Understanding Organizational Security Culture

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

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 organizational 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 need to 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 organizational 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 with "a security culture", nor are there any clear views on how to create this organizational 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 chapter we will describe a framework that can be used to explore the security culture within an organisation. While we could not find a model of organizational security culture in the literature, there are a plethora of general frameworks and models of organizational culture available. Hence, we had to decide which framework would best suit our particular application in security culture. Our final choice was a

framework by Detert et al (2000), which attempted to synthesise the general dimensions of organizational culture from organizational culture research to date. Detert's synthesis includes a review of Schein's (1992) work on Organizational Culture and Leadership, the Competing Values Framework (Cameron & Freeman 1991; Yeung et al 1991), and the Organizational 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 Organizational Security Culture framework.

This chapter outlines our adaptation of Detert's framework to a research model for Organizational Security Culture. We describe the initial adaptation based on the views on security culture reported in the literature, which may therefore not be the only adaptation possible. Hence, we do not claim that this is the definitive framework on security culture, but it has now proven its value in several case studies we performed in organizations with vastly different levels of security. We will demonstrate the effectiveness of this research model in describing and explaining an organization's security culture by presenting short descriptions of two of these case studies. We will then discuss the lessons we learned about the quality of the security culture of these organisations and suggest some guidelines on how to improve the security culture of an organization.

Developing an Organizational 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.

These eight dimensions of organizational culture are briefly identified in table 1.

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 organizational 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 Organizational Culture Framework (Detert et al 2000)

The remainder of this section draws from the TQM values determined by Detert et al (2000) and attempts to transform each dimension to apply to security in an organisation based on security literature. 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 the 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. Unfortunately, however, there is not much discussion in literature on possible long-term strategies.

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. 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 motivated in relation to IS security. To improve their attitude to security, it is also 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, as Web suggests (Webb 2000), risk management is an important aspect of information security, good security is more than just mitigating risks. 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 organizational 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 high-quality security culture must have shared visions and goals about organizational security.

In this context, it is important to realize that there will never be 100% security. According to Nosworthy (2000), there needs to be a balance of risk and control, and enforcement of security should therefore be combined with the empowerment of employees to be responsible for security.

There is also a need for an alignment of organizational 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). 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.

Exploring Organizational Security Culture

Having used an extensive literature review to adapt Deter et al's framework for use in the evaluation of the security culture of an organization, the effectiveness of this Organizational Security Culture framework must still be demonstrated in practice. In this section we will present the first two cases out of several case studies we have performed so far. The organizations used in these cases have been chosen to ensure that we covered at least one organization with a high level of security and one organization with a low-to-medium level of security.

To ensure a comprehensive coverage of most areas of Information Security in our case studies on organizational security culture, 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 (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 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 examined 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 leader in the encryption market place. The involvement in the security industry clearly 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.

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.

Again, the employees were asked about their views on their organisation's security culture:

> '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

Case Study One – Organisation A

On visiting Organisation A, it was evident that there were very tight security procedures in place. This includes internal and external cameras, proximity cards, biometric hand scanners, rooftop alarm system, passive infra-red detectors throughout the building's ceiling space to detect movement in the building, dual access to safes and white noise generators in the board room to prevent electronic eavesdropping.

Three people (to preserve anonymity, they will be named Person A, Person B and Person C) from the middle to higher levels of the organisation were interviewed in this case study. No participants from lower levels of the organisation could be interviewed for security reasons. This should not affect the results of the study, as this represents an aspect of the security culture present at Organisation A. All three interviews were taped with interviewees' consent, and transcriptions of interviews were reviewed and signed off by each interviewee. Transcripts of all three interviews were reorganised according to the eight dimensions and then analysed. The results of this analysis are shown in the following sub-sections.

The Basis of Truth and Rationality

Security is definitely very important to Organisation A. There are very strict processes and policies, and no expense is spared as to how much Organisation A spends on maintaining high security standards.

> *On the security budget:*
> 'Lack of budget is not an issue'
> Person A

All three interviewees stated that information on their computer systems is classed as very valuable to critical and digital certificates are used when sending confidential e-mails. Employees have comprehensive knowledge of the physical security in place.

> *On physical security:*
> '…there are dozens of cameras, they're all over the place, I'm not sure whether I know where half of them are!'
> **Person B**

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.

There is a belief in Organisation A that security is not managed by one person, that it is the responsibility of every person to preserve the security of their environment. It is very interesting to note that when asked how security is managed, Person B spoke about the organisation's policies, whereas Person C spoke more about the physical aspects of security. Person A was well aware that security problems are often caused by staff in getting them to follow the processes put in place. On the whole, security in Organisation A is of high importance to all employees, which is reflected by the vast amount of security in place.

Nature of Time and Time Horizon

Organization A has some long-term, as well as short-term organizational security goals. Its long-term goals are to maintain a secure physical and logical environment, while its current short-term goals are to improve 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 and individual consultations to discuss security. Security audits are performed at least four times a year, each targeting specific areas of security.

Motivation

There are 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 a presentation given during employee induction. A copy of this presentation was viewed and it showed a fair degree of depth into the security practices at this organisation. When employees commence, they are also given a copy of the security policy, which they must read through and then sign an agreement.

On what impacts employees accepting the security policy:
'Nothing, really, I guess I accept it because it's in the terms of employment, this is how we choose to operate'
Person C

As far as physical security goes, everything is monitored so it would be quite hard for employees to breach security physically. In addition, there is a lot of emphasis on trust at Organisation A.

On how security is managed:
'Management really trusts the employees to do what they need to do, so they're not nosing around and looking at people's computers, there's a lot of trust within the organisation'
Person C

'You don't want to be forcing it down people's throats'
Person B

Besides the induction training on security, 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.

On how security is promoted:
'Everyone here has a role and a responsibility'
Person A

'Security is brought up all the time, in regards to 'be aware of this', 'keep in mind this', 'this is what Organisation A's all about', so it's like internal promotion-type security'
Person B

Therefore, the motivation of employees to embrace security stems from the policies and procedures in place, as well as the trust endowed upon employees to be secure at Organisation A.

Stability versus Change/Innovation/Personal Growth

Organisation A has a strong emphasis on continuous change. Threat and Risk Assessment programs are performed constantly. These are monitored by external audits, which are carried out approximately four times a year. 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.

If security measures are not working:
'We change the process, we change the way things are done to make sure it does work'
Person A

'Things evolve here, when something is not working, the audit process will pick it up, as well as through our own experience, we learn whether or not something is doing what it should be doing, and if it isn't then it gets addressed by myself or Executive Management'
Person A

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.

On changes to security:
'Security is an ongoing process, daily, you couldn't put a time to it, it takes place all the time, it's constant'
Person A

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. This can encompass using digital certificates and encryption or having to turn on a massive alarm system if you are the last to leave the premises.

On employees feeling responsible for security:
'They adapt an attitude towards their role within the company, and they all do take on their responsibilities very seriously here'
Person A

During induction, employees receive a brief overview on most security aspects, and all employees seem to know the forms of physical security in place. An extensive employee vetting process is also carried out every three years.

If an employee of Organisation A were to make suggestions about security, it would definitely be taken seriously. Person B said that there have been a couple of suggestions that have been taken on board and put in place.

On making suggestions about security:
'People are very pro for making any suggestions about security'
Person B

'Some of our staff here are very, very clever, and we come from all walks of life, so you would not discount their knowledge and expertise in certain areas'
Person A

Although security may slow things down, the employees have learnt to live with the security in place because it 'exists the moment they walk in the door' and they are told about it before they commence working there. It does not frustrate employees to the degree that it is out of hand. It just becomes part of habit.

Isolation versus Collaboration/Cooperation

There is a high degree of responsibility given to all employees at Organisation A to cooperate to maintain security.

On the management of security:
'Security is not managed by one person, it's the responsibility of every person working for this company to contribute towards our reputation and security of this environment'
Person A

As mentioned before, management would take any suggestions made by employees for the improvement of security very seriously. This allows employees to feel responsible for cooperating with others to increase security. Security developments are carried out by the Change Management group, which is comprised of a Board of Managers from all different sections of Organisation A. Development of the security policy is also a combined effort. The Security Manager draws it up with input from the Directors and the Policy Review Team. It then goes to the Policy Approval Team through Executive Management before it gets sent to an external Government organisation for final approval. This external approval is a requirement of the industry that Organisation A is in. External auditors also evaluate the implementation of the security policy.

Control, Coordination and Responsibility

There are very tight controls over processes and policies at Organisation A. Enforcement of the security policies is the responsibility of the Security Manager. All

changes to security have to pass through the hierarchical structure in the organisation and are carried out in accordance with a strict change management process. Building access is broken down within the building, dependent on each employee's role. Other than these strict procedures, security is promoted basically through trusting employees to be responsible.

On the coordination of security:

'…..it filters down from the managers'
Person B

'Management really try to push it down from the top level by letting everybody know what the company is doing, and really having everybody involved and have a fair say, with the promotion of the company and where the company is moving. So therefore, the company trusts its employees to look out for the best for the company, and really know when things are confidential. We're given a lot of information that a normal company wouldn't give its employees about the strategic direction of the company'
Person C

It is very evident that organizational and security goals are well aligned at Organisation A.

Orientation and Focus – Internal and/or External

Organisation A is fairly externally focused. One of their prerequisites 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.

They are also very aware of the risks associated with hiring external contractors. Their security guard is an internal employee and deals with security issues on a day-to-day basis, even after hours. There is also no external access for employees to the internal networks, and their e-commerce network is set up to be aware of security issues. Since Organisation A is involved in ensuring the security of e-commerce transactions, they are very aware of the vulnerability's involved. One of the precautions they take is not having their e-commerce network connected at all to the rest of the networks in the organisation. If Organisation A were to unforeseeably be without external power, their systems would still be able to run indefinitely. So far, they have not had any problems with their e-commerce operations.

Summary of Organisation A's Security Culture

The security culture at Organisation A is fairly tightly regulated, with many strict policies and procedures in place. However, there is also an emphasis on trusting employees to be responsible for maintaining the security of Organisation A. 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.

Case Study Two – Organization B

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 quite valuable. But, because security does not seem to be taken 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, employee password confidentiality is not enforced within the organization. There have been instances of employees writing passwords down on sticky labels or giving them out to other people. There are plans 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 organizational 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 in Organization B

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, it has also influenced 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 in general 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.

Comparing the security cultures

It should be clear from the above case studies that the security cultures in both organizations are quite different.

The Basis of Truth and Rationality

Both organizations believe that their security is good. But neither organization really makes any attempt to evaluate the quality of their security. In Organization A this belief is clearly based on their trust in the extensive processes in place to improve and

maintain security. In organization B, the belief that security is good is clearly unfounded.

Our most important findings however, relate to how the importance of security for the organisation is seen by the employees and the organisation as a whole. 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. In contrast, security in organization B is generally not believed to be important. 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.

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 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.

An internal controls review is carried out within organization B annually, 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 also performance reviews on every employee twice a year, but these reviews do not look at their security status at all.

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 in a responsible manner.

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 understand that they have obligations with regards to security, as well as the consequences that may be imposed on them if they breach security.

Security procedures and processes in place 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 may possibly be detrimental to security in Organisation B.

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.

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.

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 feel that it is sometimes excessive, they generally feel very responsible for maintaining the organisation's security.

During induction, employees in Organization A receive an overview covering 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 be taken seriously: A number of employee suggestions have already been implemented.

At organisation B security is not really found to be an impediment to the daily operations of employees primarily because it is virtually non-existent. Employees on the whole do not feel responsible for security. The main security practice visible at Organisation B is the requirement of a number of different passwords to access different computer programs. However, employees seem to find this more a

hindrance than a reminder about the need for security, and there are no indications that this makes them feel any more responsible for security.

While the Security Manager may take any suggestions from employees about security seriously, the impression exists that the need to convince top management of the business value of any new security initiatives makes most suggestions futile.

Isolation versus Collaboration/Cooperation

Organisation A clearly considers it important that all its members work together to maintain security. A lot of people are involved in security management and implementation 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 also evident in the development and update of Organisation A's security policies.

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. There is evidence of limited cooperation from other areas 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 organizational level.

Control, Coordination and Responsibility

It is very evident that organizational and security goals are well aligned at Organisation A and that there are very tight controls over processes and policies. Everything related to security, including possible security incidents, escalates to the Security Manager, who ensures the enforcement of security policies with the backing of Executive Management.

In contrast, Organisation B's security goals are not aligned with its organizational goals and the Executive Management at Organisation B is extremely reluctant to support enforcement of existing policies or to take on new security initiatives. 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 new security committee operates at the corporate level, the continuous bickering about the budget indicates that management support is far from optimal.

Orientation and Focus – Internal and/or external

Organisation A has an 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. Again, their internal orientation is heavily influenced by the constant struggles to obtain adequate finance and to convince management that they should take security seriously.

Lessons Learned

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

We believe that using the Organizational Culture research model was extremely useful in understanding the quality of the security cultures of both organisations. However, we do not claim that this is the only framework for organizational 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.
As a result of these differences, we believe that there will not be a single approach to achieve an optimal security culture suited for all organizations. 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.

For those organisations that do not feel the need to have a high level of security with strict control and coordination, there are a few other important lessons that can be learned about the quality of security culture from this study. 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. Feedback from these informal processes can be used in the targeting of 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, we belief that the organisation should attempt to correct these problems first, before it allocates any additional resources to improve motivation.

Summary

While there has been an abundance of research in the area of organizational security and how it should be improved, most organizational 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 organizational 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.

The main limitations of our current research in security culture stem from our interpretation of Detert et al's (2000) Organizational Culture framework and how it relates to security. Although we have an extensive experience in IS security, the translations to organizational security culture are rather subjective and other interpretations of each of the eight dimensions may be possible.

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 Organizational 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). *Organizational 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). Organizational Culture and Human Resource Practices: An Empirical Assessment. *Research in Organizational Change and Development* 5: 59-81.