Chapter 22

NETWORK SECURITY

INTRODUCTION

Internet access has become vital to the normal operations of virtually every enterprise. In the 2006, according to industry analysts, over 90% of all respondents rated the Internet as a moderate to extremely important source of information. Studies show it has enabled enterprises to:

- Greatly facilitate collaboration between employees, partners, suppliers and clients through vehicles such as email, file sharing and web conferences
- Rapidly access information through on-line searching, databases and e-training
- Inexpensively provide services to outside enterprises through web sites, email distribution and on-line commerce applications [1]

The Internet is used widely across most enterprises, enabling them to increase productivity and the quality of services, while decreasing costs [1].

With this widespread adoption has come a change in user and management attitudes. Internet access is no longer a luxury. It is a mandatory enterprise requirement. Unencumbered, transparent access is expected at all levels in the enterprise on a non-stop basis [1].

CURRENT SECURITY RISKS

Unfortunately the Internet has a dark side too. Just as it provides transparent access to numerous external resources for an enterprise, it can also provide external parties, not all of who have good intentions, relatively easy access to the enterprise's internal computers and information. All types enterprises are at risk. On a whim, in 2006, a 22-year old hacker scanned the New York Times' Internet gateways, and was easily able to access numerous databases providing personal information on sources, employees and customers. Even highly sophisticated enterprises like computer game makers have experienced Internet

breaches. One particular game maker had information and source code for pending product releases posted on the Internet, a breach that had a severe financial impact. The following are some network security facts:

- The average cost of an external security breach in 2006: $660,000.
- The average cost of a virus infection in 2006: $125,000.
- The average cost of a DoS attack in 2006: $631,000 [1].

The diversity of methods used to malevolently access or attack enterprises' computers through the Internet is truly stunning. On top of this, inappropriate internal use of the Internet is also turning out to be a big issue. Table 22-1 shows some of the forms of abuse reported by IT managers to be of greatest concern [1]:

Table 22-1. Network abuses.

Type of Attack	**Description**	**Economic Implication**
Hackers	Hackers, or skilled programmers who find challenge in breaking into other people's computer systems, were traditionally the greatest threat to organizations' computer security. While they still pose a threat, widespread deployment of countermeasures such as firewalls has caused other forms of more sophisticated malicious attacks to emerge.	After breaking into a system a hacker may steal, delete or alter valuable data, programs or identities.
Malware	Malware (viruses, worms, etc.) are pieces of disguised code that are typically designed to cause an undesirable event, such as altering existing computer files or making the computer inoperable. They can be transmitted by disk, email or other communications vehicles. Because email usage is so prevalent, and traditional security systems remain vulnerable to viruses, viruses are now one of the major security concerns of IT managers. Eighty-nine (89%) percent if all infections stem from email attachments.	The cost of lost productivity, restoring damaged files and cleaning up viruses was a staggering $58.7 billion worldwide in 2006.
Spam	Unsolicited commercial email messages (spam) are not created with the same malicious intent as threats like viruses, but are now having a negative economic impact on the same order of magnitude.	Spam clogs networks, hogs disk space, and wastes countless hours of users' time reading and dealing with the messages. Estimated cost to U.S. and European enterprises in 2006 was $12.3 and $6.9 billion respectively. Evidently spammers don't have a life and have a lot of time on their hands.