

Dave Dumas, Senior Security Consultant, Digital Equipment Corporation

Internet risk assessment must address a myriad of specific Internet threats. By running a "risk assessment workshop" an organization can determine security needs and develop a security strategy that covers both personnel and technology issues.

The risks of the Internet reflect its size: 50 million users, 30 thousand networks, 10+ million computers, 137 countries. As capacity, connectivity and mobility increase, so does risk. Prominent sites are probed daily. Banks may get 50 or more probes a day. Successful attacks are automated and posted to electronic bulletin boards; attack methodologies quickly spread.

On the other hand, 90% of all attacks come from inside sources, primarily by disgruntled or laid-off employees. Another inside attack, social engineering, is widespread and effective. The attacker researches an organization, then uses that information to deceive users or administrators into granting him or her access.

Organizations must understand security issues. They must stay current on tools (such as SATAN), security user groups, hacker web sites and liability issues. Still, the technological approach must reflect business needs: ease of use, industry standards, employee skill-sets, etc. To determine security needs, an organization can run a risk assessment workshop.

A risk assessment workshop includes 8 to 12 subject matter experts from within an organization, outside computer security experts and a moderator. The participants analyze the following: threats (hackers, viruses, disgruntled employees); targets (files, applications, hardware); probability of attack (number per year), impact (cost) of attacks, and countermeasures. Then the participants create threat/object pairs (for example, hacker/database) and analyze the vulnerability and impact for each. From this analysis, the organization can determine its security strategies.