Посилання на статтю

Samuel Gyedu Using information security system model as a management tool for ensuring information security in an organization / Samuel Gyedu // Управління проектами та розвиток виробництва: Зб.наук.пр. – Луганськ: вид-во СНУ ім. В.Даля, 2014 - №4(52). - С. 103-108.

UDC 005.934:005.57

Samuel Gyedu

USING INFORMATION SECURITY SYSTEM MODEL AS A MANAGEMENT TOOL FOR ENSURING INFORMATION SECURITY IN AN ORGANIZATION

Information security system model is generated and interpreted from the organization economic security point of view. The model is a base for measuring and managing the information security system of organization in a well-structured and control manner to meet the strategic plans. Fig. 2, Ref. 17.

Keywords: information security management, physical security, information security, knowledge security and personnel security

Самуель Гієду

ВИКОРИСТАННЯ СИСТЕМНОЇ МОДЕЛІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ЯК УПРАВЛІНСЬКОГО ІНСТРУМЕНТА ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ОРГАНІЗАЦІЇ

Запропонована системна модель інформаційної безпеки організації, яка інтерпретована з позицій економічної безпеки. Показано, що модель являє собою основу для добре структурованого та контрольованого вимірювання та управління системою інформаційної безпеки з метою виконання стратегічних планів організації. Рис.1, дж. 17.

Самуэль Гиеду

ИСПОЛЬЗОВАНИЕ СИСТЕМНОЙ МОДЕЛИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ КАК УПРАВЛЕНЧЕСКОГО ИНСТРУМЕНТА ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОРГАНИЗАЦИИ

Предложенная системная модель информационной безопасности организации, которая интерпретирована с позиций экономической безопасности. Показано, что модель представляет собой основу для хорошо структурированного и контролируемого измерения и управления системой информационной безопасности с целью выполнения стратегических планов организации. Рис.1, ист. 17.

JEL 022

INTRODUCTION

Information security system model is a set of activities that an organization and management aimed at protecting the interests of the organization's information from external and internal threats [1]. Information security management is the term used for

the planning and supervisory functions that are required to assure the meaningful development, practical feasibility and effectiveness of a well thought-out and systematic process of information security [2]. Information security is a systematic approach for organization to remain secure and manage the sensitive and important information of an organization. It helps organizations to keep information assets secure. Information security management is the monitoring, managing and controlling of vital and sensitive information an organization to ensure continuous flow of information. It is activities that relate to the protection of information and information assets against the risks of loss, misuse, disclosure or damage. An information security management system focused on managing information security within an organization. Organizations must change to the holistic management of information security, requiring a well-established information security management system to addresses all aspects in an organization that deals with creating and maintaining a secure information environment. Information security plays an important role in protecting the information assets of an organization. There are a lot of security incidents among which are personnel leaving the organization with information and internet websites frauds, server hacking and data leakage. Organizations should be aware of these and devote resources and strategies for the protection of information assets. Every organization must be more concern and concentrate on information security. Information security management plays an important role in protecting the assets of an organization. The organization should set a benchmarks or standards to help ensure an adequate level of security is attained, resources are used efficiently, and the best security practices are adopted in ensure and maintain information security [3]. Information Security Management System can be defined as a management system used for establishing and maintaining a secured information environment [4]. Establishing physical security is not a project with a limited time span but a continuous process. The appropriateness and effectiveness of all elements of the information security management system must be checked continuously. This means that not only individual information security safeguards must be checked but also the information security strategy must be reviewed on a regular basis [5].

Problem statement of this article. The reason behind information security management is that many organization all over the world has found it difficult to come out with a well-organized ways on how to protect information of their organization both internally and externally. Many researchers have come out with methods, models and ways of protecting the information of an organization but these methods, models and ways work well for few organizations. Some researchers have also come out with methods and models for solving this problem but it is difficult for most of the organization to implement and use them. So what is the ideal and the most appreciable methods or models for ensuring information security in our modern organizations.

***Analysis of the last researches*.** A brief discussion of the role of an information security management system (ISMS). A management system describes the people, processes and technologies used to focus and manage the activities of an organization. Each organization builds a unique system that is supportive of the goals of that organization. The system will reflect different disciplines depending on the values and culture of the organization

An information security management system (ISMS) is focused on managing information security within an organization, a topic that is of growing concern to many organizations as they deal with the challenges presented in the information society including evolving information security and privacy legislation. Published guidelines (OECD, Cyber security), and threats natural (fire, flood, earthquake, tornados) or human introduced (viruses, spam, privacy, hacking, industrial espionage.

Organizations should establish comprehensive policies for privacy and security management and ensure that technology vendors address these policies in the software [6]. In information security management system the information protected includes electronic format on computer or network, paper-based information and intellectual property [7]. information security corporation can be effectively used by either small or large organizations, and can be tailored to support the protection of information in diverse organizations including data processing centers, software development, e-commerce, health care organizations, finance, manufacturing, service organizations, non-governmental organizations, colleges, and not-for-profit organizations [8, 9]

The short falls of these researchers of the above articles are that they only sees information security management as a system which focused on only natural and human aspect of information security which needs to be protected. They also considered information security as only information technology, e-commerce and health. In actual fact information security management should be seen as an interconnected system model with all the elements in them. This article is to address the issues of interconnected system which is the most appropriate way of solving the problems of information leakages in an organization.

The researcher employs the idea of the economic system model developed by professor valentine Rach. His system model of economic security talks about the four interconnected elements which are production service, management service, supporting service and security service to ensure activity continuity of an enterprise. This article used four different interconnected elements which are best fit for the ensuring of information security in an organization and was developed based on the economic security system model.

Objective of the article. The aim of this article is to establish a well-organized information security management system model with a goal, interconnected elements and achieved result to help organizations all over the world to solving the problems with regards to information security management of an organizations.

MAIN FINDINGS

Main body of the article. Relying on all previous points and statements, we suggest the information security management system model for an organization, presented on fig. 1.

All of the interconnected elements in the fig 1 has been explained below. It is meant for the interpretation of the information security management system model for better understanding and early to be used by concerned organizations who would like to use it.

Physical security is defined as that part of security concerned with physical measures designed to safeguard personnel and the environment of an organization to prevent unauthorized access to equipment, installations, material, and documents. For organization to enjoy business continuity it has to physically protect the environments in which it operates. By so doing the organization is also ensuring the safety and the health of the workers. Physical security is crucial to prevent theft, risk and dangers that can damage the organization. However, adequate security requires investment. The Security Rule defines physical security as physical measures, policies, and procedures to protect a covered entity's electronic information systems and related buildings and equipment, from natural and environmental hazards, and unauthorized intrusion. It is often the first concern in facilities with high asset concentration, especially using in critical systems for business processes. Physical security is especially important for IT resources, as their proper operation demands that the hardware assets and infrastructure they are running on be kept away from anything that could hinder their function. This includes tampering by unauthorized personnel

and unforeseen events like accidents and natural disasters. The appropriateness and effectiveness of all elements of the information security management system must be checked continuously for the organization to be operation.

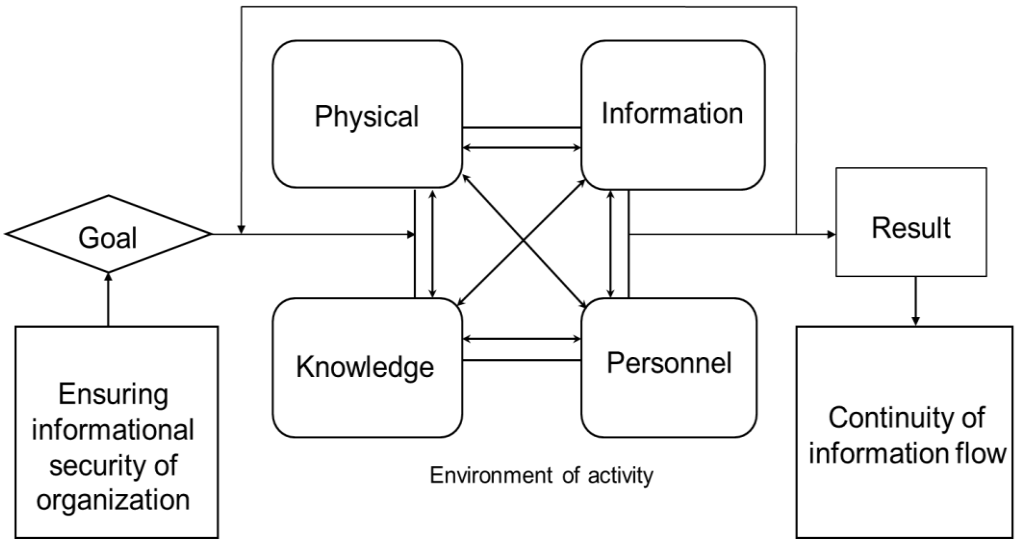

Fig. 1. The information security management system model for an organization

The purpose of information security is to protect information of all kinds and from all sources. This information might be printed on paper, kept on computer systems or stored in the minds of the users. IT security primarily deals with protecting information stored electronically and with its processing. The classic core principles of information security, namely confidentiality, integrity and availability, form the basis for its protection. Information security must be integrated in all the institution's processes and projects in which information is processed and utilized. Information security requirements must not only be considered when procuring IT but also when designing business processes and training staff members. In ensuring information security the management must actively initiate, manage and supervise the security process. Information is data that has been processed into a form that is meaningful to the recipient [10]. Information is that which is conveyed, and possibly amenable to analysis and interpretation, through data and the context in which the data are assembled. Information is the change determined in the cognitive heritage of an individual. Information always develops inside of a cognitive system, or a knowing subject. Information management is the collection, processing, distribution and management of information from one or more sources of an organization. Information management is the process of collecting, organizing, classifying and disseminating information throughout an organization so as to make it purposeful to those who need it [11]. It is a corporate responsibility that needs to be ensured by the management and the staff of an organization. Organizations must hold its employees accountable to capture, manage, store, share, preserve and deliver information appropriately and responsibly. Part of that responsibility lies in training the organization to become familiar with the policies, processes, technologies and best practices security on information ensuring resources that are useful and relevant to the organization.

Knowledge security is a product of activity of people an ideological expression of features and bonds of the natural and human environment in the form of signs and

symbols. Knowledge management focuses on how an organization identifies, creates captures, acquires, shares, and leverages knowledge [12]. Growing interest in knowledge management stems from the realization that in the knowledge era, organizational knowledge is a strategic corporate asset that needs to be garnered, retained, updated, disseminated and applied to organizational problems [13, 14]. Knowledge security is the process of planning, organizing, motivating, controlling and ensuring safety in the minds of workers. It is a systematic and active security ideas, information, and knowledge residing within organization's employees. These systems in the organization ensure that all the knowledge-related assets are improved and effectively employed. Knowledge management is quickly gaining recognition as a key determinant of value in the organizational success, and competitive edge [15]. In an attempt of the organization to ensure information security then it is essential to creating the right conditions for individuals to learn and apply their knowledge to the benefit of the organization. The application of one's knowledge can hopefully be converted into relevant information that can be shared and used to create value for the organization. It helps organization to identify, select, organize, disseminate, transfer information which enables decisions making and problem-solving.

The personnel security element represents the human resources and the security issues that surround them. It represents a human collective and must take into account values and behaviors. In order to ensure information security in an organization, the organization should address the safety and health of the workers, better remuneration and motivations to retain and maintain its human resource. The organization can ensure information security by preventing labour-turnover. In the sense that workers leaving the organization normally leave with information, knowledge and the experience gained in that organization which can bring about activity rupture.

In all conditions the organization should know that human resource is the most important resource of an organization and at the same time the main source of threats of an organization.

***Conclusion and perspectives of future researches*.** Information security management of an organizations can be ensured by measuring and managing their information security system in a well-structured and control manner to meet the strategic plans of the organization. If organizations see and manage the four interconnected elements of information security management system model which are physical, information, knowledge and personnel, this will help these organizations to ensure continuing of the organization. Organizations that will adopt and implement this newly developed information security management system model can be assured that they are reflecting one of the best practices of information security management which will help in the continuity of the organization. The executive and operational management of organizations today realize that the successful protection of information assets depend on a holistic approach towards the establishment and implementation of system models. Success in organization depends on ability to monitor, direct and implement the information and the minds of the workers in the right direction. The ability of the organization to extract and implement knowledge is the best weapon in the information security management system which can guaranty the continuity of information flow of the organization.

REFERENCES

1. Rossoshanskaya, O. (2000). Features of planning projects on the basis of system model, project management and development of production, 1(1), 11-16.

2. BSI (2008). BS 100-1: Information security management system. Bonn. Retrieved from: http://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications-/BSIStandards/standard_100-1_e_pdf.pdf?__blob=publicationFile.

3. BSI (2008). BS 100-1: Information security management system. Bonn. Retrieved from: http://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI-/Publications/BSIStandards/standard_100-1_e_pdf.pdf?__blob=publicationFile.

4. Eloff, M.M, Von Solms, S.H, (2000). Information Security management: a hierarchical framework for various approaches, Computers & Security, Vol.19, No3, 243-256.

5. ISO (2013). ISO/IEC 27002: Information technology. Security techniques. Code of practice for information security controls. Geneva, Switzerland.

6. Pumphrey, L.D, Trimmer, K., and Beachboard, J. (2007). Enterprise Resource Planning Systems and HIPAA Compliance, Research in Healthcare Financial Management, vol.11, no.10, 57-75.

7. BS (2002). BS7799-2: Information security management system. Specification with guidance for use. Retrieved from: http://www.aitel.hist.no/fag/dsh-m/lukket/lek03/fagstoff/BS-7799.pdf.

8. IAF (2003). EA-7/01. EA Guidelines on the Application of EN 45012 IAF Guidance on Application of ISO/IEC Guide 62, Iss.3.

9. ISO (2005). ISO/IEC 27001: Information technology. Security techniques. Information security management system: requirements. Geneva, Switzerland.

10. Davis, G.B., & Olson, M.H. (1985). Management Information Systems, conceptual foundation, structure and development, 2nd. New York, McGraw-Hill.

11. Albert, S. (September 7, 1998). Knowledge Management: Living up to the hype? Midrange system, 11(13), 52.

12. Clemmons Rumizen, M. (2002). The Complete Idiot's Guide to Knowledge Management. Indianapolis, USA: Alpha.

13. Drucker, P. F (1994). Post-Capitalist Society, Harper-Business, New York, NY.

14. Steward, T. A (1997). Intellectual capital: The New Wealth of Organization, Doubleday/Currency New York, NY.

15. Geisler, E. & Wickramasinghe, N. (2009). Principles of Knowledge Management: Theory, Practices, and Cases. New York, USA: M.E. Sharpe.

16. Rach V, Rach, D. (2000). Risk management in projects implemented in transitional economy: financial products for the real sectors in Ukraine. Proceeding of international conference, Kyiv, 25-26.

17. Duncombe, J. U. (1959).Infrared navigation Part I: An assessment of feasibility, ‖ IEEE Trans. Electron Devices, vol. ED-11, Jan., 34-39.

Рецензент статті
д.е.н., проф. Ляшенко О. М.

Стаття надійшла до редакції
29.11.2014 р.