Chapter 7

A Mark-Up Language for the Specification of Information Security Governance Requirements

Anirban Sengupta  
Jadavpur University, India

Chandan Mazumdar  
Jadavpur University, India

ABSTRACT

As enterprises become dependent on information systems, the need for effective Information Security Governance (ISG) assumes significance. ISG manages risks relating to the confidentiality, integrity and availability of information, and its supporting processes and systems, in an enterprise. Even a medium-sized enterprise contains a huge collection of information and other assets. Moreover, risks evolve rapidly in today’s connected digital world. Therefore, the proper implementation of ISG requires automation of the various monitoring, analysis, and control processes. This can be best achieved by representing information security requirements of an enterprise in a standard, structured format. This paper presents such a structured format in the form of Enterprise Security Requirement Markup Language (ESRML) Version 2.0. It is an XML-based language that considers the elements of ISO 27002 best practices.

INTRODUCTION

An enterprise information system consists of assets (Information Assets, Software Assets, Hardware Assets, and Service Assets) and their inter-connections. These assets may contain vulnerabilities (ISO/IEC, 2005), which can be exploited by threats (ISO/IEC, 2005), to cause breach of security parameters (like confidentiality, integrity, and availability). An enterprise should ensure that all its users (both external and internal) are provided with a secure information systems...
ISG requirements of an enterprise depend on several factors. Though the major determinant is the business goal, the operational context, technology used, organizational structure and network connectivity also play important roles in determining the approach towards ISG. Information Security needs of an enterprise are not static, but depend on the dynamics of operation, changing business goals, changes to legal framework, changes to risk perception, etc. Hence, ISG is not a one-time affair; it is a continuous process of analysis, design, implementation, monitoring and adaptation to changing information security needs. In many enterprises, the changes encountered are frequent. Moreover, even for a medium-sized enterprise, the number, and complexity, of assets and their inter-connections are usually huge. The management of such a complex and dynamic process needs structured representation of enterprise security requirements specification documents, and their automatic analysis and generation with interoperable features.

In this paper, the design of Enterprise Security Requirement Markup Language Version 2.0 (ESRML 2.0) is presented. It is an XML (W3C, 2003) based structured language for specifying enterprise information security requirements to facilitate the automatic analysis, design and governance of Enterprise Information Security. This was first introduced in Sengupta and Mazumdar (2010). It has been subsequently enhanced and is being described in this paper in detail. ESRML 2.0 is based on ISO 27002 Best Practices for Information Security Management (ISO/IEC, 2005). Security standards consolidate and specify best practices for achieving desired information security goals. In order to successfully implement ISG in an enterprise, it is important to adopt relevant information security best practices (Williams, 2001). ISO 27002 is one of the most widely accepted international standards that specifically address ISG issues of an enterprise (Solms & Solms, 2009). It provides detailed guidelines on how a secure management framework should be implemented, and how it should demonstrate compliance with laws, regulations, and standards (these are the principal requirements of ISG). It consists of eleven security clauses. They are: Security Policy, Organization of Information Security, Asset Management, Human Resources Security, Physical and Environmental Security, Communications and Operations Management, Access Control, Information Systems Acquisition, Development and Maintenance, Information Security Incident Management, Business Continuity Management, and Compliance. Under each clause, there are certain security objectives to be fulfilled. Each objective can be attained by a number of controls. These controls may prescribe management measures like guidelines and procedures, or some security infrastructure in the form of tools and techniques.

Rest of this paper is organized as follows. First, a survey of related work is given. Then, the design of ESRML 2.0 is presented. After that, the usefulness of ESRML 2.0 is described. Finally, the paper concludes with a brief description of WISS-DOM (Web-Enabled Information System Security Design and Operational Management) tool suite that has been implemented using ESRML 2.0. A Sample Security Requirement Specification using ESRML 2.0 has been included in the Appendix.

RELATED WORK

Paul Williams (2001) discussed the role of information security within a corporate governance framework. He stated that the four basic outcomes of ISG should be (i) alignment of investment in