December 2003

A Research Model for Investigating Human Behavior Related to Computer Security

Kregg Aytes
Idaho State University

Terry Conolly
University of Arizona

A Research Model for Investigating Human Behavior Related to Computer Security

Kregg Aytes
Idaho State University
aytekreg@isu.edu

Terry Connolly
University of Arizona
connolly@u.arizona.edu

Abstract

Computer security issues have typically been approached from the perspective of building technical countermeasures to reduce risk. Recently, researchers have recognized that computer users play an important role in ensuring secure systems by implementing those technical countermeasures. As a means of encouraging safe computing practice, user training and awareness have been touted. However, simply providing training and awareness does not ensure that users will always use safe practices. This paper introduces a model of user behavior that emphasizes the factors relating to the user's perception of risk and the choice based on that perception. As research in progress, we also briefly describe an ongoing study to further investigate this model. We will present results from this study at the conference.

Keywords: Computer security, information security, risk perception

Introduction

Researchers interested in the security and integrity of information systems have long concerned themselves with technological countermeasures to threats. In recent years, it has become evident that technological measures alone cannot provide adequate security (Rhodes, 2001; Schneier, 2000). This is for two reasons: First, threats constantly change through active human participation; that is, the "bad guys" are always going to be looking for ways around the technological countermeasures. Second, even if the countermeasures are adequate at a particular point in time, it is up to people to effectively implement those countermeasures. In most systems, both systems administrators and users share some responsibility for implementing effective countermeasures. Systems administrators are responsible for such things as applying security patches, properly configuring servers and firewalls, etc. Users are responsible for correctly implementing countermeasures such as protecting their passwords from disclosure, choosing good passwords, and making use of virus protection software. Unfortunately, neither group of people always follows safe practices. Some in the computer security field blame risky behavior on laziness and ignorance (Tuesday, 2001), and therefore tout as the solution better training and awareness (Rhodes, 2001).

Those espousing training and awareness as the solution suggest that user behavior is the result of two primary factors: Awareness that threats exist, and training in the proper use of countermeasures. Basic assumptions to this line of thinking is that much of the training will consist of making users aware of organizational policies and procedures related to countermeasure use, and either that users will somehow be intrinsically motivated to comply with these policies, or compliance can be mandated. While training and awareness are certainly necessary antecedents to the effective use of countermeasures, this somewhat simplistic approach to human behavior ignores the fact that in many situations, users may choose to not implement countermeasures. If training and awareness alone were the answer, we would not expect that large virus outbreaks like the recent SQL Slammer (actually, a worm) that hit Microsoft SQL Servers in January 2003. This worm took advantage of a vulnerability in SQL Server that had been widely publicized many months before. Apparently, many systems administrators did not apply the appropriate patch until after they had been hit by the fast-propagating worm. The fact that even systems administrators, who as a group would be expected to be more knowledgeable and aware of security issues than end users, still do not properly apply countermeasures suggests that training and awareness alone may not be enough.

Clearly, human behavior is an important issue for information security. However, there is very little extant research on why people so often engage in risky computing practices, nor in how their behavior could best be modified. One place to look is the rich

collection of research into human decision behavior. Unfortunately, little published research into human behavior related to computer security exists. As pointed out by Siponen (2000), the majority of work done in user training and awareness has focused on the development of standards related to knowledge and skills. These training materials, however, fall somewhat short of ensuring learning, as they do not take into account behavioral theories related to learning and motivation (McLean, 1992; Siponen, 2000). Siponen (2000) then goes on to present the use of countermeasures from a perspective that includes explicit acknowledgement of theories related to attitudes, motivation, and behavior. Although recognizing the importance of behavioral issues, this description of a variety of approaches that could be used to modify user behavior (appeals to logic, morals and ethics, emotions, etc.) falls short of presenting a testable model explaining the potential sources of risky user behavior.

Straub and Welke (1998) investigated the knowledge of security risks and countermeasures held by managers and the effect this knowledge had on their information security planning. They found that significant awareness training and a prescribed planning model tended to affect managers' subsequent security planning. While security planning is an important component of increasing security, it is not the same as changing actual user behavior.

In summary, while there has been some limited investigation into user behavior and information security, still unanswered is the question of why users engage in risky behavior. Answering this question would go a long way towards helping information security professionals better structure security policies and awareness and training efforts. To better help understand the role of human behavior as it relates to information security, we present in this paper a decision model of countermeasure use that assumes a choice between risky and safe computer-related practices.

Proposed Research Model

When viewing the use of countermeasures as a choice made by the user, we have available to us a substantial body of research investigating the perceptions of risk and decision making under uncertainty. This research is particularly relevant, as choices about safe computing practices are quite similar to choices studied in this referent literature, such as general technological risk (Fischhoff, et al., 1978) and seatbelt use (Slovic, et. al., 1978). We present here a model based on concepts from this referent literature. It assumes that risky computing behavior is a result of individual choices at least weakly guided by considerations of the probability and desirability of choice consequences. We are not, of course, postulating a highly rational, utility-maximizing user – a huge empirical literature (e.g. Goldstein & Hogarth, 1997; Connolly, Arkes & Hammond, 2002) attests to the implausibility of such an assumption. We do, however, propose that conscious thought about consequences plays some role in guiding risky behavior. (If the evidence fails to support even this weak assumption, alternative theoretical frameworks such as habit formation, peer pressure or simple impulsivity would have to be considered). The basic outline of our model is presented in Figure 1.

The decision model presented in Figure 1 consists of six main components: Information sources, the user's knowledge, the user's perceptions (e.g., interpretation of the applicability of the knowledge), a choice process, the behavior associated with the choice (to use or not use countermeasures), and a resulting outcome that then feeds back as a source of new information.

Information about computer security threats, vulnerabilities, and countermeasures comes from a variety of sources. Some of these sources are relatively formal, such as training programs and organizational policies and procedures. Other sources include the news media, friends and coworkers, and personal experience. These information sources provide the "facts" that form the user's knowledge. Some of these important facts include:

- Knowledge of threats and vulnerabilities: awareness and understanding of the various threats to security, such as computer viruses, hackers, etc., along with an understanding of how vulnerable their own systems may be.
- Awareness of countermeasures: awareness that there are means of reducing risk, such as using virus protection software, not sharing passwords, etc.
- Potential consequences to self: understanding the potential negative consequences if security is violated, including loss of data, compromised privacy, etc.
- Potential consequences to others: knowledge that while there may be little or no personal consequences, friends, coworkers, and the vast number of Internet users may be negatively impacted when one's system is compromised.
- Ease of recovery: although data may be lost and files corrupted, a well planned, implemented, and tested backup and recovery procedure may mean that negative consequences are only temporary.

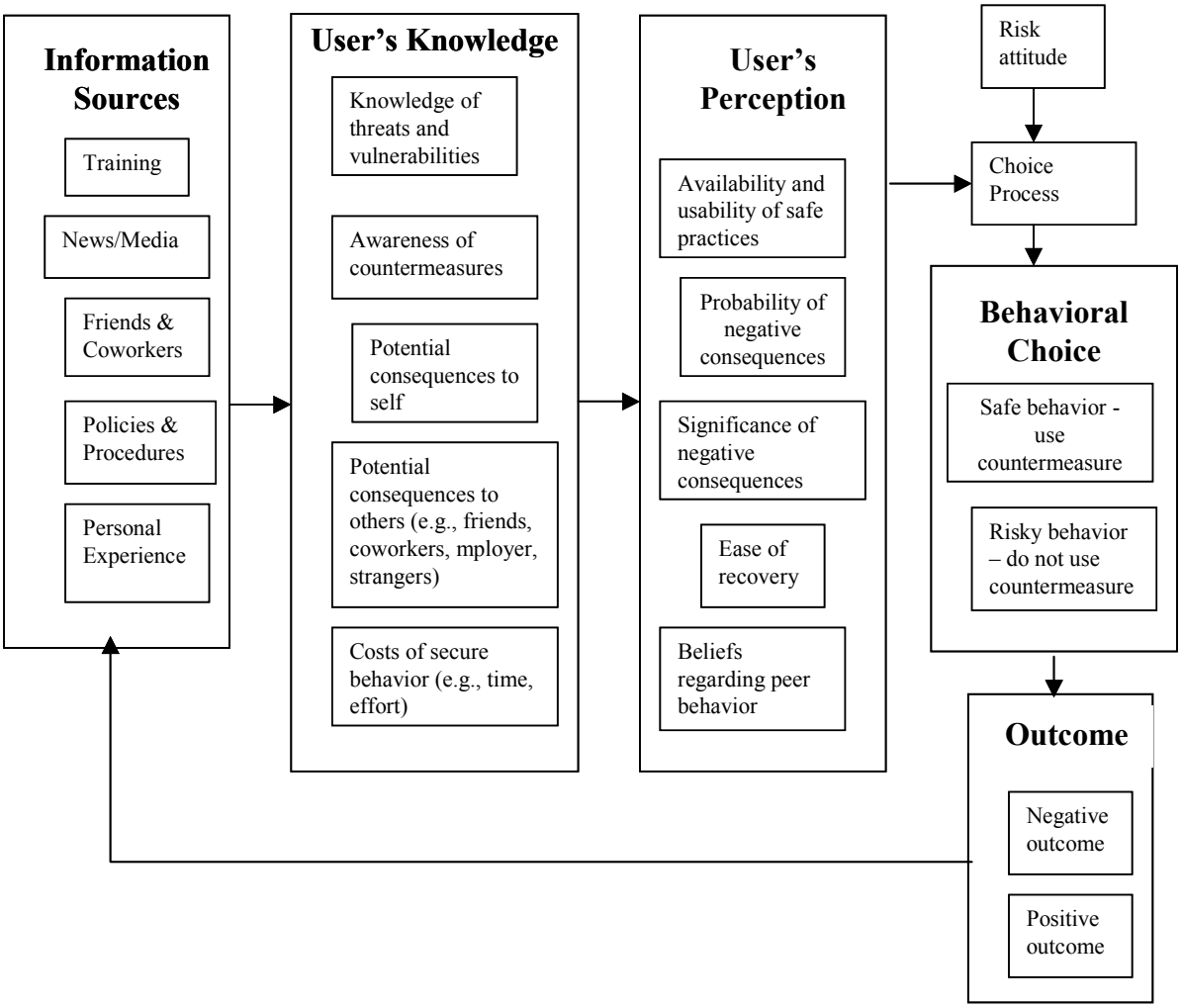

Figure 1. Research Model

In this model, the knowledge of the user is concerned with the "facts" regarding the *potential* risk, broadly stated. This potential risk as described by the facts, however, must be perceived by the user to be relevant to his or her situation. This perception is affected by a number of factors. In referring to the general issue of risk perception, Slovic (1987) states, "In particular, laboratory research on basic [risk] perception and cognitions has shown that difficulties in understanding probabilistic processes, biased media coverage, misleading personal experiences, and the anxieties generated by life's gambles cause uncertainty to be denied, risks to be misjudged,…and judgments of fact to be held with unwarranted confidence." Therefore, our model considers the user's perceptions to be an important factor in the choice process. Specifically, we propose that the following perceptions play an important role:

- Availability and usability of safe practices: Users must not be simply aware and capable of implementing countermeasures, but must also perceive that the countermeasures are available for use without undue effort.
- Probability of negative consequences: Users must perceive that there is a non-zero probability that potential threats will be realized. An extensive literature (e.g. Slovic, Fischhoff & Lichtenstein, 1979; Zeckhauser & Viscusi, 1990) shows that humans estimate and react to small probabilities in non-normative ways, either exaggerating or ignoring the risks involved. A related literature (e.g. Fischhoff, Bostrum & Quadrel, 1993) suggests that we are insensitive to the compounding of small probabilities with repeated exposure. It seems likely that the risks involved in many unsafe computing practices will be both small in individual instances and compounded by repetition, so both types of distortions may be found.
- Significance of negative consequences: Users must believe that if a threat is realized, there will be significant negative consequences to themselves or others. Research on the public's perceptions of risk across a wide variety of hazards has

shown that the higher a hazard's "dread factor" (i.e., the more significant the perceived consequences), the higher its perceived risk (Slovic, 1987).

- Costs of secure behavior: There are costs, both individual and organizational, to implementing countermeasures, and these costs are weighed against the benefits of reducing computer security. For example, it is difficult to have highly secure systems while at the same time making the information in the systems easily available to all those that might need it. From an individual perspective, there is a cost in time that it takes users to scan email for viruses. In deciding what risks are acceptable, decision makers often perform a cost/benefit analysis (Fischhoff, et. al., 1979). While it is doubtful that individual users perform a formal analysis of this type, it is likely that they take into account the personal costs to implementing countermeasures.
- Beliefs about peers' behavior: Users are likely to model their behavior based on what they believe others are doing. A potential deterrent to risky behavior is the potential that others may "blame" him or her for problems caused, particularly if one's behavior is significantly more risky than that of others.

The sum of these perceptions results, governed perhaps by a person's general attitude towards risk (e.g., Weber and Milliman, 1997), results in a choice by the user to either apply a countermeasure or not, which then results in a positive or negative outcome. The choice and its resulting outcome form the basis for a feedback loop providing new information (or reinforcement of existing information) that will then be used in the next choice process. Once again, using seat belt usage as an analogy for using countermeasures, "Each safe trip rewards (reinforces) the non-use of seat belts; the expense of buckling up has been saved without incurring any cost. On the other hand, travelers who do use belts are punished (negatively reinforced) by the effort, inconvenience, and discomfort they have incurred without any concrete reward….Thus, safe driving experiences can be expected to lead to non-use of seatbelts." (Slovic, 1978, p282). It is also probably the case, of course, that negative outcomes may increase the use of countermeasures.

Implications of the Model

This model raises numerous issues regarding the relationships of its various components and its overall efficacy in predicting user behavior. To begin investigating this model, we have designed a questionnaire that attempts to answer many of the questions that could be generated. In this initial study, we are concerned with only one category of threat and its related countermeasure: computer viruses spread through email and the use of virus scanning software. Questions we are investigating include:

- What is the relationship between general knowledge about computer viruses and the perceptions of the probability of and significance of negative consequences?
- What is the relationship between users' perceptions of the probability of and significance of negative consequences and users' choices regarding the use of countermeasures?
- How does personal experience (e.g., being infected with a virus) affect perceptions of risk?
- How does personal experience affect the choice of whether to use countermeasures?

Data collection with this questionnaire is currently underway. Results of this study will be available for presentation at the conference. We hope to begin building a foundation for future research and the refinement of a model to explain user behavior as it relates to computer security risks and the use of countermeasures. The findings resulting from the further examination of such a model should result in recommendations for increasing the use of safe computing practices among the user population.

References

Connolly, Terry, Arkes, Hal, and Hammond, Kenneth. "Judgment and decision making: An interdisciplinary reader". New York: Cambridge University Press, 2002.

Fischhoff, Baruch, Bostrum, Ann and Quadrel, Marilyn. "Risk perception and communication." Annual Review of Public Health, Vol. 14, 1993, pp.183-203.

Fischhoff, B., Slovic, P., Lichtenstein, S., Read, S, and Combs, B. "How safe is safe enough? A psychometric study of attitudes towards technological risks and benefits," Policy Sciences, 9, 1978, 127-152.

Fischhoff, B., Slovic, P., Lichtenstein, C. "Weighing the risks: Which risks are acceptable?" Environment, 2(4), 1979, pp. 17-20, 32-38.

Goldstein, William, and Hogarth, Robin. "Research on judgment and decision making". New York: Cambridge University Press, 1997.

McLean, K. (1992), "Information security awareness - selling the cause", Proceedings of the IFIP TC11/Sec'92, 27-29 May, Singapore.

Rhodes, Keith. "Operations security awareness: The mind has no firewall." Computer Security Journal, Vol 18 (3), 2001.

Schneier, B. Secrets and Lies: Digital Security in a Networked World. New York: Wiley Computer Publishing, 2000.

Siponen, M. A conceptual foundation for organizational information security awareness. Information Management & Computer Security, 8(1), 2000 pp. 31-41.

Slovic, P., Fischhoff, B., and Lichtenstien, S. (1978). "Accident probabilities and seat belt usage: A psychological perspective," Accident Analysis and Prevention, (10), pp. 281-285.

Slovic, P. (1987) "Perception of Risk," Science, (236), pp. 280-285.

Tuesday, Vince. "Human factor derails best-laid security plans," Computerworld, April 30, 2001, pp. 52-55.

Weber, E., and Milliman, R. "Perceived risk attitudes: Relating risk perception to risky choice," Management Science, 1997, 43(2), pp.123-144.

Zeckhauser, Richard and Viscusi, Kip. "Risk within reason," Science, (248), 1990, pp.559-564.