Chapter IV
The Weakest Link:
A Psychological Perspective on Why Users Make Poor Security Decisions

Ryan West
Dell, Inc., USA

Christopher Mayhorn
North Carolina State University, USA

Jefferson Hardee
North Carolina State University, USA

Jeremy Mendel
North Carolina State University, USA

ABSTRACT

The goal of this chapter is to raise awareness of cognitive and human factors issues that influence user behavior when interacting with systems and making decisions with security consequences. This chapter is organized around case studies of computer security incidents and known threats. For each case study, we provide an analysis of the human factors involved based on a system model approach composed of three parts: the user, the technology, and the environment. Each analysis discusses how the user interacted with the technology within the context of the environment to actively contribute to the incident. Using this approach, we introduce key concepts from human factors research and discuss them within the context of computer security. With a fundamental understanding of the causes that lead users to make poor security decisions and take risky actions, we hope designers of security systems are better equipped to mitigate those risks.

INTRODUCTION

Humans are fallible. That means exploitable. Recorded in every religious text and mythology is the evidence of human imperfection. We lose our wallets, forget our passwords, and drive over the speed limit when we are in a hurry. Yet somehow, we managed to develop manifestations of pure logic in the form of computing systems. At the helm of all this technical sophistication and complexity, unfortunately, is a user.

True Story:

"Company X" is a large nationwide hotel chain across the United States. Each hotel has two wireless networks, one accessible to hotel guests and one accessible to hotel employees. The hotel employees use this for reservations, reporting, and so forth. Once a month, a number of reports are rolled together by the IT manager, who puts them into a presentation for his upper management. The executives present this report as part of a monthly presentation to the parent company who owns the hotel chain. The parent company and the hotel chain have different policies and firewall settings, and the IT manager for the hotel chain has not, in 3 years, been able to figure out how to make them mesh without causing breakages down the line. As a result, once a month, when the executives give their presentation, the IT manager drops the firewall for the hotel chain for the duration of the presentation.

User error and poor human factors design contribute to many of the top computer security risks faced today. According to a recent CSI/FBI computer crime and security study, losses due to computer security incidents were estimated to total more than $52 million across the 313 companies surveyed (Gordon, Loeb, Lucyshyn, & Richardson, 2006). Of the most common security incidents reported in the study, losses related to viruses or malware totaled an estimated $15.7 million, losses associated with the unauthorized access of information totaled $10.6 million, and losses caused by laptop or other hardware theft totaled $6.6 million.

When it comes to data loss within organizations, it appears that users are more of a problem than hackers or malware. According to a 2007 report from the IT Policy Compliance Group, mistakes made by internal employees accounted for approximately 75% of all data losses (Gaudin, 2007). In contrast, malicious activity such as Internet-based threats, attacks, and hacks, accounted for about 20% of data losses.

On the home front, a 2004 survey from AOL and the National Cyber Security Alliance reported that 72% of home users surveyed did not have a properly configured firewall (America Online and the National Cyber Security Alliance, 2004). In addition, approximately 40% of users with home wireless networks had no encryption configured.

In all of these cases, there are human factors issues associated with the acceptance and usability of security mechanisms, user perceptions of risk and how it motivates their behavior, and decision making strategies which pit convenience against security.

The focus of this chapter is not on the technologies of computer security but on the psychology of those who use them. Human decision-making has been a topic of study in social sciences for well over a century (Goldstein & Hogarth, 1997). The research shows that individuals are often less than optimal decision-makers when it comes to reasoning about risks (Simon, 1956). Not only do internal factors such as prior experience and knowledge specific to the decision maker influence the quality of decisions but many naturalistic or environmental factors such as time pressure (Hammond, 2000) and situational context (Klein, 1998) also effect decisions. Thus, there are a variety of data sources available to describe the nature of predictable and exploitable characteristics in the human decision making process. Understanding these principles and how users come