

Business Rationale for Cyber Security

A Critical Challenge

Millions of messages, data files and transactions flow through business networks and across the Internet each day, collectively driving the U.S. economy. Our nation's dependence on this vast electronic infrastructure is unquestioned; certainly few businesses can survive without safe networks and reliable Internet access.

At the same time, companies are increasingly at risk from cyber attack. Malicious intruders can bring business to a halt, as in a distributed denial-of-service attack that renders a system temporarily inoperable; or they can create thornier problems, as when a hacker unleashes data-destroying code or downloads proprietary secrets. In addition, attacks are seldom isolated: a breakdown in one company can reverberate throughout an entire economic sector, disrupting the flow of vital goods and services to many end-users.

Most businesses understand that cyber security is critical to their operations. Unfortunately, the information assurance community has yet to develop the risk analysis tools needed to understand the economic complexities that influence companies' security purchases. Deciding how much to spend on what level of protection depends on numerous variables, many of them poorly understood. How, for example, does one measure success when a thwarted attack cannot be distinguished from the lack of attack? Similarly, how does one calculate the costs of inadequate protection when the degree of risk is unpredictable? Finally, how does one account for inadequate security on the part of suppliers and others in one's business network? What happens, in other words, when a cyber attack directed at one company ripples throughout an entire supply chain? And perhaps most important, how does one compare investments in cyber security to other investment opportunities, such as R&D or enhanced marketing?

With its focus on risk-modeling tools and analyses, the *Business Rationale for Cyber Security* project represents a key step in addressing the business challenge of making better cyber security investment decisions.

Project Overview

Launched in April 2007, the *Business Rationale* project represents the first comprehensive study of cyber security economics. Involving more than a dozen experts from four research institutions, the project brings a multi-disciplinary and collaborative approach to this critical need. The project takes a solutions-oriented approach, with team members collecting data, assessing strategies and creating decision-making models.

Central to the study are two questions:

- What data are needed to create a reliable investment model and related decision-making tools?
- What impact do various investment decisions—or lack thereof—have, not only on a single business, but on related businesses and the broader economic sector?

I3P

Institute for Information
Infrastructure Protection

The Institute for Information Infrastructure Protection (I3P) is a national consortium of leading academic institutions, federally-funded laboratories, and non-profit organizations dedicated to strengthening the cyber infrastructure of the United States.



The I3P *Business Rationale* project takes a quantitative approach to cyber risk management by aiming to create tools that organizations can use to quantify and improve their cyber security decision-making. Specifically, how can a company, having only limited knowledge of the threats it faces, a poor grasp of the probable consequences of an attack and no way to predict the economic impact of potential security solutions, rationally set investment levels for cyber security?

Team Members

Dartmouth College
RAND Corporation
University of California,
Berkeley
University of Virginia

Working with Industry

The *Business Rationale* project is partnering with a reasonably broad set of companies and industry leaders to better understand specific security needs within the business sector and also the multiple impacts a security breach can have both within and beyond a single company. As part of their analysis, researchers will measure such parameters as the likelihood of attack, the prospective consequences of an attack, and the reduction of risk created by differing levels of cyber security investment. At the same time, the team is working to develop tools to facilitate rational investment decisions.

Specifically, the team is undertaking the following strategies:

- Analysis of how specific companies track and respond to cyber security threats and implement protective measures
- Examination of how companies utilize risk analysis to support their cyber security decision-making, with a specific look at group decision-making and its underlying assumptions
- Assessment of the information flow among and within companies to determine the potential impact of a security breach throughout a supply chain
- Development of models and open-source software to help organizations better understand critical inter-dependencies, that is, how cyber security decisions broadly affect their business and also impact their partners' and suppliers' businesses
- Study of how legal forces, such as security breach notification laws and federal regulation, affect cyber security investment decisions

Making an Impact

By developing tools to facilitate appropriate cyber security choices, the *Business Rationale* project addresses a critical need.

Not only are data obtained by the *Business Rationale* team contributing significantly to our understanding of a corporation's economic position vis a vis cyber security, but the group's solutions-oriented approach is producing tools to directly help harden our nation's cyber infrastructure. Specifically, the project's goals are to:

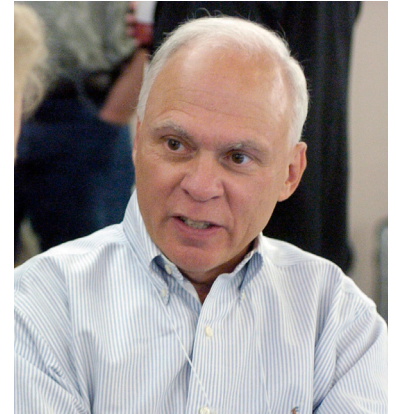
- Determine what impact cyber security investing has not only on an individual business but on an entire economic sector
- Help industry better understand its vulnerabilities with respect to cyber investment
- Introduce decision-making tools to allow end-users to quantify and evaluate their cyber security investments, including trade-offs
- Inform policymakers who may in turn take action to promote cyber security investment and compliance
- Develop marketable tools to facilitate rational investments in cyber security

Overall, the data and tools developed by the team are expected to play a key role in helping organizations make better cyber security decisions and thus—indirectly—help strengthen the information security of the U.S. economy.

This material is based upon work supported by the U.S. Department of Homeland Security under Grant Award Number 2006-CS-001-000001, under the auspices of the Institute for Information Infrastructure Protection (I3P) research program. The I3P is managed by Dartmouth College. The views and conclusions contained in this document are those of the authors and should not be interpreted as necessarily representing the official policies, either expressed or implied, of the U.S. Department of Homeland Security, the I3P, or Dartmouth College.



Institute for Information
Infrastructure Protection



“Our team faces a number of interesting challenges. Among them, how does one effectively measure the return on investment for a strategy that—if temporarily successful—provides no data to support continuing need?”

Barry Horowitz,
University of Virginia
and Team Leader

Information about the project can be found at:

www.thei3p.org

or by contacting
Barry Horowitz,
Team Leader, at
barrymhorowitz@virginia.edu
or
Charles C. Palmer,
I3P Director for Research at
charles.c.palmer@dartmouth.edu

The I3P is managed by Dartmouth College

