Chapter 4

A SECURITY POLICY: THE FOUNDATION OF YOUR PROTECTION

INTRODUCTION

While Internet connectivity offers enormous benefits in terms of increased access to information, Internet connectivity is dangerous for sites with low levels of security. The Internet suffers from glaring security problems that, if ignored, could have disastrous results for unprepared sites. Inherent problems with TCP/IP services, the complexity of host configuration, vulnerabilities introduced in the software development process, and a variety of other factors have all contributed to making unprepared sites open to intruder activity and related problems [1]. Enterprises are, rightly concerned about the security implications of using the Internet, and ask the following questions:

- Will hackers disturb internal systems?
- Will valuable enterprise data be compromised (changed or read) in transit?
- Will the enterprise be embarrassed [1]?

All of preceding are valid concerns. Many technical solutions are emerging to address basic Internet security concerns. However, they come at a price. Many of the solutions limit functionality to increase security. Others require significant tradeoffs in terms of ease-of-use. Others cost traditional resource-staff time to implement and operate and money to buy and maintain equipment and software [1].

The purpose of an Internet Security Policy is to decide how an enterprise is going to protect itself. The policy will generally require two parts: a general policy and specific rules (which are the equivalent of system specific policy described in the preceding). The general policy sets the overall approach to Internet Security. The rules define what is and what is not allowed. The rules may be supplemented with procedures and other guidance [1].

For Internet policy to be effective, the policy maker must understand the tradeoffs being made. The policy must also be in synchronization with other related policy issues. This chapter attempts to provide technical professionals with the information they need to explain

Internet policy issues to policy makers. It provides a construct for linking high-level policy to detailed technical decisions [1].

The Internet is a vital resource that is changing the way many enterprises and individuals communicate and do business. However, the Internet suffers from significant and widespread security problems. Many agencies and enterprises have been attacked or probed by intruders, with resultant losses to productivity and reputation. In some cases, enterprises have had to disconnect from the Internet temporarily, and have invested significant resources in correcting problems with system and network configurations. Sites that are unaware of or ignorant of these problems face a risk that network intruders will attack them. Even sites that do observe good security practices face problems with new vulnerabilities in networking software and the persistence of some intruders [1].

The fundamental problem is that the Internet was not designed to be very secure. Some of the inherent problems with the current version of TCP/IP are:

- Ease of eavesdropping and spoofing
- Vulnerable TCP/IP services
- Lack of policy
- Complexity of configuration [1]

Ease Of Eavesdropping And Spoofing

The majority of Internet traffic is not encrypted. E-mail, passwords, and file transfers can be monitored and captured using readily available software [1].

Vulnerable TCP/IP Services

A number of the TCP/IP services are not designed to be secure and can be compromised by knowledgeable intruders. Services used for testing are particularly vulnerable [1].

Lack Of Policy

Many sites are configured unintentionally for wide-open Internet access without regard for the potential of abuse from the Internet. Many sites permit more TCP/IP services than they require for their operations and do not attempt to limit access to information about their computers that could prove valuable to intruders [1].

Complexity Of Configuration

Host security access controls are often complex to configure and monitor. Controls that are accidentally misconfigured can result in unauthorized access [1].

MAJOR TYPES OF POLICY

Computer security policy means different things to different people. It can mean senior management's directives to create a computer security program, establish its goals and