

The Economics of Cyber Security

June 2006

PROJECT OVERVIEW

The Economics of Cyber Security Research Project is supported by the Institute for Information Infrastructure Protection (I3P). The multi-disciplinary research, being conducted at leading national facilities, aims to provide decision-makers with data and analysis to help them make informed decisions about protecting the nation's critical infrastructures. The project is organized and coordinated around three views of the problem: a national, an enterprise and a technology perspective.

PROJECT GOALS

The goal of the research team is to use its findings to inform future government policies and corporate decision-making. The research team seeks to:

- Understand the barriers and incentives to investment in cyber security
- Identify the most serious threats
- Quantify the costs of cyber security and the effects of cyber attacks
- Measure and model the effectiveness of current security tools, processes and policies

KEY QUESTIONS

- How are information security decisions made?
- How can we make more informed and realistic security decisions?
- What data are available, and how credible are they?
- What market and policy mechanisms are most effective in promoting security?

PROJECT SUCCESS

The research will reveal a detailed and nuanced picture of the dependence of U.S., sector and enterprise economies on the security and integrity of the information infrastructure. The results will include a set of macro- and micro-economic models and findings about the nature of information security decision-making. The project provides knowledge and tools to help use market forces, policy levers and technological design to increase the security of the information infrastructure.



PLANNED RESULTS

- Decision-makers can evaluate and contrast the likely economic consequences of a variety of proposed policies involving investment priorities and resource allocations.
- Security decisions can be informed not only by technological availability, but also by the economic, organizational, behavioral and cultural considerations at enterprise and sector levels.

TEAM MEMBERS

The research team is composed of researchers and engineers from the following institutions:

- Dartmouth College Tuck School of Business
- I3P Administrative Office
- Critical Infrastructure Protection Program, George Mason University
- MIT Lincoln Laboratories
- RAND Corporation
- University of Virginia

The Economics of Cyber Security

June 2006

RESEARCH APPROACH

The research is organized in three threads:

- Thread I addresses national concerns, by viewing problems on a macro-economic scale. Its research assesses how industry sectors interact within the U.S. economy, particularly in terms of how impairments to the information infrastructure can destroy economic capabilities and generate ripple effects throughout the U.S. economy.
- Thread II examines enterprise considerations, looking at how firms apply security technologies and deal with the effects of security breaches. In particular, this research generates information about how enterprises make security investment decisions and balance their security costs with other economic demands.
- Thread III considers the technology behind the information infrastructures, examining threats against core infrastructure technologies and developing a set of least-cost responses and policy recommendations to stimulate deployment.

RESEARCH PRODUCTS CURRENTLY UNDER DEVELOPMENT INCLUDE:

- Macro and micro models to aid understanding of risk and decision-making
 - Models from the national, enterprise and technology perspectives
 - A macro-economic decision support tool (currently in prototype form)
 - Scenarios and frameworks to integrate the three perspectives

- An integrated picture of economic dependence on the security and integrity of the information infrastructure.
 - Publications bringing together many disciplines
 - Standards and policy proposals to increase the incentives for infrastructure security deployment

WORKING WITH INDUSTRY

The research team is working closely with industry and government stakeholders by: conducting workshops; performing case studies and interviews; working on standards groups and committees; developing tools; and publishing and disseminating findings. All results are made realistic by working with and vetting by industry and government stakeholders.

More Information:

Information about the project can be found at <http://www.thei3p.org/research/economics/index.html>

I3P Publications can be found at www.thei3p.org/about/publications.html

Points of Contact:

Project Leader: Shari Lawrence Pfleeger [pfleeger@rand.org](mailto:spfleeger@rand.org) (703) 413-1100 Ext.5525

I3P Assistant Director for Research and Analysis : Eric Goetz, egoetz@thei3p.org (603) 646-0692

This work was produced under the auspices of the Institute for Information Infrastructure Protection (I3P) research program. The I3P is managed by Dartmouth College, and 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 authors and do not necessarily represent the official position of the U.S. Department of Homeland Security, the Science and Technology Directorate, the I3P, or Dartmouth College.