Chapter 2.1
A Simulation Model of IS Security

Norman Pendegraft
University of Idaho, USA

Mark Rounds
University of Idaho, USA

ABSTRACT

The value of IS security evaluated by simulating interactions between an information system, its users and a population of attackers. Initial results suggest that the marginal value of additional security may be positive or negative as can the time rate of change of system value. This implies that IT security policy makers should be aware of the relative sensitivity of attackers and users to security before setting IT security policy.

INTRODUCTION

This paper offers a simulation model of the interaction between an information system (IS) and populations of users and attackers. The model incorporates plausible interactions between the rate of attacks, the value of the IS, user sensitivity to security, user specific response curve to security and the level of security. These interactions are incorporated into a reservoir / flow model using the IThink simulation software.

DOI: 10.4018/978-1-61350-323-2.ch2.1

The purpose of this research is to develop a model sufficiently robust to provide management insight into the merits of alternative responses. For example: does it make more sense to train users to be more productive with existing security or to make a system more robust while under attack. There are many variables that cannot be controlled with certainty, so answering this question precisely would be difficult. But even the capacity to perform relative assessments has potential value to an IS manager. Given the current state of the art in quantifying the value of security measures and the difficulty of accurately assessing attack costs,

it is unlikely that exact quantitative comparisons between possibilities will be possible any time soon. However, a comparative model will still provide value in decision making and will also be valuable as an educational tool. Ultimately, we hope to extend the work to better determine under what circumstance each of these strategies might prove superior. The chapter should be viewed as exploratory.

This chapter is organized as follows. Section two examines previous work and the security problem; in section three, the methodology and the model are described. Section four includes the results and our discussion.

BACKGROUND

Previous Work

Much of the research on information systems security focuses on the costs and risks of various security schemes. A common practice is to analyze the level of risk for any given security outcome and perform cost/benefit analysis on the results as exemplified by Gordon and Loeb (2002).

For the purposes of this research, we model attackers as a homogeneous group of rational criminals. While there are many sorts of attackers this simplification makes the results much more understandable. We base the rational activities of our attacker upon the economics of criminal activity, first studied by Becker (1968). He assumed that criminals responded rationally to a set of incentives and studied the impact of issues like likelihood of punishment and severity of punishment on their behavior. Others extended this work, for example, Block and Heineke (1975) offered a labor theoretic model of criminal activity.

Rogers (1962, 1976) offers a model of user. In his model early adopters of technology behavior differently from late adopters. There are several theoretical models of IS (Information System) use that have seen empirical justification. TAM, the Technology Acceptance Model (Davis 1989) offers a means of analyzing the impact of ease of use upon Usage. It has been successful in establishing such a link, but does not explicitly consider other IS quality issues such as data quality and completeness.

The IS Success Model (ISM) explicated by DeLone and McLean (1992) includes constructs of information and system quality and posits that system and information quality lead to increased user satisfaction and increased use which in turn leads to net benefits. DeLone and McLean (2003) recently revised that model to expand measure of quality to include service quality and to explicitly include a feedback loop from net benefits to intention to use.

Wixom and Todd (2005) recently integrated TAM and ISM, and their results suggest that there is a link between system and data quality on the one hand and system usage on the other. On the other hand, Zhu and Kraemer (2005) argue that firm value is increased by IS usage in E-business applications.

TAM also supports a link from security to usage. In general, security will reduce ease of use which TAM predicts will reduce usage. Recent reports in the popular press (Richmond 2004, Grow 2005) suggests that attackers are motivated by economic interests and therefore are attracted by high value targets. These reports confirm the notion that increases in system value lead to increases in attacks.

We have also assumed that the security and value functions are continuous in nature. While security decisions are at least partially discrete, Rajuput, Chen, and Hsu (2005) demonstrate that security is being broken up into ever smaller increments as the users are given more and more options and the systems are more refined and complex. The result is that security choices are reasonably continuous.