By Jim Canterucci

Intranet Security

Because intranets contain confidential information about organizations, it is critical that this information does not get into the wrong hands.

By definition, intranets do not have to provide access to the Internet or other networks. However, there is valuable information available to employees on the World Wide Web. If a company provides access to the Internet via an internal corporate network, that introduces risks. They include viruses that can be downloaded accidentally onto an intranet from the Web. Security weaknesses may also be found in the use of modems, connection to remote offices, and access to office buildings.

It is important to develop and execute a comprehensive security plan. The plan should address such issues as

- what resources need protection
- how important the resources are
- which people pose a risk to those resources
- how likely threats are
- what impact threats can have
- what measures can be taken to protect corporate assets in a timely and cost-effective way
- what the ongoing review and monitoring strategies are to keep the plan up to date.

The most obvious enemy to intranet security is a hacker, a technically savvy outsider. A hacker may break into a corporate intranet just for fun or a challenge. Other threats include an expert retained by a competitor to wreak havoc on a company's intranet. This kind of person is also known as a "cracker," someone that engages in telecommunications and computer intrusion.

In addition to outside threats, there is an increasing trend toward security breaches initiated by current and former employees.

It is important to evaluate the most likely threats and prepare for them. Security approaches range from completely ignoring threats to outright paranoia. When protecting against potential internal breaches, security measures sometimes can stifle corporate communication and collaboration. The amount of risk a company is willing to endure is important. A balance must be achieved that is comfortable for the organization.

To help you make informed decisions about intranet security, there are a few basic security terms you should know.

Firewalls. These are hardware or software systems that protect one part of a network from another, or protect an internal network from the outside world. A firewall determines who will cross a network boundary. It also defines a standard way to recognize or authenticate authorized users.

A firewall can also provide a log of activities and potential attacks, and it can alert administrators to security breaches.

Proxy firewall. This product acts as a gatekeeper in that the proxy server gains access to internal systems rather than allowing authorized users direct access.

Routers. These products, working at the network level, filter packets of information based on the address of the individual or the protocol being used. This approach alone is less secure than a proxy solution.

Privacy

A company's security policy should address the privacy of the authorized network users. The best network managers track user activity to prevent security breaches and are sensitive to employees' privacy. Employees, however, should assume that all electronic communications during work hours, or that are related to work can be monitored.

As intranet technology becomes more pervasive and complex, it's important for trainers and HRD practitioners to become familiar with privacy and security issues. Here are some resources where you can find additional information.

Web sites.

- Internet Firewalls—Frequently Asked Questions, http://www.v-one.com/pubs/fw-faq/faq.htm
- Firewall Product Overview, http://www.access.digex.net/~bdboyle/firewall.vendor.html
- COAST Security Resources, http://www.cs.purdue.edu/coast/coast.html
- Planitary Firewall White Paper, http://www.planitary.com/firewalls/docs/toc.html
- WWW Security FAQ, http://www-genome.wi.mit.edu/WWW/faqs/www-security-faq.html

Books.

- *Internet Security Professional Reference*, New Riders Publishing, 1996
- *Internet Firewalls and Network Security*, New Riders Publishing, 1996
- *Actually Useful Internet Security Techniques*, New Riders Publishing, 1996
- *Building Internet Firewalls*, O' Reilly & Associates, 1995
- *PC Week Intranet and Internet Firewall Strategies*, Ziff-Davis Press, 1996

Jim Canterucci *is founder and CEO of Transition Management Advisors. Web site http://www.corpchange.com; phone 800/370-7373.*