Chapter 83
Complex Interdependency of IT Security Risk in B2B Supply Chain

Tridib Bandyopadhyay
Kennesaw State University, USA

ABSTRACT

Managers often decide to integrate supply chains of collaborating firms. Whether such decisions are for competitive posture, cost saving or operational efficiencies, it is important to understand that supply chains integrate not only the flow of goods but also the information processes and assets and more often than not, the IT networks of the firms. Thus two developments occur. First, IT security losses of one firm collocate at the other firm's servers as information assets like demand forecasts are shared. Second, the Intranets of both firms get connected with the help of VPN or similar technologies, making it possible that a breach can travel from one firm to the other. This in turn makes IT security risks of SC firms strategically interdependent. This chapter analyzes such interdependent IT security risks and provides insights for SC and IT managers who are poised to collaborate with other downstream or upstream partner firms.

INTRODUCTION

Communication networks have been the enablers of many reengineering efforts across supply chains (henceforth SC). Electronic Data Interchange (EDI), Continuous Replenishment Program (CRP) and Vendor Managed Inventory (VMI) systems now link the computer networks of manufacturers, distributors, and retailers within the supply chain. The benefits to SC firms from these communication linkages are numerous. EDI reduces transaction costs and transaction errors (Srinivasan, Kekre, & Mukhopadhyay, 1994), (Mukhopadhyay, Kekre, & Kalathur, 1995). CRP reduces inventory holding and shortage costs, improves fill rates and inventory turnover (Clark, & Hammond, 1997) and (Lee, Theodore, & Kar, 1999), and VMI ensures efficient use of shelf-space and appropriate retail marketing decisions (Waller, Johnson, & Davis, 1999). As a result, interconnected network systems have become commonplace across SCs.

DOI: 10.4018/978-1-7998-7705-9.ch083

Unfortunately, interconnected networks also tend to increase the overall likelihood of IT security breaches. Indirect breaches via partnering firms are now possible through the interconnecting link. This problem is further aggravated because information exchange in SC now increasingly occurs over networks designed to operate on top of the public Internet. For example, small and medium enterprises (SMEs) now increasingly utilize XML technology in a cost-effective fashion to integrate their disparate back-end processes and data formats on a standard set of tags from their industry (Samtani, 2002). Although cost effective, these open standard arrangements are inherently less secure than the traditional networks like EDI, where the combination of the dominant partner model, dedicated servers, and algorithmically compressed and VAN mediated data transmission all contribute to a very high level of information security. As a result, a hacker who has penetrated one firm due to its poor information security may access other connected firms relatively easily (Grance, Hash, Peck, Smith, & Korow-Diks, 2002). IT Security experts are also increasingly concerned about break-ins that could come via a company's partners and vendors.

The fact that firms in a SC can be progressively compromised beginning with one single firm has significant implications. It creates the circumstances of *Network Effect,* an economic concept where one firms' value forms an action depends on the equivalent actions by other firms in the same network (Liebowitz, & Margolis, 1994). Although we are looking at a specific case of *negative* or undesirable effect on IT security risk here, network effect could as well be positive. For example, as more firms bought fax machines in the latter part of the twentieth century, the benefit of having a fax machine increased exponentially since increasingly more firms could exchange information with the help of these fax machines.

The negative network effect suggests if one firm secures its network inadequately; other firms in the SC may suffer from *indirect* breaches through the first firm even after hardening their own networks against external elements[1]. In other words, The IT security health of the first firm could negatively impact other firms' motivation to invest in IT security. There is yet another fascinating angle to the above observation. When a firm invests in IT security, the overall network security of the SC improves, and the benefit is shared by all firms. Knowing this however, firms may (a) either wait indefinitely for the first movers, perpetuating a low IT security health in the SC, and/or (b) decide to enjoy the benefits of other firms' security investments but not reciprocate with their own investments, giving rise to *free rider behavior*.

Either way, the above understanding presents a grim outcome. But does this necessarily mean that SC firms are destined to exhibit network effect in IT security risks only in the undesirable, negative direction? The brief answer to the question above is '*no*'! However, in order to understand the full depth of this problem and see how the interdependent risks may remain moderated, one will have to analyze the SC relationship in greater detail and from an IT security perspective. This is what we delve and explain in this chapter.

IT Security Risk Interdependencies in Supply Chain

IT security risk is essentially the product of the *likelihood* of a breach and the eventual *loss* that this breach could cause. It has already been explained how interconnecting links increase the *likelihood* of breach, introduce undesirable investment behavior, and bring interdependency in IT security risk of SC firms. We now explore the other aspect interdependency that may exist in the way *loss* is realized in SC. The primary focus of this discussion will center on exploring positive network effect, since that could potentially bring a desirable balancing force which can combat the negative network effect arising out of the interconnectivity between SC firms.