

available at [www.sciencedirect.com](http://www.sciencedirect.com)journal homepage: [www.elsevier.com/locate/cose](http://www.elsevier.com/locate/cose)
**Computers  
&  
Security**


# Organisational security culture: Extending the end-user perspective

A.B. Ruighaver\*, S.B. Maynard, S. Chang

Department of Information Systems, University of Melbourne, Australia

## ABSTRACT

### Keywords:

Security culture  
Organisational culture  
Security governance  
Motivation  
Risk analysis

The concept of security culture is relatively new. It is often investigated in a simplistic manner focusing on end-users and on the technical aspects of security. Security, however, is a management problem and as a result, the investigation of security culture should also have a management focus. This paper describes a framework of eight dimensions of culture. Each dimension is discussed in terms of how they relate specifically to security culture based on a number of previously published case studies. We believe that use of this framework in security culture research will reduce the inherent biases of researchers who tend to focus on only technical aspects of culture from an end-users perspective.

© 2006 Elsevier Ltd. All rights reserved.

## 1. Introduction

It was not until the start of this century that researchers first began to recognise that an organisation's security culture might be an important factor in maintaining an adequate level of information systems security in that organisation (Schwarzwalder, 1999; Breidenbach, 2000; Von Solms, 2000; Andress and Fonseca, 2000; Beynon, 2001). None of these authors, however, presented a clear definition of what they meant with "a security culture", nor were there any clear views on how to create this organisational culture to support security.

In the last few years, research in this new area of (information) security culture has been expanding rapidly. Unfortunately, a lot of this research still has a limited focus and often only concentrates on the attitudes and behaviour of end-users as well as on how management can influence these aspects of security culture to improve the end-user's adherence to security policies (Schlienger and Teufel, 2002; Ngo et al., 2005). Schlienger and Teufel (2003) more or less defines

security culture as "all socio-cultural measures that support technical security measures", which not only limits its focus to a small sub-dimension of information security, but also enforces the old belief that information security is mostly a technical problem. Information security is, in general, a management problem and the security culture reflects how management handles this problem. Subsequently, we will argue that technical security measures and security policies will often need to be (re)designed to support an organisation's security culture.

In this paper we propose that security policy development is just one of the areas that will be influenced by an organisation's culture. Nosworthy (2000), for instance, states that an organisation's culture has a strong influence on organisational security, as it may 'hinder change'. Borck (2000) states that 'beyond deploying the latest technology, effective security must involve the corporate culture as well'. There is strong suggestion from the literature that the study of security culture cannot be carried out in isolation of wider organisational culture. For example, in their review of organisational

\* Corresponding author.

E-mail addresses: [anthonie@unimelb.edu.au](mailto:anthonie@unimelb.edu.au) (A.B. Ruighaver), [seanbm@unimelb.edu.au](mailto:seanbm@unimelb.edu.au) (S.B. Maynard), [shanton.chang@unimelb.edu.au](mailto:shanton.chang@unimelb.edu.au) (S. Chang).

0167-4048/\$ – see front matter © 2006 Elsevier Ltd. All rights reserved.

doi:10.1016/j.cose.2006.10.008

behavioural studies, Mowday and Sutton (1993) point out that contextual factors play a significant role in influencing individual and group behaviours within organisations. The contextual factors here often reflect the organisation's culture.

In the following sections we will describe how we used Detert et al.'s (2000) framework of eight 'overarching, descriptive culture dimensions' to explore the security culture within quite a few organisations with vastly different levels of security. As several of these case studies have been published previously (Shedden et al., 2006; Maynard and Ruighaver, 2006; Koh et al., 2005; Tan et al., 2003; Chia et al., 2003, 2002), we will concentrate on the resulting insights that these case studies have given us into each of these dimensions of an organisational security culture.

## 2. Exploring organisational security culture

Our initial research in organisational security culture adopted a framework with eight dimensions from Detert et al. (2000). Detert et al. (2000) synthesised the general dimensions of organisational culture using current organisational culture research on areas such as Organisational Culture and Leadership (Schein, 1992), Competing Values (Cameron and Freeman, 1991) and Organisational Culture Profile (Klein et al., 1995). Detert et al. (2000) illustrate their framework by linking it to a set of values and beliefs that represent the 'cultural backbone' of successful Total Quality Management (TQM) adoption. For a group of security experts with limited initial knowledge of organisational culture, this clear description of the cultural aspects of TQM convinced us of the power of this framework in exploring security culture. The eight dimensions of organisational culture are briefly identified in Table 1.

## 3. Interpreting organisational security culture

In the remainder of this paper we give our current views of what the important aspects are of security culture for each of these dimensions. These views have been constructed over a number of years and have been influenced by the case studies the authors have completed in various aspects of security including governance and security culture (Shedden et al., 2006; Maynard and Ruighaver, 2006; Koh et al., 2005; Tan et al., 2003; Chia et al., 2003, 2002). In some of the case studies, the security culture was observed as part of understanding other aspects of security, whilst in others, there was a specific focus on the security culture of the organisation. While a few of our case studies have been in organisations that have a high level of security enforced by a strict enforcement of rules and regulations, the majority of our research has been in organisations where decision making about security is distributed and loosely controlled. Whilst this may have slightly coloured our views expressed below, the inclusion of organisations with strict security as well as those with less strict security allows this research to be informed by different organisation types and thus different types of organisation and security culture.

The rest of this section uses each of the dimensions of the security culture model to describe the important aspects of security culture.

### 3.1. The basis of truth and rationality

What we initially considered to be our most important findings in our early research on security culture related to how the importance of security for the organisation is seen by the employees and the organisation as a whole. Obviously, different organisations need different levels of security, but although the security requirements for a particular company may not be as high as the security requirements of other companies, achieving optimal security for that organisation's particular situation will still be important; as is the need to ensure that their employees believe that security is important. While the literature on security culture recognizes that the most crucial belief influencing the security in the organisation is the belief, by both employees and by the organisation itself, that security is important (Connolly, 2000), not much is mentioned about the importance of the other beliefs that an organisation may have about security.

After more extensive research (Shedden et al., 2006), we found that any beliefs that the decision makers within the organisation have about the quality of security, and about the quality of the different processes used to manage security, are often much more important than the end-user's beliefs about security. Many of the organisations investigated, whether they have low or high security requirements, believe that their security is good. However, most of these organisations do not really make any attempt to evaluate the quality of their security, or even attempt to measure its success, except anecdotally. Similar problems exist with the organisations' beliefs about the quality of their risk analysis and security audits.

In those case study organisations where there is a high degree of security, the assessment of the quality of security tends to focus on the trust of the extensive security processes in terms of policy and procedures. However, in those organisations with less emphasis on security it is clear that their assessment that the security within the organisation is good, may often be flawed. Even though they have a lower requirement for security these organisations tend to treat security spending as a cost to the organisation, and it often is a struggle to gain funding for security initiatives as a result. This tends to send out conflicting messages to employees. On one hand, management states that security is important to the organisation, however, on the other hand, it is not willing to support and fund security initiatives. Thus a conflict may occur as to what is the truth in the organisation regarding security.

The quality of a security culture should, however, not only be determined by the beliefs that an organisation has, but more by how the organisation evaluates and manages the basis of truth and rationality in the various beliefs that end-users and managers hold about that organisation's security. Staff being critical about their own beliefs and an organisation having processes in place to challenge the quality of the beliefs of its employees is what distinguishes a good security culture from a bad one.

Download English Version:

<https://daneshyari.com/en/article/454636>

Download Persian Version:

<https://daneshyari.com/article/454636>

[Daneshyari.com](https://daneshyari.com)