Information Security Service Branding – beyond information security awareness

Rahul Rastogi
Institute for ICT Advancement,
Nelson Mandela Metropolitan University, South Africa
rahul.rastogi@eil.co.in

and

Rossouw von Solms
Institute for ICT Advancement,
Nelson Mandela Metropolitan University, South Africa
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 behavior 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. 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 behavioral as well as attitudinal. The behavioral obstacles make it difficult for end-users to undertake 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 obstacles lead to more serious problems as they prevent end-users from even intending or initiating behaviors to comply with the security policies and controls. These attitudinal obstacles manifest themselves as a low level of commitment of end-users which makes them prone to sacrificing security in the pursuit of their work [9]. Attitudinal obstacles arise from the negative image of information security in the minds of end-users. As stated by Chipperfield and Furnell, "one significant challenge is the image of security, in the sense that no one ever really encounters it for a good reason" [7].

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 [18] 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 [5], [7]. In this context, end-users, more often than not, develop a negative image of information security [7]. This leads to a resistance towards information security and an inclination to readily switch from compliance to non-compliance [1], [2], [7], [10], [22].

According to [2], 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. [2]. 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 state that restricting access to information and IT systems can lead to interference in the completion of end-user activities [17]. These "security hindrances" represent the problems faced by end-users as security procedures and controls interfere with their work [17]. In such situations, security is often sacrificed in the pursuit of work [9].

According to [10], 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 [3]. Furthermore, the negative image of information security is further reinforced by the overly technical and admonitory nature of the information security communication such as documentation [3]. 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. This negative image leads end-users 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 [12] and ISO/IEC 27002:2005 [13] emphasize the value of ISA to the effectiveness of information security policies and controls in the organization. According to ISO 27002:2005 [13], 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 [12] 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 [13] 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 behavior of end-users in the organization. According to [19], most organizations treat ISA as consisting of "passing around security guidelines in a factual manner". Albrechtsen terms this present-day ISA approach as "expert-based one-way communication directed towards many receivers" [2]. Chipperfield and Furnell concur and state that the most common approach to ISA in the organization is to provide documented security policy to end-users [7].

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" [19]. Albrechtsen also states that this approach fails as most end-users remain unaffected [2]. Siponen

concludes that an ISA approach based on mere dissemination of information is bound to fail [19]. According to [7], 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) 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"* [4]. AMA 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"* [4]. Various other authors have highlighted the image aspect of a brand through defining associated terms such as "brand image", "brand meaning" and "brand personality". Keller defines "brand image" as "perceptions about a brand as reflected by the brand associations held in consumer memory" [14]. 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 defines "brand meaning" as "what comes immediately to consumers' minds" when the brand is mentioned [6]. 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 [6] presents a model for branding of services, as shown in Figure 1 (from [6]). In Berry's 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 [6].

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. In view of the importance of the brand, organizations need to work consciously towards creating their brand. The service-branding model of Berry [6] was also discussed. The next section discusses ISSB seeking to address the shortcoming of present ISA efforts and provides a framework for branding information security in the organization.

5. INFORMATION SECURITY SERVICE BRANDING

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; and 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.

ISSB consists of applying concepts of service branding to information security. The ISSB process, based upon [6], 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.

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. The ISSB process is depicted in Figure 2. Each of the above steps is discussed in greater detail below.

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.

Communicating the brand to end-users

Communicating the brand to end-users requires creation of deep and broad brand awareness. Keller calls this brand salience [15]. 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 mentions that the communications should include "sub-brands" or specific behaviors e.g. not sharing passwords, and linking them to the overall goals of information security in the organization [15]. This way these specific behaviors 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 behaviors while discrediting improper security practices. Posters, emails, slogans, videos, information security weeks, screen-savers, etc. could be used as the media for communication.

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.

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.

According to [7], 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 [16], segmentation requires a trade-off between costs and effectiveness. A finely grained segmentation will lead to more effective communication but at increased cost. Keller has suggested the following segmentation bases: descriptive or customer-oriented (based on what kind of person the customer is) and behavioral or product-oriented (based on how the customer thinks or uses the product) [16]. Keller has also suggested other segmentation bases that build on brand loyalty. These other segmentation bases include demographic, psychographic and geographic attributes [16].

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 state that end-users in an organization can be differentiated on the basis of their level of commitment to information security [11]. 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 have indicated that different people have different cultural biases and this affects their risk perceptions and approaches to information system risk management [21]. 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.

7. REFERENCES

[1] A. Adams & M.A. Sasse, "Users are not the enemy", **Communications of the ACM**, Vol. 42, No. 12, 1999, pp. 40-46.

[2] E. Albrechtsen, "A qualitative study of users' view on information security", **Computers & Security**, Vol. 26, Issue 4, 2007, pp. 276-289.

[3] E. Albrechtsen & J. Hovden, "The information security digital divide between information security managers and users", **Computers & Security**, Vol. 28, Issue 6, 2009, pp. 476-490.

[4] American Marketing Association. Dictionary [online]. [cited 20 June 2010] Available from Internet: URL http://www.marketingpower.com/_layouts/Dictionary.aspx?dLetter=B

[5] R. Baskerville, "Information systems security: Adapting to survive", **Information Systems Security**, Vol. 2, No. 1,1993, pp. 40-47.

[6] L.L. Berry, "Cultivating Service Brand Equity", **Journal of the Academy of Marketing Science**, Vol. 28, No. 1, 2000, pp. 128-137.

[7] C. Chipperfield & S. Furnell, "From security policy to practice: Sending the right messages", **Computer Fraud & Security**, Vol. 2010, Issue 3, 2010, pp. 13-19.

[8] L. De Chernatony, "Towards the holy grail of defining 'brand'", **Marketing Theory**, Vol. 9, Issue 1, 2009, pp. 101-105.

[9] K.C. Desouza, & G.K. Vanapalli, "Securing Knowledge Assets and Processes: Lessons from the Defense and Intelligence Sectors", **Proceedings of the 38th Hawaii Intrenational Conference on System Sciences**, 2005.

[10] P. Dourish, R. Grinter, J. Delgado de la Flor, & M. Joseph, "Security in the Wild: User Strategies for Managing Security as an Everyday, Practical Problem", **Personal and Ubiquitous Computing**, Vol. 8, No. 6, 2004, pp. 391-401.

[11] S. Furnell, & K.L. Thomson, "From culture to disobedience: Recognising the varying user acceptance of IT security", **Computer Fraud & Security**, Vol. 2009, Issue 2, 2009, pp. 5-10.

[12] 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.
[13] 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.
[14] K.L. Keller, "Conceptualizing, Measuring, and Managing Customer-Based Brand Equity", **Journal of Marketing**, Vol. 57, January, 1993, pp. 1-22.
[15] K.L. Keller, "Building Customer-Based Brand Equity", **Marketing Management**, July/August, 2001, pp. 14-19.
[16] K. L. Keller, **Strategic Brand Management**, 3/e. New Delhi: Prentice Hall of India, 2008.
[17] G.V. Post, & A. Kagan, "Evaluating information security tradeoffs: Restricting access can interfere with user tasks", **Computers & Security**, Vol. 26, Issue 3, 2007, pp. 229-237.
[18] R. Rastogi, & R. von Solms, "A Service-oriented Approach to Information Security Management", **Proceedings of the 7th Annual Conference on Information Science, Technology & Management (CISTM)**, 2009.
[19] M.T. Siponen, "A conceptual foundation for organizational information security awareness", **Information Management & Computer Security**, Vol. 8, Issue 1, 2000, pp.31 – 41.
[20] J.M. Stanton, K.R. Stam, P. Mastrangelo, & J. Jolton, "Analysis of end user security behaviors", **Computers & Security**, Vol. 24, No. 2, 2005, pp. 124-133.
[21] A. Tsohou, M. Karyda, S. Kokolakis, & E.A. Kiountouzis, "Formulating information systems risk management strategies through cultural theory", **Information Management & Computer Security**, Vol. 14, Issue 3, 2006, pp. 198-217.
[22] A. Whitten, & J.D. Tygar, "Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0", **Proceedings of the 8th USENIX Security Symposium**, 1999.

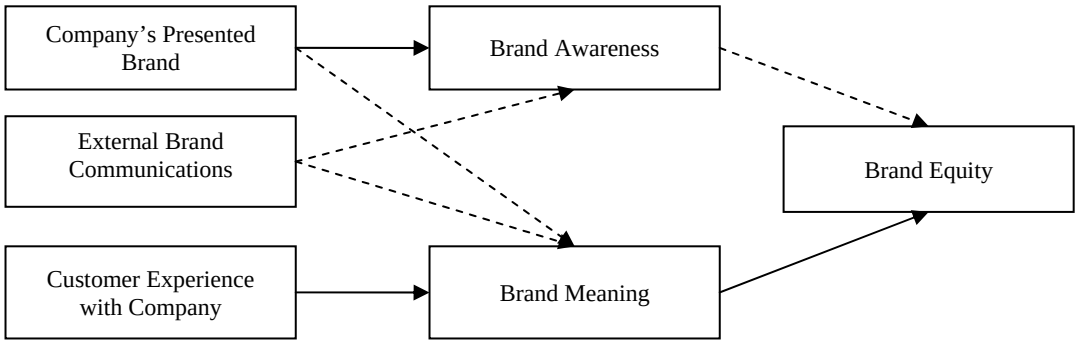

Figure 1: Service Branding Model (from Berry, 2000)

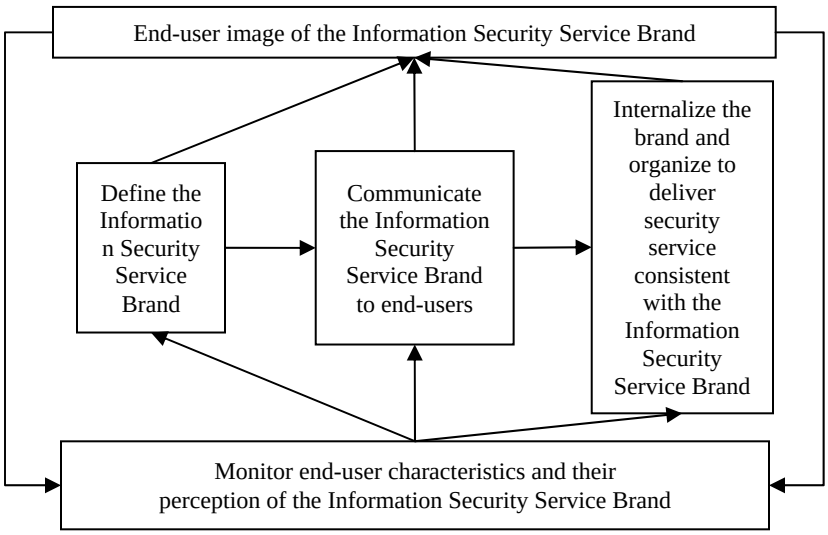

Figure 2: Information security service branding process