Chapter 5.11
Computer Security and Risky Computing Practices:
A Rational Choice Perspective

Kregg Aytes
Idaho State University, USA

Terry Connolly
University of Arizona, USA

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 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 dollars 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 the survey has been conducted. Financial losses have climbed each year, and most categories of attacks have either 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 such as sharing passwords, creating and using "weak" passwords that can be easily 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). This is 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, how they could affect the organization, and to get users to understand the importance of engaging in safe computing behavior (Peltier, 2000). Fear of negative consequences is a common theme of these programs. Many of the security standards that have developed over the last 20 or 30 years originated in the federal government—often in the Department of Defense, where compliance can be mandated with more success than in private industry. Some authors suggest that security can be increased by also implementing positive motivators for users (Parker, 1999; Tuesday, 2001).

Unfortunately, these training and remediation efforts are designed largely in the absence of reliable knowledge about the behaviors they are seeking to change. We know very little about why computer users choose to engage in unsafe computing behaviors. Are they unaware that they are doing so? Do they know about the safer behaviors they could choose, and do they have the training to implement those behaviors effectively? Do they misjudge the likelihood that their unsafe behaviors will lead to bad consequences, or believe that the consequences will not, in fact, be very serious? Are their behaviors simply a matter of knowing better but doing worse, of succumbing to the temptations of the moment instead of doing the prudent thing? Our hope is that a better understanding of the individual's decision process relating to safe or unsafe computing behaviors will provide a better basis for strategies aimed at influencing the process.

Viewing the practice of safe computing behaviors as a rational decision process is consistent with several well-researched theories related to the use of information technology. Fishbein and Ajzen's (1975) Theory of Reasoned Action (TRA) and Davis, Borgozzi and Warshaw's (1989) Technology Acceptance Model (TAM) both view the use or non-use of an information system to be based on, among other things, behavioral intentions. Those behavioral intentions are the result of a choice the users make based on their attitudes and their perceptions of the norms concerning the behavior. For example, the TAM model posits that a person's intention to use a system is determined by the person's attitude towards a system and the person's beliefs about the probability that the system will increase his or her job performance (Jackson et al., 1997). That is, a person makes a rational choice to either use or not use an information system based on several decision criteria. This intention to use an information system is then a major determinant of a person's actual behavior. Put in the context of safe computing behaviors, we believe that a person's intention to employ safe computing behaviors (e.g., scan for viruses, change passwords, etc.) is also a rational choice based on the person's perceptions about the usefulness of the safe behaviors and the consequences of not engaging in safe behavior.

This study had two main goals. First, we wanted to document the prevalence of unsafe computing practices in one population. For all the concern noted above about unsafe computing practices, we were unable to find any systematic