

Laura Iwan, Director, HEALTHCOM Services Support, NYS Department of Health

An introduction to Internet security issues discussed in more detail by other presenters: the cost of security attacks, common threats and vulnerabilities, security controls, and resources.

Computer security attacks cost as much as \$10 billion a year. An attack can damage data integrity, confidentiality or availability. Organizations must understand the potential costs: How would incorrect data affect decision making? What will happen if confidential information is made public? What is the cost (in lost time and credibility) of interrupted service? To understand threats, organizations should ask themselves: Does the information have a dollar value? While more security equals more cost, the cost is slight compared to a single breakdown of services.

Vulnerabilities exist in all computer systems and all Internet services (SMTP, Telnet, FTP, HTTP, etc.). Email can be intercepted or spoofed. In Email spoofing an attacker assumes a false identity to solicit information or access. Hackers also exploit root compromises on old systems, poor passwords, IP spoofing, misconfigured networks, and packet sniffers. Internal attacks represent even more danger: over 80% of all break-ins come from internal staff or staff that has recently left an organization.

Internet security starts with proper administrative and physical security. Firewalls and bastion hosts should be employed where necessary. Administrators should monitor and log all activity. For mail threats, an organization may consider authentication and/or encryption technologies.

System administrators should stay current on system vulnerabilities and controls. Resources include "double-edged swords" such as SATAN, ISS, and hacker discussion lists, as well as "lifeguards": CERT, FIRST, CIAC, NIST, COAST, and the many World-Wide-Web sites devoted to security issues.