Employing Cost Effective Internet-Based Networking Technologies to Manage B2B Relationship: The Strategic Impact on IT Security Risk

Tridib Bandyopadhyay, Kennesaw State University, USA

ABSTRACT

Using Internet-based technologies to establish network connectivity between firms can create conduit for propagation of threat vectors. Sharing data and information assets with other firms may give rise to external seats of loss exposure. Together, these practices complicate the IT security risk in business relationship: misaligned incentive for IT security investment and free rider behavior arise. Naïve pursuit to enter into business relationships using Internet-based technologies can prove myopic because the IT security risk profile of the resultant B2B network may be untenable. This research exhibits the impact of sharing and linking of information and network assets on IT security risk in modern business relationship with the help of a 2-firm symmetric B2B. This work demonstrates why managers should consider expanding their business relationship to include IT security initiatives as well, especially when they employ Internet-based technologies to interlink their networks.

Keywords: B2B, B2B Cyber Security, Internet-Based Network Security, Internet-Based Network Technologies, IT Security

INTRODUCTION

Firms engage in inter-firm, business-to-business networking (henceforth B2B-NW) on a regular basis, and this trend is expected to continue. By the year 2012, the total business value transacted on B2B-NW is expected to grow up to $6.3 Trillion - 40% of the total inter-firm trade in US (Laudon & Traver, 2009).

As transactions over business to business networks grew over time, the enabling networking technologies experienced major changes (Figure 1). B2B-NW began in the early 1970s with the automated order entry systems that employed phone modems. This was followed by the proprietary protocols and systems like the electronic data interchange systems (EDI). Commercialization of the Internet in the ’90s introduced the Internet-based technologies, which made B2B-NW increasingly affordable,
scalable and practicable; especially for the small and medium firms. Although EDI remains the largest segment with continued support from large organizations Kairab (2004), the fastest growing segment is non-EDI B2B commerce (Laudon & Traver, 2009), which relies solely on Internet-based networking technologies to maintain B2B relationship.

Benefits aside, B2B-NW increases the likelihood of IT security breach in the interconnected firms. Indirect breaches via the network link become possible. Earlier networks like the EDI ensured a high level of IT security by the combination of dominant partner model, dedicated servers, and algorithmically compressed, and VAN mediated data transmission. Unfortunately, the Internet-based arrangements are inherently less secure. When firms utilize Internet-based technologies in B2B-NW, a hacker who has penetrated one firm due to its poor security may access other connected firms relatively easily (Camp & Wolfram, 2004; Grance et al., 2002). IT Security experts are also increasingly concerned about break-ins that could come via a company’s partners and vendors (online.wsj.com/PA2VJBNA4R/arti-
cle_print/SB112128442038984802). Thus it is important for the IT managers to understand the strategic IT security impact on a B2B-NW when the interconnectivity between the B2B firms become increasingly more vulnerable due to the adoption of Internet-based networking technologies – the goal of this study. How exactly does the increased likelihood of breach in a B2B-NW impact the IT security of the partnering firms? A straightforward answer to this question is difficult because when firms engage in B2B-NW to gain value, their IT security risks become interdependent. Consider the following:

1. When a firm secures its network and server inadequately, the other firms in the B2B-NW face elevated likelihood of breach even after hardening their own network perimeters against external elements. This happens because a breach seeded at the firm can travel over the trusted B2B link to other firms in the network. Clearly, The IT security health of the first firm impacts the other firms’ motivation to maintain their IT security.

Figure 1. Technology progress in B2B
Related Content

Building a Trusted Environment for Security Applications
www.igi-global.com/chapter/building-trusted-environment-security-applications/76522?camid=4v1a

A Survey of Risk-Aware Business Process Modelling
www.igi-global.com/article/a-survey-of-risk-aware-business-process-modelling/181854?camid=4v1a
Access Control Specification in UML
www.igi-global.com/chapter/access-control-specification.uml/24057?camid=4v1a

Distributed Key Management Scheme Based on CL-PKC in P2P Networks
www.igi-global.com/chapter/distributed-key-management-scheme-based/65771?camid=4v1a