



Adware and Spyware and Spam — Oh My!

It's a dangerous world, but forget lions and tigers and bears. Today's network security managers must defend against everything from mundane incompetence to full-scale criminal assault.

Forget miracle products, too — no IT cop-in-a-box can solve all your security concerns. A decade of advances in network complexity has changed the concept of security, from a purchased product to a process. Every strong network security program proceeds from management's commitment to policies and procedures that are effective, workable, clearly communicated and enforced.

The past decade has also produced a recognized set of best practices. Here are some of the most important.

Begin with a comprehensive written security policy.

Review it regularly, update it as needed and require every employee to sign it.

Start from "Deny All." Make your system fail-to-safe:

Permit zero access except by explicit, documented permission from an authorized and accountable individual.

Encrypt sensitive data. Use proven technologies such as IPSec, SSL, Triple DES or WEP (changing WEP keys frequently).

Control access and traffic across all boundaries.

Physical security covers sensitive areas, environmental controls, emergency generators, fire suppression, emergency lighting, and video surveillance. And don't forget logical security measures like strong passwords, antivirus

software, user access reviews, vulnerability scanning, VPN for remote access, and patch management.

Implement role-based authentication and authorization procedures. Apply these as needed for network administrators, remote users, employees and business partners.

Filter content. Exclude items that could cause network vulnerabilities (malicious e-mail attachments, hacker tools, viruses), expose the company to liability (pornography, criminal enterprise, anonymizers) or impede network function (music downloads, streaming content, adware, spyware, spam).

Conduct regular third-party audits and assessments. Once you've fortified your network, enlist objective eyes to assess vulnerabilities and recommend improvements.

Security is a process, and we can help you implement it. Call us to discuss ideas for strengthening your network protections.