1 November 2004

What Drives Information Security Investment?

By INSTITUTE FOR SECURITY TECHNOLOGY STUDIES

ISTS Senior Research Fellow Scott Dynes wants to know what makes organizations adopt higher levels of information security, and he examines the economics of this area to determine if risk management is a factor in information security investments. In the fall of 2003, Dynes, at the behest of former ISTS policy director Adam Golodner and in collaboration with fellow ISTS Research Fellow Michael Freeman as well as Eric Johnson and Hans Brechbuhl of the Center for Digital Strategies at the Tuck School of Business, started looking at the market drivers of information security.

"A year ago, most businesses looked at information security as a cost of doing business – therefore, it was not a great incentive for firms to make further security investments," explains Dynes.

Given that the information infrastructure of the Internet is a critical part of business operations, Dynes and his collaborators became interested in understanding the risks firms face through their use of the Internet, and how they manage those risks.

Dynes studies how firms view the extent of their security responsibilities. "Companies are mainly taking a local view of security. They need to think more globally about what will happen if a critical supplier suffers a debilitating cyber event," says Dynes. "Many issues that go into thinking about infrastructure protection are questions we are exploring in our field study of firms and their supply chains."

Currently, the field study includes looking at what influences a firm's definition of adequate information security and the process by which firms make security investment decisions. Dynes believes that understanding the investment process is necessary for knowing the absolute and relative effectiveness of various market, economic and regulatory incentives for firms to adopt greater levels of information security.

The field study also takes a global view, exploring the magnitude of the risks resulting from the use of the Internet to integrate supply chains and extended enterprises. According to Dynes, there's a wide variation in the dependence firms have on communication with their business partners, and in the attention they pay to the information security of their partners. As an example of the latter, he says, "Typically, when financial firms outsource to another firm that will be holding customer data, they will take complete responsibility for assuring the outsourcing partner meets their information security requirements. There's a lot less rigor outside the financial industry."

Understanding how risks are transferred through these interrelations will enable security specialists in firms and government to better define what are appropriate levels of information security for particular industries.

For more information about this study, contact Scott Dynes at sdynes@dartmouth.edu or visit http://mba.tuck.dartmouth.edu/digital/Research/ResearchHighlights/SecurityField.html.