IDEA GROUP PUBLISHING
701 E. Chocolate Avenue, Hershey PA 17033-1240, USA
Tel: 717/533-8845; Fax 717/533-8661; URL-http://www.idea-group.com
ITB8344

Chapter VII

Establishing the Business Value of Network Security Using Analytical Hierarchy Process

Susan J. Chinburg, Ramesh Sharda, and Mark Weiser
Oklahoma State University, USA

Information technology (IT) has become a critical functionality for business today. Choosing the appropriate network security that will protect IT functions and meet business needs can be a bewildering but necessary process. The problem is deciding what and how much to do. The objective of this paper is to propose a new process that will facilitate the mapping of network security to the business's priorities using well-known classification schemes and decision support systems. Establishing a relationship between such diverse functions requires that the two areas be described in terms that can be related. Network security is described in terms of services and mechanisms that provide the functionality using the Open System Interconnection (OSI) Security Architecture classification. Business value and activities are described using Michael Porter's business value chain. First, the classification schemes for each area are subjectively related to establish an initial functionality/business value relationship. Second, a decision support tool called analytic hierarchy process (AHP) is used to establish an

This chapter appears in the book, *Creating Business Value with Information Technology: Challenges and Solutions* edited by Namchul Shin.

analytical and more objective relationship between the two classification schemes. The result of this work is a prioritized list of security services related to business needs instead of just being driven by technological criteria. An example that illustrates this concept is described in the paper. To the best of the authors knowledge, this is the first application of using AHP in the decision-making process of choosing network security in relationship to business needs.

INTRODUCTION

Information technology (IT) has become a critical functionality of business today. Securing business assets related to network functionality in a manner that justifies cost has become critical to the business process. Choosing the appropriate network security for the business can be bewildering at best. It is well agreed that network security must be addressed, but the problem is deciding what to do and how much to do (Schneier, 2000). There is not a "one-size-fits-all" solution. For example, deciding how much security is needed to protect cash resources depends upon the perspective of the business. The hot dog vendor and the large bank on the same street corner both need to secure cash, but the level of need is very different for each business, as well as the resources available to implement the security solution. In today's business environment, where IT investments are subject to increasing cost-benefit analysis and justification (Lewis, 2001), the IT professional must be able to relate IT investments to business needs. The business professional must be able to relate the business needs to the IT investments. Therefore, a business value justification is needed to answer the question of what and how much.

Network security is an oxymoron. Networking means to share and connect, while security usually refers to shutting and locking the door. Establishing a relationship between these two opposing concepts provides a challenge within itself. To compound the difficulty for the business, the language that surrounds network security is usually shrouded with technical terms that are not well understood by the business community. In this paper, a proposal is made to map network security to business needs so that technical security experts are able to more readily understand how security issues fit the business needs and so that business experts can understand which technical security concepts will fit their business needs. The goal is to allow the security technical professional a way to implement a security solution that fits the needs of that business.

This paper is organized as follows. First, two classifications schemes are related to each other to establish an initial subjective mapping. Network security is described in terms of the OSI security architecture, and business activities are