Chapter 13
Information Security Management Systems
Cybernetics

Wolfgang Boehmer
Technische Universität Darmstadt, Germany

ABSTRACT

With the widespread dissemination of Information Technology in enterprises and households in the mid-90s, discussions began on how to manage it. Meanwhile, in the area of enterprise security management systems worldwide, enforced use of the Deming cycle initially worked against the implementation of policies. Standard management systems include ISMS (Information Security Management System) as specified in ISO 27001, BCM (Business Continuity Management System) as specified in BS 25999, and ITSM (Information Technology Service Management System) as specified in ISO 20000. In contrast to policies, these best-practice management systems continue to operate today with no formal method. Management systems have, however, some advantages that policies do not have. In this chapter, the authors present possible uses of policies with respect to management systems and identify potential applications. Furthermore, the authors present a field study, cited here, which highlights the advantages of management systems in practice. Moreover, this chapter shows how a formal description of an information security management system can be created by means of discrete-event systems theory and how an objective function for management systems can be defined.

INTRODUCTION

With the spread of information technology (IT) over the past 15–20 years, a discussion quickly began on how best to protect them. Initially, technical approaches were favored. As policies for enterprise security protection were widely adopted, however, their limits of applicability quickly became apparent. These developments took place over the decade from 1998 to 2008. For application in entire companies, however, management systems are more suitable than policies, as current trends suggest.
The first management system that was organized as a continuous improvement process and brought economic considerations into the field of corporate security was the British Standard, BS 7799-2, in 1998. Meanwhile, in the area of corporate security (enterprise security), management systems based on the Deming cycle became established worldwide, including ISMS (Information Security Management System) as described in ISO 27001, BCM (Business Continuity Management System) as described in BS 25999, and ITSM (Information Technology Service Management System) as described in ISO 20000. In the case of ISMS, a clear trend over time can be identified, representing an increase of approximately 1,000 certificates per year since the standard was published in November 2005.

After this first phase of development in the last decade, the following questions about management services, among others, are still being discussed, with a focus on corporate security (enterprise security):

1. How to distinguish between the formulation and implementation of policies and management systems
2. How to measure the performance of management systems
3. Whether and how management systems can be linked
4. Whether and how a target function can be formulated for a management system
5. How to embed management systems in a business and a business infrastructure.
6. How to implement management systems in an agile manner

Numbers 1 to 5 of these issues will be addressed in this chapter; the remaining issue, number 6, is still an open research topic.

This chapter is organized as follows. The next section provides an overview of policies and management systems and the differences between them. The distinction is made by means of the theory of open, closed, and isolated systems. Then the following section highlights the link between systems theory and management systems, and a formal description of a management system is developed using ISO 27001 as an example. The question of modeling the controlled system is discussed in subsequent chapters with reference to various examples and to a qualitative and quantitative description of the plant. Then a field study is presented in which the preventive mitigation of risks is discussed using a risk-oriented management system based on ISO 27001. The results suggest that in addition to the ISO 27001 standard, the BS 25999 standard is also of great importance in this context and that a purely qualitative analysis of emergency processes is not sufficient. For these reasons, a method for quantifying a Business Continuity Plan (BCP) is also discussed in this section.

Finally, the question of a target function for the information security of management systems will be addressed. This discussion is necessary because, in contrast to purely economics-oriented management systems, a tradeoff exists in management systems for corporate security. This tradeoff can be resolved in various ways, for example iteratively, because it is an NP-hard problem.

OVERVIEW OF MANAGEMENT SYSTEMS AND POLICIES

The development of management systems with a focus on IT security and information security began in the late 90’s and continues today. In information technology, policies have had a far-reaching significance and have been the object of many research projects. A basic description of policies can be found in (Bishop, 2003, p. 3–11 and p. 95 ff). Today, policies are successfully used in firewall configuration, authentication, and network-based factory management, to name just a few areas. A policy must initially be static in
Related Content

Classification of Cybercrimes and Punishments under the Information Technology Act, 2000
www.igi-global.com/chapter/classification-of-cybercrimes-and-punishments-under-the-information-technology-act-2000/156450?camid=4v1a

Policy Enforcement System for Inter-Organizational Data Sharing
www.igi-global.com/article/policy-enforcement-system-inter-organizational/50306?camid=4v1a

Privacy and Security in the Age of Electronic Customer Relationship Management
www.igi-global.com/article/privacy-security-age-electronic-customer/2457?camid=4v1a

A Methodology for Developing Trusted Information Systems: The Security Requirements Analysis Phase
www.igi-global.com/chapter/methodology-developing-trusted-information-systems/23132?camid=4v1a