Computers & Security (2004) **23**, 191—198

ELSEVIER

Computers & Security

www.elsevier.com/locate/cose

Towards information security behavioural compliance

Cheryl Vroom, Rossouw von Solms*

Port Elizabeth Technikon, Port Elizabeth, South Africa

Received 3 November 2003; accepted 19 January 2004

KEYWORDS
IT auditing;
IS security auditing;
Organizational culture;
Organizational behaviour;
Security compliance

Abstract Auditing has always played an important role in the business environment. With the introduction of information technology and the resulting security challenges that organizations face daily, it has become essential to ensure the security of the organization's information and other valuable assets. However, one aspect that auditing does not cover effectively is that of the behaviour of the employee, which is so crucial to any organization's security.

The objective of this paper is to explore the potential problems concerning the attempt to audit the behaviour of the employee. It will be demonstrated that it is extremely difficult to audit human behaviour and so an alternative method to behavioural auditing needs to be found, where policing the employee is not necessary, but instead a softer, more informal approach is used to change the culture to a more information security conscious one.

Introduction

The role that computers have played in organizations has changed over the years. No longer are businesses simple brick-and-mortar buildings; nowadays some organizations are global institutions spanning across many countries and consisting of thousands of employees.

While this offers so many opportunities, it also has the potential to create many risks. Business transactions and information processing are more vulnerable than ever to threats and risks and need to be protected from these. For this reason information security has become vitally important to virtually any business. The need to verify and investigate that all transactions are correct and unhampered is essential to the success of the organization.

This paper explores the role that auditing plays in the organization with regard to information security. Special attention is paid to the human factor involved in the security of the organization's assets and the disadvantages involved with attempting to audit the behaviour of these employees.

An alternative method to monitoring or auditing the individual needs to be found and therefore this paper examines the behaviour and culture of the organization at all levels with the

* Corresponding author.
E-mail addresses: cherylv@webmail.co.za (C. Vroom), rossouw@petech.ac.za (R. von Solms).

0167-4048/$ - see front matter © 2004 Elsevier Ltd. All rights reserved.
doi:10.1016/j.cose.2004.01.012

objective of finding a viable option to auditing the individual.

Auditing in business

For as long as business transactions have been carried out, there has been a need to verify these transactions to ensure that they are correct and justified and therefore auditing is used in the organization.

According to the International Auditing Guidelines, auditing is defined as (Taylor et al., 1987, p. 23):

> "*the independent examination of financial information of any entity, whether profit-oriented or not, and irrespective of its size, or legal form, when such an examination is conducted with a view to expressing an opinion thereon*"

Auditing is used as a safeguard in order to improve and add value to the operations of the organization. Auditing dates back as far as 3500 BC, where evidence has shown that transactions were double-checked and verified for accuracy and fairness (Sawyer and Dittenhofer, 1996, p. 7).

This traditional form of auditing concentrates on the financial aspect of the business, but as organizations have expanded globally, auditing the financial transactions only is no longer enough. The introduction of information technology into the organization's daily operations has ensured that auditing beyond only the financial documentation is required.

Nowadays, computers play an irreplaceable role in business with virtually all organizations using some form of technology to engage in day-to-day operations, whether it is simply faxes and electronic mail, or more technology-based transactions (Langelier and Ingram, 2001, p. 2). Further, in these daily computerized transactions, some form of control or auditing is needed to ensure that this information maintains its integrity, confidentiality and availability (COBIT, 2003). Information technology (IT) auditing is used to fill this void.

IT auditing

IT auditing has developed as a result of information technology increasingly being utilized in all aspects of business and the need to address the risks associated with information processing through technology. The Committee of Sponsoring Organization of the Treadway Commission (COSO) defines the objective of IT auditing as (Paliotta, 1999, online):

> "*using appropriate technological tools and expertise, evaluate the adequacy and effectiveness of control systems addressed to the risks emanating from an organization's application of technology in support of its business objectives*"

In essence, the role of the IT auditor has evolved from the traditional auditor in that it now focuses on information technology and the technical infrastructure of the organization.

For example, software is used to track events on the network, such as modifying directory entries, directory creation and detection, etc. Any violations that occur are then logged and the IT auditor can then review these audit logs using special filters, which produce reports showing specific activities (Sheldon, 2001).

In order to carry out their activities, such as the one above, the auditors make use of the security policies as a baseline from which to operate (Fraser, 1997, p. 8). The security policy of the organization is a formal statement containing the security rules of the company and concerns all people who have access to the technology and information assets (Fraser, 1997, p. 8).

Information security policies

The information security policies of the organization deal with the processes and procedures that the employee should adhere to in order to protect the confidentiality, integrity and availability of information and other valuable assets (BS 7799, British Standards Institution, 1999, p. 1). They contain the security goals of the company as set by the senior management in accordance with the vision of the organization.

In essence they are the guidelines that dictate the rules and regulations of the organization, which in turn govern the security of information and its related information systems (Halliday and von Solms, 1997, p. 12) and the auditors use these security policies to carry out their audit.

However, some type of auditing needs to be done on these policies of the organization to ensure that they are indeed in the best interests of the company as well as in agreement with best practice standards. While IT auditing concentrates mainly on the technological side of the business, IS security auditing has developed to specialize in the

security of information processing as dictated by these information security policies. The policies, as well as the processes, procedures, controls etc., need to be audited to ensure that they are in line with the objectives, goals and vision of the organization.

IS security auditing

IS security auditing involves "providing independent evaluations of an organization's policies, procedures, standards, measures and practices for safeguarding electronic information from loss, damage, unintended disclosure, or denial of availability" (Langelier and Ingram, 2001, p. 6). These audits are performed when the specific audit objective is to evaluate the security of information or the audit objectives are broader, but evaluating security is a necessary part of the audit plan.

This form of auditing has become an important aspect in auditing the organization today. It is useless to audit a company's financial accounts without first evaluating and verifying that the security involved in protecting this information is appropriate and adequate (Langelier and Ingram, 2001, p. 6).

However, the forms of auditing that have been examined only deal with the technological, strategic or operational side of the organization. From the previous sections it can be concluded that traditional auditing concentrates on the financial transactions of the organization. IT auditing addresses the technological side and the infrastructure of the business and IS security auditing contends with the actual security issues with regard to information and the other valuable assets of the organization.

Each of these forms of auditing deals only with the technical aspects of the organization. The finances, technology, security and infrastructure of the business are all dealt with, but one aspect is not addressed, that of the human factor. Whether paper-based or computerized transactions occur, this auditing is technical in nature and it tends to ignore the human side of operations. The behaviour of the employee is not taken into consideration, only the results of the behaviour.

For example, if an unauthorized employee attempts to access information, the audit logs will record this. Unfortunately, it may go undetected until the auditor reviews the documentation. The results of the employee's behaviour and actions have been detected and audited, but not the behaviour itself. This demonstrates that auditing verifies only the consequences of the behaviour, not the actual behaviour.

In order to understand the enormous influence that the employee has on the business with regard to information security, the role that people play in securing information must first be examined.

The human factor

The role of the employees is vital to the success of any company, yet unfortunately they are also the weakest link when it comes to information security. Security incidents regarding insiders of the organization exceed the amount of security breaches with outsiders, which demonstrates the fact that the actual employees are an enormous threat to the well being of the company (Information Security Industry Survey, Briney, 2001, p. 6).

According to the 2001 Information Security Industry Survey, of all the security breaches perpetrated by the employees of the organization, 48% of them were accidental. This demonstrates that not all security breaches are maliciously intended, but may be the result of negligence or ignorance of the security policies of the organization. Of the remaining security breaches, 17% was intentionally committed, and of the other 35%, it was unsure whether it was malicious or not.

Fig. 1 demonstrates the percentage of insider security breaches experienced by companies in 2000 and 2001, according to the 2001 Information Security Industry Survey. These statistics show that the employees are responsible for a large number of security incidents in companies.

This behaviour of the employees is not acceptable, therefore efforts need to be made in order to reduce these percentages, yet companies tend to ignore these statistics and instead focus on the outsider breaches. They spend more money on strengthening the technical side of the organization, but relatively little attention is paid to the human aspect with regard to security incidents

Insider Security Breach	2000	2001
Installation / Use of unauthorized software	78%	76%
Using company resources for illegal purposes	60%	63%
Using company resources for profit	60%	50%
Abuse of computer access controls	56%	58%
Physical theft, sabotage or intentional destruction of computing equipment	49%	42%
Installation / Use of unauthorized hardware	47%	54%
Electronic theft, sabotage or intentional destruction of information	22%	24%
Fraud	9%	13%

Figure 1 Information security industry survey—insider breaches.

(Information Security Industry Survey, Briney, 2001, p. 4).

It is imperative that the employees behave and act responsibly in order to adhere to the prescribed security policies of the organization, and to do this some form of evaluation is required to investigate the performance of the security behaviour of the individual.

However, very little evidence could be found that auditing of the behaviour of the employee with regard to information security occurs in practice. A parallel must be drawn where this type of evaluation is used in business expansively, and is well documented, in order to investigate whether it would be a viable option to audit the behaviour of the employee.

In conclusion, there is a real need to find a method to ensure that the behaviour of the employee is in compliance with the company policies. By auditing the individuals, attempts could be made to stem the occurrences of security incidents from within the organization.

Problems evaluating employees

Investigating employee behaviour with regard to information security would be similar to conducting performance appraisals. Both analyze employee behaviour with regard to certain aspects of the business, except that performance in the workplace is more outcomes-based and so can be more easily evaluated. Yet, even in this type of appraisal, there are a number of documented problems (Szilagyi and Wallace, 1990, p. 527).

In the court case, Brito vs. Zia, Zia, a major subcontractor of Los Alamos National Labs, lost their case for laying off a number of employees due to performance appraisals. The employees won their case for two reasons. Firstly, the performance evaluations were not conducted in a controlled environment, and secondly, many of the supervisors making the evaluations were not sufficiently familiar with those employees they were evaluating (Szilagyi and Wallace, 1990, p. 515).

The major problems associated with performance appraisals, as demonstrated in the example above, can be summarized in two words—reliability and validity (Szilagyi and Wallace, 1990, p. 527). Together they describe the adequacy of the information gathered as well as the quality of the entire evaluation process. If the appraisal and the ensuing information is not reliable and valid, then the resulting basis for decision-making would prove to be useless.

The problem is that there are so many factors that can negatively influence the validity and reliability of the appraisal and its results (Cooper, 1981, p. 220). Fig. 2 highlights the problems

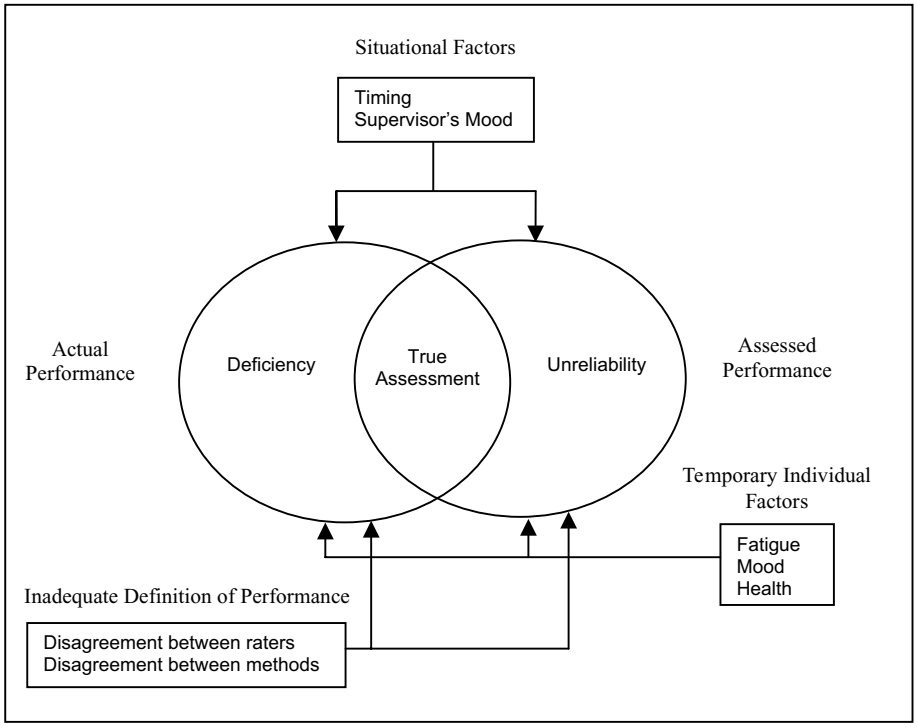

Figure 2 Cooper's sources of error in performance appraisal.

involved in performing accurate appraisals and the reasons for these problems. The methods used to evaluate performance vary, combined with negative individual and situational factors, all impact negatively on appraisals.

For example, personal factors of the employee or the evaluator would affect the outcome. The mood of the evaluator or his dislike for an employee would affect the appraisal. Likewise, a family crisis for the employee would influence his or her performance of the day of the appraisal.

All these factors at some point play a part in distorting the accuracy of a performance appraisal. It can be argued that similar problems would also arise when attempting to "audit" or evaluate the employee's behaviour with regard to information security.

Aside from these two major factors, namely reliability and validity, that would affect the outcome of an evaluation of an employee, a number of practical obstacles come into play when attempting to investigate the employee and his behaviour. In order to do a thorough evaluation, large amounts of resources and manpower would be needed. There are just too many factors that have the potential to play a disruptive role when attempting to audit employee behaviour.

People do not behave like machines in that they are erratic and unpredictable at times and therefore constant monitoring of employees would be impractical, expensive and time-consuming. The legal implications also need to be taken into consideration if management is going to use these evaluation results for basing decisions regarding the employment of the person, as shown in Brito vs. Zia.

The problems mentioned above are only a few of many that would be encountered when attempting to evaluate people and their information security behaviour in the organization. A formalized, structured approach would prove to be extremely difficult, both logistically and practically.

For these reasons, an alternative approach needs to be found, where auditing the employee is not necessary, yet where the actions and behaviour of the employee are proven to be in line with the objectives of the organization as dictated by the policies. In order to do this, the organization and the interaction between the employees need to be studied. Therefore the culture of the organization should be examined. Understanding how people behave individually and as a whole in an organization would assist in attempting to structure the business in a way that would be conducive to information security consciousness.

Organizational culture

According to Edgar Schein, a leader in the study of culture, organizational culture can be defined as (Schein, 1999):

> *"the pattern of basic assumptions that a given group has invented, discovered, or developed in learning to cope with its problems of external adaptation and internal integration, and that have worked well enough to be considered valid, and, therefore to be taught to new members as the correct way to perceive, think, and feel in relation to those problems."*

Organizational culture includes the ideas shared by the people of the company and communicated between each other, basically a system of learned behaviour (Szilagyi and Wallace, 1990, p. 9) and this culture is the single most important factor accounting for success or failure in an organization (Deal and Kennedy, 1982).

A utopian information security culture would be where the employees of the organization follow the guidelines of the organization voluntarily as part of their second nature. For example, it becomes routine for an employee to back up his or her files on the laptop on the first Monday of every month, because it is part of the culture and everybody automatically does it.

By further investigating organizational culture, Schein has developed a model dividing culture into three main layers, as shown in Fig. 3.

The first level is that of the artifacts in the organization. These artifacts are visible and easily spotted by an outsider (Schein, 1999, p. 15). Examples of these would be the architecture and decor of the company. In the information security context, the actual physical security of the organization, such as locked doors, would be an artifact.

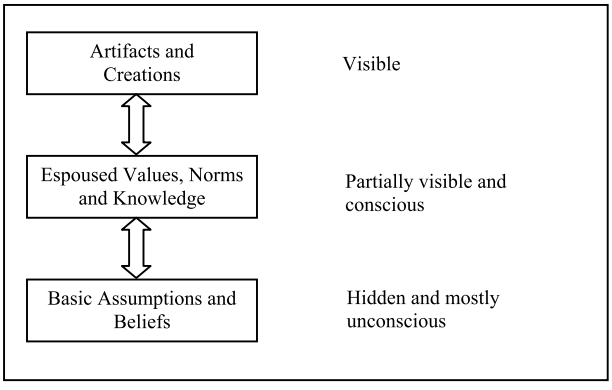

Figure 3 Schein's model of organizational culture.

The second level in Schein's model is the espoused or shared values. These are partially visible in the organization and reflect the values of a particular group of individuals (Schlienger and Teufel, 2002, p. 3). Examples of these include good communication and teamwork (Schein, 1999, p. 17). The information security strategy dictated by the senior executives and resulting in the artifacts in the form of information security policies, would be considered the espoused values of the organization.

The final and deepest level in the organization would be the basic tacit assumptions. These are hidden and largely unconscious and occur very much at the individual level. These assumptions are the underlying beliefs and values of the people in the company. They were normally the original thoughts and beliefs of the founders that have unconsciously been communicated to the employees and form the core of the organization (Schein, 1999, p. 19).

Each of these layers influences the level above or below it. For example, a change in the basic assumptions would result in a change in the shared values of the company. This in turn would affect the artifacts and how outsiders viewed the business. Shared knowledge of the information security policies and an underlying belief in the importance of information security would result in a change in behaviour of individuals and eventually in the organization as a whole.

The culture of the organization would have a huge impact on the security of information, and this could be negative or positive. It is imperative that the culture reflects a positive attitude to information security throughout the whole organization. The behaviour of the employee must be examined so that alternative methods to auditing are found.

Organizational behaviour

Once the cultural side of an organization is understood, one can begin to see how it can be changed to a more secure society. By changing the organization to one that is more in line with information security, the behaviour of the individual will adapt to incorporate security consciousness.

In order to achieve this security awareness, the company needs to be changed at three levels because organizational behaviour occurs on these three levels and different factors affect each one. The three levels of organizational behaviour are (Szilagyi and Wallace, 1990, p. 11):

- The individual
- The group
- The formal organization

As every person is unique, each individual brings various characteristics into the organization. Likewise, there would be assorted organizational forces that would affect the individual employee's attitude, motivation, job satisfaction, etc. Other areas of individual interest would be his or her personality and how it influences and is influenced by the work environment (Szilagyi and Wallace, 1990, p. 11). Thus, the behaviour of the individual plays an important role in the development and evolution of the organizational culture and factors that affect this behaviour need to be conducive to information security.

The group, made up of individuals, develops unique characteristics beyond those of the person and his personal contributions. Groups need to be examined independently and not just as the individuals that make them up (Szilagyi and Wallace, 1990, p. 11). The group values and norms would play an essential role in the way groups of employees would act and behave whilst busy with organizational duties.

The formal organization can be compared according to characteristics common to them, for example the size of the company. The formal organization is influenced by the environment around it and consequently influences its employees and internal operations (Szilagyi and Wallace, 1990, p. 11). Each of these levels in organizational behaviour is not mutually exclusive, but influences each other to form the culture of the business.

Each level in the organization has a different type of behaviour. The way individuals act is different from how the group to which they belong reacts to a situation. In order to change the culture of the organization, it has to be changed at all three of these levels. By changing each level, the overall result would be a change in the culture of the organization. For example, by influencing the group to become more security conscious, the organization as a whole would benefit and therefore the culture would be altered to incorporate information security in everyday routine.

Changing the culture

It would be beneficial to an organization to be able to incorporate security behaviour into the routine of the employees. To achieve this, it would be necessary to change the information security culture of the organization to one that is more in line with the security policies of the business.

In order to begin changing the culture, it is necessary firstly to pinpoint the areas that require change. This can be done by simultaneously investigating the levels of organizational behaviour and Schein's Organizational Culture Model. Schein's model can be used to see how it influences each level in the organization (Fig. 4).

Each level of the organizational behaviour needs to be examined and how it affects the culture of the organization. By categorizing the organization into various groupings, it is a more simplified process to begin with changing the problems associated with information security.

For example, by examining the group, the process can begin by looking at each of the cultural influences and changing them separately. The group is affected and affects the artifacts of the organization. Similarly, the espoused values of the culture influences and is influenced by the group. The basic tacit assumptions and underlying beliefs make up the personality of the individual and the factors which influence this personality directly affect the groups of which the individual is a member.

The following example demonstrates the way in which organizational culture can be changed. Firstly, organizational behaviour is used to change the shared values and knowledge of the group. Once group behaviour begins to alter, it would influence the individual employees and likewise have an eventual effect on the formal organization. The artifacts of the organization would reflect these changes that have been put in place. Slowly but surely, by changing one aspect, it will filter through the organization at a formal and individual level and the culture will eventually change into a more secure one.

In terms of the normal procedures of auditing, the idea of auditing or monitoring the behaviour of the employee is extremely difficult, if not impossible, as discussed previously. The number of factors that could affect the outcome of an audit of the employee, as well as the logistical problems, proves that it is not a favourable means to influence the employee to comply with the organization's information security policies.

An alternative method to auditing should be found and to do this the culture of the organization is a good, solid starting point. Understanding organizational behaviour and how the employee is influenced, would prove extremely helpful in changing the culture of the organization into a more security conscious one.

Conclusion

Auditing has been used in business for a long time, but unfortunately it does not seem like a viable option when dealing with people. The way individuals react to different situations varies from person to person; depending on their personalities and factors which influence them and so cannot be audited en masse as can be done with machines. An alternative method to behavioural auditing needs to be found, but in order to achieve this, the organization, its culture and the organizational behaviour need to be examined.

By studying the organizational culture and behaviour simultaneously, an approach can be found that would change the overall culture of the organization, one level at a time. By using this approach, a less structured and formalized one to auditing or policing, but involving every level of the organization, the change will be gradual but unforced. It would encourage employees to adopt the change as second nature and not resist it because it was forced upon them through the negative aspect of auditing and policing. The benefits of changing culture to engage security automatically in everyday life would positively affect the success of the organization. This can be done using

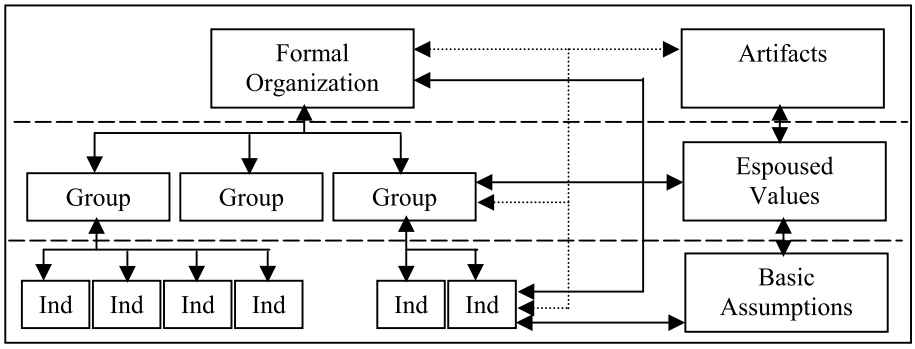

Figure 4 Interaction between the organizational culture and behaviour.

a subtle approach as a viable alternative to forcing employees to think about information security.

References

Briney A. 2001 Information security industry survey. [online]; 2001. Available from: http://www.infosecuritymag.com. [cited September 30, 2002].

British Standards Institution. Code of practice for information security management. DISC PD 0007. London; 1999.

COBIT. Available from: http://www.isaca.org [cited July, 2003].

Cooper WH. Ubiquitous halo. Psychol Bull 1981;218—44.

Deal T, Kennedy A. Corporate culture (the rites and rituals of corporate life). New York: Addison-Wesley; 1982.

Fraser B. Site security handbook. Pittsburgh: Carnegie Mellon University; 1997.

Halliday J, von Solms R. Effective information security policies. In: von Solms R, editor. Information technology on the move, Port Elizabeth. Port Elizabeth Technikon; 1997, pp. 12—20.

Langelier C, Ingram J. National State Auditors Association and the U.S. General Accounting Office: Management Planning Guide Information System Security Auditing. [online]; 2001. Available from: http://www.gao.gov. [cited May 11, 2002].

Paliotta A. A personal view of a world class IT auditing function; 1999. Available from: http://www.isaca.org/art11.htm. [cited July 07, 2002].

Sawyer LB, Dittenhofer MA. Sawyer's internal auditing—the practice of modern internal auditing. 4th ed. Florida: The Institute of Internal Auditors; 1996.

Schein E. The corporate culture survival guide. San Francisco: Jossey-Bass Publishers; 1999.

Schlienger T, Teufel S. Measuring information security culture—a practical approach; 2002.

Sheldon T. Linktionary.com—networking defined and hyperlinked. [online]; 2001. Available from: http://www.linktionary.com/linktionary.html. [cited August 23, 2002].

Szilagyi AD, Wallace MJ. Organizational behavior and performance. 5th ed. Illinois: Scott, Foresman and Company; 1990.

Taylor IR, Kritzinger L, Puttick G. The principles and practices of auditing. Cape Town: Juta & Co Ltd; 1987.

Rossouw von Solms is a professor in Information Technology at the Port Elizabeth Technikon in South Africa. He has published and presented numerous papers in the field of information security. He has been a member of IFIP TC11 since 1995.

Cheryl Vroom is a full-time student in the Department of Information Technology at the Port Elizabeth Technikon in South Africa. She is currently researching towards a master's degree in Information Technology.