Chapter 11
Achieving a Security Culture

Adéle Da Veiga
https://orcid.org/0000-0001-9777-8721
University of South Africa, South Africa

ABSTRACT

A security culture can be a competitive advantage when employees uphold strong values for the protection of information and exhibit behavior that is in compliance with policies, thereby introducing minimal incidents and breaches. The security culture in an organization might, though, not be similar among departments, job levels, or even generation groups. It can pose a risk when it is not conducive to the protection of information and when security incidents and breaches occur due to employee error or negligence. This chapter aims to give organizations an overview of the concept of security culture, the factors that could influence it, an approach to assess the security culture, and to prioritize and tailor interventions for high-risk areas. The outcome of the security culture assessment can be used as input to define security awareness, training, and education programs aiding employees to exhibit behavior that is in compliance with security policies.

INTRODUCTION

The protection of information in an organization is a combined effort of technological, procedural as well as human-related controls (ENISA, 2017). Management that understands the behavioral and cultural aspects of their organization can use it to reduce the risk end-users could pose to information protection (Whittman & Mattord, 2012). One of the human or behavioral controls that organizations can focus on is to inculcate a strong security culture (AlHogail, 2015; ENISA, 2017; Geeling, Brown, & Weimann, 2016). A strong security culture is a culture where information is protected throughout its lifecycle when employees process and interact with it, introducing minimal risk from accidental or ignorant behavior as part of everyday practice in the organization (Da Veiga & Martins, 2015a).

DOI: 10.4018/978-1-6684-3698-1.ch011

A strong or positive security culture in an organization is essential to mitigate risk from a human perspective in order to secure information (AlHogail, 2015; ENISA, 2017). This will contribute to reducing the risk of employee misbehavior, increase the overall security policy and regulatory compliance, improve the organization's security stance and aim to minimize financial loss due to security incidents or breaches related to employee behavior (Mahfuth, Yussof, Baker & Ali, 2017; Van Niekerk & Von Solms, 2010; Verizon, 2017). It is critical to evaluate the security culture continuously and to address identified gaps to improve employees' compliance with security policies and requirements. Organizations can achieve this by regularly conducting an assessment of the security culture, monitoring the change and implementing corrective actions to influence the culture positively (Da Veiga & Martins, 2015a).

This chapter defines the concept of a security culture in the context of an information security and cybersecurity culture. An overview of the development of it in an organization is discussed, focusing on the internal factors that could potentially influence the security culture. A security culture assessment approach is discussed with practical advice to roll out such an assessment in an organization. The emphasis is on understanding what the as-is security culture is in order to implement corrective actions to influence it positively. Examples are given of how to analyze the data, which management can use to define change management plans using methods such as awareness, training and education.

Defining a Security Culture

A security culture can be seen as the unconscious manner in which things are done in an organization to secure information. Every organization has a security culture, which is a subculture of the wider organizational culture (Da Veiga & Martins, 2017; Hayden, 2016; Schlienger & Teufel, 2003; Van Niekerk & Von Solms, 2005). The security culture can be explained as the "way things are done" in the organization to secure information. The way things are done by employees are underpinned by their assumptions, values, beliefs and attitudes (Schein, 1985, Van Niekerk & Von Solms, 2005), which is described as, "the way an organization functions as a sort of collective unconscious for the organization" (Hayden, 2016, pp. 44).

The manner in which employees undertake to protect information when they process it, is based on their shared tacit assumptions, as formed by their beliefs and values, and relates to the motivation for their decisions (Da Veiga & Eloff, 2010; Van Niekerk & Von Solms, 2006). The espoused values such as honesty and fairness form over time and relate to what employees believe should be done to protect information (Da Veiga & Martins, 2015b; Van Niekerk & Von Solms, 2006). The security culture of an organization is visible in tangible aspects of the organization, which are referred to as artifacts, underlined by the values of the organization. These tangible aspects could relate to the security policies and related training sessions, an incident-reporting or helpline, monthly awareness e-mails, the use of technology such as digital certificates for e-mail and so on (Okere, Van Niekerk, & Carroll, 2012; Schein, 1985; Schlienger & Teufel, 2003).