1 Introduction

1.1 *Purpose*

This document is intended to help an organization create a coherent Internet-specific information security policy. It provides a brief overview of the Internet and its constituent protocols. It discusses the primary uses of the Internet, and the associated policy implications. And it provides sample policy statements for low, medium and high risk/protection environments.

Readers who need a more general introduction to computer security can find it in NIST Special Publication 800-12, *An Introduction to Computer Security: The NIST Handbook.*

1.2 *Intended Audience*

This document was written for three kinds of readers:

- High-level managers who need to understand some of the risks and implications of Internet usage so that they can appropriately allocate resources and delegate responsibility,
- Mid-level managers who will need to set issue-specific policies, and
- Low-level managers and technical people who need to understand the policy roots of the technical controls they will be asked to implement and the rules they will need to teach the users of the information systems.

Each policy area will contain a description of the concern and sample policy statements for low, medium and high protection environments, where appropriate.

1.3 *Internet Background*

The Internet is a world-wide “network of networks" that use the TCP/IP (Transmission Control Protocol/Internet Protocol) protocol suite for communications. The Internet was created to foster communication among government-sponsored researchers. Throughout the 1980's, the Internet grew steadily to include educational institutions, government agencies, commercial organizations, and international organizations. In the 1990's, the Internet has undergone phenomenal growth, with connections increasing faster than any other network ever created (including the telephone network). Many millions of users are now connected to the Internet, with roughly half being business users (Vinton Cerf. A National Information Infrastructure. *Connexions*, June 1993). The Internet is being used as the basis for the National Information Infrastructure (NII).

1.4 *Why create Security Policy for Internet-Related Issues?*

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.

Organizations are, rightly concerned about the security implications of using the Internet:

- Will hackers disturb internal systems?
- Will valuable organizational data be compromised (changed or read) in transit?
- Will the organization be embarrassed?

All of these 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 resources—staff time to implement and operate and money to buy and maintain equipment and software.

The purpose of an Internet Security Policy is to decide how an organization 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 above).[1] 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.

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 document 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.

The Internet is a vital resource that is changing the way many organizations and individuals communicate and do business. However, the Internet suffers from significant and widespread security problems. Many agencies and organizations have been attacked or probed by intruders, with resultant losses to productivity and reputation. In some cases, organizations 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.

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 -- the majority of Internet traffic is not encrypted. E-mail, passwords, and file transfers can be monitored and captured using readily available software.
- 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.
- Lack of policy -- many sites are configured unintentionally for wide-open Internet access without regard for the potential for 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, and
- Complexity of configuration -- host security access controls are often complex to configure and monitor; controls that are accidentally misconfigured can result in unauthorized access.

1.5 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 assign responsibilities. It can mean mid-level managerial decisions regarding issues like e-mail privacy

[1] There is a third type of policy that is defined in Internet security literature. It is a technical approach. This book defines the technical approach as analysis that supports the general policy and specific rules. It is, for the most part, too technical for policy-making officials to understand. As such it is not useful as policy. However, it is imperative for defining the possible solutions that will define the tradeoffs, which is an essential element of setting policy.

or fax security. Or it can mean low-level technical security rules for particular systems.[2] In this document, the term *computer security policy* is defined as the *documentation of computer security decisions* — which covers all the types of policy described above.[3]

In making these decisions, managers face hard choices involving organizational strategy, competing objectives, and resource allocation. These choices involve protecting technical and information resources, as well as guiding employee behavior.

The essential element of policy is that is a decision. It provides direction for an organization. In order for the policy to be useful, it is essential that a different direction could have been realistically selected. Because policy sets a direction, it can be used as the basis for making other lower level decisions. High-level policy should not need to be changed frequently.

It is also essential that the policy be implemented in such a way that the organization actually goes that direction. Two common problems with organizational policy are that:

1. The policy is a platitude rather than a decision or direction.
2. The policy is not really used by the organization. Instead it is a piece of paper to show to auditors, lawyers, other organizational components, or customers, but it does not affect behavior.

It may be helpful to consider some examples to explain these essential elements of policy.

Example #1: A company decides to have a policy promoting computer security. The policy reads something like: “It is the policy of this company to protect the confidentiality, integrity, and availability of data” It is passed out to employees as a memo signed by the company president. However, what company is going to have a policy saying that it does not care about security? And how would an employee change his or her behavior based on this memo? A policy which stated a goal of protecting data and then assigned responsibility to a specific organizational element to develop a security program, assigned significant resources to that element, and put good people on the program would be more effective. The implementation of the policy, in this example, includes putting good people and other significant resources on the program. That is how the employees know that this is a real decision, not a show to appease an auditor.

Example #2: A technical administrator (who is male) decides that good security requires that users do not share accounts. So the administrator gets his management to sign a directive requiring this (by stating that this is the generally accepted security practice). However, the users do not know how to share files without sharing accounts, so they ignore the directive. The manager did not really understand what she (the manager is female[4]) was signing or its implication for operations. The policy did not really set a direction because the manager did not understand. A more astute manager should have asked why the technical administrator needed such a policy. (If it is good practice, why does it need a directive?) She would have found out, then, about the underlying problems. She would have found out there was a real choice to be made, operate insecurely or put resources into setting up new procedures and training users.

Managerial decisions on computer security issues vary greatly. To differentiate among various kinds of policy, it is helpful to categorize them into three basic types:

Program policy sets organizational strategic directions for security and assigns resources for its implementation. Program policy is used to create an organization’s computer security program. A

[2] These are the kind of policies that computer security experts refer to as being *enforced* by the system's technical controls as well as its management and operational controls.

[3] In general, policy is set by a manager. However, in some cases, a group (e.g., an intra-organizational policy board) may set it.

[4] Please forgive us the political correctness of having one male and one female. It makes telling the story so much easier since we can use he and she to differentiate our characters.

management official, normally the head of the organization or the senior administration official, issues program policy to establish (or restructure) the organization's computer security program and its basic structure. This high-level policy:

1) defines the purpose of the program and its scope within the organization;

2) assigns responsibilities (to the computer security organization) for direct program implementation, as well as other responsibilities to related offices (such as the Information Resources Management [IRM] organization); and

3) addresses compliance issues.

Issue-specific policies address specific issues of concern to the organization. Whereas program policy is intended to address the broad organization-wide computer security program, issue-specific policies are developed to focus on areas of current relevance and concern (and sometimes controversy) to an organization. Management may find it appropriate, for example, to issue a policy on how the organization will approach contingency planning (centralized vs. decentralized) or the use of a particular methodology for managing risk to systems. A policy could also be issued, for example, on the appropriate use of a cutting-edge technology (whose security vulnerabilities are still largely unknown) within the organization. Issue-specific policies may also be appropriate when new issues arise, such as when implementing a recently passed law requiring additional protection of particular information. Program policy is usually broad enough that it does not require much modification over time, whereas issue-specific policies are likely to require more frequent revision as changes in technology and related factors take place.

In general, for issue-specific and system-specific policy, the issuer is a senior official; the more global, controversial, or resource-intensive, the more senior the issuer is.

System-specific policies focus on decisions taken by management to protect a particular system.[5] Program policy and issue-specific policy both address policy from a broad level, usually encompassing the entire organization. However, they do not provide sufficient information or direction, for example, to be used in establishing an access control list or in training users on what actions are permitted. System-specific policy fills this need. It is much more focused, since it addresses only one system.

Many security policy decisions may apply only at the system level and may vary from system to system within the same organization. While these decisions may appear to be too detailed to be policy, they can be extremely important, with significant impacts on system usage and security. These types of decisions can be made by a management official, not by a technical system administrator.[6] (The impacts of these decisions, however, are often analyzed by technical system administrators.)

[5] A *system* refers to the entire collection of processes, both those performed manually and those using a computer (e.g., manual data collection and subsequent computer manipulation), that performs a function. This includes both application systems and support systems, such as a network.

[6] It is important to remember that policy is not created in a vacuum. For example, it is critical to understand the system mission and how the system is intended to be used. Also, users may play an important role in setting policy.