Exploring Organisational Security Culture:
Developing a comprehensive research model.

P.A. Chia
Email:pauline.chia@ernstyoung.com.au

S.B. Maynard
Email: seanbm@unimelb.edu.au

A.B Ruighaver
Email: anthonie@unimelb.edu.au

Department of Information Systems,
University of Melbourne, Australia

Abstract

Until now the concept of 'security culture' has not been clearly defined in the literature. To develop a research model that can be used to assess the quality of an organisation's security culture, we adapted a comprehensive framework from organisational culture. This framework was chosen because it summarised existing organisational culture literature succinctly into eight descriptive dimensions, and also identified a set of Total Quality Management (TQM) values pertinent to each dimension that were useful in translating it to a security research model. In this paper we present a description of the first of several case studies to demonstrate the effectiveness of this research model in describing and explaining the security culture of this organization.

Introduction

Traditionally, research on organizational security has often focused on those aspects of security that should be prevalent in an organisation with good security, such as developing a security policy (Wood 2000), educating employees (Freeman 2000) and ensuring management support of these initiatives (Hinde 1998). Although these aspects are important, many organizations have not even started to implement proper security policies. And, if they have, they often find that without an organisational culture to support their development, the enforcement of these policies through the traditional cycle of awareness training and compliance testing is likely to be less than optimal.

Security policy development is just one of the areas that need to be supported by an organisation's culture. Conolly (2000) believes that organisations must have a culture that makes it clear that security is important. Verton (2000) states that the challenge for many security awareness programs is the corporate culture and a business will have good security if its corporate culture is correct. Nosworthy (2000) states that an organisation's culture has a strong influence on organisational security, as it may 'hinder change' and ascertain appropriate changes according to critical business processes. Borck (2000) states that ‘beyond deploying the latest technology, effective security must involve the corporate culture as well.

While many other researchers also 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), none of these authors present a clear definition of what they mean by “a security culture”, nor are there any clear views on how to create this organisational culture to support security. Correspondingly, there has also been little research in the area of how to evaluate the security culture of an organisation.

In this paper we will attempt to fill this gap adding to the growing area of organisational security by describing a research model developed to assess the security culture within an organisation. As we did not find a comprehensive research model in the literature on organisational security culture, we looked for a general framework from organisational culture that could provide a theoretical framework for our work.

While there are a plethora of frameworks and models in organisational culture literature, Detert et al (2000) present a framework that synthesises the general dimensions of organisational culture, derived inductively from organisational culture research to date. This includes a review of Schein’s (1992) work on Organisational Culture and Leadership, the Competing Values Framework (Cameron & Freeman 1991; Yeung et al 1991), and the Organisational Culture Profile (Klein et al 1995).

To demonstrate the usefulness of their framework of eight ‘overarching, descriptive culture dimensions’ Detert et al linked their framework to a ‘comprehensive set of values and beliefs’ that influence successful Total Quality Management (TQM) adoption. The comprehensiveness of Detert et al’s (2000) framework when applied to TQM convinced us of its usefulness as the basis for defining a similar Organisational Security Culture framework.

This paper outlines the adaptation of Detert’s framework to our Organisational Security Culture research model. The adaptation is based on the views on security culture reported in the literature, as we reviewed in the introduction above, and it is therefore not the only adaptation possible. While it is undoubtedly not the definitive framework on security culture, it has now proven its value in three case studies we performed in organizations with vastly different levels of security. In this paper we present a short description of the first of these case studies, in a large organization with a medium level of security, to demonstrate the effectiveness of this research model in describing and explaining the security culture of this organization.

Developing the Organisational Security Culture Research Model

To demonstrate the usefulness of their eight dimensions, Detert et al linked their framework to a set of values and beliefs that represent the ‘cultural backbone’ of successful Total Quality Management (TQM) adoption. The next section draws from the TQM values determined by Detert et al (2000) and attempts to use knowledge from the literature reviewed on security culture to transform each dimension to apply to security in an organisation. The following subsections show the outcome of this analysis.

The Basis of Truth and Rationality

The basis of truth and rationality in TQM relies on factual information and scientific methods. Similarly the quality of a security culture will be determined by basis of truth and rationality in the various beliefs that employees' hold, as compared to the policies the organisation maintains about security. These beliefs will be in terms of what employees believe is good security and what they believe is bad security and how the adequacy and effectiveness of security is measured.

The literature on security culture recognizes that the most crucial belief influencing the security in the organization is the belief, by both employees within an organisation as well as by the organisation itself, that security is important. Connolly (2000) states that recognition of the importance of security is critical to business survival.

Whiting (1999) asserts that top management often demand proof of a financial return for major IT projects and in some companies, 'doing it by numbers' is ingrained in the culture. This can have a severe negative influence on the belief that security is important. An organisation with a good security culture would not measure security in terms of it being an expense, but as an investment resulting in future benefits to the organisation (Avolio 2000).

Nature of Time and Time Horizon

TQM places an emphasis on long-term commitment and strategic management. Similarly, organisations with high-quality security culture should ultimately have long-term security plans and strategies. Wood (2000) states 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.

Motivation

Most employees in a TQM organisation are intrinsically motivated to do a good job, but are often thwarted by the system in which they work or by fear and coercion. The motivation of employees to embrace security may also be affected by the implementation and management of security processes and technologies. These processes will either hinder or benefit the overall security of an organisation.

More importantly, there is no evidence that employees are intrinsically motivated to adopt secure practices. Employees need to learn that security controls are necessary and useful; otherwise they will spend a lot of time attempting to bypass them (Lau 1998). Therefore, organisations with a good security culture need to have appropriate processes in place to make it easier for employees to be intrinsically motivated in relation to IS security. To improve their attitude to security, it is important that a degree of trust is involved and that responsibility to act in an appropriate manner is delegated to employees themselves.

Stability versus Change/Innovation/Personal Growth

In TQM, a premium is placed on change and continuous improvement. In security there is often 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. While risk management is an important aspect of information security (Webb 2000), good security is more than just mitigating risks. Hence although change should be carefully managed, security is never 100% and organisations therefore need to ensure that their ‘security posture is not static’ (Shinn 2000). They have to realize that an organisation’s security procedures and practices need to improve continually, and that steps are constantly being made to enrich organisational security.

Another common problem in organisations is that many are prepared to ignore some of the minor security risks. Few organizations are risk averse. Often particular risks only assume importance after a high profile incident (Nickles 2000). Hence, being pro-active, rather than reactive to security breaches is preferable.

Orientation to Work, Task, Co-workers

Employees should be made to feel responsible for security in the organisation. This will again be influenced by the impact that security has on the work that employees are required to carry out and whether or not security is found to be an impediment to the daily operations of an employee.

Education of employees on their roles and responsibilities related to security is also crucial (Freeman 2000). Adequate user education can ‘eliminate inadvertent disclosures, and even help users contribute to total system security by educating them on proper access control methods, and sensitising them to things like potential intruders watching users over their shoulder for passwords’ (Hartley 1998).

Isolation versus Collaboration/Cooperation

Cooperation and collaboration are a necessity for a successful TQM organisation. The nature of human relationships in establishing and upholding security standards is similarly very important. Every member of an organisation should be involved in some way with maintaining security. In addition, the security policy should be created collaboratively using the input of people from various facets of the organisation to ensure its comprehensiveness and acceptance (Clark-Dickson 2001).

Control, Coordination and Responsibility

Shared visions and goals are necessary for a TQM organisation’s success. Similarly, an organisation with a quality security culture must have shared visions and goals about organisational security. According to Nosworthy (2000), there needs to be a balance of risk and control. Therefore, enforcement of security should be combined with the empowerment of employees to be responsible for security.

There is also a need for an alignment of organisational and security goals. The security policy must support the organisation’s business objectives, or management will not support it (Blake 2000). The tone for security must be set from the top of the organisation (Hinde 1998), and a culture of security awareness needs to be instigated from the highest levels of an organisation (Verton 2000). Education of employees on security should be driven by ‘upper management and the security team in unison’

(Shipley 2000). Overall responsibility of security should be given to an empowered security team who can overlook these aspects.

Orientation and Focus – Internal and/or external

While TQM has a clear focus on customer satisfaction, literature on security culture is unclear on what a proper focus would be to achieve a high-quality security culture. Hence, currently this dimension in our framework is probably the least developed.

As security in an organisation is influenced by both external factors and internal needs, we believe that ideally a balance of these two is needed. An organisation should not only look at their own security needs and how to meet them, but also maintain a minimum level of security to cope with changes in their environment and unforeseen threats.

The case study

Overview

To show the effectiveness of the Organisational Security Culture framework described in the previous section, we will present here the first of three case studies we have currently undertaken on the quality of security culture.

Developing the Case Study

To ensure a comprehensive coverage of most areas of Information Security in this case study, we created a set of open interview questions covering both a broad range of security issues, identified from the security literature, as well as all dimensions of our framework. The security issues covered were on security policies (Clyde 1999; Andress & Fonseca 2000; Conolly 2000; Clark-Dickson 2001), risk assessments (Barnard & von Solms 2000; Webb 2000), security management (Avolio 2000; Barnard & von Solms 2000; von Solms 2000), security awareness (Andress & Fonseca 2000; von Solms 2000; Beynon 2001), security audits (Hartley 1998; Breidenbach 2000), personnel security (Hartley 1998; Breidenbach 2000; Freeman 2000) and physical access controls (Borck 2000; Shinn 2000).

The questions were structured to determine the interviewees' involvement in, and awareness of, their organisation's security. Each interview was divided into three sections. The first section was concerned with demographics and general personal information about the interviewee. The purpose of these questions was to establish the role of the interviewee within the organisation, as well as finding out how they manage their own personal security. The next section comprised very general questions about how security is managed at their organisation. The questions were intentionally broad to allow the interviewee to formulate their own interpretation of the questions. The final section was made up of fairly specific questions to cover aspects that were not addressed in the second section to obtain a more thorough view of the security culture in the organisation.

The Case

The Organisation is the Australian operation of a global company in the Finance/Insurance industry. The Australian organisation has about three thousand employees, and there are about 55,000 employees globally. The organization's headquarters are overseas, from which a lot of their security initiatives are dictated. While the level of IS security at this organisation is probably low-to-medium, they are working on improving their security.

After obtaining approval of the organization, three people were selected from different levels and areas of the organisation with the purpose of obtaining diverse opinions on security. Interviews were approximately one hour in length and were taped. As most interviews were held within the organisation some of the security in place at the organisation was observed first-hand as well. For security reasons, not much documentation could be viewed; however, we did manage to have a look at a draft security policy. Following the case study each interview was transcribed, with each transcript reviewed and signed off by the interviewee. Where needed, follow up questions were conducted via e-mail and telephone.

The Basis of Truth and Rationality

As the company depends on information to run their business, information is seen as pretty valuable. But, because security is not taken very seriously by management, it is quite difficult for the importance of security to gain a lot of recognition at this organisation.

> On the security budget:
> 'We're very short staffed, very under budget, as in no budget, but hopefully things will turn around next year'
> Person A

Before last year, there was no formalised security function and even now, IS security is still in its infancy. No background checks are done on employees, only reference checking. There is an Internet Usage and E-mail Policy that is signed by every employee when they commence employment. However, enforcement is minimal and most employees would probably read it without giving it much thought. The main physical security measure is a Digital Key System (DKS) key that allows employees access to the organisation's floors. Apart from this, no other physical security seems to be in place.

> On the security expenditure:
> 'If the business can't say that they're going to make money from it, then it won't happen, that's the bottom line'
> Person A

Surprisingly the interviewees believed that, despite the struggle for financial support, the security in place was quite good.

Nature of Time and Time Horizon

Security goals are generally short-term due to the lack of budget required to carry out long-term goals. As security is still very young, the main goal is to build 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.

> On employee security awareness:
> ‘It is sold to you at the beginning, but unless there has been a breach by someone, I don’t think that it is actually ever addressed again’
> Person B

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. There are performance reviews on every employee twice a year, but these do not review security at all and security measures are not checked, nor updated regularly. This stresses the reactive environment present at this organisation.

Motivation

Since there are not many security processes or monitoring practices in place, employees are not very motivated to adopt secure practices. Nevertheless, employees do understand what their obligations are with regards to security, as well as the consequences that may be imposed on them if they breach security.

> On the security risk of staff:
> ‘We’ve had a few people sacked over the past few months because of breach of policy’
> Person A

As mentioned before, 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. Moreover, it is not enforced that employees should keep their passwords confidential. There have been instances of employees writing them down on sticky labels or giving them out to other people. There is a new initiative being planned to make a computer package available to educate employees on security, but it may not be compulsory for employees to use it.

Stability versus Change/Innovation/Personal Growth

Although there are good intentions for the continuous improvement of security, budget limitations are a significant drawback to these initiatives. Therefore, security changes are more 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.

> On implementing the security policy:
> ‘it’s change management, and no one likes change, no one likes someone else to tell them ‘well this is how we do it’, so, it makes it interesting and difficult’

Person A

There is a tendency towards stability, rather than change. Particularly in a large organisation like this, it can be extremely difficult to change the mindset of high level management and a large number of employees.

Orientation to Work, Task, Co-workers

Security is not really found to be an impediment to the daily operations of employees primarily because there simply is not a lot there. However, the number of passwords that an employee must remember to get into various systems is at least four. This can be a bit of an inconvenience and they are currently trying to obtain the strategies they need to reduce sign-on.

Suggestions made about security may be taken seriously by the Security Manager, but convincing top management is difficult.

On making security suggestions:
'Whether suggestions get taken seriously up the line's another thing'
Person B
'Unless it's got Executive support, that's critical to its success and adoption'
Person C

Employees on the whole do not feel responsible for security. There is the idea that employees should, but this has not come to fruition.

On whether employees feel responsible for security:
'No! I've gotta change that mindset, but that'll take time….'
Person A

Isolation versus Collaboration/Cooperation

Currently there are only a few people who are involved in managing the security at this organisation. There is no evidence that there is much collaboration between employees to maintain proper security. However, a positive aspect is that the security policy was developed in conjunction with various team leaders, by asking for their input and feedback.

Control, Coordination and Responsibility

Being a very large organisation, it can be very hard to coordinate and control the security throughout the organisation, especially when the security function is so small. It is also evident that there is currently no correlation between organisational strategies and security. To address this problem, a security committee has been formed recently. This security committee is made up of five to six people from different areas of the organisation and intends to meet up at least once a quarter, depending on what is required. Initial indications are, however, that it is still quite difficult to convince the two executives on the security committee to provide adequate financial support for security.

> Security is all about money:
> ‘With security, you’ve got to find whatever the button is to push to get them to find the money, spend the money, it’s all about packaging it up to be a business enabler’
> Person A

Orientation and Focus – Internal and/or external

This organization currently still has a fairly internal security focus due to the constant struggles to obtain finance and convincing management to take security seriously.

> 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 B

Overview of the Security Culture

Although there are good intentions to improve security, these are hindered by a lack of budget and a lack of support from Executive management. Not only has this resulted in a message from the organization to employees that security is not important, these issues are also influencing most other dimensions of the security culture. There is a very short-term focus and, rather than being pro-active, the organisation is mainly reactive to security breaches. The lack of security processes in place hinders employee motivation and employees do not on the whole feel responsible for security. Although the organisation is very large, only a small number of people are involved with managing and coordinating security.

The recent formation of a security committee may address a number of these problems. Even though management support and budget may not increase significantly, it is important that the influence of these issues on security culture is minimized. Changing the belief of employees that security is not important does not have to cost much and neither does trying to improve their motivation. The fact that executive management is involved, together with an indication that the security budget is at least increasing, can be used to reinforce the message that security is important. It may, however, be more difficult to convince the security committee that, instead of directly spending everything on implementing security measures, some of their limited budget should be used to improve security culture.

Conclusion

There has been an abundance of research in the area of organisational security and how it should be improved, but most only focus on certain aspects of security and not how these aspects should be assimilated into an organisation’s culture. Thus, until now the definition of a ‘security culture’ has been quite vague. This research set out to develop a research model for organisational security culture that can be used to assess the quality of an organisation's security culture.

Due to the lack of research on an organisation's security culture, an Organisational Culture framework by Detert et al (2000) was adopted and transformed. Detert et al's framework was chosen because it summarised existing organisational culture literature succinctly into eight descriptive dimensions, and also identified a set of Total Quality Management (TQM) values pertinent to each dimension. Using this information, together with a broad range of organisational security issues found in literature, we developed a comprehensive research model for evaluating an organisation's security culture.

The main limitations of this current research model stem from our interpretation of Detert et al's (2000) Organisational Culture framework and how it relates to security. Although we have an extensive experience in IS security, the translations to organisational security culture are rather subjective and other interpretations of each of the eight dimensions may be possible. While Detert et al's (2000) original framework covers a broad range of issues in organisational culture, the resulting research model only concentrates on those organisational security issues identified in literature.

To demonstrate the usefulness of this research model in assessing the quality of an organisation's security culture, we presented the first of several case studies we have performed so far. Aware of the possible limitations of our research model, we ensured that our interview questions did not only cover all dimensions of this research model, but also ensured that they comprehensively covered most areas of IS security as well.

We believe that our case study produced a comprehensive description of the security culture of this organisation and we were able to identify a number of problems within this organisation related to their security culture. We have currently not identified any issues that did not fit in to our research model.

While identifying problems with the quality of an organisation's security culture is one thing, suggesting solutions to these problems is another. In this paper we have not attempted to suggest any solutions. We are confident that, through the use of this research model in further case studies, we will not only improve our understanding of organisational security, but also will gain useful insights in how to improve security culture.

References

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

Avolio, F. (2000). "Best Practices in Network Security." Network Computing 11(5): 60-64.

Barnard, L. & R. von Solms. (2000). "A Formalised Approach to the Effective Selection and Evaluation of Information Security Controls." Computers and Security 19(2): 185-194.

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.

Borck, J. (2000). “Advice for a Secure Enterprise: Implement the Basics and See That Everyone Uses Them.” InfoWorld 22(46): 90.

Cameron, K & S. Freeman. (1991). “Cultural Congruence, Strength and Type: Relationships to Effectiveness.” Research in Organisational Change and Development 5: 23-58.

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.

Freeman, E. (2000). "E-Merging Risks: Operational Issues and Solutions in a Cyberage." Risk Management 47(7): 12-15.

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

Hinde, S. (1998). "Recent Security Surveys." Computers and Security 17(3): 207-210.

Klein, A., R. Masi & C. Weidner. (1995). "Organisation Culture, Distribution, and Amount of Control, and Perceptions of Quality." Group and Organisation Management 20: 122-148.

Lau, O. (1998). "The Ten Commandments of Security." Computers and Security 17(2): 119-123.

Nickles, A. (2000). "A Wake Up Call for Security." Midrange Systems 13(4): 52, 54.

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

Schein, E. (1992). Organisational Culture and Leadership (2nd Edition). San Francisco: Jossey-Bass.

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.

Shinn, M. T. (2000). “Security for your e-business.” Enterprise Systems Journal 15(8): 18.

Verton, D. (2000). “Companies Aim to Build Security Awareness.” Computerworld 34(48): 24.

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

Whiting, R. (1999). “Warehouse ROI.” InformationWeek May(735): 99-104.

Webb, S. (2000). “Crimes and Misdemeanours: How to Protect Corporate Information in the Internet Age.” Computers and Security 19(2): 128-132.

Wood, C. (2000). “Integrated Approach Includes Information Security.” Security 37(2): 43-44.

Yeung, A., J. Brockbank & D. Ulrich. (1991). “Organisational Culture and Human Resource Practices: An Empirical Assessment.” Research in Organisational Change and Development 5: 59-81.