Chapter 9
Identification of Information Security Management Factors

Hamed H. Dadmarz
Independent Researcher, Iran

ABSTRACT

Considering the important role of information in organizations, an appropriate management is required for maintaining the security of the information. The information security management system is part of a general management system in an organization and based on the business risk approach aims to establish, implement, use, monitor, revise, maintain, and improve security that leads to the protection of information and minimizes unauthorized access. The main objective of this chapter is to identify factors and indicators of information security based on the information management system. For this purpose, after reviewing the literature and having opinions of 30 experts, a conceptual framework for public organizations is proposed that includes information security management factors such as financial, technical, operation and communication, human resources, data and information classification, environmental and physical, and managerial.

INTRODUCTION

Security refers to a set of measures, methods, and tools for preventing unauthorized access and modification in computer and communication systems. Recently, the security of information exchange environment in developing countries is at an undesirable level, especially in the public organizations. One of the main reasons for the current situation is lack of technical and operational infrastructure for security such as the security assessment system of the information exchange, the certification system, the system of analysis and management of security risks, the system for preventing and confronting the incidents of information exchange, the crime prevention system for information exchange and other security infrastructures as well as the effective measures to immunize information exchange environment of public organizations.

Regardless of the above reasons, the disordered situation of security of information exchange between public organizations will cause disruptions in the proper functioning of these organizations and reduce their credibility from one hand and will waste national capital on the other hand. Therefore, along with developing a strategic document for the security of a country's information exchange, it is necessary to pay attention to the issue of the security of the information exchange among public organizations. In addition to reducing the damage caused by the current situation of security in public organizations, it will have an effective role in the process of developing a strategic document for the security of national information exchange (Boiko & Shendryk, 2017).

More than one-third of the security defects in computer systems are caused by the employees and one-third of the worst security incidents is due to viruses (Malekolkalami, 2013). In order to implement an effective security capacity, organizations need to determine their weakest connection points, and design extensive security architecture for the realization of security management objectives (Barnard & Von-Solms, 1998).

The purpose of information security is to ensure the confidentiality, integrity, and availability of information. Therefore, it should be considered that the information security management system (ISMS) has several steps and requires a dynamic process to accurately identify, assess, and calculate information risks. It is clear that organizations with hundreds and sometimes thousands of assets are faced with many types of threats and vulnerabilities as well as a wide variety of risk scenarios that make the management of such a volume of information in a safe way very difficult or literally impossible without prioritizing them. In addition to risk assessment and the way of addressing them, a prioritization method can provide a

13 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage: www.igi-global.com/chapter/identification-of-information-security-management-factors/216165

Related Content

COVID-19 Pandemic: Assessment of Behavior and Attitudes in Medical Waste Management Among Healthcare Workers in Kuwait
Fatimah Al-Dashti, Anwaar Mohammad Alkandari, Shihanah AlMutairiand Ahmed Al-Saber (2022). *International Journal of Electronic Government Research (pp. 1-21).*
www.irma-international.org/article/covid-19-pandemic/313176

E-Government Policy Implementation in Brunei: Lessons Learnt from Singapore
Mohammad Habibur Rahman, Patrick Kim Cheng Low, Mohammad Nabil Almunawar, Fadzliwati Mohiddinand Sik-Liong Ang (2012). *Active Citizen Participation in E-Government: A Global Perspective (pp. 359-377).*
www.irma-international.org/chapter/government-policy-implementation-brunei/63379

Policy Testing in Virtual Environments: Addressing Technical and Legal Challenges
Magdalini Kardara, Omri Fuchs, Eleni Kosta, Fotis Aisopos, Ilias Spaisand Theodora Varvarigou (2012). *International Journal of Electronic Government Research (pp. 1-21).*
www.irma-international.org/article/policy-testing-virtual-environments/70073

Transnational Information Sharing, Event Notification, Rule Enforcement and Process Coordination
S. Su, J. Fortes, T.R. Kasad, M. Patil, A. Matsunaga, M. Tsugawa, V. Cavalli-Sforza, J. Carbonell, P. Jansen, W. Ward, R. Cole, D. Towsley, W. Chen, A.I. Antón, Q. He, C. McSweeney, L. de Brens, J. Ventura, P. Taveras, R. Connolly, C. Ortega, B. Piñeres, O. Brooks, G.A. Murilloand M. Herrera (2005). *International Journal of Electronic Government Research (pp. 1-26).*
www.irma-international.org/article/transnational-information-sharing-event-notification/1998

E-Barangay: A Framework for a Web-Based System for Local Communities
and Its Usability
Rex Perez Bringula, Mark Anthony D. Vale, Jenard A. Napolis, Franklin Pillos
Olivaand Daniel Joseph T. De La Serna (2022). *International Journal of Electronic
Government Research (pp. 1-13).*