The Causes. *MIS Quarterly*, 1(3), 17-32.

Burrell, G., & Morgan, G. (1979). *Sociological paradigms and organisational analysis*. London: Heinemann Educational Books Ltd.

Clarke, S., & Drake, P. (2003). A social perspective on information security: theoretically grounding the domain. In S. Clarke, E. Coakes, M. G. Hunter & A. Wenn (Eds.), Socio-Technical and Human Cognition Elements of Information Systems (pp. 249-265). London: Information Science Publishing.

Davis, S. M. (1985). *Managing Corporate Culture*. Cambridge, MA: Ballinger.

Dhillon, G. (1995). *Interpreting the management of information systems security*. Doctoral Thesis, Information Systems Group, London School of Economics. Retrieved June 20, 2010, from http://www.lse.ac.uk/collections/informationSystems/pdf/theses/dhillon.pdf.

Dhillon, G., & Backhouse, J. (2001). Current directions in IS security research: Toward socio-organizational perspectives. *Information Systems Journal*, 11(2), 127-153.

Frangopoulos, E. (2007). *Social engineering and the ISO/IEC 17799:2005 security standard: a study on effectiveness*. Master of Science Thesis, School of Computing, University of South Africa. Retrieved June 20, 2010, from http://uir.unisa.ac.za/bitstream/10500/2142/1/dissertation.pdf.

Furnell, S. (2010). Jumping security hurdles. *Computer Fraud & Security*, 2010(6), 10-14.

Gronroos, C. (2007). Service management and Marketing: Customer management in service competition (3rd ed.). Delhi, India: John Wiley & Sons Ltd.

Hirschheim, R. & Klein, H. (1989). Four Paradigms of Information Systems Development. C*ommunications of the ACM*, 32(1989), 1199-1216.

Hussain, Z., & Taylor, W. A. (2007). Evaluating the behaviour of information systems developers: The relevance and utility of paradigms. *Behaviour and Information Technology*, 26(3), 221-236.

ISO/IEC 9241-210 (2010). Ergonomics of human-system interaction - Part 210: Human-centred design for interactive systems. ISO/IEC 9241-210:2010, International Organization for Standardization and International Electrotechnical Commission.

Martins, A., & Eloff, J. P. H. (2002). Promoting information security culture through an information security culture model. In Proceedings of ISSA2002, Johannesburg, South Africa.

Mather, J. (2008). Creating the service culture. *Human Resources*,18-19.

McFadzean, E., Ezingeard, J.-N., & Birchall, D. (2006). Anchoring information security governance research: Sociological groundings and future directions. Journal of Information System Security, 2(3).

Orlikowski, W. J., & Gash, D. C. (1994). Technological frames: Making sense of information technology in organizations. *ACM Transactions on Information Systems*, 2(2), 174–207.

Ramachandran, S., Rao, S.V., & Goles, T. (2008). Information security cultures of four professions: A comparative study. In Proceedings of the 41st Annual Hawaii International Conference on System Sciences. ISBN: 978-0-7695-3075-8.

Rastogi, R., & von Solms, R. (2009). A service-oriented approach to information security management. In G. Dhillon (Ed.), Proceedings of the 7th Annual Conference on Information Science, Technology & Management (CISTM) “Sustaining a Knowledge Economy”. July 13-15. DC: Information Institute Publishing. ISBN: 978-1-935160-06-9.

Saltzer, J. H., & Schroeder, M. D. (1975). The protection of information in computer systems. *Communications of the ACM*, 17(7),

Schein, E. H. (1996). Three cultures of management: The key to organizational learning. *Sloan Management Review*, 38(1), 9-20.

Schein, E. H. (2004). *Organizational culture and leadership* (3rd Ed.). San Francisco: Jossey-Bass.

Schultz, E. E., Proctor, R. W., Lien, M., & Salvendy, G. (2001). Usability and security: An appraisal of usability issues in information security methods. *Computers & Security*, 20(7), 620-634.

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.

White, E. F. R., & Dhillon, G. (2005). Synthesizing information system design ideals to overcome developmental duality in securing information systems. In Proceedings of the 38th Annual Hawaii International Conference on System Sciences (HICSS'05) - Track 7. ISBN: 0-7695-2268-8.

Zeithaml, V. A., Bitner, M. J., Gremler, D. D., & Pandit, A. (2008). *Service marketing – integrating customer focus across the firm (4th ed.)*. Delhi, India: Tata McGraw-Hill Publishing Company Ltd.

Zurko, M. E., & Simon, R. T. (1996). User-centered security. New Security Paradigms Workshop.