AUDITING THE EMPLOYEE IN THE WORK ENVIRONMENT WITH REGARD TO INFORMATION SECURITY

CHERYL VROOM AND ROSSOUW VON SOLMS
Port Elizabeth Technikon, cherylv@webmail.co.za, rossouw@petech.ac.za

Key words: Information Security, Security Auditing, International Auditing Guidelines.

Abstract: This paper serves as part of an ongoing research project into the behaviour of the employee within the work environment regarding information security. Can an employee be audited, like the financial transactions or the information systems? The human factor is of vital importance to the security of information in the organization nowadays, and this element should also be investigated in order to ensure that the policies and procedures are followed properly and effectively.

1. INTRODUCTION

In the current Information Age, organizations often succeed or fail as a result of how efficiently and effectively they are able to process and convert data into useful and valuable information. (Chambers & Court, 1991, p. 12)

This information has become the key factor in decision-making (Vroom & von Solms, 2001, p. 8) causing it to be the company's most valuable asset and should therefore be protected at all costs from any type or level of threat. Safeguarding of information is a priority nowadays, and the employees of the organization play a vital part in the protection of this information.

2. HISTORY OF INFORMATION SECURITY

Information Security and the role of the employee has changed dramatically over the last few decades. (Thomson & von Solms, 1998, p. 167) As the computers in business evolved, so did the profile of the employee within the organization.

Originally, organizations made use of standalone mainframes housed in a separate building in a strictly controlled environment. (Schweitzer, 1987, p. 169) Access to these computer centers was restricted to authorized personnel only and these employees were highly trained computer specialists. The security required was very physical in nature, such as access control and protection against environmental factors, such as floods, fires, etc.

However, with the introduction of the multi-user environment, and thus resource-sharing, the risks to the organization's information increased. (Barnard & von Solms, 1998, p. 172) Many employees could now access information at the same time from various locations.

Physical security was no longer enough and technical controls were introduced as further protection, such as password authentication and authorization. But as further technological advances were made, these controls were insufficient.

With the advent of personal computers and the increasing availability and reliability of networks, many challenges have been brought into the area of information security. (Thomson & von Solms, 1998, p. 168) Previously, the employees that operated the computers were IT specialists, but the profile of the user has shifted since then. Now, virtually all employees have access to the systems of the business, whether computer literate or not. (Thomson & von Solms, 1998, p. 167) Technical and physical controls are not adequate enough to secure the systems and safeguard the assets. The employees have become central to the securing of information and other valuable assets of the organization.

The behaviour of the user can now determine whether information of the organization is kept safe and secure. For example, a password system can be in place to protect valuable information, but if the user writes down the password, the system is compromised and the sensitive and confidential information that the password system should be protecting becomes vulnerable. Therefore, the behaviour of the user is paramount to the protection of company assets.

In order to regulate this behaviour, the employees of the organization need strict and proper guidelines for securing the information. These can be found in the information security policies of the business. The objective of the information security policy is to provide management with direction and support for information security.

3. INFORMATION SECURITY POLICIES

The primary information security policy document should be approved by management and communicated to all employees. Guidance within the policy should include the following: (BS 7799, 1999, p. 3)

- A definition of information security with its overall objectives and scope,
- A statement of management intent, supporting the goals and principles of information security,
- An explanation of the security policies, principles, procedures, etc. as it pertains to the organization,
- Responsibilities for information security management,
- References to documentation that support the policy, namely more detailed security policies.

The detailed security policies consist of the guidelines and procedures that employees need to follow in order to adhere to the primary information security policy of the organization. Employees must also understand that there are consequences and repercussions if the guidelines are not followed.

The difficulty lies in how to establish whether these policy procedures have been followed or not and if they have not, if it was the direct result of employee error. Traditional auditing techniques have been used over the years to examine the financial side of the business, but can it also be used to audit individuals to ascertain if employees of the organization are abiding by the information security policies? In order to establish whether this can be done, traditional auditing and the more recent security auditing techniques have to be studied.

4. HISTORY AND DEVELOPMENT OF AUDITING

Evidence of traditional auditing methods dates back as far as 3500 BC, where the records of the Mesopotamian civilization show tiny marks next to numbers involved in financial transaction. (Sawyer & Dittenhofer, 1996, p. 7)

Auditing has developed systematically through the middle ages and the Industrial Revolution into recent times. Modern auditing began to evolve in South Africa when The Institute of Accountants and Auditors in the South African Republic was formed in 1894 as the first professional accounting body. (Taylor, Kritzinger & Puttick, 1987, p. 3)

According to the International Auditing Guidelines, auditing is defined as (Taylor, Kritzinger & Puttick, 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"*

With the introduction of computers into the business environment and forming an integral part in the daily transactions, traditional auditing is only one component for ensuring that the proper methods are followed. As external and internal threats become more prevalent, companies are being compelled to prove compliance with best practices on security. (Lee, 2002) With this in mind, security auditing has become an essential part of the organization today. An example of this is that the London Stock Exchange already demands auditing for security requirements of listed firms.

Security auditing involves providing independent evaluation of an organization's policies, procedures, standards, measures and practices for safeguarding electronic information from loss, damage, unintended disclosure, or denial of availability. It also serves as a bridge between the executive and the IT level. These security audits confirm to upper management that the policies proposed and active within the business are being carried out effectively (Mimoso, 2002) and that the objectives of the auditor are accomplished.

In order to execute the duties of the auditor responsibly and properly to achieve these objectives, the auditing process entails a series of procedures and activities, which are divided into four concise sections as determined by the GAASS AU015 – The Audit Process: (Taylor et al., 1987, p. 35)

- *Pre-engagement activities*
  These include determining the skills and competence requirements and establishing the terms of engagement.

- *Planning*
  There are a number of distinct sub-stages within the planning section:
  - Obtaining knowledge of the organization
  - Consideration of inherent risk
  - Obtaining an understanding of the system, including internal controls
  - Formulating an audit approach
  - Studying internal controls on which reliance is intended

- *Compliance and substantive procedures*
  This stage is to ensure that controls have worked effectively throughout the auditing period.

- *Evaluating, concluding and reporting*
  The final stage of the audit process involves evaluating and concluding of all information and drafting the audit report.

However, although both traditional and security auditing is vital to maintain and ensure the security of the organization, there is a third facet to auditing of information. Just as the physical and technical controls are no longer enough to secure information because the human factor comes into play, so is the case for auditing of information.

Although auditing analyses in order to find inconsistencies, it does not trace back to the reason why it happened or what can be done to improve it. It examines the problem but not the source of the problem. This is especially relevant in the case of the people of the organization. Traditional auditing techniques can be used to establish whether a procedure or guideline has not been followed, but it cannot determine if the employee did not adhere to the guideline, why it was not followed and how it can be rectified or improved.

Auditing "the mind" of the employee cannot be done using exclusively traditional methods. To do this psychology needs to be involved when examining the source of non-compliance with the information security policies.

5. PSYCHOLOGY IN THE WORK ENVIRONMENT

A number of factors can influence an employee when following guidelines and procedures in a work environment. These need to be studied in order to gain a better understanding of the psyche and resulting behaviour of the people engaged in the organization.

Once this is better understood, effort can be made in order to identify the reasons in behaviour that lead to insubordination with regard to guidelines within the policies. Only then can the deviations from the security policies by the employee be rectified efficiently and effectively.

There are many elements that influence differences in work behaviour, categorized under either individual or situational variables. (Kruger, Smit & Le Roux, 1996, p 12)
Individual variables include the following: (McCormick & Ilgen, 1982)

- Abilities
- Aptitude
- Intelligence
- Personality
- Age
- Sex
- Physical characteristics
- Motivation

Situational variables are related to the influences of the external environment and these can be divided into two categories: (Kruger et al., 1996, p. 13)

- *Working Conditions*
  These comprise of factors surrounding the working environment, such as working methods, equipment, work space, layout, etc.

- *Organizational and Social Variables*
  This refers to the nature of the organization, training available to the employees, the social environment and cultural factors.

These variables influence the behaviour and reactions of the employees to guidelines specified by the organization through the security policies. The goal of the organization is to function as effectively as possible so that objectives are reached and productivity remains within the accepted levels. By not following the guidelines of the policies, employees risk these objectives.

There are a number of psychological reasons that would prevent employees from adhering to these policies, either intentionally or unintentionally. It is important for management to understand basic concepts that lead to guidelines not being followed. Two of these reasons are frustration and conflict, each of which is discussed in the sections below.

5.1 FRUSTRATION

Frustration is a primary factor in causing employees to deviate from organizational policy. According to Plug et al. (1987), frustration can be described as:

> *"the blocking of purposeful behaviour or preventing a person from reaching a goal that will fulfill his/her wish or satisfy his/her need"*

There are several sources of frustration for a person in the work environment: (Kruger et al., 1996, p 69)

- *Environmental Frustration*
  Obstacles are in place that prevents the employee from reaching his/her goal.

- *Delay*
  Constant delay from achieving a goal is a source of frustration.

- *Lack of Resources*
  Extreme frustration can be caused by a lack of resources required to achieve a goal.

- *Personal Factors*
  These include personal loss, a feeling of failure or helplessness which all contribute to the feeling of frustration.

This frustration, regardless of the reason, causes the employee to react in the working environment. There are two types of reactions to frustration: (Kruger et al., 1996, p. 71)

- *Aggression*
  According to Plug et al. (1987), aggression is described as "*a motive for attacking, destructive behaviour or the behaviour itself.*" An example of aggression would be an employee pushing someone in his/her way.

  It was discovered that frustration often precedes aggression. (Freedman, Carlsmith & Sears, 1974) Other stimuli for aggression may also exist, for example, threatening behaviour towards an employee, which causes him/her to become aggressive.

- *Defense Mechanisms*
  People can normally react rationally to anxiety or fear, but on occasion, the individual makes use of an unconscious level of irrational protection methods when he/she does not have the ability to contend with the problem. These methods are known as defense mechanisms.

  The most important defense mechanisms that can influence the work environment include the following:

  - *Rationalization –*
    Fabrications are used to justify or hide behaviour.
  - *Projection –*
    The employee projects his/her own faults onto external objects
  - *Reaction formation –*
    Behaviour patterns are developed that are opposite to their unconscious urges.
  - *Displacement or Substitution –*
    Substitution of feelings from one object to another.
  - *Compensation –*
    The employee experiences a feeling of failure and tries to compensate by achieving in another area.
  - *Regression –*
    When threatened, the person reverts to a former type of behaviour.

- *Identification –*
  Attempts to copy the behaviour of another person.

This kind of behaviour, due to frustration, can hamper the ability of the employee to work to his/her full potential in an effective manner and in accordance with the policies of the organization.

Frustration could cause an employee to react irrationally and in doing so, compromise the security of the organization through non-compliance with the policies and procedures that are established specifically for securing information.

The other concept that can handicap an employee's work performance is conflict experienced in the work environment. Management need to understand this concept, in order to recognize and possibly prevent potentially explosive situations.

5.2 CONFLICT

Conflict is depicted as the "*simultaneous presence of opposite behaviour tendencies or urges*". (Plug et al., 1987, p. 77) There are several types of conflict: (Kruger et al., 1996, pp. 77-80)

- *Approach-Approach Conflict*
  This happens when the choices are equally attractive, occur at the same time and are irreconcilable.

- *Avoidance-Avoidance Conflict*
  This type of conflict is encountered when the choices or objectives are both unattractive, occur simultaneously and are irreconcilable.

- *Approach-Avoidance Conflict*
  This occurs when only one choice or objective exists and can be either negative or positive

- *Multiple Approach-Avoidance Conflict*
  This case occurs when there are two choices or objectives, both with positive and negative qualities.

The psyche and motive of the employee needs to be understood before an attempt can be made to identify and rectify the behaviour that is not in accordance with the best interest of the organization.

Management need to be aware of their employees' demeanor, as this is an indication of their judgement and could therefore predict the behaviour of the person, which could conflict with the organization's policies.

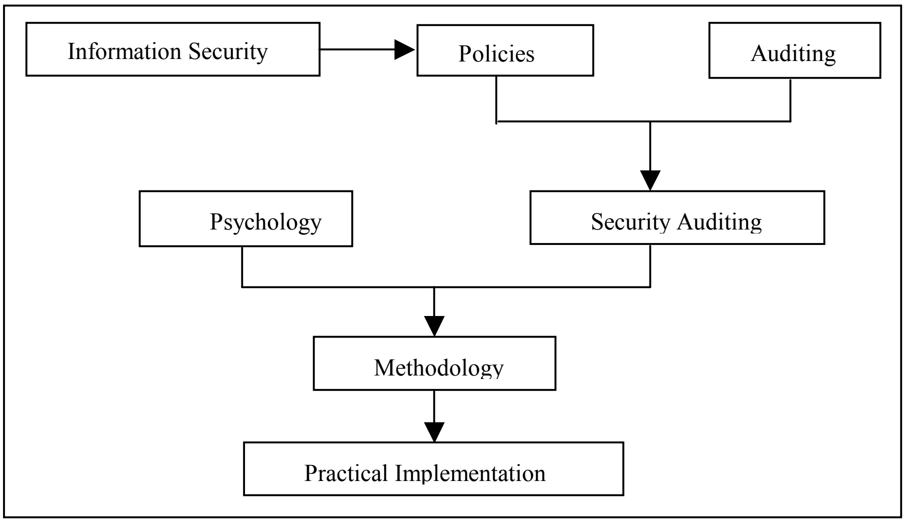
By combining all aspects discussed previously, a foundation can be built for auditing the employee, using adapted security auditing techniques and psychology in the work environment.

6. METHODOLOGY FOR AUDITING THE EMPLOYEE

Security auditing evolved from traditional auditing in order to check and ensure the efficient implementation of the information security policies of the organization.

By adapting security auditing techniques using psychology, it is hoped a methodology can be constructed that will effectively "audit" the employee in the work environment to reveal the reasons for non-compliance with policies, if such is discovered.

Once a methodology has been established, a practical implementation within the organization can be formulated. This practical implementation will eventually serve as an essential element in the protection of assets and the valuable information of the organization.



1.1.1 Research Process

7. CONCLUSION

Information remains the organization's most vital and valuable asset and the human factor plays a greater part than ever in the protection of these assets. Technical and physical controls are limited in their ability to protect by the employees of the organization. The behaviour of all personnel plays a crucial role in the securing of information. Anyone who does not follow the safety guidelines set out in the information security policies risks the security of the business.

Although auditing has traditionally checked financial transactions and more recently the information systems, no attention has been paid to auditing the employee. Traditional auditing methods need to be adapted to enable auditors to understand the behaviour and motivation of the employee in order to prove whether a person has followed the security policies of the organization and if not, why not.

Once this can be established, effort can be made to improve either the behaviour of the employee or change the information security policies to make them more effective in securing the information and assets of the business.

This paper is part of an ongoing research project and the full solution and conclusion are not yet available.

8. REFERENCES

Barnard, L. & von Solms, R. (1998). The evaluation & certification of information security against BS 7799. Information Management and Computer Security 6(2), pp.72-77. MCB University Press.

British Standards Institution. (1999). Code of Practice for Information Security Management. DISC PD 0007. London.

Chambers, A.D. & Court, J.M. (1991). Computer Auditing 3rd Edition. London:Pitman Publishing.

Freedman, J.L, Carlsmith, J.M. & Sears, D.O. (1974). Social Psychology. Englewood Cliffs:Prentice-Hall.

Kruger, S.J., Smit, E. & le Roux, W.L. (1996). Basic Psychology for Human Resource Practitioners. Kenwyn:Juta & Co Ltd.

Lee, C. (2002). Security auditing industry set to grow. [online]. [Cited April 25, 2002] Available from Internet URL http://www.vnunet.com/News/1128237

McCormick, E.J. & Ilgen, D. (1982). Industrial Psychology. London:George Allen & Unwin.

Mimoso, M.S. (2002). Security audits a burden, blessing for CEOs. [online]. [Cited April 25, 2002] Available from Internet URL http://searchsystemsmanagement.techtarget.com/originalContent/0,289142,sid20_gci815265,00.html

Sawyer, L.B. & Dittenhofer, M.A. (1996). Sawyer's Internal Auditing – The Practice of Modern Internal Auditing 4th Edition. The Institute of Internal Auditors:Florida.

Scheitzer, J.A. (1987). How Changes in Computing Practices Affect Security. Computer Security – Readings from 'Security Management' Magazine, pp.167-180. Stoneham:Butterworth Publishers.

Taylor, I.R., Kritzinger, L. & Puttick, G. (1987). The Principles and Practices of Auditing. Cape Town:Juta & Co Ltd.

Thomson, M. & von Solms, R. (1998). Information Security Awareness: educating your users effectively. Information Management and Computer Security 6(4), pp.167-173. MCB University Press.

Vroom, C.S. & von Solms, R. (2001). A Practical Approach to Information Security Awareness in the Organization. Unpublished Btech Thesis. Port Elizabeth:Port Elizabeth Technikon.