



## Sharing information on computer systems security: An economic analysis

Lawrence A. Gordon <sup>a</sup>, Martin P. Loeb <sup>b,\*</sup>,  
William Lucyshyn <sup>c</sup>

<sup>a</sup> *Ernst & Young Professor of Managerial Accounting and Information Assurance, Robert H. Smith School of Business, University of Maryland, College Park, MD 20742-1815, USA*

<sup>b</sup> *Professor of Accounting and Information Assurance, Deloitte Touche Faculty Fellow, Robert H. Smith School of Business, University of Maryland, College Park, MD 20742-1815, USA*

<sup>c</sup> *Research Director, Defense Advanced Research Projects Agency (DARPA) and Senior Research Scholar, School of Public Affairs, University of Maryland, College Park, MD 20742-1815, USA*

---

### Abstract

The US federal government has fostered a movement toward sharing information concerning computer security, with particular emphasis on protecting critical infrastructure assets that are largely owned by the private sector. As information security is paramount to accurate financial reporting and the provision of timely and relevant managerial accounting reports for decision-making, the issue of sharing information on computer systems security has direct relevance to accounting, as well as to public policy. This paper presents a model to examine the welfare economic implications of this movement. In the absence of information sharing, each firm independently sets its information security expenditures at a level where the marginal benefits equal the marginal costs. It is shown that when information is shared, each firm reduces the amount spent on information security activities. Nevertheless, information sharing can lead to an increased level of information security. The paper provides necessary and sufficient conditions for information sharing to lead to an increased (decreased) level of information security. The level of information security that would be optimal for a firm in the absence of information sharing can be attained by the firm at a lesser cost when computer security information is shared. Hence, sharing provides benefits to each firm and total welfare also increases. However, in the absence of appropriate incentive mechanisms, each firm will attempt to free ride on the security expenditures of other

---

\* Corresponding author. Tel.: +1-301-405-2209; fax: +1-301-405-0359.  
E-mail address: [mloeb@rhsmith.umd.edu](mailto:mloeb@rhsmith.umd.edu) (M.P. Loeb).

firms (i.e., renege from the sharing agreement and refuse to share information). This latter situation results in the underinvestment of information security. Thus, appropriate incentive mechanisms are necessary for increases in both firm-level profits and social welfare to be realized from information sharing arrangements.

© 2003 Elsevier Inc. All rights reserved.

*Keywords:* Information sharing; Cyber security; Information security economics; Homeland security

---

## 1. Introduction

The Internet revolution has dramatically changed the way individuals, firms, and the government communicate and conduct business. For example, the telecommunications, banking and finance, energy, and transportation industries, as well as the military and other essential government services, all depend on the Internet and networked computer systems to conduct most of their day-to-day operations. However, this widespread interconnectivity has increased the vulnerability of computer systems—and more importantly, of the critical infrastructures they support—to information security breaches. According to the Report of the President's Commission on Critical Infrastructure (1997, p. ix), “This interconnectivity has created a new dimension of vulnerability, which, when combined with an emerging constellation of threats, poses unprecedented national risk.”

In response to this new vulnerability, organizations have created an arsenal of technical weapons to combat computer security breaches. This arsenal includes firewalls, encryption techniques, access control mechanisms, and intrusion detection systems. The federal government has responded with a major reorganization (forming the Department of Homeland Security, which is responsible for cyber security and infrastructure protection), and is developing a National Strategy to Secure Cyber Space. Unfortunately, to date these measures have met with only limited success. This limited success is highlighted by Richardson (2003, p. 21) in the Executive Overview of the 2003 survey conducted by the Computer Security Institute and Federal Bureau of Investigation, “the most important conclusion one must draw from the survey remains that the risk of cyber attacks continues to be high. Even organizations that have deployed a wide range of security technologies can fall victim to significant losses.”

Campbell et al. (2003) found empirical evidence that some security breaches result in statistically significant decreases in the market value of firms. Further evidence of the continuing problems associated with computer security breaches is provided by the fact that Representative Stephen Horn, in his third annual report card on computer security, found little improvement within the

متن کامل مقاله

دریافت فوری ←

**ISI**Articles

مرجع مقالات تخصصی ایران

- ✓ امکان دانلود نسخه تمام متن مقالات انگلیسی
- ✓ امکان دانلود نسخه ترجمه شده مقالات
- ✓ پذیرش سفارش ترجمه تخصصی
- ✓ امکان جستجو در آرشیو جامعی از صدها موضوع و هزاران مقاله
- ✓ امکان دانلود رایگان ۲ صفحه اول هر مقاله
- ✓ امکان پرداخت اینترنتی با کلیه کارت های عضو شتاب
- ✓ دانلود فوری مقاله پس از پرداخت آنلاین
- ✓ پشتیبانی کامل خرید با بهره مندی از سیستم هوشمند رهگیری سفارشات