RESEARCH ARTICLE OPEN ACCESS

Information Security Management in Distributed Systems (ISMDS)

Augustine O. Ugbari [1], Ikechukwu O. Uche [2]
Department of Computer Science [1]
University of Port Harcourt
Choba, Nigeria
Shell Petroleum Development Company of Nigeria [2]
Port Harcourt, Nigeria

ABSTRACT

To follow security and privacy standards, businesses around the globe look up to Information Security standards to not only protect their business data and asset but also promote integrity. Information technology has made it possible for every sector of the society to operate with electronic records over distributed systems. As a result, sensitive information which exists on computer systems, present possible danger of being easily vandalised or abused. To this effect security standards and guidelines have been put in place to ensure organisational security efficiency. This paper identifies key information security management (ISM) systems and then analyses their effectiveness in distributed systems.

Keywords:- Information Security, Security Evaluation, Security Standards

I. INTRODUCTION

Commercial organisations and governments rely heavily on information to conduct their daily activities [1]. It is a well-known fact that information is an asset and the value of any organisation or institution is a function of the information they possess. Before the dawn of the computer age information was primarily stored and conveyed by means of print media (hard copy documents) and other physical means. In our present society information is not only available in hard copies but primarily via electronic data processing (EDP or Soft copies). EDP media comes in various form; they could be found in audio, video, text or even encrypted form just to mention a few. Though they may vary in their form (means by which they can be access) they all share the same characteristics which makes them different from hard copy information. These characteristics make information availability and accessibility more efficient but they also generate security concerns [2]. These characteristics include: Density, Obscurity, Accessibility, Forgery, Retentivity, Profligacy.

EDP is denser in nature compared print media. They can't be accessed by physical examination except through specialized software. They can be easily accessed remotely. Unauthorised modification can be easily made to the EDP. Even when data is deleted from the system they could be recovered using special techniques. In most cases EDP software makes copies of the files when being processed. After processing, some of these copies are not deleted and could be accessed even after the EDP has been deleted form the system.

These characteristics of EDP files are amplified in distributed systems in which data is shared over the network. The main areas of vulnerability in distributed systems could be found in the system (processors, storage device, communication facility, remote terminals), users and system personnel. A fault in the system processing unit could leave the data corrupt or inaccessible. Data stored in storage devices could be easily duplicated or deleted. Hardware or software failure could also easily lead to data compromise. Communication signals could become faulty and the system could be accessed (hacked) by unauthorised users.

As a result of these vulnerabilities, information security has become a huge concern as modern economy is greatly dependent on EDP as a means of everyday activities ranging from business transaction to causal communication. This has brought about the development of information security standard which is expected to be implemented by corporate organisation, government, institutions and even individuals to manage information security. These standards came in response to industrial demands and the need to prove the competence of organisation in the safeguarding of customer information and sensitive data [3].

There are various international standards that have been developed but this paper would deal primarily with the ISO/IEC 27000 series, ISO/IEC 15408 and GASSP. It looks at the functional benefit of these standards and how they have evolved to their present state. It also considers the integrity of these standards and the criteria used in developing them. It then examines risk assessments in a dynamic society and then managing security incidents in organisations.

II. SELECTED ISM STANDARDS

There are various ISM standards, most of which have been developed for specific purposes. Though some of them may be generic in their functionality (like ISO/IEC 27002) others are specific to the particular industries (like the ISO/IEC 27011). These standards have been developed by various international bodies which all consider information as an asset and they all aim to achieve a common goal "which is to suitably protect this asset in order to ensure business continuity, minimize business damage, and maximize return on investments." (ISO 17799). These standards include ISO 2700 series, Common Criteria/ISO 15408 and GMITS 13335 to mention a few.

A. ISO 27000 Series:

The ISO 27000 series of standards have been specifically reserved by ISO for information security matters and they contain individual standards and documents. A number of these are already well known (like the ISO/IEC 17799) and have been previously published, while others are scheduled for publication with final numbering and publication details yet to be determined [1].

The ISO 27000 series of standards includes:

- ISO 27000 – principles and vocabulary (in development)
- ISO 27001 – ISMS requirements (BS7799 – Part 2)
- ISO 27002 – ISO/ IEC 17799:2005 (BS7799 – Part 1)
- ISO 27003 – ISMS Implementation guidelines
- ISO 27004 – ISMS Metrics and measurement
- ISO 27005 – ISMS Risk Management
- ISO 27006 – ISMS Accreditation of organizations guidelines
- ISO 270xx – other published standards, as well as allocation for future use

1) **ISO 27001**: This standard takes its origin from the BS 7799-2 standard. This was in response to industrial demands in the early 1990's which in 1993 led to the development of a "Code of practice for Information Security Management" and later evolved to become the first version of BS 7799 standard which was published in 1995 [3]. The SB 7799 standard is divided into two sections as follows: Part 1: Code of Practice and Part 2: Specification of Information Security Management System. BS 7799 was primarily developed as an auditing guide for organisation and it details information security concepts to be followed by organisations. The ISO 27001 standard, along with the ISO 27002, was revised and republished in 2013, to make them more uniform and compliant with the other ISO standards.

2) ISO 27002: Just like the ISO 27001 the ISO 27002 standard take its root from the BS 7799-1 (Part 1) standard. In December 2000 ISO/IEC 17799:2000 was adopted from the BS 7799-1 standard as a result of the growing demand for an internationally recognised information security standard under the aegis of an internationally recognised body, such as the ISO. The second edition of the ISO/IEC 17799 was in 2007 converted to the ISO 27002 in order to conform to the ISO 27000 series. ISO 27002 differs from ISO 27001 in that it is an implementation guide, based on suggestions. The primary aim is to achieve a sound and comprehensive information security infrastructure [3].

3) ISO 27003: This is a new standard intended to offer guidance for the implementation of an Information Security Management System [1]. It was published in 2010 to describe the process of specification of the ISMS, covering planning and preparation, and eventual implementation.

4) ISO 27004: The ISO 27004 standard covers information security system management measurement and metrics. It also includes suggested ISO 27002 aligned controls. It was first published in 2009, and a revised edition issued in 2016. The revised edition is perceived to be more practical than the previous edition.

5) ISO 27005: The ISO 27005 standard is designed primarily for information security risk management. It is a methodology independent ISO standard, merely specifying a series of activities to be carried out in managing Information systems risks. The latest edition (published in 2011) reflects the general principles of the related ISO Risk Management standard (ISO 13000:2009) in the context of ISM risks.

6) ISO 27006: The ISO standard provides guidelines for the accreditation of organizations offering ISMS certification. The latest (3rd) edition was published in 2015.

B. Common Criteria ISO/IEC 15408:

In June 1993 the United States, Canada, France, Germany and United Kingdom combined separate criteria to form a single set of IT security criteria which is known as the Common Criteria (CC). After extensive public review and evaluations CC version 2.1 was developed in August, 1999 and is referred to as ISO 15408. The CC was developed as a procedure for evaluating the security of information technology (IT) products and systems. This global effort aims to map out an IT Security evaluation methodology, fully accepted and beneficial to all users. [4].

C. GASSP (Generally Accepted System Security Principles):

GASSP was developed as a result of more organizations sharing information electronically and a common understanding of what is needed and expected in securing information technology (IT) resources. GASSP provided the framework for well-structured establishments to reference when engaged in small or large scale business. This guideline is designed to be used by all business stakeholders including

Management, internal auditors, users, system developers, and security practitioner. This would enable them obtain better understanding of the necessary security requirements for their IT systems

The main principles behind GASSP is to focus on security from a more holistic perspective. When developing IT security policies these principals become highly essential particularly if the system being developed is new. They cover broad areas like accountability, cost effectiveness, and integration.

GASSP also provides common IT security practices generally used today which promotes effective IT security program. They provide a measure to determine the level of security with an organization and in the process, build business trust. GASSP consists of eight principles, each of which are applied to fourteen unique practices. The principles are effective tools when implemented by organisations for IT security at all levels as they standardise the creation program policy. [5]

III. EVALUATING INFORMATION SECURITY MANAGEMENT AND ITS PROPERTIES

It is no doubt that information security management (ISM) guidelines are essential for the certification and even managing of organizations. But can these standards be trusted to meet the needs they claim? There are two main criteria which would be considered in assessing the security guidelines, these includes the “scope of the application” (Is it generic, universal or company specific?) and “type of evidence” (Is the research process visible? Is the evidence sound?) [6].

A. Scope of application

It is evident that most security guidelines are generic in nature. This gives them the advantage of being implemented over a wide range of industry, organizations and governments. But it should be acknowledged that the nature of functionalities of these organizations differ from one another. “General or generic security practices may overlook specific requirement, which may result in expenditure in the wrong places, resulting to waste and potential insecure systems” [6]. It is expected that a company-specific ISM guideline should be tailored according to the organization’s distinct security targets and necessities. This brings a need for ISM to be designed more to the specific organisational needs than being left in generic form [6].

B. Type of evidence

There are two forms by which evidence could be generated in research and development effort. These are validation and argumentation forms of evidence. Most modern research is based on empirical evidence which can be easily analysed and validated (8). This raises a lot of issues with the presence ISM guidelines as most of these guidelines are produced from common practice and general approval. This approach to research has led to certain weaknesses in the available standards/guidelines, part of which includes traditional views. Guidelines based on traditional views are based on generic or universal principles. Generic and universal guidelines are not particular about organisational differences thus ignoring the organization’s uniqueness. It should be noted that most ISM standards/guidelines clearly state that their guidelines are starting point for developing organization specific guidelines. It becomes clear that because an organisation is using certain practice does not prove that such practice is better or weaker since there is no evidence of the reliability of the guideline.

It is therefore expected that the authors of the guidelines should ensure that the guidelines are empirically validated.

IV. MANAGING ISM IN CHANGING ENVIRONMENT

In our present-day economy so many businesses thrive with mergers and acquisition of other companies. This benefit comes with a price paid by difficult managing the ISM of the new system. In most cased a total revaluation of the entire system may be necessary as previous ISM implementations would be inadequate. One area greatly affected in the ISM system in changing environment is the area of Risk assessment. “Risk assessment or Analysis is a large process of security management” and “…is concerned with discovering threat path between potential attackers and critical assets, and its generally carried out during a system design and then at fixed intervals during its operational life.” [7]

In the past various risk analysis approaches have been presentment. [8] identified the need to use abstract models of systems, which allow a combination of security design and stakeholder analysis, independent of physical implementation. This approach is still very useful today as it adds in using systematic calculation methods to make risk analysis since it identifies the scope for abstract modelling.

Chivers (2009) proposed a more effective mean for managing risk analysis by employing risk profile. In his model, he grouped systemic problems of evaluating threat path into local properties for individual system components.

V. CONCLUSION

There are numerous reasons why every organisation would need to spend effort and resources in implementing ISM. Though an empirical conclusion cannot be deduced to indicating which ISM is most appropriate, organizations are left with their local jurisdictions to implement ISM based on government policies and industrial requirement. These standards after implementation vary from organization to organization but as we have seen in this paper and there is no way to validate these specific standards.

It is then important that ISM standards be expanded and be more organisation-specific as more empirical approaches are needed to be employed in ascertaining the efficiency of the standards.

REFERENCES

[1] Kerry-Lynn Thomson, Rossouw von Solms, "Towards Corporate Information Security Obedience," in *IFIP International Federation for Information Processing (IFIPAICT),* Boston, 2004.

[2] J. Ralph H. Sprague, "Electronic Document Management:," University of Hawaii, [Online]. Available: http://sprague.shidler.hawaii.edu/MISQ/MISQfina.htm. [Accessed 16 March 2017].

[3] T. Carlson, "Information Security Management: Understanding ISO 17799," International Network Services Inc., 2001.

[4] "Information Security. ISO 15408 Common Criteria Certification Explained," Common Criteria, 2012. [Online]. Available: https://www.midshire.co.uk/wp-content/uploads/2012/10/ISO15408_IT_Security_Certification_FactSheet.pdf.

[5] Marianne Swanson and Barbara Guttman, "Generally Accepted Principles and Practices for Securing Information Technology Systems," NIST Special Publication 800-14, 1996.

[6] Mikko Siponen and Robert Willison, "Information security management standards: Problems and solutions.," *Information & Management,* vol. 46, no. 5, p. 267–270, 2009.

[7] Howard Chiversa, John A. Clarkb, Pau-Chen Chengc, "Risk profiles and distributed risk assessment," *computers & security,* vol. 28, p. 521–535, 2009.

[8] R. Baskerville, "Information systems security design methods: implications for information systems development," *ACM Computing Surveys,* vol. 25, no. 4, pp. 375-414, December 1993.

[9] Von Solms, R. and Solm, S. H., "Information security governance: Due care. Computer & Security.," vol. 25, pp. 494-497, 2006.

[10] "An Introduction to ISO 27001, ISO 27002....ISO 27008," [Online]. Available: http://www.27000.org/. [Accessed 17 01 2016].

[11] A. Aizuddin, "The Common Criteria ISO/IEC 15408 - The Insight, Some Thoughts, Questions and Issues.," InfoSec Reading Room SANS, 2001.