IDEA GROUP PUBLISHING

ITB11307

701 E. Chocolate Avenue, Suite 200, Hershey PA 17033-1240, USA
Tel: 717/533-8845; Fax 717/533-8661; URL-http://www.idea-group.com

This chapter appears in the book, *Advanced Topics in End User Computing, vol. 4* edited by
M. Adam Mahmood © 2005, Idea Group Inc.

Chapter XIII

Computer Security and Risky Computing Practices: A Rational Choice Perspective

Kregg Aytes, Idaho State University, USA

Terry Connolly, University of Arizona, USA

ABSTRACT

Despite rapid technological advances in computer hardware and software, insecure behavior by individual computer users continues to be a significant source of direct cost and productivity loss. Why do individuals, many of whom are aware of the possible grave consequences of low-level insecure behaviors such as failure to backup work and disclosing passwords, continue to engage in unsafe computing practices? In this chapter we propose a conceptual model of this behavior as the outcome of a boundedly rational choice process. We explore this model in a survey of undergraduate students (N = 167) at two large public universities. We asked about the frequency with which they engaged in five commonplace but unsafe computing practices, and probed their decision processes with regard to these practices. Although our respondents saw themselves as knowledgeable, competent users and were broadly aware that serious consequences were quite likely to result, they reported frequent unsafe computing behaviors. We discuss the implications of these findings both for further research on risky computing practices and for training and enforcement policies that will be needed in the organizations that these students will be entering shortly.

Copyright © 2005, Idea Group Inc. Copying or distributing in print or electronic forms without written permission of Idea Group Inc. is prohibited.

INTRODUCTION

Over the past few years, the public has become increasingly aware of computer security issues, as incidents have been covered in the popular news media. Computer viruses, denial of service attacks, and cases of intruders hacking into corporate systems and stealing confidential information are becoming more commonplace. Information technology (IT) professionals seem to be waging a constant battle to maintain control over corporate technology and information assets.

The costs of security breaches are enormous and widespread. The most recent survey of 503 corporate and government organizations conducted by the Computer Security Institute and the FBI includes these sobering facts (Power, 2002):

- 40% report intrusion into information systems from outside the organization
- 85% were hit by worms or computer viruses
- 80% acknowledged financial losses due to computer security breaches
- While only 40% quantified their losses, those that did reported a total of almost $455 million in financial losses in 2001, mostly through the theft of proprietary information and financial fraud.

More important than just the magnitude of these numbers is the fact that they have gotten worse during the seven years in which the survey has been conducted. Financial losses have climbed each year, and most categories of attacks either have gotten worse or remain substantially unchanged from previous years.

Although there are technological solutions to counteract the many security threats, most security professionals realize that technology alone is insufficient to adequately protect a firm’s assets. Because information systems involve human users, and people do not always act the way they are supposed to, users are now considered one of the major chinks in the armor of computer security countermeasures (Rhodes, 2001; Tuesday, 2001). User-related risks include such low-level insecure behaviors as sharing passwords, creating and using weak passwords that easily can be guessed, and opening e-mail attachments without checking for viruses. In addition to these risky behaviors, users pose a serious threat to computer security because hackers have learned to manipulate them into divulging confidential information (Adams & Sasse, 1999), a technique referred to as “social engineering.”

To counter the risks that users pose, security professionals propose security training and awareness programs for users (Gips, 2001; Peltier, 2000; Tuesday, 2001). The primary goals of such programs are to make users aware of the various computer security risks and how they could affect the organization, and to get users to understand the importance of engaging in safe computing behavior

Copyright © 2005, Idea Group Inc. Copying or distributing in print or electronic forms without written permission of Idea Group Inc. is prohibited.

21 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage: www.igi-global.com/chapter/computer-security-risky-computing-practices/4482

Related Content

The Effect of Social Software on Academic Libraries
Maria Cassellaand Licia Calvi (2013). *Social Software and the Evolution of User Expertise: Future Trends in Knowledge Creation and Dissemination (pp. 163-178).*
www.irma-international.org/chapter/effect-social-software-academic-libraries/69759

Analyzing the Omni-Channel Shopper Journey Configuration of Generations Y and Z
Wei-Lun Changand Li-Ming Chen (2021). *Journal of Organizational and End User Computing (pp. 1-18).*
www.irma-international.org/article/analyzing-the-omni-channel-shopper-journey-configuration-of-generations-y-and-z/293273

Combining Tailoring and Evolutionary Software Development for Rapidly Changing Business Systems
Jeanette Erikssonand Yvonne Dittrich (2008). *End-User Computing: Concepts, Methodologies, Tools, and Applications (pp. 623-636).*
www.irma-international.org/chapter/combining-tailoring-evolutionary-software-development/18212

A Petri-Net Based Context Representation in Smart Car Environment
Jie Sun, Yongping Zhangand Jianbo Fan (2013). *Mobile and Handheld Computing Solutions for Organizations and End-Users (pp. 189-201).*
www.irma-international.org/chapter/petri-net-based-context-representation/73213

Tailoring Tools for System Development
Anders I. Mørch (1998). *Journal of End User Computing (pp. 22-29).*
www.irma-international.org/article/tailoring-tools-system-development/55751