Chapter 12
Securing the Extended Enterprise: A Method for Analyzing External Insider Threat

Virginia N. L. Franqueira
University of Twente, The Netherlands

André van Cleeff
University of Twente, The Netherlands

Pascal van Eck
University of Twente, The Netherlands

Roel Wieringa
University of Twente, The Netherlands

ABSTRACT

In extended enterprises, the traditional dichotomy between insiders and outsiders becomes blurred: consultants, freelance administrators, and employees of business partners are both inside and outside of the enterprise. As a consequence, traditional controls to mitigate insider and outsider threat do not completely apply to this group of individuals, and additional or improved solutions are required. The ISO 27002 security standard, recognizing this need, proposes third-party agreements to cover security requirements in B2B relationships as a solution, but leaves open how to realize them to counter security problems of inter-organizational collaboration. To reduce this gap, this chapter presents a method for identifying external insiders and analyzing them from two perspectives: as threats and as possible mitigation. The output of the method provides input for further engineering of third-party agreements related to non-measurable IT security agreements; the authors illustrate the method using a manufacturer-retailer example. This chapter also provides an overview of the external insider threat, consisting of a review of extended enterprises and of challenges involved with external insiders.

DOI: 10.4018/978-1-4666-0197-0.ch012
1 INTRODUCTION

Today, organizations are no longer stand-alone, loosely linked only to their customers and suppliers as in the past, but are part of networks with a variety of bilateral relationships and different levels of integration and cooperation. These networks are called business networks, enterprise networks or extended enterprises (Wiendahl & Lutz, 2002; Jagdev & Thoben, 2001). Relationships between organizations are facilitated by fast and reliable communication over the Internet, by outsourcing activities that traditionally would only be performed in-house, by new economic models based on managed services, and by new technologies such as virtualization. Although extended enterprises have been around for several decades, what is new is the fact that organizations are increasingly outsourcing critical business processes, packaging services from different organizations into complex service bundles, and moving IT infrastructure to other private, shared or even public networks under the custody of third parties. The number of organizations part of an extended enterprise can be significant, typically reaching hundreds in large companies. This adds-up to other factors, such as the complexity of dependencies among participants of the network, geographic dispersion, and distributed sources of risk (Thoben & Jagdev, 2001), making it difficult to have a holistic overview of security across the entire business network. Nonetheless, extended enterprises are ever more attractive because they provide competitive advantage by allowing cost savings, time and quality-related benefits, and by increasing business flexibility; each participant in an extended enterprise specializes on its core competencies and takes advantage of other organizations’ expertise to deliver its business mission (Jagdev & Thoben, 2001).

In a traditional enterprise it is possible to separate the organization itself (e.g., its data, IT infrastructure and internal processes) from the outside world, in particular, from organizations part of its extended enterprise. However, organizational boundaries in an extended enterprise context become overwhelmingly fuzzy (Jericho-Forum n.d.; Thoben & Jagdev, 2001; Jagdev & Thoben, 2001); this contrast is illustrated in Figure 1. The overlap of organizations in the diagram represents “holes” that must be made in firewalls to give individuals from other organizations and insiders from a specific organization access to the data it owns, distributed along the extended enterprise. Since the organization that owns the data remains accountable for its protection, regardless of where and by whom it is handled, the extended enterprise creates a new security problem, which we define as the external insider threat problem. External insiders, such as freelance administrators or consultants, represent a class of individuals which do neither completely fall under the class of insiders nor of outsiders of one organization, and therefore, mitigations to insiders and outsiders do not completely solve the external insider threat problem.

1.1 Chapter Contribution and Organization

In this chapter we take the point of view of one company in an extended enterprise, which we call the focal company or focal organization, and provide an in-depth look at the external insider threat problem from the perspective of this organization, and one possible solution to the problem. Therefore, the contribution of this chapter is twofold. First, it describes (in Sections 1–4) what the external insider threat problem is and which challenges intrinsic to that problem from the perspective of the business, organizational and technical aspects arise. Second, it provides (in Sections 5–9) an overview of existing solutions, introduces a new potential solution and concludes with future directions of further solutions.

The chapter is organized as follows. Section 2 reviews the concept of trust and characteristics of outsiders and insiders, and uses this to introduce...