Chapter XV
An Adaptive Threat-Vulnerability Model and the Economics of Protection

C. Warren Axelrod
US Trust, USA

ABSTRACT

Traditionally, the views of security professionals regarding responses to threats and the management of vulnerabilities have been biased towards technology and operational risks. The purpose of this chapter is to extend the legacy threat-vulnerability model to incorporate human and social factors. This is achieved by presenting the dynamics of threats and vulnerabilities in the human and social context. We examine costs and benefits as they relate to threats, exploits, vulnerabilities, defense measures, incidents, and recovery and restoration. We also compare the technical and human/social aspects of each of these areas. We then look at future work and how trends are pushing against prior formulations and forcing new thinking on the technical, operational risk, and human/social aspects. The reader will gain a broader view of threats, vulnerabilities and responses to them through incorporating human and social elements into their security models.

INTRODUCTION

Have you noticed that when you drive a particular make of car, it appears that virtually every second or third vehicle on the road is from the same manufacturer as yours, and often the same model, too? While it could be true, depending on the brand that you choose, it is mostly perception. It is just that you are more aware of and notice this particular brand. So it is with the subject of this book.

When the editors first suggested the topic in 2006, articles examining the impact of human and social aspects of information security, though they did exist, were few and far between. Suddenly, in the early months of 2007, the gurus of information security—such as Bruce Schneier—had "found religion" and seemed to be talking and writing about little else. In a report on the 2007 RSA Conference, Ellen Messmer reported that Bruce Schneier "casts light on psychology of security," where Schneier emphasizes the importance of human factors in the security equation (Messmer, 2007). Schneier has also drafted a paper on the topic (Schneier, 2007a).

With such a boost as this, I am sure that you will see a flood of quotations, articles, and books on the topic over the next several years. As a result of this, the face of information security practice will change forever.

Historically, the average security professional has been highly technical and operational, but many have recently become more risk-aware, and will be called upon to be a psychologist and behavioral scientist as well as a security expert. To quote John Kirkwood, chief security officer at Royal Ahold, the Dutch parent of the Stop & Shop supermarket chain, in regard to security assessments: "Do it from the way the hacker would think" (Scalet, 2007). Several Stop & Shop stores in New England were victims of a scam involving the substitution of card data skimming devices for regular point-of-sale readers. Kirkwood touts the importance of convergence between information security and physical security in order to provide more complete protection. As we delve into the subject, we will see how these differences in backgrounds, knowledge, and experience between "logical" and physical security personnel, many with law enforcement origins, can enrich the threat-vulnerability model.

It is gratifying to see that the human and social aspects of information security are finally getting the attention that they deserve. As with many innovative approaches, it might attract excessive interest, certainly more than warranted, and divert attention and resources from other critical technology and risk areas before it settles into its rightful place in security professionals' toolkits. The Gartner Group has developed a life-cycle model, primarily for IT-related products, called the "hype cycle."[1] In a graphical depiction, they show the visibility of a product varies with maturity of the product over time. The first phase is the called the "technology trigger." I believe that, if we adopt Gartner's model for the social and human aspects of information security, we are currently in this first phase. Taking the Gartner model further, we can expect to go through subsequent phases named "peak of inflated expectations," "trough of disillusionment," "slope of enlightenment," and "plateau of productivity," respectively. This process is likely to take 2 to 5 years before we might reach the productivity plateau. But this can only be done with dispatch if we begin the journey. Perhaps by embarking early on this road, we can ultimately accelerate the process and achieve the desired goal of the full consideration of social and human factors more expeditiously.

In favor of giving the social and human side more consideration, one might argue that you can not know where most effectively to put your security funds without including the economic ramifications of these factors and how they affect security. This is somewhat similar to the need to include "social costs" into an economic justification of a power plant, say, that pollutes the air and raises the temperature of the adjacent river water, which it uses for cooling. The impact on society is of polluted air, which causes respiratory and other diseases, and heated and polluted water, which results in dead fish and other creatures. If these health and environmental factors are not considered, then there is little incentive for the builders of the power plant to install equipment to scrub the air before it is emitted, use less polluting fuels, and devise less damaging cooling