Annual Academic Sessions 2012
ISSN 2012-9912; ©2012 Open University of Sri Lanka

INFORMATION TECHNOLOGY AUDIT AND LEGAL COMPLIANCE FROM A SRI LANKAN PERSPECTIVE

M.K.Goonathilaka[1]

[13]*Department of Legal Studies, Open University of Sri Lanka*

INTRODUCTION

With the expansion of Information Technology every field is dominated by its influence including benefits as well as disasters. Therefore IT Audit (Information Technology Audit) has come to the forefront in all major organizations using Management Information Systems in addition to the traditional financial auditing. IT Auditing expands to various areas such as risk assessment, risk management and now embraces the legal field as well. The latest trend is legal audit embracing the IT and financial systems. The requirement of compliance of laws has emerged into the areas of audit thus giving the concept of Legal Audit. Sri Lankan Parliament has passed much legislation such as Computer Crimes Act No 24 of 2007, Companies act No 07 of 2007 and Prevention of Money Laundering Act No 05 of 2006 and compliance of the systems is sought through these new laws.

This paper attempts to discuss the procedure of IT Auditing and how it has its impacts on law taking a quantitative research approach by using 75 IT Audited Companies as a sample.

RESEARCH QUESTIONS

1. How secure are the systems of Sri Lankan IT Audited Companies?
2. How effective is the law to combat issues faced by IT Security systems in IT Audited Companies in Sri Lanka?

THE OBJECTIVES

The objectives of the study were to evaluate the security status in information systems currently used in Sri Lanka, to identify the security implications of the Sri Lankan IT Audited companies and to introduce emerging concepts of legal audit .i.e. compliance. The tool of evaluation was the Information Technology Audit (IT Audit).

SCOPE OF THE STUDY

The scope of the study is to see the Sri Lankan perspective in relation to Information Technology Audit and Legal compliance of the organizations' computer systems.

METHODOLOGY

Methodology followed in this research was mainly the literature research and a pilot case research. For this particular study pilot case study was involved where the data was collected through a questionnaire which involved a representative sample.
The pilot research was for 75 Information Systems in Sri Lanka. The sample was taken by selection of 75 Colombo Security Exchange (CSE) listed IT audited companies, by applying convenience sample method. These organizations belonged to both government and private sectors. A questionnaire was developed to identify possible information security threats in terms of physical, logical and network security measures. The designed questionnaire was

[13] Correspondences should be addressed to Ms.M.K.Goonathilaka, Department of Legal Studies, Open University of Sri Lanka (email: kusalaousl@yahoo.com)

taken as a tool to collect respective data from system users.

RESULTS AND DISCUSSION

IT Audit is a relatively new field in the companies which use computer systems as their management information systems. Engaging in IT Audit the company is able to identify its systems risk, ability to asses risks, manage risk and finally take legal measures if the security of the systems is breached. Effectiveness of IT Audit is to identify any system security breaches as findings of the risk assessment of IT Audit. IT Audit has three tests to evaluate systems security. They are Physical Security, Logical Security and Network Security respectively.

This research focused on all three areas of IT Audit in evaluating the sample under study. Physical security mainly focuses on the areas of physical issues a computer system may face. This basically includes the access to the server room, the temperature, the Air Condition and the humidity of the area where the main server/computer system is installed. Logical security looks at the major areas such as authority to use the system, logins, passwords and the authorized access to the files and documents. Network security involves the areas of networks, internet and intranet security, the access to the network of the company and the use of firewalls.

Then the discussion focuses on the findings of this research which applied the above tests by carrying out the IT Audit and the role of law played by the specific statutes. This study focused on all three areas of security information systems namely physical security, logical security and network security.

Following findings could be seen when the data was analysed. Table 1 depicts the findings of the research conducted.

Security Level	Positive Organizations	Negative Organizations	As a Percentage P= Positive N=Negative
Physical Security	69	6	P=92%, N=8%
Logical Security	70	5	P=93.33%,N=6.66%
Network Security	54	21	P=72%,N=28%

Table 1: Implemented Level of IT Security of the Representative Sample

69 organizations out of 75 had implemented physical security measures. This was as a percentage 92%. This showed a positive result in physical security implementation. Only 6 out of 75 organizations had not implemented any level of physical security. As a percentage it was only 8% of the representative sample.

70 organizations out of 75 selected organizations had implemented logical security measures. This was as a percentage 93.33%. This showed a positive result in logical security implementation. Only 5 out of 75 organizations had not implemented any level of logical security and gave a negative result of 6.66% for the logical security implementation.

When compared to physical and logical security implementation level a low percentage was seen for the network security implementation. 54 organizations out of 75 selected organizations had implemented network security measures. This was as a percentage 72%. However this percentage also showed a positive result in network security implementation. 21out of 75 organizations had not implemented network security at any level and gave a

negative result for the network security implementation. As a percentage it was 28% of the representative sample. The systems surveyed had 92% of physical security implemented. This was in the range of basic security for example having key lock systems to very high physical security implementation such as swipe cards and finger scans. However it was seen that Sri Lanka still had not gone to the extent of retina scans in terms of physical security.

This study had a limitation where the author had to rely on the questionnaire method and as a result to take the feedback and the information given by the information/system user. Also observation method was helpful when checking the physical security measures. Therefore the data given by information users for the physical security was 100% reliable and the author could validate the answers in this security area with high confidence.

Then the study focused on logical security in which 93.33% of the selected organizations had implemented logical security. As in physical security implementation level, the logical security implementation also was in the range of basic to medium and to high level implementation such as encryption.

Very few information systems had encrypted standards and user awareness on encryption. However most of the systems had password policies and password implementation. Also systems were secure in terms of authorized logins and locking the system when the user was not available.

Network security implementation result showed 72% had taken security measure in relation to network security. This was basically implementing firewalls and banning insecure websites from the corporate internet.

It could be seen from this study the information systems used in the research had overall high security measures implemented. Breach of such security measures could only be identified through conducting a proper Information technology Audit which was not in the scope of this study.

The legal measures and the role of law through the Computer Crimes Act No 24 of 2007 could be taken if such breach was uncovered and reported respectively. Then part II of the Act could take specific action in relation to investigations and the experts to be named in such an investigation procedure. Practices introduced through Prevention of Money Laundering Act No 05 of 2006 and its amendments are controls which enhance system security. Thus in addition to other audits, legal audit also comes to the limelight.

If a proper IT Audit could be conducted a clear insight to logical and network security implementation level could be revealed. However even if an IT Audit is carried out, the report which disclosed the findings were not available to all but only to the higher management like Board of Directors of the organization, since the IT Audit report was highly confidential disclosing breach of security in the organization and accessing legal measures was at the discretion of the higher management. Therefore the role played by law could be also limited in such a situation and access to the law was at the hands of the higher management of the organization.

Awareness through user education is a very good method which could be adopted within organizational level. Through this users could be educated of such security breaches and can prevent future attacks. Also user awareness of new security measures and standards like BS 7799(ISO17799) could be provided to the system users to be precautious and to strengthen their security implementation.

Complex Information Technology tools could be used to enhance and strengthen the security of the system to overcome security breaches in future. Also legal measures such as mandatory laws could be passed for organizations to be in compliance with IT security to adopt security

standards.Sri Lankan organizations had adopted one such mandatory measure was implementing IT Audit to be in compliance with Companies Act No 07 of 2007.

The objective of the study evaluating Sri Lankan information systems in terms of their security implementation standard which was achieved in this research.

Also exploring the measure of law in a case of breach of such security was also achieved by taking the options the role of law could play such as bringing the offenders to the law under the existing law such as laws to prevent money laundering,. Achieving the objectives of awareness through education and also strengthening the IT systems was also achieved.

Next the focus was on the role law and litigation plays in the above mentioned IT security risks. IT Audit would find the possible risk areas and how the Information Systems lacks protection. Also the Audit report would highlight issues and possible prevention clauses which should be taken. Not only reporting issues IT Audit could highlight the software licensing problems and the road to identify the intruders. Then the law automatically had come into the scenario. Filing action against the intruders in a court of law was the responsibility of the management of the organization. Litigation would start accordingly and to punish the offenders and demanding compensation was based on Computer Crimes Act No 24 of 2007.This clearly identified sections on how to bring offenders to the law and to punish them accordingly with imprisonment and or with fines.

The CISA Review Manual (2007) stated that legal repercussions can be there due to the computer crime issues and exposures. It further stated that there are numerous privacy and human rights laws an organization should consider when developing security policies and procedures. These laws can protect the organization but also can protect the perpetrator from prosecution. In addition not having proper security measures could expose the organizations to lawsuits from investors and insurers if a significant loss occurs from a security violation. The IS Auditor should obtain legal assistance when reviewing the legal issues associated with computer security. (CISA Review Manual, 2007)

Legal compliance is also sought through by adopting the practice of checking the systems and organizations for compliance with the existing laws of Sri Lanka. This brings the scenario of Legal Audit and in near future Computer Crimes Act No 24 of 2007 has much role to play in terms of prosecuting the offenders.

CONCLUSIONS

The importance of identifying IT security risks, the role of IT Audit and finally how the law would help to protect IT security systems are the main highlights of this paper. The conclusion stresses the fact that legislation and litigation is not the final answer, which should be in the hands of ICT professionals who should find new security measures in addition to the existing ones to override the hackers and computer attackers' new endeavors, methodologies and loopholes.

REFERENCES

CISA Review Manual.(2007).ISACA,USA.

Companies Act No 07 of 2007, Sri Lanka.

Computer Crimes Act No 24 of 2007,Sri Lanka.

Prevention of Money Laundering Act No 05 of 2006, Sri Lanka.