INFORMATION SECURITY SERVICE MANAGEMENT

R RASTOGI (Nelson Mandela Metropolitan University, Engineers India Limited)[1]
R VON SOLMS (Nelson Mandela Metropolitan University)[2]
rahul.rastogi@eil.co.in[1]
Rossouw.VonSolms@nmmu.ac.za[2]

Abstract: This paper proposes Information Security Service Management (ISSM) as an improved alternative to the present-day approach to information security management in the organisation. It first discusses the roles of information security management and the end-users in developing and maintaining the state of information security in the organisation. The paper argues that one of the serious issues of information security management, namely the non-compliance exhibited by end-users, can actually be traced back to the bureaucratic nature of present-day information security management. To provide a way out, the paper formulates the CARE principles towards a more end-user centric approach. The paper also proposes ISSM that is based on the principles of current-day service management. The paper concludes with the major components of ISSM, and provides guidance for the implementation of ISSM in the organisation.

Key phrases: information security management, information security service branding, information security service culture, information security service management, information security service support, service management

1 INTRODUCTION

Most organisations today treat information, and the associated information technology, as vital organisational assets. These assets not only provide a competitive edge to the organisation, but in most cases, these information assets are critical to the survival of the organisation. Any security breach involving these assets could result in serious implications for the organisation. Consequently, organisations today deploy considerable resources for the effective protection of their information assets.

Organisations also create an organisational structure, through some information security management system to provide information security management. The ongoing effectiveness of information security policies and controls is an issue of critical importance. In this scenario, as stated in ISO/IEC 27000 (2009), one of the critical success factors for information security in the organisation is the behaviour of users of information and related information technology, commonly known as end-users.

Information security management manifests itself in the organisation through the formulation of information security policies and controls and the mandating of 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 organisation.

The present-day approach to information security management, as exemplified by the international standards ISO/IEC 27000 (2009), ISO/IEC 27001 (2005) and ISO/IEC 27002 (2005), consists of applying the tools of awareness, education and training to improve end-user behaviours. These standards further prescribe the use of “a formal disciplinary process for handling security breaches” (ISO/IEC 27002:2005). However, this approach has failed to yield good results.

In spite of the efforts of information security management, end-users continue to exhibit significant levels of non-compliance with the information security policies and controls in the organisation (Adams & Sasse 1999:40-46; Dhillon 2001:165-172; Dourish, Grinter, Delgado De La Flor & Joseph 2004:391-401; Furnell 2010:10-14). Furthermore, actions of information security management are leading to the creation of a digital divide between information security managers and end-users (Albrechtsen & Hovden 2009:476-490). Thus, it can be said that rather than promoting end-user compliance, the actions of information security management are actually leading to increasing non-compliance by end-users. This is dubbed the end-user crisis of the present-day information security management.

In view of this self-inflicted end-user crisis, it can be argued that the discipline of information security is in need of revamping its approach to information security management in the organisation. It is the purpose of this paper to propose and formulate an improved approach to information security management that has the promise of resolving this end-user crisis. This paper proposes Information Security Service Management (ISSM) as an alternative, and hopefully, an improved approach.

The objective of the paper is presented in the form of an alternative concept to address the end-user problems currently being experienced. These problems contribute to the failure of most information security management programmes. The paper is structured in the form of an argument, primarily based on literature sources, that aims to motivate the eventual contribution. The layout and argument, of the paper is structured as follows: the present-day bureaucratic nature of information security management is decribed and how this leads to antagonism between management and the end-user. Next, an end-user centric-oriented solution to this problem will be motivated; this is followed by a possible mechanism, namely, ISSM, to implement this solution. In the rest of the paper, a possible workable implementation of ISSM is argued, based on the principles, as espoused in general service management.

2 THE BUREAUCRATIC NATURE OF THE PRESENT-DAY APPROACH TO INFORMATION SECURITY MANAGEMENT

The present-day approach to information security management (or information security management systems) suffers from shortcomings related to the management of end-user-related aspects of information security. As stated earlier, information security management plays a vital role in the establishment of information security in the organisation. However, even as information security has evolved, and since there are international standards and best practices guiding the implementation of information security in the organisation, only very restricted aspects are adopted for dealing with end-users in information security.

The major aspect of the approach to end-users may be summarised 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 (ISO/IEC 27002:2005). This approach of information security management is reminiscent of the managerial style based on the principles of scientific management and bureaucracy.

According to Frangopoulos (2010), present-day approaches to information security management are characterised 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 (2010) further states that such an approach to information security management systems corresponds to the concept of a well-oiled machine, according to the “organisation as machine” metaphor of Morgan (1996). Thus, the information security management system is expected to function as a machine, in a "precise, repeatable and predictable manner" (Frangopoulos 2010) – ignoring the inherent variability of humans and their impact on the information security management system. Thus, "despite being complete from a technical viewpoint", the present-day approach to information security management falls short on the treatment of the "idiosyncratic nature of the human element, especially within a social context". Consequently, the present-day approach to information security management suffers from "fallacious working assumptions" that have "imposed technical and physical controls [which] can mitigate all identified risks" (Frangopoulos 2010).

Frangopoulos (2007) further argues that "modern-day information security management systems implementation still relies on bureaucracy for its fundamental functions", and that "a bureaucratic structure through which regulation and control are applied is a necessary prerequisite for an information security management system to exist". Hence, present-day information security management systems are fundamentally bureaucratic and do not employ democratic processes.

Albrechtsen (2008) provides a similar analysis of present-day information security management systems: the present-day approach to information security management is bureaucratic. It suffers from two shortcomings: the inability to adjust to the dynamic nature of IT, organisations and threats; and its inappropriateness for handling the human aspect of information security. These shortcomings have led to a mutual sense of antagonism between information security managers and end-users in the organisation. This aspect is further discussed below.

3 THE MUTUAL ANTAGONISM BETWEEN INFORMATION SECURITY MANAGERS AND END-USERS IN THE ORGANISATION

Information security managers and end-users in the organisation share a feeling of mutual antagonism. Information security managers treat end-users as the weakest link (Lineberry 2007) and as a threat (Albrechtsen & Hovden 2009:476-490). Gonzalez and Sawicka (2002) call the end-users the "Achilles heel of information security". End-users harbour a similar antagonism towards information security managers (Albrechtsen & Hovden 2009:476-490, Chipperfield & Furnell 2010:13-19). Albrechtsen (2007:276-289) further describes the relationship between information security managers and end-users. The results of this study hint at the existence of a digital divide between information security managers and end-users.

Ashenden (2008:195-201) states that the role of information security managers in an organisation 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 should best be managed by technical staff. In pursuance of this approach, information security managers tend to ignore the end-users: “[T]hey focus on talking, presenting and reinforcing ideas”, and “not [on] listening to end-users” (Ashenden 2008:195-201). The neglect of end-users is further reinforced by incorrect perceptions, since 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 (2008:195-201) states that this view is “unlikely to be neutral”.

Against this backdrop, end-users develop a negative attitude towards information security policies and controls in the organisation. The advantages offered by the use of information and IT in the organisation are pitted against the restrictions imposed by information security management – in the form of information security policies and controls. Nearly two decades ago, Baskerville (1993:40-47) stated that restrictions imposed by information security policies are detrimental to the spontaneity provided by IT. More recently, Chipperfield and Furnell (2010:13-19) echoed the same sentiment, when they stated 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 2010:13-19). This leads to a resistance to information security, and an inclination to readily switch to insecure behaviours (Adams & Sasse 1999:40-46, Dourish *et al.* 2004:391-401, Chipperfield & Furnell 2010:13-19, Albrechtsen 2007:276-289, Besnard & Arief 2004:253-264, Whitten & Tygar 1999).

This section has highlighted the negative perception of information security in the eyes of end-users in the organisation. End-users form a variety of such images. These images are shaped by how end-users experience information security and its management in the organisation. These images refer to information security as an obstacle, as a low-priority activity, as unnecessary, as intrusive, as unapproachable, and so on. Because of this, end-users continue to remain indifferent to information security in the organisation. Consequently, information security management is in need of a way forward, in order to counter this negativity. This way forward is an end-user centric-information security management in the organisation. This will be discussed in the next section.

4 THE WAY FORWARD – END-USER CENTRIC-INFORMATION SECURITY MANAGEMENT

According to Frangopoulos (2010), the present-day approach to information security management represents an oxymoron, since it applies the Weberian principles of the 19th century to resolve the issue of securing information in the 21st century. Various authors have sensed the shortcomings of the present-day approach to information security management, and have suggested avenues for improvement.

Dhillon (2001) has provided principles for information security management that are more suitable to today’s needs: 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 organisation. Furthermore, information security policies and controls need to be contextualised. Schlienger and Teufel (2002) underline the problem with today’s approach to information security management. The problem lies in the conception of the human dimension of information security. 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. 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 [the] appropriate security technology".

In the end-user-centric approach, the focus of information security managers shifts from compliance to the commitment of end-users to information security policies and controls in the organisation. This shift occurs with information security managers adopting the CARE principles. The CARE principles, as the name suggests, ensure that end-users are handled with due care. 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.

4.1 Communicate

Communication provides the link between end-users and information security management; and it enables the exchange of information between the information security management and the end-users. 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. This 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 in which 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 the end-users.

4.2 Accommodate

In the present-day approach to information security management, policies and controls are designed or formulated on the basis of risk analysis that is related to the information assets of the organisation. 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 organisation.

The main objective of the 'Accommodate' element is to minimise 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 the end-user requirements. Einstein said: "Make everything as simple as possible, but not simpler". Likewise, end-user practices can be accommodated only up to a certain point. Beyond this point, the practices take the organisation 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, in order to resolve the issue.

4.3 Respond

The last element of the CARE principles is the 'Respond' element. During their day-to-day life in the organisation, end-users come across the information security policies and controls, as they interact with information and information systems in the organisation. The end-users' willingness to undertake their information security tasks and their ability to complete these tasks, will both be influenced by their perception of the level of difficulty of the tasks. Additionally, past experience of a 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 ongoing manner. The 'Respond' element of the CARE principles embodies this support. The

‘Respond’ element requires that the organisation create 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 context of their information security tasks. End-users should find it convenient to contact the support-employees – in cases 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 conducting their information security behaviours.

The previous section discussed the shortcomings of the present-day approach to information security management in the organisation. This section has discussed the way forward towards an improved alternative, as suggested by various researchers. According to these researchers, the way forward lies in an end-user-centric approach to information security management. Accordingly, the section concludes by presenting the CARE principles that could guide information security managers in adopting an end-user-centric approach to information security management in the organisation.

The next section will take this discussion forward by providing a brief overview of the service-management approach, which is a customer-centric approach in the management of organisations. The subsequent section presents ISSM, based on the service-management approach and the CARE principles, as an end-user-centric approach to information security management in the organisation.

5 INFORMATION SECURITY SERVICE MANAGEMENT (ISSM)

ISSM is an end-user-centric approach to information security management in the organisation. The basis for ISSM is the reconceptualisation 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 it paves the way for a service-management approach for end-user-centric ISSM, based on the CARE principles. This section will now discuss ISSM and its major components.

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. ISSM satisfies these needs through the application of the service-management approach, as expounded by Grönroos (1990:6-14; 1994:5-20; 2007), to information security management in the organisation.

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 to the satisfaction of the customers of the information security service: the customers being the end-users. This shift is aimed at obtaining the long-term commitment and loyalty of end-users to the organisational-information security policies and controls, which in turn should lead to improved compliance. ISSM becomes an internal service consisting of information security service managers and staff that together provide information security-service to their customers: namely, the end-users.

ISSM 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 information security management 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 more secure and confident manner.

ISSM leads to several benefits, as compared with the present-day approach to information security management. The resulting benefits and outcomes that ISSM hopes to achieve include:

- A user-centric approach to information security.
- The 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 organisation.
- Reduced incidence of end-user violations and errors related to the information security policies and controls.
- Improved levels of compliance.
- A more effective state of information security in the organisation.

This section has discussed ISSM and what service management can mean to information security management. The next section will provide more details on how ISSM can be implemented in an organisation.

6 IMPLEMENTING ISSM IN THE ORGANISATION

The previous sections have delineated the CARE principles, the reconceptualisation of the notion of the end-user in information security, and ISSM as the service-management approach for end-user-centric information security management in the organisation. This section brings all these elements together, and discusses how ISSM can be implemented in the organisation. The next three sections provide further details of the three underlying components of ISSM.

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).

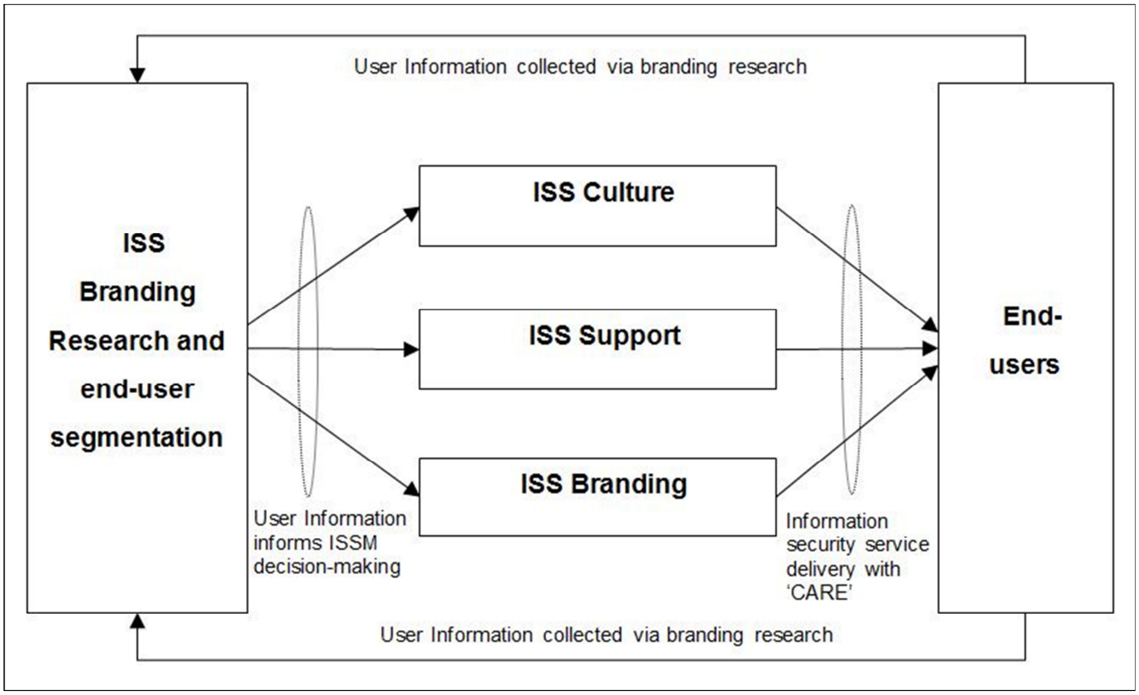
- ISSB is what wins the hearts of end-users for information security. The purpose of branding is to create a positive image for information security in the minds of the end-users, and thereby, to evoke commitment in the end-users to information security in the organisation. This also includes branding research that provides information on end-user behaviour so as to fine-tune ISSM's perceptions of end-users and their behaviours. ISSM is end-user centric; and it needs to understand the practices, needs and requirements of the end-users in the organisation.

- ISSC leads to the formulation of information security policies and controls in active co-ordination 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, in order to enable the successful delivery of ISSM.

- ISSS 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 it also 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 shown in Figure 1. These components will be discussed in greater detail in the subsequent sections.

FIGURE 1: CULTURE, SUPPORT AND BRANDING OF THE INFORMATION SECURITY SERVICE


User Information collected via branding research
ISS Branding Research and end-user segmentation
ISS Culture
ISS Support
ISS Branding
End-users
User Information informs ISSM decision-making
Information security service delivery with 'CARE'
User Information collected via branding research

Source: Own compilation

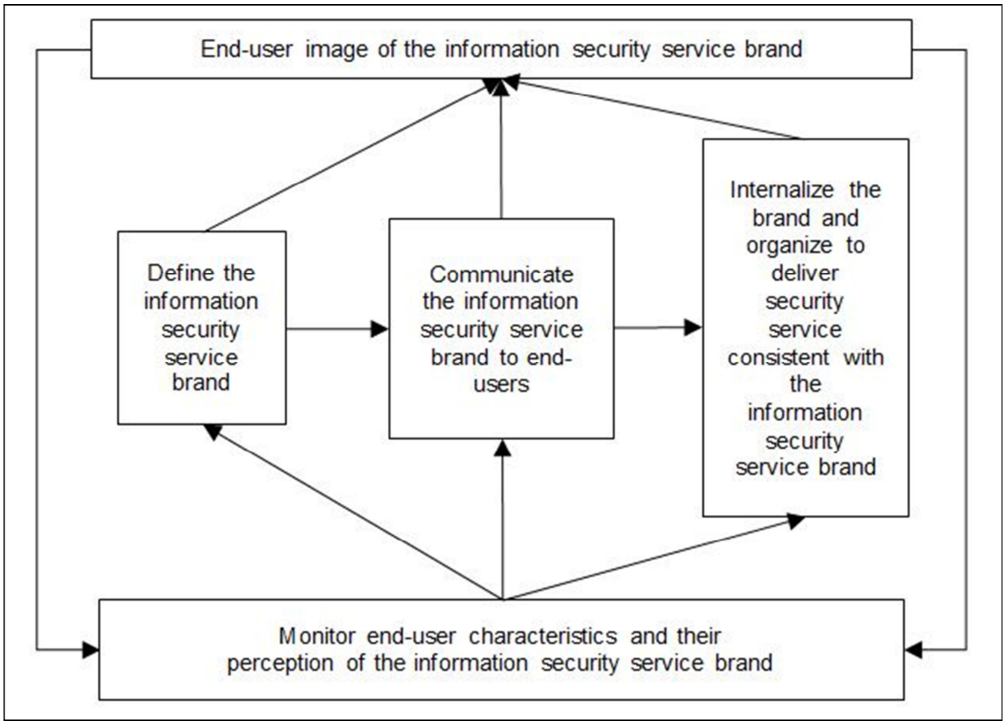
7 INFORMATION SECURITY SERVICE BRANDING (ISSB)

In an earlier section, it was mentioned that the present-day approach to information security management creates antagonism in the minds of end-users towards information security and information security management in the organisation. This antagonism or negative image of information security influences all exchanges and interactions between information security managers and end-users in the organisation, reducing the effectiveness of all information security efforts. ISSB, as a component of ISSM, attempts to reverse this negativity, by creating a positive image of information security and information security management in the perception of the end-users.

In the context of information security in the organisation, 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 organisation should translate into benefits that would include greater end-user loyalty and compliance with information security policies and controls; an increased effectiveness of awareness, training and education campaigns; a 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. Thus, it is worthwhile to utilise the principles of branding, in order to create a positive image of information security in the minds of the end-users in the organisation.

In the service-branding model of Berry (2000:128-137), 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. The ISSB process is depicted in Figure 2. In the organisation, ISSM executes the ISSB process.

FIGURE 2: ISSB PROCESS


End-user image of the information security service brand
Define the information security service brand
Communicate the information security service brand to end-users
Internalize the brand and organize to deliver security service consistent with the information security service brand
Monitor end-user characteristics and their perception of the information security service brand

Source: Own compilation

8 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 organisation; in other words, what snapshot impression, image, meaning or personality should come to the mind of end-users when they are reminded of information security. The information security service brand could also emphasise the caring and concern that the organisation shows for the information security needs and issues of end-users.

Communicating the brand to end-users, including using word-of-mouth communication to strengthen the information security service brand.

Communicating the brand to end-users requires the creation of deep and broad brand awareness. Keller (2001:14-19) calls this brand salience. In the context of ISSM, it may be said that information security must be in the minds of end-users, and end-users must be able to recall or recognise 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, for example, while handling finances in the organisation.

9 INTERNALISING THE BRAND AND ORGANISING TO DELIVER SECURITY SERVICE CONSISTENT WITH THE ISSB

The brand image in the minds of customers is created primarily by their experiences with the organisation or service. The experiences of customers are largely dependent on the internal organisation, culture and training of the service provider. In the context of information security in the organisation, end-users' experiences with information security management employees, as well as information security policies and controls, have a large impact on the perceptions that end-users will develop towards 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. Internalisation is related to the organisation of ISSM and the design of information security policies and controls. These aspects form part of the ISSS and ISSC components of ISSM. These issues will be discussed later.

10 MONITORING END-USER CHARACTERISTICS AND PERCEPTION OF ISSB, AND USING THIS INFORMATION TO MODIFY THE BRANDING EFFORTS

In the ISSB process, it is vital to monitor the characteristics of end-users in the organisation 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 (2010:13-19) state that different people receive the same message differently, depending on their personality. This indicates that to be successful, any communication programme 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 would probably be more effective than a blanket communication approach. In the context of information security in the organisation, end-users can be segmented in various ways. The segmentation of end-users should provide segments with different requirements, and therefore requiring different treatment.

This section has discussed ISSB, a process for developing the information security service brand in the organisation. The primary objective of ISSB is to reverse the negative perceptions of information security in the organisation, and instead, to create a positive image in the minds of the end-users. The next section will discuss the second component of ISSM, namely ISSS.

11 INFORMATION SECURITY SERVICE SUPPORT

Typically, end-users face significant difficulties when undertaking information security actions in the organisation. These difficulties arise from a variety of factors related to knowledge, skills and attitudes. In this situation, end-users usually have a history of unsuccessful attempts at undertaking information security actions. In the absence of any support or assistance, it is reasonable to expect end-users to feel diffident and to attempt to avoid or bypass information security behaviours.

ISSS seeks to alleviate this problem. It consists of providing support to end-users, as they interact with information security policies and controls in the organisation. End-users seek help, and ISSS supports employees by providing help to the end-users in coping with information security policies and controls in the organisation. This support eases the interactions between end-users and these 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 have the potential to lead to improved compliance by end-users, which in turn should lead to an improved state of information security in the organisation.

Information security in organisations shares some important aspects with general service management. In the domain of information security, it is to be 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 encounters, is an important determinant of customer perceptions of service quality.

Combining these aspects, it may be concluded that end-users in an organisation, as customers of the information security service, have often had dissatisfying service experiences, and that these negative experiences could 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 organisation. This gap can be bridged 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 actions; furthermore, it enhances their perceptions of behavioural control over information security actions, thus, improving their motivation in undertaking such actions.

Once end-users are able to access the support employees, the behaviour of support employees should then determine the success or failure of the ensuing service encounter. 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. According to Bitner, Booms and Mohr (1994:95-106) and Zeithaml, Bitner, Gremler and Pandit (2008), these behaviours can be classified into the following groups:

- Recovery – support employees' response to failures of the information security service, such as security breaches or failures, and difficulty experienced by end-users in working with security policies and controls.
- Adaptability – support employees' response to special needs, preferences or the requests of end-users.
- Spontaneity – unprompted and unsolicited actions by support employees to end-users.
- Coping – support employees' coping with unco-operative or unreasonable end-users.

12 INFORMATION SECURITY SERVICE CULTURE

ISSM represents a shift in the mindset of information security managers and developers in the organisation – away from the present-day firmly entrenched technical approach towards the end-user-centric approach. The ISSC seeks to accomplish this transformation, and to implement the 'Accommodate' element of the CARE principles.

The discipline of information security and the present-day approach to information security management in the organisation is characterised by a highly technical and end-user-unfriendly approach. Issues, such as the usability and acceptability of information security policies and controls have not found much favour with information security managers and developers. Consequently, 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 organisation (Furnell 2010:10-14; Schultz, Procto, Lien & Salvendy 2001:620-634). 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 approach to the formulation of information security policies and controls in the organisation. 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 programmes. Compliance is sought 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.* 2001:620-634).

Schultz *et al*. (2001:620-634) 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 organisation. ISSC remedies this problem by tackling the issue of the mindset of information security managers and developers, which lies at the root of the causal chain. ISSC provides the remedy through shaping the culture of information security managers and developers in the organisation.

The concept of culture holds an important place in organisational management, service management and information security. Davis (1985) defines culture as the *"pattern of shared values and beliefs that give the members of an organisation meaning, and provide them with the rules for behaviour in the organisation"* (Gronroos 2007). Further, service culture arises when all the organisational components, such as *"organisational routines, directions for action given by policies and management and reward systems"* converge together to emphasise good service to customers: whether internal or external.

Culture, as the attitude of its employees, is particularly important for service organisations. Because delivering a service involves the coming together of the employees and their customers, employee attitudes and performance become highly visible to customers. Hence, the attitude of employees, as a reflection of the service culture in the organisation, becomes critically important.

ISSC refers to the culture; and hence, the patterns of shared values and beliefs, amongst the ISSM managers and employees in the organisation. Just as culture and service culture apply to the employees of the organisation, 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 organisation. ISSC becomes visible when end-users come into contact with information security service members and the information security policies and controls in the organisation. Furthermore, as stated above, ISSC can arise only when all the different organisational 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 organisation'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 always play the dominant role.

ISSC is an attempt to align what information security developers and mangers say with what they actually do, that is to align the espoused policy with the enacted programme. In terms of information security, this means that developers and managers must adopt a more end-user-friendly approach, and that the organisation should provide them with the encouragement and resources to do so. This would enable the developers and managers to formulate end-user-centric information policies and controls. 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 organisation.

Leadership is a key aspect in the building of a service culture (Gronroos 2007; Bartley, Gomibuchi & Mann 2007:482-496; Mather 2008:18-19). 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 would be detrimental to establishing an ISSC – if managers do not "walk their talk", then developers too would be unable to deliver end-user centricity.

13 CONCLUSION

This paper began with the objective of proposing an improved alternative to the present-day approach to information security management in the organisation. The paper firstly argued that there is a need for revamping the present-day approach to information security management in the organisation. The present-day approach is technology-focused and bureaucratic in nature. This breeds mutual antagonism between end-users and information security managers in the organisation. The resultant non-compliance by end-users negatively affects the effectiveness of information security policies and controls in the organisation.

This paper has argued that all these problems could be traced back to the root cause – consisting of the information security managers treating end-users as their enemies. According to this paper, the solution lies in adopting an end-user-centric approach to information security management. In this direction, the paper has formulated the CARE principles, which consist of the elements of '**C**ommunicate', '**A**ccommodate' and '**Re**spond'. Adopting the CARE principles could lead to an end-user-centric approach to information security management. The paper has also proposed ISSM as the improved alternative to the present-day approach to information security management.

ISSM is based on the principles of service management; and it treats end-users as the customers, while it becomes the service provider of the information security service. It is believed that this conceptual idea, as argued in this paper, has the potential to successfully address the current end-user dilemma.

REFERENCES

ADAMS A. & SASSE M.A. Users are not the enemy. Commun. *ACM*, 12(1999), 40-46.

ALBRECHTSEN E. A qualitative study of users' view on information security. *Comput. Secur., 4(2007), 276-289.*

ALBRECHTSEN E. 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, 2008.

ALBRECHTSEN E & HOVDEN J. 2009. The information security digital divide between information security managers and users. Comput. Secur., 6: 476-490.

ASHENDEN D. 2008. nformation security management: A human challenge? Inform. Secur. Tech. Rep., 4:195-201.

BARTLEY B, GOMIBUCHI S & MANN R. 2007. Best practices in achieving a customer-focused culture. *Benchmarking: An International Journal*, 4: 482-496.

BASKERVILLE R. 1993. Information systems security: Adapting to survive. *Inform. Syst. Secur.,* 1: 40-47.

BERRY LL. 2000. Cultivating service brand equity. J. *Acad. Market Sci.,* 1:128-137.

BESNARD D & ARIEF B. 2004. Computer security impaired by legitimate users. *Comput. Secur*., 3: 253-264.

BITNER MJ, BOOMS BH & MOHR LA. 1994. Critical service encounters: The employee's viewpoint. J*. Market.,* October*:* 95-106.

CHIPPERFIELD C & FURNELL S. 2010. From security policy to practice: Sending the right messages*. Comput. Fraud Secur.*, 3:13-19.

DAVIS SM. 1985. Managing corporate culture. Cambridge, MA: Ballinger.

DHILLON G. 2001. 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, 2001.

DHILLON G. 2001. Violation of safeguards by trusted personnel and understanding related information security concerns. *Comput. Secur*, 2:165-172.

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. *Pers. Uniquit. Compt*. 6:391-401.

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. *Comput. Fraud Secur.*, 6:10-14.

GONZALEZ JJ & SAWICK AA. 2002. A framework for human factors in information security. Presented at the 2002 WSEAS International Conference on Information Security, Rio de Janeiro.

GRöNROOS C. 1990. Service management: A management focus for service competition. *Int. J. Serv. Ind. Manag.,* 1:6-14.

GRöNROOS C. 1994**.** From scientific management to service management. *Int. J. Serv. Ind. Manag.,* 1: 5-20.

GRöNROOS C. 2007**.** Service management and Marketing: Customer management in service competition. 3rd ed. Delhi, India: Wiley.

ISO/IEC 27000. 2009**.** Information technology - Security techniques - Information security management systems - Overview and vocabulary. ISO/IEC 27000:2009, International Organisation for Standardization and International Electrotechnical Commission, 2009.

ISO/IEC 27001. 2005**.** Information technology - Security techniques - Information security management systems - Requirements. ISO/IEC 27001:2005, International Organisation 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 Organisation for Standardization and International Electrotechnical Commission.

KELLER KL. 2007. Building customer-based brand equity. *Market. Manage.,* 2:14-19.

LINEBERRY S. 2010**.** The Human Element: The Weakest Link in Information Security. Journal of Accountancy. Retrieved October 22, 2010, from http://www.journalofaccountancy.com/Issues/2007/Nov/TheHumanElementThe Weakest LinkInInformationSecurity.htm, 2007.

MATHER J. 2008**.** Creating the service culture. *Hum. Resour.*:18-19.

MORGAN G. 1996. Images of organisation. Thousand Oaks, CA: Sage.

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.

SCHULTZ EE, PROCTO RW, LIEN M & SALVENDY G. 2001. Usability and security: An appraisal of usability issues in information security methods. Comput. Secur., 7: 620-634.

WHITTEN A & TYGAR JD. 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.

ZEITHAML VA, BITNER MJ, GREMLER DD & PANDIT A. 2008**.** Service marketing – integrating customer focus across the firm. 4th ed.. Delhi, India: Tata McGraw-Hill.

ZURKO ME & SIMON RT. 1996. User-centered security. New Security Paradigms Workshop.