Chapter 2

BASIC SECURITY ISSUES

INTRODUCTION

Internet security is a contradiction in terms, like the classic references to Alaskan Crab and the National Security Agency. True security can only be achieved when the information is isolated, locked in a safe, surrounded by guards, dogs and fences, and rendered inaccessible. Some would argue that even then, there is not absolute security. It simply is not possible, therefore, to render a network system completely secure, and anyone who wishes to understand and apply the principles of security to the Internet or any other network, must first understand and accept this basic tenet in order to be successful. In spite of this, managers of network systems must strive to attain this unreachable goal simultaneously [1].

The reason behind this often frustrating dilemma lies in the motivations for the development of networks. Networks were created as a remedy to the problem of data isolation in the early days of computing. "Islands of Automation" were a hindrance to conducting business successfully because critical information required by one "island" could not be accessed by others. Networks became the communication bridges by which these islands could be integrated. Since security and privacy [2] are the antithesis of sharing and distribution, Internet security must become a balance between providing appropriate access to those who need the information and safeguarding that information by denying access to those not authorized. This is all done while assuming some level of risk, which is appropriate to the sensitivity of the information that is to be guarded [1].

This is not intended to imply that Internet security is not necessary, nor that management should not strive for it. On the contrary, the explosion of information across the networks in this country and in the world has raised the specter of corporate espionage to new heights. Corporations today know that in the information age, information is power; and, those organizations which control their information appropriately, can gain a competitive advantage: those who do not are vulnerable to losing valuable trade secrets to competitive spies [1].

Equally dangerous is the possibility of loss of information or compromising that information due to acts of sabotage, such as from disgruntled employees. As employees become more mobile, and as they demand more information while they are on the road, the vulnerabilities of compromised information become more severe by an enterprise's own employees [1].

Within this perplexing situation, managers must navigate between the risks of losing information so necessary to the enterprise's operation and the costs and constraints associated with an overly aggressive security solution. This chapter is intended to help management successfully navigate this course by providing an overview of security principles and the technologies which are appropriate for securing the Internet and networks today [1].

INTERNET AND NETWORK SECURITY ISSUES: BASIC SECURITY CONCEPTS

A good place to begin is by defining the basic concepts involved in securing any object. The key words in the security lexicon are vulnerability, threat, attack, and countermeasure. An examination of each follows [1].

Vulnerability is the susceptibility of a situation to being compromised. It is a potential, a possibility, a weakness, an opening. A vulnerability in and of itself may or may not pose a serious problem, depending on what tools are available to exploit that weakness. The classic definition of vulnerability comes from Greek Mythology, with the story of Achilles, whose heel represented his greatest vulnerability [1].

A threat is an action or tool which can exploit and expose a vulnerability and therefore compromise the integrity of a given system. Not all threats are equal in terms of their ability to expose and exploit the vulnerability. For example, the Microsoft Concept virus exploits a vulnerability in Word Macros allowing access to the users' file system, but the virus itself is relatively benign. Other similar viruses could do a lot more damage [1].

An attack defines the details of how a particular threat could be used to exploit a vulnerability. It is entirely possible that situations could exist where vulnerabilities are known and threats are developed, but no reasonable attack can be conceived to use the specific threat upon a vulnerability of the system. An example of an attack is a Trojan Horse attack, where a destructive tool such as a virus is packaged within a seemingly desirable object, like a piece of free software [1].

Countermeasures are those actions taken to protect systems from attacks which threaten specific vulnerabilities. Achilles covered his heel with a protective metal plate as a countermeasure to potential attacks to his one vulnerability. In the Internet security world, countermeasures consist of tools such as virus detection and cleansing, packet filtering, password authentication, and encryption [1].

Any security scheme must identify vulnerabilities and threats, anticipate potential attacks, assess whether they are likely to succeed or not, assess what the potential damage might be from successful attacks, and then implement countermeasures against those defined attacks which are deemed to be significant enough to counter. Therefore, you can see that security is all about identifying and managing risk, and that security is a very relative