INFORMATION SECURITY: AUDITING THE BEHAVIOUR OF THE EMPLOYEE

Cheryl Vroom and Rossouw von Solms
Port Elizabeth Technikon,South Africa, cherylv@webmail.co.za, rossouw@petech.ac.za

Abstract: The following paper serves to examine the evolution of auditing in the organization from traditional financial auditing through the introduction of computers into daily transactions. It discusses the need for information security in business today and the methods that can be taken to verify that the security measures are properly utilized to ensure the safety of information systems. This paper hopes to enhance the future role of the auditor by including auditing the employee and his behaviour.

Key words: Information Security Policies, Operational Controls, Information Technology (IT) Auditing, Information Systems (IS) Security Auditing

1. INTRODUCTION

Many procedures are introduced and precautions are taken to ensure the safety of one of the organization's most crucial assets – information. The integrity, confidentiality and availability of vital company information is extremely important and needs to be protected at all costs.

Auditing plays a huge role in this protection by examining the current procedures that are in place to prevent the misuse of information and to ensure that these measures are effective and efficient. Conventional auditing methods are primarily technical in nature, examining the physical, technical and operational procedures of the business, yet one of the most crucial links to the security of information is often overlooked – the human factor. The people in the business are central to any organization, yet also the most serious threat to it, whether intentional or not. (Martins & Eloff, 2002, p1)

How can the behaviour of the employee be checked and verified to ensure that the individual is carrying out his duties to safeguard confidential and

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: 10.1007/978-0-387-35691-4_52

D. Gritzalis et al. (eds.), *Security and Privacy in the Age of Uncertainty*

valuable information? Can conventional auditing techniques be used to achieve this aim or is a new type of approach needed to ensure the behaviour of the employee is compatible with the goals of the organization with regard to information security?

To answer these questions, auditing and the methods employed by the auditor needs to be investigated with a view to adapting the role of the auditor to incorporate behavioural auditing in information security.

2. TRADITIONAL AND IT AUDITING

Throughout history, the process of auditing has been necessary whenever humans have performed some form of transactions in order to control the accuracy and honesty of finances to a large extent.

The main objective of an audit is to enable a report that is truthful and fair regarding the financial position shown by the balance sheet of the organization. The role of the auditor is to examine the financial statements prepared and provided by the owners and management to ensure that, in his or her opinion, that it is an accurate and fair account of the company's financial position. (Cooper, 1979, p2)

Traditional auditing, however, concentrates solely on the financial records of the organization and the methods that protect these finances. With the introduction of computers to assist in business, the financial side of the organization is no longer the only means that business uses to interact.

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, p12) Therefore, the controls and procedures relating to the handling of information in the organization have become extremely relevant and important. The need for auditing of the technology and tools used in business today became apparent, and therefore IT auditing developed.

However, although the advances in information technology have provided enormous benefits to companies and revolutionized the way that they operate, it also creates significant risks and challenges to the organization. (Langelier & Ingram, 2001, p4)

3. INFORMATION SECURITY AND AUDITING

The confidentiality, integrity and availability of the organization's valuable information could be compromised if proper and stringent security precautions are not in place and carried out effectively. Information security has become a cornerstone in the protection of information in virtually all

organizations nowadays. To carry out effective information security, controls are used, namely physical, technical and operational controls.

The operational controls are those that concern the behaviour and actions of the employee with regard to information security. An organization has physical controls such as lockable doors, but if the employee does not lock the door, it renders the physical control ineffective. Likewise, technical controls, such as password systems, will be impotent if the user of the system writes the password down for all to see. Locking the door and not writing the password down are deemed operational controls.

Operational controls are considered extremely important as the conduct of the employee within the organization plays an increasingly vital role in securing information. In order to regulate this behaviour and conform to the objectives of the company, the employees of the organization need strict and proper guidelines. These guidelines are set out in the information security policies of the organization, detailing the procedures, rules and regulations that need to be followed by the employees in order to preserve the integrity and confidentiality of company information.

However, these security policies need to be audited to ensure that they are in the best interests of the company with regard to the protection of its information and assets. Therefore Information Systems (IS) security auditing has been introduced to ensure that these policies, procedures and regulations are indeed effective enough to meet their individual objectives.

The IS security audits are utilized to ensure that the measures taken by a company to protect their information resources are compliant with the requirements stipulated in the security policies of the organization and to verify that any security breaches of violations are properly recorded. (atsec Information Security GmbH, 2000) Audits on systems and network, security training programs, policies, etc. are performed to ensure that evaluations on virtually all aspects of the company are provided.

However, although traditional and IT auditing, as well as IS security audits all have their role to play, there is another facet to auditing that has not been addressed directly.

The three types of auditing, discussed in the previous sections, all concentrate on the technical aspects of the business – the financial records, information technology and the information security policies and procedures of the organization. Yet auditing is not performed on the employees who actually follow the operational controls that are prescribed. It is simply assumed the employee will adhere to these audited policies.

The actions of the employee are vitally impðrtant to the security of the organization. The behaviour of the personnel and how they react in situations is paramount to the information security aspect of the business and this issue needs to be addressed to ensure that the employees and their behaviour are not the weak link in the information security chain.

4. AUDITING THE EMPLOYEE

Human behaviour is only recorded in the actions that are the result of this behaviour. For example, information can be stolen due to the employee not logging off his computer or leaving the door of his office unlocked. Both the technical and physical controls are not effective in this case because the operational control was not followed, even though the audited policy procedure should be effective if followed.

Therefore, all that auditing results can prove is that although all controls were successfully audited and shown to be effective to the security of information, the information was still stolen. This is due to the human factor. Human behaviour is not performed according to a set of written rules, but according to the personality of the individual.

However, this behaviour can be categorized. Much well-documented research has gone into human psychology and the study of human behaviour. Personnel departments use personality testing during interviews to discover whether potential employees are compatible with the objectives and structure of the organization. In the same vein, can this type of behavioural psychology be used with regard to information security?

The potential for the use of behavioural psychology in the area of information security is enormous. The ability to assess the potential of an employee to violate security policies and procedures is beneficial to the company, but unfortunately it has its drawbacks. It is unethical, and currently unlawful, to target an individual and categorize him as a potential threat to the security of a company.

It may be an academic exercise currently, but the potential for it to become a basis for practical reality in future business is possible.

5. REFERENCES

[1] atsec Information Security GmbH. (2000). Security Auditing and Revision. [online] [Cited May 11, 2002] Available from Internet URL http://www.atsec.com/e/service_auditing.php3.

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

[3] Cooper, V.R.V. (1979). Student's Manual of Auditing. London:Gee & Co (Publishers) Limited.

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

[5] Martins, A. & Eloff, J.H.P (2002) Assessing Information Security Culture. 2nd Annual Information Security for South Africa Conference 2002. Muldersdrift.