Chapter 1.11
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 0.0025 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).

There are several ways in which information can be protected. One method to safeguard information is by using controls. The concept of controls can be applied to financial auditing as well as technical computer security. General controls include personnel, physical and organizational controls as well as technical security services and mechanisms (Summers, 1997). Computer security controls can be hardware or software-based and may include biometric devices, anti-virus software, smart cards, firewalls, and intrusion detection systems that can be used to build the enterprise security infrastructure. Additionally, these controls may be preventive, detective, or corrective. This paper will focus on one such computer security control—personal firewalls. Firewalls intercept traffic and make routing and redirection decisions based on policies. Some firewalls can also inspect packets and make transformation and security decisions; therefore, they are critical components in maintaining security in organizations. There are different types of firewalls, such as hardware, software, enterprise, and personal firewalls. Personal firewalls are client-based solutions that are installed on desktop/laptop computers and may be administered individually from a central location. Successful selection and adoption of firewalls (enterprise as well as personal) is based on various factors, some of which are technical while others may be behavioral. This exploratory study looks at the new genre of personal firewalls and, based on review of the literature, attempts to identify factors that could result in successful selection of personal firewalls in organizations and further provide empirical evidence to support deployment of firewall software.

The purpose of this paper is to investigate self-referent perceptions of end-users, and use Q-Sort analysis to investigate factors affecting deployment of security firewall software in organizations. The paper is organized as follows: review of research on information security is presented to the reader along with extraction of variables from the literature that may determine firewall deployment in organizations; The Q-Sort Factor Analysis method used for the study is explained and the research design is provided; Along with data analysis, results of the study are then explained, which is followed by discussion and applications to practice. Due to the nature of research design used in this study, limitations are also explained. The study also sheds light