Chapter 17
Computer Security Practices and Perceptions of the Next Generation of Corporate Computer Users

S. E. Kruck
James Madison University, USA

Faye P. Teer
James Madison University, USA

ABSTRACT

The purpose of this chapter is to present the results of an empirical study of the computer security practices and perceptions of the next generation of corporate computer users, undergraduate university students. The authors surveyed undergraduate university students who represented 42 different majors. The findings relate to the students' usage of antivirus programs, firewalls, password security, and security patches. Student perceptions of computer security and its importance are also reported. Research in this area is important for two reasons. First, potential employers may find the results useful in assessing their vulnerability to unsafe practices from entry level employees. Secondly, research in this area can give those responsible for providing computer security education a better understanding of students' computer security training needs.

INTRODUCTION

For as long as computers have achieved widespread use in industry, computer security has been critical to the effective functioning of organizations. However, in the mid1990s when the widespread sharing of information over the Internet and the growth of e-commerce became commonplace in organizations, computer security became more important than ever and moved to center stage (Duffy & Walstrom, 2003; Gordon, Loeb, Lucyshyn, & Richardson, 2004). In the first quarter

of 2006 alone, e-commerce revenues in the United States totaled $25.2 billion dollars, up 7% from the fourth quarter 2005. Worldwide e-commerce revenues were estimated at $976.1 billion dollars (U.S. Census Bureau, 2006). With extensive commerce taking place online, individuals and companies now face a constant challenge of securing their computers and business transactions from sophisticated cyber criminals.

Society's concerns about the growing threats to computer security are well-founded. For example, when the first virus infected ARPANET in 1987, no one had any idea that within a few years computer viruses would become epidemic. We are now at the point that highly successful new viruses are introduced every week (Schultz, 2004). In addition, the newer, polymorphic viruses are capable of changing their signature every time they replicate and infect a new and different file type in order to keep from being detected.

Clearly, computer security is vital to today's organizations and economy. Industry statistics illustrate the seriousness of threats to computer security. With 137,529 reported security incidents in 2003 alone (CERT/CC, 2006), effective information security has become a necessity rather than an afterthought. Given the substantial number of security incidents in organizations and the growing reliance of corporations on the Internet, there is a need for further research by both practitioners and academicians in the area of computer security. Leach (2003) suggests that the internal threat to computer security is more pressing than external threats and is the "result of poor user security behavior." Goodwin (2005) indicates that IT training is targeted to the CIO, whereas it should be targeted to the "bottom of the pyramid." In light of the known threat caused by the improper computer security practices and perceptions of the users, many researchers bemoan that computer security awareness is just beginning to be addressed in the literature (Collins, Rawlinson, Manwani, & Allen, 2005; Dhillon & Blackhouse, 2001; Goodwin, 2005; Kirkpatrick, 2006; Leach, 2003; Siponen, 2000).

Some authors have issued a call for more computer security awareness, education, and training (Dhillon & Blackhouse, 2001; Kirkpatrick, 2006). Before university professors can effectively respond to this call to action, we must have a clear understanding of students' current computer security practices and perceptions. Therefore, the purpose of this study is to perform empirical research that documents computer security practices and perceptions among undergraduate university students.

Information gleaned through this study should be of interest to both practitioners and academicians. Because the student population of computer users is the next generation of corporate computer users, documenting students' unsafe computing practices and perceptions is important to potential employers as an aid in assessing their vulnerability to unsafe practices from entry level employees.

If universities are to provide organizations with employees who are responsible computer users, the designers of university curriculum must have a better understanding of students' computer security training needs. Computer security training for university students can be more effective if faculty have a profile of students' current computer security practices and perceptions.

RELATED LITERATURE

The related literature that is part of this study examines two aspects of computer security. First, the literature indicating the impact computer crime is having on the bottom line in organizations is summarized. This is followed by an examination of what is found in the literature pertaining to unsafe computing practices by computer users.

Impact of Computer Crime on Organizations

Unfortunately, in spite of attempts to stop or slow the problem, computer crime continues to have a substantial negative impact on the bottom line in