



Chapter VIII

Perceptions of End Users on the Requirements in Personal Firewall Software: An Exploratory Study

Sunil Hazari, University of West Georgia, USA

Abstract

Information security is usually considered a technical discipline with much attention being focused on topics such as encryption, hacking, break-ins, and credit card theft. Security products such as anti-virus programs and personal firewall software are now available for end-users to install on their computers to protect against threats endemic to networked computers. The behavioral aspects related to maintaining enterprise security have received little attention from researchers and practitioners. Using Q-sort analysis, this study used students as end users in a graduate business

management security course to investigate issues affecting selection of personal firewall software in organizations. Based on the Q-sort analysis of end users in relation to seven variables identified from review of the information security literature, three distinct group characteristics emerged. Similarities and differences between groups are investigated, and implications of these results to IT managers, vendors of security software, and researchers in information security area are discussed.

Introduction

Information must be readily available in organizations for making decisions to support the organizational mission. Murphy, Boren, and Schlarman (2000) state that due to increased connectivity and the urgency to exchange information and data among partners, suppliers, and customers on a real time basis, the need to protect and secure computer resources is greater than ever. As a result, this has created the possibility of exposing sensitive corporate information to competitors as well as hackers who can now access organizational computer resources from remote sites. The potential loss of such information to an organization goes beyond financial losses and includes the possibility of corrupted data, denial of services to suppliers, business partners and customers, loss of customer confidence, and lost sales. Security in business processes (i.e., maintaining proper authentication, authorization, non-repudiation, and privacy) is critical to successful e-business operations. Enabling business functions over the Internet has been recognized as a major component for the success of businesses, and by mitigating risks in a cost-effective manner, security is now being viewed as a component of business operations (Deise, Nowikow, King, & Wright, 2000). Decisions about information systems made by managers are vital to the success, and even survival of a firm (Enns, Huff, & Golden, 2003).

Despite increased security threats, organizations have traditionally allocated very little of the total IT budget to information security. Forrester Research estimates that in Fortune 500 companies, the average amount of money as a percent of revenue that is spent on IT security is .0025 percent or slightly less than what they spend on coffee (Clarke, 2002). Organizations must evaluate and prioritize the optimum mix of products and services to be deployed for protecting confidentiality (maintaining privacy of information), integrity (maintaining information is not altered in transit), and availability (maintaining access to information and resources) of corporate assets. The decision to deploy certain technology is based on variables such as the organizational business model, level of risk, vulnerability, cost, and return on investment (Highland, 1993).

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/perceptions-end-users-requirements-personal/7036

Related Content

The Role of User Ownership and Positive User Attitudes in the Successful Adoption of Information Systems within NHS Community Trusts

Crispin R. Coombs, Neil F. Doherty and John Loan-Clarke (2002). *Advanced Topics in End User Computing, Volume 1* (pp. 188-209).

www.irma-international.org/chapter/role-user-ownership-positive-user/4432

Security Threat Modelling With Bayesian Networks and Sensitivity Analysis for IAAS Virtualization Stack

Asvija B., Eswari R. and Bijoy M. B. (2021). *Journal of Organizational and End User Computing* (pp. 44-69).

www.irma-international.org/article/security-threat-modelling-with-bayesian-networks-and-sensitivity-analysis-for-iaas-virtualization-stack/280489

Classifying Web Users: A Cultural Value-Based Approach

Wei-Na Lee (2009). *Evolutionary Concepts in End User Productivity and Performance: Applications for Organizational Progress* (pp. 250-267).

www.irma-international.org/chapter/classifying-web-users/18656

Using Metaphors for Making Sense of End-User Attitudes and Behavior during Information Systems Development

Zahid Hussain and Khalid Hafeez (2009). *Journal of Organizational and End User Computing* (pp. 1-27).

www.irma-international.org/article/using-metaphors-making-sense-end/3855

The Administrative Use of Computers in Professional Sport Organizations

Terry R. Haggerty (1991). *Journal of Microcomputer Systems Management* (pp. 2-12).

www.irma-international.org/article/administrative-use-computers-professional-sport/55671