

Chapter 44

An Analytical Study of Methodologies and Tools for Enterprise Information Security Risk Management

Jaya Bhattacharjee
Jadavpur University, India

Anirban Sengupta
Jadavpur University, India

Mridul Sankar Barik
Jadavpur University, India

Chandan Mazumdar
Jadavpur University, India

ABSTRACT

An enterprise is characterized by its business processes and supporting ICT infrastructure. Securing these entities is of utmost importance for the survival of an enterprise and continuity of its business operations. In order to secure them, it is important to first detect the risks that can be realized to cause harm to those entities. Over the years, several kinds of security risk analysis methodologies have been proposed. They cater to different categories of enterprise entities and consider varying levels of detail during risk analysis. An enterprise often finds it difficult to select a particular method that will best suit its purpose. This paper attempts to address this problem by presenting a detailed study of existing risk analysis methodologies. The study classifies them into specific categories and performs comparative analyses considering different parameters addressed by the methodologies, including asset type, vulnerabilities, threats, and security controls.

DOI: 10.4018/978-1-5225-5481-3.ch044

INTRODUCTION

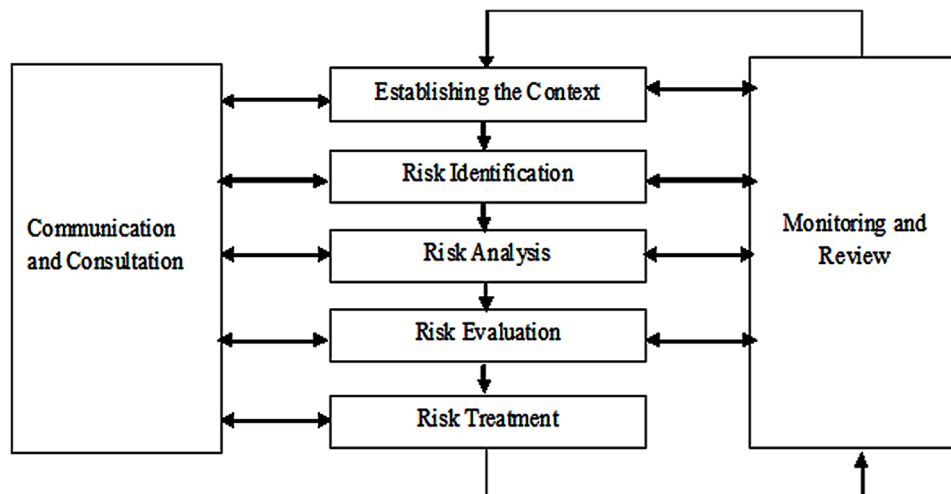
An enterprise can be defined as an organization (Industry/Govt./Academic) created for business or service ventures. The term encompasses a wide range, from a large corporation or government department to a small office / home office (SOHO). From Information Security point of view, an enterprise is characterized by its business goals, business processes, information assets, personnel, organizational structure, site (physical and virtual) and ICT infrastructure. Protection of each of these entities is of utmost importance for the survival of an enterprise and continuity of its business operations.

Usually, the business processes and ICT infrastructure (hardware, software and network assets) of an enterprise contain several weaknesses, or *vulnerabilities* (ISO/IEC, 2014), that may arise owing to improper configuration, erroneous workflows, incorrect usage, etc. *Threats* (ISO/IEC, 2014) abound in the physical and virtual worlds whose sole objective is the exploitation of vulnerabilities to breach security parameters of enterprise assets and business processes.

Information Security Risk is defined as the probability that threat(s) will exploit vulnerabilities to cause harm to enterprise assets (ISO/IEC, 2011). It refers to the effect of uncertainty on information security objectives of an enterprise. The primary objective of an information security programme is the protection of enterprise resources by managing the identified risks. *Information Security Risk Management* comprises of a set of coordinated activities to direct and control an enterprise with regard to risk (ISO/FDIS, 2009). ISO 31000 (ISO/FDIS, 2009) lists seven phases for managing risk: establishing the context, risk identification, risk analysis, risk evaluation, risk treatment, communication and consultation, monitoring and review. These are illustrated in Figure 1. As is obvious, the risk management phases are cyclic in nature and need to be applied continuously during the life-cycle of an enterprise information system.

Among the components of risk management, risk identification, risk analysis and risk evaluation are of utmost importance, and are together referred to as *Information Security Risk Assessment* (ISO/FDIS, 2009). The quantity, complexity and dynamic nature of enterprise assets and their inter-relationships pose serious challenges to the process of risk assessment.

Figure 1. Risk management process



14 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/an-analytical-study-of-methodologies-and-tools-for-enterprise-information-security-risk-management/202255

Related Content

A Test of Wagner's Heuristics for the Spare Parts Inventory Control Problem

Ibrahim S. Kurtulus (2012). *International Journal of Operations Research and Information Systems* (pp. 88-100).

www.irma-international.org/article/test-wagner-heuristics-spare-parts/73025

4SRS-SoaML Method for Deriving a Service-Oriented Architecture From Use Cases Within a SPEM Approach

Carlos Salgado, Ricardo J. Machado and Rita S. P. Maciel (2019). *Modeling Methods for Business Information Systems Analysis and Design* (pp. 93-114).

www.irma-international.org/chapter/4srs-soaml-method-for-deriving-a-service-oriented-architecture-from-use-cases-within-a-spem-approach/219165

Challenges and Solutions for Complex Business Process Management

Minhong Wang and Kuldeep Kumar (2010). *Handbook of Research on Complex Dynamic Process Management: Techniques for Adaptability in Turbulent Environments* (pp. 1-22).

www.irma-international.org/chapter/challenges-solutions-complex-business-process/36563

Assessing Digital Literacy Among Namibian Millennials and the Impact on Consumer Decision-Making Styles: A Case Study

Efigenia Madalena Mario Semente and Grafton Whyte (2020). *International Journal of Applied Management Sciences and Engineering* (pp. 54-73).

www.irma-international.org/article/assessing-digital-literacy-among-namibian-millennials-and-the-impact-on-consumer-decision-making-styles/246856

Banking Business Process Management Implementation

Michael Glykas, George Valiris, Angelika Kokkinaki and Zoi Koutsoukou (2018). *International Journal of Productivity Management and Assessment Technologies* (pp. 50-69).

www.irma-international.org/article/banking-business-process-management-implementation/193630