16

INFORMATION SECURITY CULTURE

A. MARTINS[1], JAN ELOFF[2]

[1]*am@adam.rau.ac.za*
Rand Afrikaans University, Johannesburg, South Africa
[2]*eloff@rkw.rau.ac.za*
Department of Computer Science
Rand Afrikaans University
PO Box 524
AUCKLAND PARK
2006
South Africa
2001
Tel: +27 11 489-2847 Fax: +27 11 489-2138

Key words: information security, culture, assessment, behaviour

Abstract: In every organisation an information security culture emerges from the way in which people behave towards information and the security thereof. The procedures that employees use in their daily work could represent the weakest link in the information security chain. It is therefore important to develop and improve information security culture through a structured model that addresses employee behaviour. This article will discuss the concept of information security culture and an assessment approach developed to implement and improve such a culture.

1. INTRODUCTION

We are living in an information economy in which every business depends on information assets such as information, data, hardware, software and networks to mention but a few. As a result of the rapid changes and progress in the Information Technology (IT) market, information security professionals have to move even faster to stay ahead in order to instil security solutions for information assets.

The original version of this chapter was revised: The copyright line was incorrect. This has been corrected. The Erratum to this chapter is available at DOI: 10.1007/978-0-387-35586-3_46

M. A. Ghonaimy et al. (eds.), *Security in the Information Society*

Implementing technical information security solutions is, however, not enough. The effectiveness of information security controls depends on the competency and dependability of the people who are implementing and using it [DHILL01]. There could be adequate security controls such as firewalls, but if management does not manage them effectively or if the users do not know how to operate a firewall correctly, the human element becomes the dependent factor and not the technology. At any given point users interact with computer assets in some way and for some reason. This interaction represents the weakest link in information security [SCHN00]. Recent research also indicates that insider behaviour poses a more serious threat to the security of information than outsider behaviour [BRIN00, DHILL01, GAUN00, VENT00].

The way in which people interact with information assets and how they behave in the working environment will in time become the way in which things are done in an organisation. The way things are done will become part of the organisation's culture. It is important for the correct behaviour towards information security to become part of the organisational culture. The behaviour of employees towards information must be acceptable and needs to be part of everyday life in the organisation. An example of such behaviour could be that client information needs to be handled with confidentiality or that only authorised maintenance personnel may carry out repairs and service computer equipment. To facilitate this, it is necessary to instil an information security culture in the organisation [VONS00, ELOFF00, MCLU00].

The following questions are, however, posed: "What is information security culture?" and "How does an organisation instil information security culture?" To answer these questions, the concept of information security culture needs to be defined. A model and assessment approach is then proposed, which an organisation could use to instil information security culture. Lastly, a case study is discussed in which an assessment approach was used to evaluate the information security culture of an organisation.

2. INFORMATION SECURITY CULTURE

A few researchers have already indicated in literature that information security should be viewed as a holistic issue, forming part of the *organisational culture,* and it should include issues such as people, training, processes and communications [CONN00, LEGR00]. Therefore,

organisational culture plays an important role when implementing information security [ANDR00, CONN00, NOSW00] as a holistic issue.

Probably the most well-known definition of organisational culture is "the way things are done in an organisation" [LUND96]. It is the unwritten rules of life and the assumption about the way in which work is done [YEAT96]. The organisational culture is also different for every organisation each having its own set of characteristics that it values, such as working in teams rather than as individuals [ROBB01]. Every organisation also has certain information security practices, which are followed and incorporated into the working environment that will become part of the organisational culture in the organisation. An example of such a practice is to change passwords every week or to get an auditor to assess the organisation's computer networks.

Taking the above description of organisational culture into account, information security culture can be seen as a set of information security characteristics. These characteristics, such as integrity and availability of information, need to be valued and pursued by the organisation. Information security culture is also an assumption about what is and what is not acceptable in relation to information security. It may for instance not be acceptable to throw a confidential document into a waste basket, but to shred it rather. Another example is that it is not acceptable to leave crucial business information in office areas where anyone could access or read it; it should rather be locked away.

Information security culture will also emerge from encouraging acceptable information security behaviour. An example could be that people are encouraged to report security incidents via the appropriate management channels. Management could also encourage employees to regard the work they do as part of the organisation's intellectual property, which needs to be protected.

By instilling an information security culture, information security practices such as a clear desk policy and controls such as encryption will be accepted as the way in which things are done. These practices will aid in solving the threat of internal security breaches and prevent external security breaches [VONS00, ANDR00].

Information security culture can thus be defined as the assumption about which type of information security behaviour is accepted and encouraged in

order to incorporate information security characteristics as the way in which things are done in an organisation.

3. ISSUES TO ADDRESS CONCERNING AN INFORMATION SECURITY CULTURE

Instilling an information security culture is not an easy task and can take many years [GUAN00]. Issues such as information security policy and information security awareness need to be addressed by an organisation to develop a culture conducive to the protection of information assets. Culture has to do with the way in which things are done in an organisation and thus with the behaviour of people. Therefore, organisational behaviour also has an impact on the information security culture of an organisation.

Organisational behaviour focuses on three different levels, namely the individual, group and organisational levels [KREI95, ROBB01]. The impact of information security on these three levels needs to be considered when an organisation wants to instil acceptable information security behaviour in its employees. On an individual level, employees could be encouraged to report information security incidents. Management support in information security processes could also be encouraged at a group level. An example of such behaviour at an organisational level could be that an information security policy needs to be implemented.

Figure 1 presents the three levels of organisational behaviour. At each level, different issues were identified, which need to be addressed concerning the promotion of a culture conducive to the protection of information assets. The activities of competitors could for instance have an impact on the issues in each of the three levels. An example could be that more organisations are moving towards implementing ISO17799 [ISO99] certification because their competitors or customers are demanding it. This change will have an impact on the organisational level where the information security policy will have to be reviewed. Therefore, a financial plan will also be necessary. Management will have to provide their support to implement the new processes, such as asset classification or the procedure to access database information. Individuals will also have to attend training and awareness sessions to enable them to implement the processes. This will have an influence in the way in which people behave towards securing information assets in the organisation. An information security culture emerges where specific behaviour is encouraged, such as to complying with ISO17799. Customers

could now trust that the organisation's information assets are protected and therefore be more confident to conduct business with the organisation.

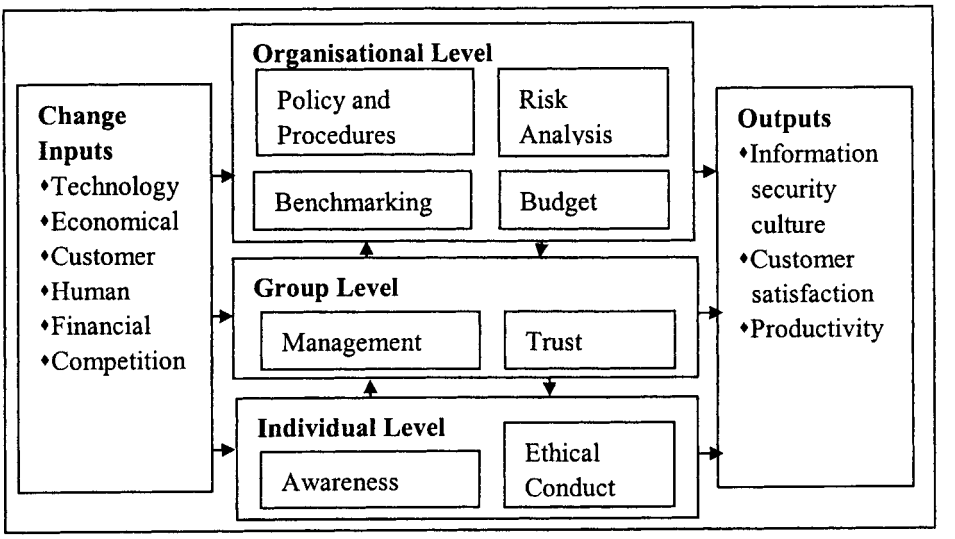

Figure 1. Information security culture model

The following paragraphs provide a brief discussion on each of the three levels and the different issues in each level.

3.1 Organisational Level

All processes and structures start at organisational level. Processes such as risk assessment and procedures for reporting security incidents need to be developed. Structures for information security processes will be established through policies providing the lay-out and framework to implement the processes. Policies on employee behaviour, e.g. what is and what is not acceptable, need to be compiled. Without these processes in place, individual employees will not know how to behave or what is expected of them even though they may be willing to adhere to the information security policy, for instance.

3.1.1 Policies and Procedures

The information security policy dictates employee behaviour and states what is expected of employees, which in time becomes part of the information security culture. For employees to behave according to what is expected, they need to be aware, educated and trained.

3.1.2 Benchmarking

By benchmarking an organisation, guidelines on information security processes, such as awareness, training and asset classification, are incorporated into the organisation. This will enable the organisation to compare itself to other similar organisations and to international standards. It will also provide guidance for the employees' interaction with information assets so that they behave accordingly, thereby ensuring the security of information. This will aid in instilling an accepted information security culture.

3.1.3 Risk Analysis

Through risk analysis, organisational assets, threats to them, and security measures can be identified to develop the information security policy. This will enable the organisation to incorporate the necessary information security culture, which could differ between organisations. For instance, for a health care organisation, privacy issues will be a much more important characteristic to pursue in order to protect patient records compared to customer records of a retail store. Employees need to perceive risk analysis as an accepted activity and part of everyday life in the organisation in order to incorporate it as part of the information security culture.

3.1.4 Budget

A financial plan is necessary to implement the issues concerning an information security culture. For instance, employees need training, technical controls need to be implemented and teams need to be enabled to assess the security of networks. Spending on the issues that need to be implemented, e.g. the compilation of an information security policy, needs to be accepted as an everyday activity. Spending on information security will result in a potential revenue generator and business differentiator as it becomes part of the information security culture [MARK01].

3.2 Group Level

Policies will have no meaning if management does not ensure its commitment to and involvement in, them. Management needs to give its support and instil an environment of trust in the organisation in order to implement the issues at organisational level.

3.2.1 Management

Management is responsible for information security [LERG01]. Management develops an organisation's vision and strategy required to protect information assets, which are implemented in the organisation. People will behave in a certain way, guided by the philosophy and strategy, which they follow to ensure the protection of information assets. In time, a culture will begin to emerge, reflecting the vision and strategy as well as the experiences the people had when implementing it. Therefore, management needs to model the correct behaviour since it will become accepted as the way in which things are done and will be the reference for employee behaviour, which will later develop in a certain culture into the organisation.

3.2.2 Trust

Information security is arguably the most important issue in instilling trust in an IT environment [VONS00]. If management trusts its employees and the employees trust management, it is easier to implement new procedures and guide employees through changes of behaviour regarding information security. The perceptions of employees and management of trust between them need to be positive and should be seen as one of the organisation's characteristics, which will aid in instilling an information security culture.

3.3 Individual Level

Individual employees in an organisation each have their own attitudes resulting in certain behaviour. They need to be aware of the processes that were defined at organisational level in order to behave accordingly, since their behaviour and conduct will determine the success of the organisational and group level issues. But if they are not guided and made aware of the issues, they will not be able to act accordingly even if they are willing to do so at an individual level.

3.3.1 Awareness

Since the effectiveness of information security controls depends on the people who are implementing and using it, employees need to be enabled through awareness and training to behave according to what is expected of them in order to ensure the security of information assets. There is a need for an information security culture where employees are enabled and equipped to behave in such a way that they do not pose a threat to the security of information assets in the organisation.

3.3.2 Ethical Conduct

Good practices are not added to an organisation through regulation, incentives and monitoring. They must rather form part of the culture, which is established throughout the organisation [LEGR00]. Therefore, employees need to incorporate ethical conduct or behaviour relating to information security as part of their everyday life in the organisation [TROM01]. Ethical conduct e.g. not copying organisational disks at home or using the Internet for personal gain during working hours, needs to be enforced as the accepted way of behaving in the working environment for the correct information security culture to emerge in time.

3.4 Change

Changes regarding information security need to be accepted positively and managed in such a way that employees are able to incorporate the changes into their working environment. The accepted changes will then in time become part of the information security culture.

An organisation can use the model in figure 1 to guide it in instilling an information security culture. It would, however, be necessary to determine what level of information security culture is present in the organisation. This would give the organisation an idea of what to improve and where to focus its attention in instilling or improving the information security culture. It is necessary to determine employees' perceptions and attitudes regarding the issues that need to be addressed to instil an information security culture.

4. AN ASSESSMENT APPROACH FOR INSTILLING AN INFORMATION SECURITY CULTURE

An assessment approach consisting of a questionnaire was developed to assess the information security culture in an organisation. The main purpose of the questionnaire is to obtain an indication of the information security culture at individual, group and organisational levels. This is determined by different statements based on the nine issues portrayed in figure 1, which need to be addressed at all three levels.

4.1 Structure of the Questionnaire

The questionnaire was constructed by developing forty-five statements, which assess the attitudes and perceptions of employees regarding the

different issues concerning the information security culture. Different measurement scales were used to evaluate the employees' perceptions of the different statements. Multiple-choice scales consisting of a few possible responses from which the respondent could select either one or more than one response were used. Likert-type scales were also used to derive the respondents' degree of agreement or disagreement with other respondents [SURV00]. The following Likert-type scale was used where a respondent could select only one option, namely "Strongly disagree", "Disagree", "Unsure", "Agree" and "Strongly Agree". Table 1 is an extract from five of the statements used in the questionnaire.

Table 1. Extract from the assessment questionnaire

STATEMENTS
1. I know what the term information security implies.
2. I think it is important to implement information security in the organisation.
3. I am trained in the information security controls I am supposed to use.
4. Management assists in the implementation of information security issues.
5. The organisation has a written information security policy.

4.2 Case Study

A case study was conducted in an IT consultancy organisation to evaluate its information security culture. Prior to the evaluation, there was an information security policy in the organisation but no one was aware of it or knew that it was implemented. Information security was not a priority in the organisation and not much effort was made in managing and implementing it effectively. Although the organisation had not had any reports of external security breaches, there were indications of internal security breaches. Before the assessment, management was unsure whether it had an acceptable level of information security in the organisation. Management also felt that information security was not one of its top priorities and that there were no explicit expectations regarding information security behaviour in the organisation.

5. RESULTS

Survey Tracker [SURV00], a statistical software program, was used to analyse the data. Figure 2 gives an indication of the overall findings of the case study, portraying the information security culture of the organisation. The frequency of respondents who felt positive about the issues is given in percentage, which is portrayed against each of the information security culture issues.

A cut-off of 64% on the frequencies was used. This percentage provides a reasonable cut-off to distinguish between positive and potential negative perceptions [ODEN97]. Every bar above the horisontal line indicates a positive area and every bar below the line a developmental area.

The results confirmed that there is a need to incorporate information security as part of the organisation's strategy and that employees are very willing to do this, but that management needs to ensure its commitment and provide guidance in what is expected of employees.

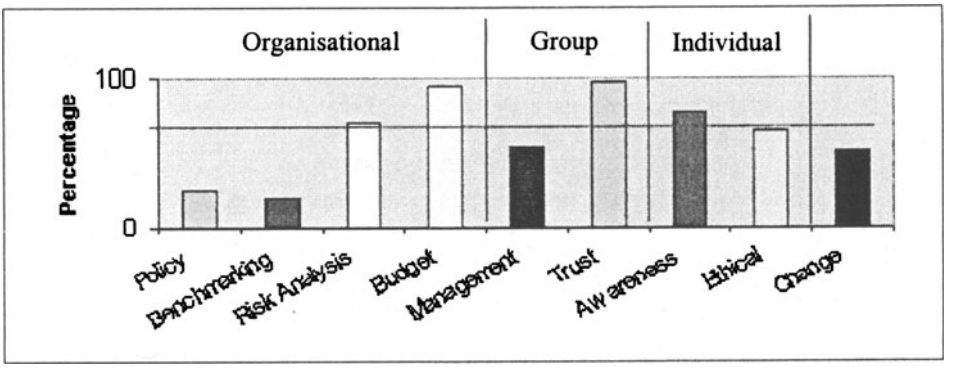

Figure 2. Information security culture

The following is a summary of the findings and recommendations that were made to improve the information security culture.

- The organisational level was one of the critical developmental areas. Most employees were unaware of the information security policy and what was expected of them to aid in securing the organisation's information assets. This implies that the information security policy needs to be reviewed and incorporated into the working environment for the requirements to become part of the everyday activities of the employees.
- At group level, the management issue needs attention. Management needs to incorporate information security as one of the characteristics of the organisation and demonstrate its commitment to, and involvement in, the processes of implementing it effectively. Management needs to appoint a specific team or person to take responsibility for instilling the correct way in which things are done regarding information security.
- At individual level, employees need guidance in what behaviour is acceptable and what is not. The organisation needs to implement procedures such as awareness sessions and training programmes to support and communicate the information security policy from the organisational level. This will encourage employees to adhere to the information security policy, thereby instilling the correct behaviour, which is needed for an acceptable information security culture.

Since the questionnaire was very short and to the point employees were willing to participate in the case study and provide their opinions. They enjoyed forming part of an organisational process to improve information security processes, which also involve them. After the case study, management submitted the findings to the appropriate staff to take responsibility for implementing the changes and reviewing the organisation's information security. Management felt that the results and recommendations could aid the organisation in instilling the correct information security culture.

6. CONCLUSION

An information security culture and the issues that need to be addressed concerning such a culture were defined. The definition can be used as a reference for organisations to understand the concept of information security culture in knowing what it involves and implies.

The assessment approach, which was developed to evaluate the information security culture at the three different levels, was found to provide a thorough indication of the status of the information security culture of an organisation. By making use of the assessment approach, organisations can improve their information security culture by instilling the accepted behaviour at all three levels. In making use of this approach, an organisation can follow the path of enabling itself and its staff to incorporate information security practices as part of their everyday activity in the organisation, which will in time become part of the organisation's information security culture.

In conclusion, one should remember that organisations do not change, but people change organisations. Therefore, an organisation's information security culture needs to be improved by taking human behaviour into consideration to implement information security effectively and lay a foundation to implement the more technical aspects of information security.

7. LIST OF SOURCES CONSULTED

[ANDR00] Andress, M., Manage people to protect data, InfoWorld, Volume 22, Issue 46, 13 November 2000

[BRIN00] Briney, A., Security focused, Information Security, 2000

[CONN00] Connolly,P.J., Security starts from within, InfoWorld, Volume 22, Issue 28, 10 July 2000

[DHILL01] Dhillon, G., Violation of safeguards by trusted personnel and understanding related Information Security concerns,

Computers & Security, Volume 20, Issue 2, 1 April 2001

[ELOF00] Eloff, M.M, Von Solms, S.H., Information Security Management: An approach to combine process certification and product evaluation, Computers & Security, Volume 12, Issue 18, 1 December 2000

[GAUN00] Gaunt, N., Practical approaches to creating a security culture, International Journal of Medical Informatics, Volume 60, Issue 2, 1 November 2000

[ISO99] International Standards Organisation, http://www.iso.ch

[KREI95] Kreitner, R., Kinicki, A., Organisational Behaviour, IRWIN, Chicago, 1995

[LEGR00] Le Grand, C. and Ozier, W., Information Security Management Elements, March 2000, http://www.itaudit.org/forum/auditcontrol/f305ac.htm

[LUND96] Lundy, O. & Cowling, Strategic Human Resource Management, Routledge, London, 1996

[MARK01] Mark, L. Learn to value security as an asset. Computer Weekly, 12 April 2001

[MCLU00] Mclure, S., Scambry, J., Security watch, InfoWorld, Volume 22, Issue 47, 20 November 2000

[NOSW00] Nosworhty, J.D., Implementing Information Security in the 21st century – do you have the balancing factors? Computers and security, Volume 19, Issue 4, 1 April 2000

[ODEN97] Odendaal, A., Deelnemende bestuur en korporatiewe kultuur: Onafhanklike konstrukte? 1997

[ROBB01] Robbins, S., Organisational Behaviour, Ninth edition, Prentice Hall, New Jersey, 2001

[SCHN00] Schneier, B., Secrets and lies, Digital Security in a Networked World, John Wiley & Sons, Inc, NY, 2000

[SURV00] Survey Tracker, http://www.surveytracker.com

[TROM01] Trompeter, C.M. & Eloff, J.H.P, A framework for the implementation of Socio-ethical controls in Information Security, Computers and Security, Volume 20, Issue 5, 1 July 2001

[VENT00] Venter, H.S. & Eloff, J.H.P, Network Security: Important Issues, Network Security, Volume 2000, Issue 6, 1 June 2000

[VONS00] Von Solms, B., Information Security – The third wave? Computers and Security, Volume 19, Issue 7, 1 Nov 2000,

[VONS00] Von Solms, R., Information Security Management: why standards are important, Information Management & Computer Security, Vol7, Issue1, pp.50-57, 1999

[YEAT96] Yeats, D., Cadel J., Project management for information systems, Second edition, Pitman Publishing, London, 1996