IRM PRESS
701 E. Chocolate Avenue, Suite 200, Hershey PA 17033-1240, USA
Tel: 717/533-8845; Fax 717/533-8661; URL-http://www.irm-press.com
ITB15309

This chapter appears in the book, ***Computer Security, Privacy, and Politics: Current Issues, Challenges, and Solutions*** by **R. Subramanian** © 2008, IGI Global

Chapter X

Information Systems Security:
A Survey of Canadian Executives

Frederick Ip, Queen's University, Canada

Yolande E. Chan, Queen's University, Canada

Abstract

This study assists organizations and researchers in examining investments in IS security. A questionnaire was developed and administered to managers in Canadian financial firms and educational organizations. The survey examined security threats and the countermeasures adopted by organizations to prevent and respond to security breaches. Data gathered were used to investigate the relationships between investment in security, perceived security, and organizational performance.

Introduction

Motivation for studying information security practices of organizations has come in part from the vast amount of concern, evidenced by media attention, on the topic of information security post-911. In the US Federal Bureau of Investigation and

Computer Security Institute's joint 2004 CSI/FBI Computer Crime and Security Survey, an estimated $141 million in losses from cyberspace breaches was reported by respondents (Gordon, Lawrence, Loeb, Lucyshyn, & Richardson, 2004). In addition, there have been highly publicized security breaches at data miners such as Lexus-Nexus and ChoicePoint (Saporito, 2005).

A December 29, 2005 *Security Focus* article states, "computer users and network administrators likely feel less safe after 2005. High-profile leaks of financial data left more than 50 million accounts containing credit card information and, in some cases, confidential details at risk" (Lemos). Hulme (2005) reports that "data breaches have been announced by some of the country's well-known banks, entertainment companies, telecommunications providers and universities. And this proves that such breaches can occur at even the most security conscious and diligent companies" (p. 34).

Estimates of the numbers of customers affected by breaches continue to be staggering. Culnan states in *The Cutter Benchmark Review* (2006), the "new [United States] laws requiring firms to notify customers in the event of a security breach resulted in reports of over 130 breaches affecting more than 55 million Americans" (Culnan, p. 6).

This study focuses on the security processes and resources used by organizations, the nature of security breaches faced, and employee perceptions of information security. First, related literature is presented. This is followed by a discussion of the research model and of research instruments developed to measure the constructs in the model. Next, a survey is described. We close by presenting key findings and recommendations.

Literature Review

This section provides an overview of the importance of security to the stewardship of information and knowledge in organizations. Using the Resource-Based View of the firm (RBV), the information resource and information-based competition are described.

Information and Knowledge

A distinction is often drawn in the literature between data, information and knowledge (Alavi & Leidner, 2001). Knowledge exists in people's minds. However, knowledge