Research Brief

RAND Homeland Security

A RAND INFRASTRUCTURE, SAFETY, AND ENVIRONMENT PROGRAM

Cybersecurity Economic Issues

Corporate Approaches and Challenges to Decisionmaking

RAND RESEARCH AREAS
THE ARTS
CHILD POLICY
CIVIL JUSTICE
EDUCATION
ENERGY AND ENVIRONMENT
HEALTH AND HEALTH CARE
INTERNATIONAL AFFAIRS
NATIONAL SECURITY
POPULATION AND AGING
PUBLIC SAFETY
SCIENCE AND TECHNOLOGY
SUBSTANCE ABUSE
TERRORISM AND HOMELAND SECURITY
TRANSPORTATION AND INFRASTRUCTURE
WORKFORCE AND WORKPLACE

Abstract

The emerging field of cybersecurity economics could benefit from better data, better understanding, and better methods for using resources wisely, not only to protect critical products and services but also to provide assurances that software will work as expected. This research brief presents findings that address these key cybersecurity concerns, perceptions of the importance of cybersecurity, and considerations for cybersecurity investment decisions. In particular, it suggests that companies, the government, and other organizations can help improve our understanding of cybersecurity economics by monitoring cybersecurity incidents and responses, soliciting and using standard terminology and measures, and sharing data whenever possible.

Cybersecurity economics is an emerging field. There is a significant need for better data, better understanding, and better methods for using resources wisely, not only to protect critical products and services but also to provide assurances that software will work as expected. In two articles, RAND senior scientist Shari Lawrence Pfleeger and her colleagues addressed these key cybersecurity concerns and identified how different types of companies or organizations perceive the importance of cybersecurity and make cybersecurity investment decisions.

Corporate Approaches to Cybersecurity

Companies and organizations can use a wide variety of security practices and policies to describe, implement, and monitor cybersecurity. To understand what influences security-related investment decisions and how business perspectives affect cybersecurity perceptions, RAND researchers interviewed the chief security officers of six companies in the Internet supply chain. These leaders revealed vastly different attitudes about the role of security in the context of their corporate goals. The analysis suggests that a company's culture and approach to market discipline can predict corporate attitudes about cybersecurity.

To understand these security approaches, the RAND team considered a business framework that could help explain the interview results and also identify which one of three market disciplines companies embrace to compete in the marketplace: operational excellence, product leadership, or customer intimacy.[1] This framework has been useful in other software-engineering contexts in which it has assisted technology adoption within the context of corporate culture. In addition, the authors believe that the framework can be used not only to analyze existing security attitudes but also to predict likely future cybersecurity actions and attitudes.

An *operationally excellent* company strives to provide both high-quality customer service and the lowest prices for its goods and services. It emphasizes efficiency and dedication to quality control along with a carefully managed supply chain. Because security is a facet of quality, an operationally excellent company takes security very seriously. By applying standards, controlling processes, and encouraging certification, operationally excellent companies consider security to be central to their trusted brand.

By contrast, a *product leader* focuses on features and functionality, prizing innovation as it experiments with new offerings. Whereas opera-

[1] Michael Treacy and Frederik D. Wiersema, *The Discipline of Market Leaders: Choose Your Customers, Narrow Your Focus, Dominate Your Market*, Reading, Mass.: Addison-Wesley, 1995.

This product is part of the RAND Corporation research brief series. RAND research briefs present policy-oriented summaries of published, peer-reviewed documents.

Headquarters Campus
1776 Main Street
P.O. Box 2138
Santa Monica, California
90407-2138
TEL 310.393.0411
FAX 310.393.4818

© RAND 2008

www.rand.org

tionally excellent companies take few risks, product leaders encourage new ventures and a steady stream of new products. Although they take security seriously, good-enough security is a guiding principle; innovation—not process—is the key to avoiding or preventing security problems. As a result, security takes a back seat to performance, is less centralized, and is not the key determinant of a product's success.

The third market discipline, *customer intimacy*, emphasizes customer needs and requests and excels at meeting them. Security is important for customer-intimate companies when customers express security needs. Thus, the security organizations of customer-intimate companies are less top-down than those of operationally excellent companies, and their centralized procedures involve significant customer interaction. As a result, security is built into products and services only when the customer demands security.

Numerous Cybersecurity Uncertainties

No matter what an organization's cybersecurity posture, it needs data on which to base its security decisions. However, lack of data and uncertainty about the data frequently inhibit sound corporate decisionmaking.

One significant problem is the *lack of standards* in defining, tracking, and reporting security incidents and attacks. Different surveys ask vastly different questions about "electronic attacks," "virus encounters," "virus disasters," "data intrusions," and "security incidents," among many other terms. Thus, much of the reported evidence is categorized differently from one study to another, and the answers are based on respondents' perceptions, not on consistent capture and analysis of solid empirical data. Moreover, the *lack of careful sampling* often obscures which population the reported data describe. This hodgepodge of definitions, concepts, and survey types makes it difficult for software managers to know what cybersecurity data to collect and how to compare them with survey results.

Understanding the *source and effects of attacks* is similarly problematic. Several surveys note that the sources of attacks are unknown in a significant percentage of cases. In addition to the number and types of attacks, significant variations exist in terms of effect, particularly the cost of an attack. Software managers need this cause-and-effect information, not only to design more secure systems but also to estimate resource needs for preventing, mitigating, and recovering from attacks, particularly attacks against the development platforms on which new software is created.

A more significant problem is the *difficulty in detecting and measuring both the direct and indirect costs of security breaches*. There are neither accepted definitions of loss nor standard, reliable methods to measure it. For example, one survey notes that respondents historically underestimate costs by a factor of seven to 10.

Survey results also highlight another gap concerning security investments: *how much organizations have invested in security protection, prevention, and mitigation*. Little is known about how companies make investment decisions or how effective their security investments are. Inputs required for such decisionmaking—such as the rate and severity of attacks, cost of enterprise-wide damage and recovery, and actual cost of all types of security measures—are not known with any accuracy. Simple questions, such as how much more security an extra dollar buys, go unanswered.

Faced with these challenges, a RAND study by Davis et al. implemented a national computer security survey on behalf of the Bureau of Justice Statistics and the U.S. Department of Homeland Security. This first large-scale, carefully sampled survey of the state of U.S. cybersecurity was intended to improve the nature and quality of data available to U.S. decisionmakers. By asking broad questions of 36,000 businesses representing all sectors of the economy, the survey results will be similar to the FBI's annual crime statistics, providing a baseline from which cybersecurity trends can be derived. This computer security survey has demonstrated the significant barriers to information sharing that must be overcome before industry surveys are likely to provide a good picture of industry's exposure to cybercrime and the costs and actions necessary to mitigate it.

Inputs Required for Sound Cybersecurity Decisionmaking

Software project managers *need better data* to support their decisionmaking about security. Ideally, a data source should provide information to support the following tasks:

- Project managers must decide how to allocate resources to *monitor and address cyber incidents*. Survey data can inform resource-allocation decisions and trend data about cybersecurity incidents, which can support more effective strategic planning.
- Government, industry, and monitoring organizations must *implement standards and guidelines*, which will facilitate the search for common problems and possible solutions. Standardization of vulnerabilities, types of attack, and techniques used in attacks can permit cross-project analysis that suggests best practices involving the most cost-effective technologies, policies, procedures, and organizational structures.
- *The insurance industry* could play a growing role in securing cyberspace. Credible survey data could be used to set policy terms and standards for insurability against cyberattacks. This information would inform decisions

about how much security to build into a product and how much it would cost.
- There also is a need for *critical infrastructure–protection benchmarks*, which could support the analysis of attack frequency, severity trends, and consequent losses; determination of best practices for addressing current and changing vulnerabilities; and the implementation of regular standards updates.
- *Measures of effectiveness* are needed to provide feedback on the efficacy of campaigns to strengthen cybersecurity. Such measures could influence perception and empirical measurement of security strategies' effectiveness, development and dissemination of good metrics, perceived and actual effects of regulations and standards and their enforcement, and perceived and actual effects of both public- and private-sector education strategies.

To better understand the cybersecurity challenges, *multidisciplinary research is needed* within and across the boundaries of engineering, business, and arts and science. Although there is a paucity of empirical analysis and a lack of agreement on findings, researchers are working on five key issues: software quality, market interventions, evaluations, corporate decisionmaking, and cybersecurity modeling.

Conclusions

Companies, the government, and other organizations can be active players in improving our understanding of cybersecurity economics by monitoring cybersecurity incidents and responses, soliciting and using standard terminology and measures, and sharing data whenever possible. They can participate in surveys and studies to better understand the nature and extent of such incidents. By sharing information with researchers and colleagues, they can enable business sectors to take a coordinated approach to preventing and mitigating attacks, as well as inform government policies that affect cybersecurity. And finally, they can apply appropriate business measures so security investment decisions can eventually harmonize with other corporate investment decisions. ■

This research brief describes work done for RAND Infrastructure, Safety, and Environment and documented in two articles (Shari Lawrence Pfleeger and Rachel Rue, "Cybersecurity Economic Issues: Clearing the Path to Good Practice," *IEEE Software*, Vol. 25, No. 1, January–February 2008, pp. 35–42, and Shari Lawrence Pfleeger, Martin Libicki, and Michael Webber, "I'll Buy That! Cybersecurity in the Internet Marketplace," *IEEE Security and Privacy*, Vol. 5, No. 3, May–June 2007, pp. 25–31). Other relevant research is available in a RAND report: *The National Computer Security Survey (NCSS): Final Methodology*, by Lois M. Davis, Daniela Golinelli, Robin Beckman, Sarah K. Cotton, Robert H. Anderson, Anil Bamezai, Christopher R. Corey, Megan Zander-Cotugno, John L. Adams, Roald Euller, and Paul Steinberg, TR-544-BJS (available at http://www.rand.org/pubs/technical_reports/TR544/), 2008, 90 pp., $24, ISBN: 978-0-8330-4467-9. This research brief was written by Michael Neumann. The RAND Corporation is a nonprofit research organization providing objective analysis and effective solutions that address the challenges facing the public and private sectors around the world. RAND's publications do not necessarily reflect the opinions of its research clients and sponsors.
RAND® is a registered trademark.

RAND Offices
Santa Monica, CA • Washington, DC • Pittsburgh, PA • New Orleans, LA/Jackson, MS • Doha, QA • Cambridge, UK • Brussels, BE

RB-9365-1 (2008)

Homeland Security

A RAND INFRASTRUCTURE, SAFETY, AND ENVIRONMENT PROGRAM

THE ARTS
CHILD POLICY
CIVIL JUSTICE
EDUCATION
ENERGY AND ENVIRONMENT
HEALTH AND HEALTH CARE
INTERNATIONAL AFFAIRS
NATIONAL SECURITY
POPULATION AND AGING
PUBLIC SAFETY
SCIENCE AND TECHNOLOGY
SUBSTANCE ABUSE
TERRORISM AND HOMELAND SECURITY
TRANSPORTATION AND INFRASTRUCTURE
WORKFORCE AND WORKPLACE

This PDF document was made available from www.rand.org as a public service of the RAND Corporation.

This product is part of the RAND Corporation research brief series. RAND research briefs present policy-oriented summaries of individual published, peer-reviewed documents or of a body of published work.

The RAND Corporation is a nonprofit research organization providing objective analysis and effective solutions that address the challenges facing the public and private sectors around the world.

Support RAND

Browse Books & Publications

Make a charitable contribution

For More Information

Visit RAND at www.rand.org

Explore RAND Homeland Security

View document details

Limited Electronic Distribution Rights

This document and trademark(s) contained herein are protected by law as indicated in a notice appearing later in this work. This electronic representation of RAND intellectual property is provided for non-commercial use only. Unauthorized posting of RAND PDFs to a non-RAND Web site is prohibited. RAND PDFs are protected under copyright law. Permission is required from RAND to reproduce, or reuse in another form, any of our research documents for commercial use. For information on reprint and linking permissions, please see RAND Permissions.