UNDERSTANDING ORGANISATIONAL SECURITY CULTURE.

P. A. Chia

Department of Information Systems
University of Melbourne
Victoria 3010
Australia

A.B. Ruighaver

Department of Information Systems
University of Melbourne
Victoria 3010
Australia
anthonie@unimelb.edu.au

S.B. Maynard

Department of Information Systems
University of Melbourne
Victoria 3010
Australia
seanbm@unimelb.edu.au

ABSTRACT

Based on a research model borrowed from organisational culture we conducted two explorative case studies to investigate how we can evaluate and improve the quality of the security culture in organisations. In this paper we described the differences in the security culture of these two organisations, and how their culture relates to their widely different security requirements. We identified two major problems with the security culture of one organisation, which according to anecdotal evidence will be commonly found in mainstream organisations with a low-level of security. We suggest that by being aware of these problems, and of the possible solutions we propose, these organisations will be able to significantly improve their security culture.

1. INTRODUCTION

Many researchers contend that the security culture in an organization is important [Sizer and Clark, 1989; Schwarzwalder, 1999; Breidenbach, 2000; von Solms, 2000; Andress and Fonseca, 2000; Clark-Dickson, 2001; Beynon, 2001], but none of these authors present a clear definition of what they mean with “a security culture”. Correspondingly, there has also been little research in the area of how to evaluate the security culture in an organisation.

Security continues to be and probably will always be a people problem, both from an end-user and a security management point of view. While security training is essential because 'users react more positively to security requirements if they understand them' [Hartley, 1998], Nosworthy suggests that this training on the awareness of security should be ongoing and must encourage and motivate people to be secure in their day-to-day operations [Nosworthy, 2000]. Without an appropriate security culture to support end-user security, however, both this expensive training and the original investment in the security infrastructure may be wasted.

As we could not find any significant research to date that has confronted assessing and improving the quality of organisational security from a cultural perspective, we chose to approach these issues through a few explorative case studies based on a general framework of organisational culture developed by Detert, Schroeder and Mauriel [Detert et al, 2000]. Detert et al. developed their framework by reviewing existing culture frameworks and using qualitative content analysis to organise them into 'eight overarching, descriptive dimensions of culture'.

In this paper we use Detert's framework to explore the difference in the organisational security culture between two organisations that are operating at almost the opposite ends of the scale where their levels of security implementation is concerned. The first organisation is offering a product in the IS security industry itself and has, in order to get accreditation, implemented a very high level of security. The second organisation is more in the main stream and is believed to be representative for those organisations that feel no need to implement more than just a basic level of security.

The next section will first provide a brief overview of the security culture we found in each of these two organisations, and is followed by an extensive comparison of the differences in security culture between the two companies. Presenting the full case study of each organisation is not possible within the limits of this publication, but we hope to publish a more extensive description of each case later. This paper will concentrate on the lessons learned from contrasting the security culture in these two organisations and offer suggestions on how organisations with fairly low requirements for IS security should still be able to achieve an acceptable security culture.

2. THE ORGANISATIONS

At indicated before, the organisations were chosen because one was considered to be extremely secure (Organisation A), while the other was considered less secure (Organisation B). After obtaining the approval from management, we selected three people within each organisation from different levels and areas. Interviews were approximately one hour in length and were taped. Most interviews were held inside the organisations, to ensure some of the security in place at each organisation was observed first-hand. For security reasons, not much documentation could be viewed from either organisation. However, a security induction presentation from Organisation A and a draft security policy from Organisation B were viewed.

Organisation A is a small organisation with less than fifty employees with three offices around Australia. It is a leading player in the encryption market place. Its involvement in the security industry without doubt influences the awareness of security in the organisation and, on visiting Organisation A, it was evident that there were very tight security procedures in place. For security reasons, no participants from lower levels of the organisation could be

interviewed. We believe this has not affected the results of the study, but it does represent an interesting aspect of the security culture present at Organisation A.

Although the security culture at Organisation A is fairly tightly regulated, with many strict policies and procedures in place, there is also an emphasis on trusting employees to be responsible for maintaining the security. There is a balance of long-term and short-term security goals and security awareness is promoted through informal meetings. A strong emphasis on change is prevalent and although security measures may frustrate the employee, it is widely accepted that these measures are justified. There is a strong enforcement of security from top management, but security is also seen as a collaborative effort with a strong external focus.

At the end of each interview, the employees were asked about their views on their organisation's security culture:

> 'Very strict'
>
> Person A
>
> 'Probably larger, if you can quantify it in that way, it's bigger than most companies, whether it's consciously or subconsciously, it's always drummed into people, because we are a security company, we pride ourselves on security and everyone is aware of security , so it's pretty high'
>
> Person B
>
> 'Sometimes it's a pain in the bum to try and get from place to place…...but we trust each other as individuals, and therefore we're pretty serious about security….''
>
> Person C

Organisation B is in the Finance/Insurance industry. It is significantly larger than Organisation A, with about three thousand employees in Australia, and about 55,000 employees globally. Organisation B's headquarters are overseas, from which a lot of their security initiatives are dictated. Until last year there was no formalised security function, but recently a security committee has been formed to coordinate the development of a security infrastructure in line with international industry standards.

Although there are good intentions for security at Organisation B, these are hindered by lack of budget and lack of support from Executive management. The new security committee is made up of five to six people from different areas of the organisation and they intend to meet up at least once a quarter, depending on what is required. However, convincing the two executives on the security committee to support security financially is still quite difficult.

For such a large organisation there are only a small number of people coordinating security. There remains to be a short-term focus and, rather than being pro-active, the organisation is still very reactive to security problems. Due to the lack of security processes in place, employee motivation to embrace security is hindered and employees do not on the whole feel responsible for security.

> 'The culture does not fit with normal security cultures. The culture within IT is different as they understand what could happen but people in the business don't'
>
> Person D

'I think that as a culture, they're probably very immature when it comes to things like security, they don't really understand the impact. I don't think that they are really listening to what's happening out there in the world when people breach security. And let's face it, they can bring a company down very quickly'

Person E

'I think that we've got a reasonable security culture, I'd acknowledge that we could tighten it up, but the standards that we've had in the past would be inappropriate for the future because technology's changing….there's a constant need to upgrade it'

Person F

3. COMPARING THE SECURITY CULTURE

The eight dimensions of organisational culture as developed by Detert et al (2000) are briefly identified in table 1. Our discussion of the difference in security culture between the two organisations will follow the general structure of this framework, but will attempt to re-focus each dimension on issues related to security.

1. The Basis of Truth and Rationality

What employees in an organisation believe is real or not real, and how what is true is ultimately discovered. This may affect the degree to which people adopt either normative or pragmatic ideals.

2. The Nature of Time and Time Horizon

The time horizon that an organisation takes affects whether or not leaders and other organisational members adopt long term planning and goal setting, or focus primarily on the here-and-now.

3. Motivation

What motivates humans and whether people are motivated from within or by external forces. Whether people are inherently good or bad, whether people should be rewarded or punished, and whether manipulating others' motivation can change effort or output.

4. Stability versus Change/Innovation/Personal Growth

Some individuals are open to change (risk-takers), whereas other individuals have a high need for stability (risk-averse). Risk-taking organisations are said to be innovative with a push for constant, continuous improvement. Risk-averse organisations focus on 'not rocking the boat'.

5. Orientation to Work, Task, Co-Workers

The centrality of work in human life and the balance between work as a production activity and as a social activity. Some individuals view work as an end in itself with a 'task focus', concerned fundamentally with work accomplishment and productivity. Other individuals see work as a means to other ends, such as having a comfortable life and developing social relationships.

6. Isolation versus Collaboration/Cooperation

Underlying beliefs about the nature of human relationships and about how work is most effectively and efficiently accomplished, either by individuals or collaboratively.
7. Control, Coordination and Responsibility
Organisations vary in the degree to which control is concentrated or shared. Where control is 'tight', there are formalised rules and procedures that are set by a few, to guide the behaviour of the majority. Where control is 'loose', there is flexibility and autonomy of workers, with fewer rules or formal procedures and shared decision-making.
8. Orientation and Focus – Internal and/or External
The nature of the relationship between an organisation and its environment and whether or not an organisation assumes that it controls, or is controlled by, its external environment. An organisation may have an internal orientation (focusing on people and processes within the organisation) or external orientation (focusing on external constituents, customers, competitors and the environment), or have a combination of both.

Table 1: The Organisational Culture Framework [Detert et al 2000]

3.1. The Basis Of Truth And Rationality

In terms of security in an organisation, there are many aspects for which the basis of truth and rationale can be of interest. An example is what employees believe is good security and what they believe is bad security and how the adequacy and effectiveness of security is measured. There is no indication in literature, however, that these beliefs have a significant influence on the quality of the security culture in an organisation.

After a thorough evaluation of the literature we decided that for now the main focus should be on the basis of truth and rationale for the belief that security is important. Connolly (2000) even states that recognition of the importance of security is critical to business survival. Our research, therefore, looks at how both the employees, and the organisation itself, see the importance of security for the organisation.

Security is definitely very important to Organisation A. There are very strict processes and policies, and no expense is spared as to how much the organisation spends on maintaining its high security standards. All three interviewees stated that information on their computer systems is classed as very valuable to critical and that digital certificates are used when sending confidential e-mails.

In contrast, it is quite difficult for security to gain a lot of recognition at organization B, because security is not taken very seriously by the business. Even though the employees do realize that the company depends on information to run the business, their beliefs about the importance of security are influenced by a continuous struggle in the security committee for financial support and the impression they get from top management that security is considered to be an expense, not an investment.

Organisation B does not realise, that although their security requirements may not be as high as some other companies, achieving optimal security for their particular situation is still important, as is the need to ensure that their employees believe that security is important.

3.2. Nature of Time and Time Horizon

Organisation A has a good balance of long term and short-term goals. Its long-term goals are aimed at maintaining a secure physical and logical environment, while its short-term goals are currently concentrating on improving the dissemination and education of staff on security. Although there are no ongoing security awareness programs, there are weekly meetings where security issues may be brought up as well as individual consultations to discuss security.

Security audits are performed at least four times a year, each targeting specific areas of security at Organisation A, while personnel are reviewed every twelve months.

Security at Organisation B is still very young and its security goals are generally short-term due to the lack of budget required to carry out any long-term goals. The organisation is aiming to develop long-term goals related to the building of a solid security infrastructure in line with International Security Standards. Due to the lack of resources and staff, there are no regular security awareness programs performed. Security is discussed briefly at the induction of an employee but not much at all after that.

A controls review is carried out internally once a year, in addition to the external auditors who also do a controls review. However, these are very high-level reviews with insufficient depth into security, and most security measures are not checked or updated regularly. There are performance reviews on every employee twice a year, but this does not review their security status at all.

3.3. Motivation

Organisation A has very strict security policies in place which employees are expected to obey. These policies cover aspects such as locking laptops, using digital certificates and protecting your own digital certificate. Most of these policies are outlined in an extensive presentation given during employee induction. There is ongoing interaction with staff on the awareness of security, but no formal security awareness programs. Security is promoted through meetings and informal conversations with employees, with an emphasis that the organisation trusts the employees to act responsible.

Organisation B does not have many security processes or monitoring practices in place and employees are not very motivated to adopt secure practices. Password confidentiality is not enforced and there have been instances of employees writing them down on sticky labels or giving them out to other people Nevertheless, employees do understand that they have obligations with regards to security, as well as the consequences that may be imposed on them if they breach security. There is an Internet Usage and E-mail Policy that is part of the employee contract signed by the employee when they commence, but after they start working, security does not get much of a mention.

Security procedures and processes in place do have an effect on the motivation of employees to embrace security. Although Organisation A has very strict policies and procedures in place, this was found to be beneficial to the employees' ownership of security. In contrast, Organisation B has very few security processes, which prevents employees from being aware of security. Although both organisations place a lot of trust in employees to maintain security, this might possibly be detrimental to security in Organisation B.

3.4. Stability versus Change/Innovation/Personal Growth

Organisation A has a strong emphasis on continuous change. Threat and Risk Assessment programs are performed constantly. Each individual risk has a mitigation strategy dependent on the type of risk, and all changes to security must go through a change management process. There are steps made to ensure that this is not a token process, it is one of their most important processes.

Meetings may be called if there is any urgent requirement for change. If the organisation feels that a security process is not adequate, their security policy is updated to reflect a new and more accurate process. This is then approved through the hierarchical structure of the company.

Although there are good intentions for the continuous improvement of security in organization B, budget limitations are a significant drawback to these initiatives. Therefore, security changes are often reactive rather than pro-active. For example, changes to the security policy were made only when the Privacy Legislation came into action and changes were legally required.

3.5. Orientation to Work, Task, Co-workers

Security has a large impact on the work carried out in Organisation A. There are many access and verification restrictions for employees, both physically and logically. However, as much as employees may quip that it is a bit over the top, they generally feel very responsible for maintaining the organisation's security.

During induction, employees receive a brief overview on most security aspects, and all employees seem to know the forms of physical security in place. They also realize that any suggestions they have about security will definitely be taken seriously: A couple of suggestions have already been taken on board and put in place.

At organisation B security is not really found to be an impediment to the daily operations of employees primarily because there is not a lot there. Employees on the whole do not feel responsible for security. The main security procedure visible at Organisation B is the requirement of a number of different passwords to access different computer programs. However, this was found to be more a hindrance to employees than a reminder about the need for security, and there are no indications that this makes them feel any more responsible for security.

While suggestions made about security may be taken seriously by the Security Manager, the impression exists that the need to convince top management of the business value of any suggestion makes acceptance difficult.

3.6. Isolation versus Collaboration/Cooperation

A lot of people are involved in security management and implementation in Organisation A and all changes have to be approved by the Change Management group, which is comprised of a Board of Managers from all different sections. The extensive collaboration and cooperation is evident in the development and update of Organisation A's security policies. The Security Manager is responsible for drawing up the revised policy with input from the Directors and a Policy Review Team. It then goes to the Policy Approval Team through Executive Management before it is sent to an external Government organisation for final approval. The external approval is a requirement of the industry that Organisation A is in.

There is a general belief in Organisation A that security is not managed by a single person, but that it is the responsibility of every person to preserve the security of their environment. The organisation clearly considers it important that all its members work together to maintain security. Employees in Organisation A constantly keep abreast of the latest security initiatives. Many have memberships of various security communities and go to various security seminars to keep updated on options for improving security.

Even though Organisation B now has a security committee, there are still only a few people involved with the actual management and implementation of IS security. Because there are so many projects on at the same time, they find it hard to collaborate. However, there is some evidence of cooperation from the rest of the organisation in that the current security policy has been developed in conjunction with various team leaders, who were asked for their input and feedback. But end-user security is generally left up to the employees themselves and there does not seem to be much involvement of end-users in maintaining or improving security at the organisational level.

3.7. Control, Coordination and Responsibility

It is very evident that organisational and security goals are well aligned at Organisation A. and there are very tight controls over processes and policies. Everything escalates to the Security Manager, who ensures the enforcement of security policies, with the backing of Executive Management. All changes to security go through the hierarchical structure in the organisation and are carried out through the Change Management process.

In contrast, Organisation B's security goals are not aligned with its organisational goals and the Executive Management at Organisation B is extremely reluctant to take on security initiatives unless there is some financial justification for it. There are no tight controls over processes and policies and a lack of resources has resulted in little coordination of security within the organisation. Although the security committee operates at the corporate level, the continuous bickering about the budget indicates that management support is far from optimal.

3.8. Orientation and Focus – Internal and/or external

Organisation A has a external orientation with a clear focus, as one of their main security requirements is that they must conform to external audit and government requirements. This affects their security policies, security budget and hiring of personnel. They use an external vetting service to check the security of all employees, including criminal history checks, insolvency checks and character references.

The focus of Organisation B is less clear and mostly internal. While their goal is to bring IS security in line with international industry standards, it is unclear what that means for the security requirements of the organisation and their internal orientation is heavily influenced by the constant struggles to obtain adequate finance and to convince management that they should take security seriously.

4. DISCUSSION

Our main aim of this study has been to achieve a better understanding of what a security culture really is and how security within an organisation is influenced by security culture. In this section, we will use our extensive experience in security to try to extrapolate what the differences between the two organisations mean and to identify what lessons can be learned.

We do realize that just two case studies is not enough to ensure that any results we found can be generalized to other organisations, but our explanations below are supported by anecdotal evidence we found in other organisations.

We believe that using the Organisational Culture research model was extremely useful in understanding the quality of the security cultures of both organisations. We do not claim that this is the only framework for organisational culture that can be adapted to a research model for security culture, nor do we claim that the resulting research model is complete.

In this particular study of security culture we developed most of our interview questions through an extensive literature review aimed at identifying every important aspect of security culture. We then organised the resulting questions using the research model we had chosen to ensure that we had comprehensively covered all dimensions. We finally added some general interview questions on security, again making sure we covered most areas of IS security. This has increased our confidence that our research data is as comprehensive as possible.

When we compare the security culture of these two organisations, there are some differences that in our view do not directly reflect on the quality of the security culture in each organisation. If an organisation is required to have its security accredited, there will be logical consequences for the control and coordination of security and for the organisation's focus and orientation. An organisation without this requirement has more freedom of choice in these areas. Even without accreditation any organisation with a requirement for high security will, of necessity, be risk-averse while other organisations may choose to be more risk taking.

The challenge for organisations with medium–to-low requirements for security is how to cope with a more loose control and coordination of security, and to ensure that there is a careful process to avoid taking any unnecessary risks and to deal with any unknown (future) risks. The general consensus in literature is that, independent of whether you choose to mitigate certain risks or not, there is a minimum level of security that is required. It is not clear, however, what exactly this minimum level of security is. Similarly, it is also not clear what the focus and orientation should be in those organisations that do not need or want to get accredited.

There are a few important lessons that can be learned about the quality of security culture from this study, but only for those organisations that do not feel the need to have a high level of security with strict control and coordination. There are several deficiencies in the security culture of organisation B that, in our view, could have been avoided if the organisation had been aware of their own security culture and its importance.

The most obvious problem with its security culture is that the organisation and its employees believe that security is not important. That belief is accentuated by the emphasis within the organisation on the need to make a business case for each new initiative and the lack of an adequate budget to implement the preferred level of security. Organisations can avoid that trap by concentrating on the importance of getting the optimal level of security right and by emphasising that improving security is an incremental process. Instead of trying to set a short-time goal based on the level of security that you would like to achieve, set a long-term goal based on the direction that the organisation would like to follow to reach a more optimal level of security and decide on what the next small step in that direction should be.

The next problem encountered in organisation B is that only a small group is involved in planning, managing and implementing security. Again the belief that security is not important and a lack of budget can make it difficult to overcome this problem. Still, getting more people involved in security is a long-term investment and can actually reduce the cost in other areas of security. Employees involved in the development of a security policy can become a

valuable resource and can be used to provide informal awareness training as well as informal monitoring of compliance to be used in targeting formal awareness training and future policy development.

Both involving more people in security and increasing the belief that security is important will also influence the motivation of employees to be security conscious and take responsibility for their own security. Although reducing negative attitudes and increasing motivation are important issues in improving the quality of a security culture, we believe that it is more important that organisations identify whether these other two problems exist first. If found, the organisation should attempt to correct these problems before it allocates any additional resources to improve motivation.

5. CONCLUSIONS

While there has been an abundance of research in the area of organisational security and how it should be improved, most organisational security literature only focuses on certain aspects of security and not on how these aspects should be assimilated into an organisation's security culture. To improve our understanding of what a security culture is we investigated two organisations with widely different needs for security using an explorative case study approach based on a research model borrowed from Detert et al (2000). Their framework was chosen because we believe it summarised existing organisational culture literature succinctly into eight descriptive dimensions.

In this paper we described the differences in the security culture of these two organisations and we discussed how these differences have increased our understanding of security culture. We identified two major problems with the security culture of one organisation, which based on additional anecdotal evidence might be found fairly often in organisations with a similar low-level of security.

We suggest that by being aware of these problems, and of the possible solutions we proposed, organisations would be able to significantly improve their security culture.

6. REFERENCES

Andress, M. & B. Fonseca. (2000). "Manage People to Protect Data." InfoWorld 22(46): 48.

Beynon, D. (2001). "Talking Heads." Computerworld 24(33): 19-21.

Breidenbach, S. (2000). "How Secure Are You?" InformationWeek(800): 71-78.

Blake, S. (2000). "Protecting the Network Neighbourhood." Security Management 44(4): 65-71.

Clark-Dickson, P. (2001). "Alarmed and Dangerous." e-Access **March 2001**.

Conolly, P. (2000). "Security Starts from Within." InfoWorld **22(**28): 39-40.

Detert, J., R. Schroeder & J. Mauriel. (2000). "A Framework For Linking Culture and Improvement Initiatives in Organisations." The Academy of Management Review **25(**4): 850-863.

Hartley, B. (1998). "Ensure the Security of Your Corporate Systems (Developing a Security Policy)." E-Business Advisor 16(6): 30-32.

Nosworthy, J. (2000). "Implementing Information Security in the 21st Century - Do You Have the Balancing Factors?" Computers and Security 19(4): 337-347.

Sizer, R. & J. Clark. (1989). "Computer Security - A Pragmatic Approach For Managers." Information Age 11(2): 88-98.

Schwarzwalder, R. (1999). “Intranet Security.” Database and Network Journal 22(2): 58-62.

Von Solms, B. (2000). “Information Security - The Third Wave?” Computers and Security **19**(7): 615-620.