Available online at www.sciencedirect.com

SciVerse ScienceDirect

journal homepage: www.elsevier.com/locate/cose

Computers & Security

CISOs and organisational culture: Their own worst enemy?

Debi Ashenden [a,*], Angela Sasse [b]

[a] Cranfield University, Informatics & Systems Engineering, Defence Academy of the UK, Shrivenham, Swindon SN68LA, United Kingdom
[b] Dept. of Computer Science, University College London, United Kingdom

ARTICLE INFO

Article history:
Received 9 January 2013
Received in revised form
4 September 2013
Accepted 9 September 2013

Keywords:
Security awareness
Human factors
Information security management
Organisational culture
Discourse analysis

ABSTRACT

Many large organisations now have a Chief Information Security Officer (CISO[1]). While it may seem obvious that their role is to define and deliver organisational security goals, there has been little discussion on what makes a CISO able to deliver this effectively. In this paper, we report the results from 5 in-depth interviews with CISOs, which were analysed using organisational behaviour theory. The results show that the CISOs struggle to gain credibility within their organisation due to: a perceived lack of power, confusion about their role identity, and their inability to engage effectively with employees. We conclude that as the CISO role continues to develop CISOs need to reflect on effective ways of achieving credibility in their organisations and, in particular, to work on communicating with employees and engaging them in security initiatives. We also identify a key responsibility for effective CISOs; that is to remove the blockages that prevent information security from becoming 'business as usual' rather than a specialist function. For researchers, our findings offer a new piece of the emerging picture of human factors in information security initiatives.

1. Introduction

Information security aims and objectives need to be aligned with formal business processes as well as organisational culture (Dhillon and Backhouse, 2001). As a result of standards such as ISO 27001 information security is often incorporated into business processes, however, it is a more complex problem to align information security with organisational culture. Organisational culture comes into being in the gaps within and between formal business processes and takes the shape of employee values, beliefs and assumptions (Schein, 2004) about what are acceptable short cuts, workarounds, or informal ways of working in the organisation.

CISOs have traditionally taken an authoritarian stance when trying to realise information security aims (Dhillon and Backhouse, 2001). This approach can work well in organisational hierarchies (particularly in the armed forces and the police) but we are seeing an increase in flatter and more open organisational structures that are at odds with this approach. In recent years end users have been recognised as the weakest link in the security chain and this has led to significant changes in the role of the CISO.

To a large extent, protecting information depends on change management, in particular persuading employees of the need to behave securely. This, in turn, depends on how the need for change is communicated, and received, by employees who are

[*] *Corresponding author*. Tel.: +44 (0)1793785479.
E-mail address: d.m.ashenden@cranfield.ac.uk (D. Ashenden).
[1] CISO – Chief Information Security Officer.

0167-4048/$ – see front matter © 2013 Elsevier Ltd. All rights reserved.
http://dx.doi.org/10.1016/j.cose.2013.09.004

on the front line of information security. As a result many CISOs are now expected to develop an organisational culture that supports information security by implementing successful security awareness programmes. These relatively new aspects of the role require CISOs to be successful change agents. To do this they need to be able to reflect on, and understand, the impact of their role on organisational culture.

There has been little information security research that helps us to understand the impact of the CISO on organisational change. Research in the field of management studies, however, has identified key resources that need to be available to a change agent in order for them to be successful. These resources include: expertise, credibility (this includes stature and prestige in the organisation), political access to senior management and control of rewards and sanctions (Hardy, 1996).

While successful CISOs will seek to understand the attitudes of end users towards information security there is little evidence that they reflect on their own attitudes and behaviours and how these contribute to the success or failure of change initiatives. The purpose of this research therefore is to start this reflective process and to reveal the strengths and weaknesses of CISOs in building a culture of information security. In this study we aim to understand whether the CISO is likely to be an effective change agent for organisational culture.

The research comprised five in-depth interviews in a range of organisations and included both the public and private sector. The interviewees were senior managers responsible for ensuring the security of information within their respective organisations. The interviews were semi-structured around a map of topics related to information security awareness and communication. The methodological approach was qualitative and analysed the discourse of the interviewees. The theoretical framework used for the analysis was a model developed within organisational behaviour research to understand the role of discourse in changing organisational culture.

The substantive aim of the research was to understand CISOs' perceptions and attitudes that would impact on their ability to change behaviour within the culture of their organisations. The methodological aim was to assess whether a qualitative, discourse analytic approach would yield an understanding of CISOs' perceptions and attitudes and to test a validated approach from organisational behaviour by applying it to information security.

This paper starts with a brief review of related work in the field of information security and defines the contribution that organisational behaviour makes to the effective delivery of information security messages. The research method is described along with the analytical approaches used to interpret and frame the results. The results of the research follow, together with a discussion of the results. Finally the paper concludes by outlining the implications of the research and the contributions made.

2. Background and related work

Information security researchers have recognised the importance of addressing the informal processes within organisations that often undermine the documented and approved formal processes. Such informal processes are largely determined by the organisational culture. A small number of researchers have repeatedly suggested that there is a need to achieve a better understanding of the social aspects of the organisation; in particular the human element (Dhillon, 1995; Dhillon and Backhouse, 2001). While this has been explored at a conceptual and theoretical level (Thomson and Von Solms, 2005; Siponen, 2001) there are very few empirical studies (Adams and Sasse, 1999; Albrechtsen, 2007).

Conceptual studies have used theories from psychology and marketing to build models and frameworks and develop guidelines for the design and implementation of security awareness programmes (Siponen, 2000, 2001). Research has also been carried out examining information security behaviours, attitudes and organisational culture conceptually (Thomson & von Solms, 2005; Helokunnas and Kuuisisto, 2003) but there has been no empirical research that focuses on the role of the CISO as a change agent. Albrechtsen's (2007) research, however, showed that CISOs tend to use a one-way model of communication with end users – pushing information out but not listening to what is communicated back or exploring how their messages are received.

The failure of a one-way model of communication has been highlighted in other fields by Wertsch (2001) who criticises the unidirectionality of the flow of communication in Reddy's Transmission Model of Communication in which the receiver is passive and there is no feedback loop between the sender and receiver. Albrechtsen's (2007) research suggests that users want a 'user-involving approach' to security awareness and that, 'Mass-media based awareness campaigns, have, according to the interviewed users, no significant long-term effects on users' behaviour and awareness' (p. 286). As Adams and Sasse (1999) point out, insufficient communication with employees, 'causes them to construct their own model of possible security threats and the importance of security and these are often wildly inaccurate' (p. 43). From this we can perhaps conclude that it is communication of the right type that is most important.

Our research uses discourse analytic techniques to examine the ways that CISOs communicate information security requirements. This approach has its roots in social psychology, and is increasingly being valued in organisational studies as a way to get beneath the formal structures in an organisation and to understand the importance of the underlying social dynamics. Discourse analysis is the term given to a range of analytical techniques that explore language in use in specific contexts. It differs from content analysis in its attention to the role of context in the way language is used. This turn to language has been a feature of organisational research in recent years (Oswick et al., 2000; Alvesson and Karreman, 2000; Hardy, 2001; Grant et al., 2005) and has been used, albeit infrequently, in information systems research (Heracleous and Barrett, 2001).

The key characteristics of discourse analysis are that it is anti-realist and constructivist (Bryman, 2001). Anti-realism is the belief that there is no external reality waiting to be discovered by the researcher because reality comes into being through the use of language. Discourse analysis is constructivist in a number of ways. Firstly, language constructs and reproduces versions of the social world (Saunders et al., 2007)