



## Maintaining Network Security – Your Top Priority What It Means To You

[www.crosslinpc.com](http://www.crosslinpc.com)  
[www.statsolutionsusa.com](http://www.statsolutionsusa.com)

By: Terry Saltsman, Ph.D.

View the November 4, 2002 issue of *NetworkWorld* magazine and you will discover that over the next year companies will spend about \$4 billion dollars for network security. It is the “hot topic” for 2003 and will stretch many of the resources of IT consulting professionals, CIOs, and CEOs. The reasons for concern about network security are numerous. First there are the hackers – individuals who see the challenge of defeating corporate IT security systems. Second, there is the Microsoft backbone on which 85% of all networks run – it’s chockfull of security holes. Third, there is the realization that all a company is can be found on its network and the compromise or loss of that data can lead to the demise of the corporation. So what are the risks to a company outside of the obvious erosion of customer trust or interrupted service? The purpose of this article is to address some of the more common security holes that can be found every day in network systems everywhere.

- **The Employee Security Hole.** Past and present employees are the greatest risk factor to your network security and exposure to risk. Those employees who have recently gone – and even some who have been gone for up to a year or two – may seek access to sensitive and confidential information after leaving and often will seek to expose that information for personal gain. This breach can also create liabilities to those companies that have been compromised, especially in highly regulated industries like healthcare and monetary institutions. Also, we have seen examples in which former employees have gained access to company email accounts and used them improperly, leading to claims for sexual harassment and discrimination.
- **Attack of the “Denial of Service.”** Everyone has heard of the attack on Amazon.com’s network that led to several days of lost revenue during the holiday season of 2002. During this attack, hundreds of thousands of emails and queries were repeatedly sent to the company every few minutes. The server, unable to handle the demand, simply shut down. Hackers often commit this sort of act for two reasons: first, to prove that they can close down the e-business side of the operation, and second, to prevent companies from performing routine billing activities, eventually strapping the companies for cash. Legal experts indicate that there can be liability issues for negligence (or breach of contract, as applicable) for failure to secure the computer and protect it from such attacks, thus causing downtime, loss of business, and reduced profit.
- **Compromising or Loss of “Confidential” Documents.** Obviously, the most troubling aspect of network security is when confidential information is compromised or lost, especially under the various privacy and security laws in existence today – such as found in HIPAA. Corporations operating in the public domain are obligated to safeguard the personal information that can identify a client or patient.