

## Security: It's not just for big companies

In the old days, "putting your business on the line" meant taking risks with new ventures or investments.

---

Today, the same phrase can be applied to all companies that depend on networks and the Internet to run their businesses.

There's no question that companies big and small can use the Internet to enormous advantage. But at the same time, putting a business online involves risks. The Internet is a public electronic highway, and companies who travel this route are more exposed than those who stay confined to a closed, private road.

People who run small businesses may feel less vulnerable to security-related problems because they think that only big companies are the targets of attacks. After all, who would take the time to launch a denial-of-service attack against a small law firm or an auto parts dealer?

The truth is that companies of all sizes are at risk from indiscriminate, self-propagating viruses and disgruntled employees. In fact, **small companies may be more vulnerable** because most don't have the luxury of employing dedicated security staff or even network operations pros to help secure their networks.

### Security threats are on the rise

According to the Computer Emergency Response Team, "computer security vulnerabilities have more than doubled in recent years." And according to research from Riptech, now a part of Symantec, "general Internet attack trends are showing a 64% annual rate of growth."

These rather sobering statistics are only half the disturbing news. The other half is the damage that these attacks can cause:

It is estimated that the worldwide impact of malicious code was \$13.2 billion in the year 2001 alone, with the largest contributors being SirCam at \$1.15 billion, Code Red (all variants) at \$2.62 billion, and "Nimda" at \$635 million. (Source: Computer Economics, Jan. 2, 2002.)

The "Code Red" worm affected more than 359,000 servers in less than 14 hours; more than 2,000 new hosts were infected each minute. (Source: Cooperative Association for Internet Data Analysis, July 25, 2001.)

### What are the threats?

Keeping business information and network resources safe is a much broader challenge than simply locking out viruses. According to the FBI and the Computer Security Institute, 60% of information-related crime is committed by internal sources. Angry employees might infect corporate networks with viruses or delete crucial files.

Employees don't even have to be disgruntled to do harm to corporate networks. Very often they simply don't follow common-sense security policies, such as choosing hard-to-guess passwords and changing them frequently. They may violate privacy by attempting to snoop around for salary information, end-of-quarter financials, or other sensitive data. When security measures are not in place, even an innocent mistake, such as unintentionally downloading harmful files from the Internet, can bring down a network.

External threats come in many different forms, ranging from jokester hackers to "crackers" with malicious intent. Some of the most common attacks include:

**Denial of Service:** Occurs when an intruder overloads an IP network. Flooded with packets, the network can't handle legitimate traffic, cutting off employees, customers and business partners.

**IP spoofing:** An intruder forges source addresses in IP packets in order to gain network access, and is then able to launch Denial of Service attacks and inflict other damage.

**Application-level attacks:** Intruders enter your network through a computer program.

**Trojan horses:** These programs, inserted into a network covertly, appear to be useful programs, but actually inflict damage when launched.

**Viruses and worms:** Viruses compromise desktop data or applications. Worms damage an individual desktop, then use the resident address book to send themselves to other users.

## Who needs to be secure?

**A company's size or market is not a predictor of its safety.** A small business must be rigorous about security if it has:

The need to offer partners, customers, and employees access to network-based resources and/or access to information via virtual private networks (VPNs), extranets, dial-up connections, or other external connections.

Broadband or wireless connections.

An internally hosted Web site or any Web site that handles sensitive e-business transactions.

Employees who telework (telecommute) or connect to the network while traveling.

A firewall as the company's only network safeguard, or any security device that is not receiving regular, proactive maintenance or review.

Security products (for example, firewall, intrusion detection) from multiple vendors.

## The consequences of security breaches

Security threats are more than just a distraction. An attack directed at financial or personal records or business-critical applications is potentially devastating. But even indiscriminate attacks can result in the loss of valuable data, high repair costs, negative publicity, legal liability and the loss of hours or even days of productivity.

In addition, the specter of security vulnerabilities can be damaging to a company's reputation. When virus attacks against major corporations are featured on the nightly news, smaller companies may find themselves needing to reassure customers, business partners, and even employees that their information and transactions are safe.

Companies must institute policies and safeguards that not only are effective but are also perceived as effective.