COMPUTER INFORMATION SECURITY AUDIT: PROCEDURES FOR POLICY DESIGN AND IMPLEMENTATION.

J. U. B. AZUBIKE (Ph.D, FCA)
Chief Lecturer in Accounting, Abia State Polytechnic, Aba.
Email: jubelazubike@yahoo.com | Phone No: 08033503747.

ABSTRACT
"Audit" is a word which generally sends shivers down the spine of even the most hardened chief executive. Most audits that we know today cover mainly financial affairs and physical security matters giving rise to financial audits and physical security audits respectively. These audits are often conducted by financial auditors. Information security audits on the other hand is concerned with the confidentiality, availability and integrity of an organization's computer information network. Relevant secondary data were obtained from existing literature to expound this new but pertinent audit exercise. The paper has also recommended it to all organizations that are Information Communication Technology (ICT) driven.

INTRODUCTION

Information security audit is essentially an assessment of how effectively an organization's security policy is being implemented. It is a systematic, measurable technical assessment of how the organization's security is employed at a specific site. Information security audits are part of the on-going process of defining and maintaining effective security policies. The audits provide a tool for a fair and measurable way to examine how secure a site really is. Information security audits are performed through personal interviews, vulnerability scans, examination of operating system settings, analyses of network shares and historical data (Gailegos, Senft, Mansona and Gonzale :2004). The audit attempts to answer some key questions such as:

- Are passwords difficult to crack?
- Are there audit logs to record who accesses data?
- Are audit logs reviewed?
- Have all necessary applications and computer services been eliminated for each system?
- Have custom built applications been written with security in mind?
- How have these custom applications been tested for security flaws?
- How is back-up media stored? Who has access to it? Is it up-to-date?
- Is there a disaster recovery plan? Have the participants and stakeholders ever rehearsed the disaster recovery plan?
- How are configuration and code changes documented at every level? How are these records reviewed and who conducts the review (Kessinger: 2010). These are issues often addressed in an information security audit. However, this study aims at addressing the following: to ascertain the relationship between information security audit and physical security audit, to evaluate information security audit tools, and to make appropriate recommendations.

INFORMATION SECURITY STANDARDS

In the United States of America, the Cyber Consequences Unit (CCU) has developed a cyber security checklist to help US federal agencies to determine the possible consequences of risks posed by the current state of their IT systems. In addition, Information Security Auditing Standards are mandatory requirements for certification holders' reports on the audit and its findings. Auditing Guidelines and Procedures are detailed guidance on how to follow those standards. The Information Security Auditing Guidelines are guidelines an Information Security Auditor will normally follow with the understanding that there may be situations that the auditor will not follow that guidance. (Adaikkappan: 2009). The Open Source Security Testing Methodology Manual (OSSTMM) is an opened standard methodology for information security tests. When an internal testing methodology is used, the brain trust of a handful of information security

experts is leveraged. This manual is powerful because it provides the collective best practices, legal and ethical condusive global security testing community (Adaikkappan,2009).

LOGICAL SECURITY AUDIT AND TOOLS

The first step in any audit is to seek to understand its components and its structure. The following are key points in auditing logical security: passwords, termination procedures, special user accounts and remote access (Kessinger, 2010). Every company should have written policies regarding passwords and employee's use of them. Passwords should not be shared and employees should have mandatory scheduled changes. They should also be aware of proper log on/log off procedures. Also helpful are security tokens, small devices that authorized users of computer programmes or networks. The most popular type of security token (RSA's SecurID) displays a number which changes every minute. Users are authenticated by entering a personal identification number and the number on the token. (Kessinger, 2010).

The existence of proper termination procedures ensures that old employees can no longer access the network. This can be done by changing passwords and codes. Also all identify cards and badges that are in circulation should be documented and accounted for. Remote access is often a point where intruders can enter a system. The logical security tools used for remote access should be very strict. Remote access should be logged. Special user accounts and other priviledged accounts should be monitored and have proper controls in place.

Network security is achieved by various tools including firewalls, proxy servers, encryption and antivirus software. (Information Security Audit Compliance Association ISACA:2003). Firewalls are a basic part of network security. They are often placed between the private local network and the Internet. Firewalls provide a flow through for traffic in which it can be authenticated, monitored, logged, and reported. Some difficult types of firewalls include: network layer firewalls, screened subnet firewalls, packet filter firewalls, dynamic packet filtering firewalls, hybrid firewalls, transparent firewalls and application level firewalls.

Proxy servers hide the true address of the client workstation and can also act as a firewall. Proxy server firewalls have special software to enforce authentication. Proxy server firewalls act as a middleman for user requests. The process of encryption involves converting plain text into a series of unreadable characters. If the encrypted text is stolen or attained while in transit, the content is unreadable to the viewer. Once encrypted information arrives at its intended recipient, the decryption process is deployed to restore the hypertext back to plain text (Gordon: 2006).

Logical security includes software safeguards for an organization's systems, including user identity and password access, authentication, access rights and authority levels. These measures are to ensure that only authorized users are able to perform actions or access information in a network or a workstation. Antivirus software programs such as McAfee and Symantec software locate and dispose off malicious content.

These virus protection programs run live updates to ensure they have the latest information about known computer viruses (ISACA:2004).

Auditing systems tack and record what happens over an organization's network. Log management solutions are often used to centrally collect audit trails from heterogeneous systems for analysis and forensics. Log management is excellent for tracking and identifying authorized users that might be trying to access the network, and what authorized users have been accessing in the network and changes to users' authorities. Software that record and index user activities within window sessions such as Observe Information Technology (ObservIT) provide comprehensive audit trail of user activities when connected remotely through terminal services, citrix and other remote access software. (ISACA: 2005)

AUDIT PLANNING, PREPARATION AND OBJECTIVES

The security auditor would first obtain background information about the company and its critical business activities before conducting a data centre review. The review has the objective to align data centre activities with the goals of the business while maintaining the security and integrity of critical information and processes. According to Kolker (2006), the following procedures help to effectively determine if whether or not the client's goal is being achieved.

- Meet with Information Technology (IT) Management to determine possible areas of concern,

- Review the current IT
- Review the company's IT policies and procedures,
- Review job descriptions of data centre employees, and
- Evaluate the company's IT budget and systems planning documentation. The auditor should consider multiple factors that relate to data centre procedures risks in the operating environment and assess the controls in place that mitigate those risks.

Hamidovic (2011) observes that information security audit test has the underlisted objectives which the auditor reviews:

- Personnel procedures and responsibilities including systems and cross-functional training,
- The data centre has adequate physical security controls to prevent unauthorized access to the data centre.
- Appropriate back-up procedures are in place to minimize downtime and prevent loss of important data.
- Adequate environmental controls are in place to ensure equipment is protected from fire and flooding.
- The data centre has adequate physical security controls to prevent unauthorized access to the data centre.

To collect evidence to satisfy data centre, audit objectives involves travelling to the data centre location and observing processes and procedures performed within the data centre. Certain review procedures should be conducted to satisfy the pre-determined audit objectives. These include:

- Data centre personnel – They should be adequately educated about data centre equipment to properly perform their jobs.
- Policies and procedures – All data centre policies and procedures should be documented and located at the data centre. Important documented procedures include: data centre personnel job responsibilities, backup policies, security policies, employee termination policies and overview of operating systems.
- Backup procedures - The auditor should verify that the client has backup procedures in place in the case of system failure. The client should maintain a backup data centre at a separate location that allows them to continuously continue operations in the instance of system failure.
- Equipment – The auditor should verify that all data centre equipment is working properly and effectively. Equipment utilization reports, equipment performance measurements and system downtime records all help the auditor determine the state of data centre equipment.
- Physical security/environmental control – The auditor should assess the security of the client's data centre. Physical security includes bodyguards, locked cages, mantraps, single entrances, bolted down equipments and computer monitoring systems. Additionally, environmental controls should be in place to ensure the security of data centre equipment. These include airconditioning units, raised floors and humidifiers. (Hamidovic, 2011)

PROCEDURE FOR POLICY DESIGN AND IMPLEMENTATION

Management adopts an organization's internal control structure. It selects control policies, practices and procedures for its accounting systems to provide reasonable assurance of preventing and detecting errors and irregularities. These help to safeguard assets and to ensure accurate and reliable accounting data. These control policies, practices and procedures that ensure accurate and reliable data provide data integrity. Because computers contain records and authorize transactions regarding assets, the controls that safeguard computer files also safeguard assets thereby providing data security (Boockholdt:1999). Security features prevent unauthorized access and thereby safeguard the organization's assets. A computer-based system that safeguards its data from risk is one that provides adequate data security (Boockholdt:1999).

According to Gordon (2006), an efficient information security system can be achieved if the auditor bears the following issues in mind while designing and implementing information security audit systems:

- weaknesses in data security allow risks from three sources: internal, external and collusive;
- All accounting data are important, but certain data and files are vital to the operation of any organization. These include accounts receivable and accounts payable,
- Managers are continually concerned about the actions and plans of competing companies. Espionage is primarily an external threat. However, a competitor may also gain access to sensitive data by collusion with an employee,
- Computerized data files contain much personal information about individuals. Disclosure of this information is an invasion of privacy. Threats to privacy come from hackers and from employees,
- Major frauds endanger the ability of an organization to continue its operations. Control policies and procedures protect against fraud by lower-level employees, and
- The use of database management system (DBMS) ordinarily results in greater reliability of data than in a traditional data file system. This centralized control reduces the risk of fraud and error.

Further to the above, Boockholdt (1999) opines that the auditor should observe the under listed guidelines in computer information security audit system design and implementations. The auditor should design the system in such a way to:

- Ensure that the system should be able to tell the user what to do next after every step,
- Use a display to communicate only one data in the system at a time,
- Ensure that information stays on the screen long enough for users to read them,
- Use display features to emphasize important things,
- The system should be designed to anticipate the errors a user is likely to make in systems audit.

CONCLUSION AND RECOMMENDATIONS

Information security audit differs from a normal physical security audits. Information security audit is essentially an audit of how confidentiality, availability and integrity of an organization's information is assured. An information security audit is one of the best ways to determine the security of an organization's information without incurring the cost and other associated damages of a security incident.

The study has shown that by and large, the two concepts of application security and information are both in many ways connected and they both have the same goal to protect the integrity of the companies data and to prevent fraud. The paper evaluated the various information security audit tools including firewalls, proxy serves, encryption and antivirus software. The study shows that all the information security audit tools are useful and relevant for information security audits.

It is recommended that continuous information security audits should be implemented or conducted even more regularly than a physical security audit. It is also recommended that application of logical security audit tools of firewalls, proxy servers, encryption and antivirus software be used in the conduct of the audit.

REFERENCES

Adaikkappan, A. (2009), **Application Security** Controls: An Audit Perspective, Online: http://www. wikipedia. com, Retrieved 25/04/2011.

Boockholdt, J. (1999), **Accounting Information Systems**, Boston: Irwin McGraw-Hill Companies.

Galleyos, F. Senft S, Manson DP, & Gonzales, C. (2004), **Technology Control and Audit**, NY, Auerbach Publications.

Gordon, L. (2006), **Top 100 Network Security Tools** Online: http://www.wikipedia.com, Retrieved 25/04/2011.

Hamidovic, H. (2011), **The Relevance of IT on Criminal Investigations,** http://www.wikipedia.com, Retrieved 26/04/2011.

Kessinger, B. C. (2010), **Information Technology Compliance Past, Present and Future**, http://www.wikipedia.com, Retrieved 25/04/2011.

Information Security Audit Compliance Association, ISACA (2003), **Approach to Auditing Network Security**, http://www.wikipedia.com, Retrieved 26/04/2011.

Information Security Audit Compliance Association, ISACA (2004), **What Auditors should know about Encryption**, http://www.wikipedia.com, Retrieved 26/04/2011.

Information Security Audit Compliance Association, ISACA (2005), **Is Auditing Procedures Firewalls,** http://www.wikipedia.com, Retrieved 25/04/2011.

Kolker, R. (2006), **Examining Data Centres,** http://www.wikipedia.com, Retrieved 25/04/2011.

Price Sean M. (2008**) Evaluating Privacy Controls**, http://www.wikipedia.com, Retrieved 26/04/2011.