# Organizational Security Culture: More Than Just an End-User Phenomenon

Anthonie B. Ruighaver and Sean B. Maynard

Department of Information Systems
University of Melbourne, Australia
{anthonie, seanbm}@unimelb.edu.au

**Abstract.** 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 discusses security culture based on an organisational culture framework of eight dimensions. 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.

## 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 organization [1]. None of these early researchers, however, presented a clear definition of what they meant with "a security culture", nor were there any clear views on how to create this organizational 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 [2]. Schlienger et al [3] 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 argue that technical security measures and security policies will often need to be (re)designed to support an organisation's security culture.

Please use the following format when citing this chapter:
Author(s) [insert Last name, First-name initial(s)], 2006, in IFIP International Federation for Information Processing, Volume 201, Security and Privacy in Dynamic Environments, eds. Fischer-Hubner, S., Rannenberg, K., Yngstrom, L., Lindskog, S., (Boston: Springer), pp. [insert page numbers].

## 2 Exploring Organizational Security Culture

Our initial research in organisational security culture [4] adopted a framework with eight dimensions from Detert et al [5], who had illustrated their framework by linking it to a set of values and beliefs that represent the 'cultural backbone' of successful Total Quality Management (TQM) adoption. These eight dimensions of organizational culture are briefly identified in Table 1.

**Table 1.** The Organizational Culture Framework [5].

| |
|---|
| 1. **The Basis of Truth and Rationality** |
| 2. **The Nature of Time and Time Horizon** |
| 3. **Motivation** |
| 4. **Stability versus Change/Innovation/Personal Growth** |
| 5. **Orientation to Work, Task, Co-Workers** |
| 6. **Isolation versus Collaboration/Cooperation** |
| 7. **Control, Coordination and Responsibility** |
| 8. **Orientation and Focus – Internal and/or External** |

In the remainder of this paper we give our current views of what the important aspects are of security culture in each of these dimensions. 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. This may have slightly coloured our views expressed below.

### 2.1 The Basis of Truth and Rationality

What we initially considered our most important findings in our early research on security culture related to how the importance of security for the organization is seen by the employees and the organization as a whole. Obviously, different organizations 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 organization'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 organization is the belief that security is important [6], not much is mentioned about the importance of other beliefs. We found that the beliefs of the decision makers within the organisation 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-users beliefs. Many of the organizations that we

investigated do, for instance, believe that their security is good. But most organizations did not make any attempt to evaluate the quality of their security. Similar problems seem to exist with their beliefs about the quality of their risk analysis and security audits.

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.

### 2.2 Nature of Time and Time Horizon

As literature already indicated [7], we found that all too often the security focus of an organisation is on things demanding immediate attention, not on the things that may prove more important in the long run. If an organisation had any long-term goals, these only covered a time frame of one or two years and were simply aimed at building a security infrastructure in line with International Security Standards.

While we argue that organisations with a high-quality security culture should place an emphasis on long-term commitment and strategic management, we found no good examples in practice. Unfortunately, there is not much discussion in literature on possible long-term strategies either. There seems to be a tendency, however, to completely overhaul security management/governance structures when current security is no longer adequate and/or becomes too expensive to maintain. Once again, we did not find any evidence that those initiating this restructuring have even considered what long-term strategies and plans can or should be developed and by whom.

### 2.3 Motivation

Organisations with a good security culture need to have appropriate processes in place to ensure employees are motivated in relation to security. While literature suggests that employees need to learn that security controls are necessary and useful to discourage them from attempting to bypass these controls [8], motivation should not only be aimed at ensuring that an employee's behaviour is not compromising IS security. Unfortunately, security is one of the few areas in organisational culture where punishment still plays a large role and where active participation in achieving goals is rarely encouraged.

### 2.4 Stability versus Change/Innovation/Personal Growth

In organisations that have a high requirement for security, we found a tendency to favour stability over change. Change is often seen as bad, as it can result in the introduction of new risks or in the invalidation or bypass of controls to existing risks.

However, although change should be carefully managed, security is never 100% and organisations need to ensure that their security posture is not static.

While most organisations that have lower requirements for security do not have this "fear" of change, they often fail to realize that an organisation's security procedures and practices need to improve continually, and that the organisation will need to constantly adapt its security to the inevitable changes in the organisation's environment. Organisations that have adopted a security policy lifecycle methodology will have a culture of continuous change in that area of security, but it is not clear whether this will extend to other areas such as security strategy development and security governance processes, or even implementation of security measures.

### 2.5 Orientation to Work, Task, Co-workers

An important principle in information security is that there is always a trade-off between the use of an organisation's assets and their security. By limiting access to an asset, we can significantly improve its security. However, limiting access can sometimes result in a serious impediment to the daily operations of employees. Finding a balance between security and how constrained employees feel in their work is therefore an important aspect of a security culture. Of course, staff will feel less restricted if they are motivated and feel responsible for security

While it is obvious that employees should be made to feel responsible for security in the organisation, it is just as important that staff responsible for particular security areas have as strong sense of ownership [9]. Both can be negated easily when staff feels that management does not take any suggestions for the improvement of security seriously. Hence, a positive response from management and a continuous adaptation of security practices to at least some of the suggestions may not only help improve security itself directly but also help improve the orientation of staff towards security.

### 2.6 Isolation versus Collaboration/Cooperation

We have been surprised in how often we encountered that an organisation's security planning and implementation was handled by only a small group of specialists and managers. While organisations often realise that security policies should be created collaboratively using the input of people from various facets of the organisation to ensure its comprehensiveness and acceptance, they tend to ignore that principle in the day to day management of security. As a result, the efforts of the security management team are often negated by other decisions taken by managers in the business units and on the work floor.

Our current research in security governance processes and structures at the middle management level [10] is indicating that this lack of collaboration with the stakeholders in the day to day decision making on security is not only likely to negatively impact motivation and orientation to work, but may often also lead to a dangerously narrow focus of security. As coverage is just as important in information security as the quality of the selected security controls, ignoring particular areas such as personnel security or data security can lead to a significant collapse of an organisation's security posture.

### 2.7 Control, Coordination and Responsibility

This dimension of an organization's security culture is clearly related to the security governance in that organization and has been the main reason that our security group extended its research from security culture to security governance. The primary feature of security governance in an organization is whether there is a tight control or loose control. An organization with centralized decision making has a tight control, while an organization that has flexible decentralized decision making is likely to have a loose control, although change management processes may still influence how loose the control actually is.

It should be clear that security culture is not independent from organizational culture, so tight control of security in an otherwise loosely controlled organization is not likely to work very well. We believe that this lack of alignment between organizational culture and intended security culture is often one of the major reasons why acceptable use policies fail.

It does not matter whether there is a tight control or a loose control of security, it is still essential that there are clear guidelines on who has decision rights in the different areas of security and when. This aspect is often called responsibility and ensuring that all responsibilities have been assigned is a required feature of any strategic security policy.

With responsibility comes accountability. We believe that an important aspect of the security culture is how the organization handles accountability for decisions in security management. Lack of even the most simple accountability processes, such as simple feedback loops where decisions are discussed with higher levels of management, is a fairly common occurrence in security management.

### 2.8 Orientation and Focus – Internal and/or external

The orientation and focus of an organization's security clearly depends on the environment in which the organization operates. If the organization is forced to conform to external audit and government requirements, the emphasis of their risk management processes is often only on meeting these requirements, not on improving their security. Other organizations aim to bring their IS security in line with international industry standards and, again, the emphasis is often geared towards passing an audit to prove that they have achieved this goal, rather than on achieving the best security for the organization within the obvious limitations of resources and budget.

As security in an organisation is influenced by both external factors and internal needs, we believe that an ideal security culture has a balance between an internal and external focus. The external focus should at least include an awareness of the organisation's external security environment and how this changes over time. This will allow the organisation to pro-actively meet any new threats. Just as important, however, is that the organisation builds up an awareness of its internal security environment. If the organisation is not trying to identify what security breaches occur and why they occur, it will never know if its security strategies are working and how it can improve the implementation of these strategies.

## 3 Conclusion

While there has been an abundance of research in the area of organizational security and how it should be improved, the majority focuses only on certain discrete aspects of security and not how these aspects should be assimilated into an organisation's culture. Even our own research in security culture initially had a clear bias to end-user issues. However, the broad framework we adopted from organisational culture research has ensured that we not only recognised this bias in our research, but also provided insight in how to extend our research in new areas such as security governance and risk assessment.

In investigating security cultures in organisations, we have often found that many specific aspects of a security culture, such as attitudes, norms, and shared expectations do not fit nicely within a single dimension of our framework. It is obvious that the concept of a security culture is too complex to be covered by a single framework or model. We do believe, however, that any researcher involved in investigating any aspect of an organisation's security culture will find the use of this framework essential in ensuring that they take a comprehensive view of how the many dimensions of an organisation's security culture relate to that particular aspect they are interested in.

## References

1. Von Solms, B.: Information Security - The Third Wave? Computers and Security, Vol. 19. No. 7. (2000) 615-620.
2. Schlienger, T. and Teufel S.: Information Security Culture - The Socio-Cultural Dimension in Information Security Management. IFIP TC11 International Conference on Information Security, Cairo Egypt (2002).
3. Schlienger, T. and Teufel, S.: Analyzing Information Security Culture: Increased Trust by an Appropriate Information Security Culture. 14th International Workshop on Database and Expert Systems Applications (DEXA'03), Prague Czech Republic (2003).
4. Chia, P. Maynard, S., Ruighaver, A.B.: Understanding Organisational Security Culture. In Information Systems: The Challenges of Theory and Practice, Hunter, M. G. and Dhanda, K. K. (eds), Information Institute, Las Vegas, USA. (2003) 335–365.
5. Detert, J., R. Schroeder & J. Mauriel.: A Framework For Linking Culture and Improvement Initiatives in Organisations. The Academy of Management Review, Vol. 25. No. 4. (2000) 850-863.
6. Conolly, P.: Security Starts from Within. InfoWorld, Vol. 22. No. 28. (2000) 39-40
7. Wood, C.: Integrated Approach Includes Information Security. Security, Vol. 37. No. 2. (2000) 43-44.
8. Lau, O.: The Ten Commandments of Security. Computers and Security, Vol. 17. No. 2. (1998) 119-123.
9. Koh, K. Ruighaver, A.B. Maynard, S. Ahmad, A.: Security Governance: Its impact on Security Culture. 3rd Australian Information Security Management Conference, Perth Australia (2005).
10. Tan,T.C.C. Ruighaver, A.B.: Developing a framework for understanding Security Governance. 2nd Australian Information Security Management Conference, Perth Australia (2004).