A Field Study of Extended Enterprise Security*

Scott Dynes [1,2]
M. Eric Johnson [1]
[sdynes, M.Eric.Johnson]@Dartmouth.edu
[1]Glassmeyer/McNamee Center for Digital Strategies
Tuck School of Business at Dartmouth College
[2] Institute for Security Technology Studies, Dartmouth College

Extended Abstract

As organizations increasingly rely on the internet for their internal and external business processes, each firm's security decisions have an impact on the overall security of the information infrastructure for the thousands of suppliers, collaborators, and channel partners that they interact with as part of that firm's extended enterprise (a collection of firms that design, produce, and market a product or service [Dav2004]).

Each firm in the extended enterprise must have access to critical business information such as product specifications, marketing plans, and vast transactional data on product sales and movement within the supply chain. Managing the security of this sensitive information flowing across the extended enterprise is a significant and under-researched topic. Firms often make information security decisions with very limited information about the threats their systems face, the strength of their systems against these threats, and the efficacy of additional security measures. Outsourcing and globalization present even more difficult security issues.

Understanding the economics of information security within and across firms will necessitate understanding the process by which firms adopt information security mechanisms; this will expose existing drivers and possible incentives promoting greater information infrastructure security. Separately, understanding the risks referred across the extended enterprise is critical to defining a level of information security to minimize those risks, and is a step towards developing a business case for the security needs of the firm as well as addressing what level of security is needed for the greater public good.

While there are a few papers that have studied return on investment (ROI) on information technology (IT) security investments at the firm level ([Gor2002], [Soo2001]), little empirical work has been done at the firm level to understand the processes involved in information security. Like the interdependent security risks faced by other business partnerships [Kun2004], such as baggage handling in the commercial airlines, we hypothesize that information security risks across trading partners exhibit many important risk management challenges.

We have identified three research efforts that address the core information security issues pertaining to the efficacy of economic and other potential drivers of information security, the risks to which critical business infrastructures (supply chains) are being exposed, and to what extent security decisions need to be made with an eye to managing risks beyond one's local organization. These research efforts are:

To understand how firms adopt information security capabilities: How do firms currently make security investment decisions? What are the key drivers?

To access interdependency risk magnitude: How large is the real or perceived security problem for the extended enterprise? What are the security risks and how do those risks translate into business risks? Knowing how vulnerable or resilient supply chains and extended enterprises are to security failures of one of their members will directly inform the policy debate about how much information security is needed for the greater public good [Dyn2004].

To evaluate the information security gap: Are larger companies only as secure as their least-secure supplier? Are larger firms making better security investments (and better patch management decisions) than smaller firms, creating a security gap in the extended enterprise, which may render all interdependent companies as vulnerable as the weakest critical company in their extended enterprise [Joh2004]? Is anyone managing the risk across the extended enterprise? Should large, relatively secure firms be concerned about collaborating with smaller, less secure firms?

This paper presents results of a study that explores these questions through field research of firms of different sizes and their supply chains.

* This research was partially supported under Award number 2003-TK-TX-0003 from the U.S. Department of Homeland Security, Science and Technology Directorate. Points of view in this document are those of the author(s) and do not necessarily represent the official position of the U.S. Department of Homeland Security or the Science and Technology Directorate

References

[Dav2004] Davis, E.W. and R.E. Spekman, Extended Enterprise. FT Prentice Hall, NY, NY (2004).

[Dyn2004] Dynes, S. B. C. "Security and Privacy: At Odds With Speed and Collaboration?" http://mba.tuck.dartmouth.edu/digital/Programs/CorporateRoundtables/SecurityAndPrivacy/Overview.pdf

[Gor2002] Gordon, L. A. and M. P. Loeb, "The Economics of Information Security Investment," *ACM Transactions on Information and System Security*, (November 2002), pp. 438-457.

[Joh2004] Johnson, M. E. "The safety of secrets in extended enterprises," *Financial Times*, 18 August 2004, A7.

[Kun2004] Kunreuther, H. (2004) "Risk Analysis and Risk Management in an Uncertain World," Forthcoming in *Risk Analysis*, Wharton School Working Paper.

[Soo2001] Soo Hoo, K. J., Sudbury, A. W., and Jaquith, A. R. (2001) "Tangible ROI through secure software engineering," *Secure Business Quarterly: Special Issue on Return on Security Investment*, 1(2), Q4, 2001. A publication of @stake.