If you think that your network doesn't contain any data worth stealing, think again. For example, your personnel records probably contain more than enough information for an identity thief: names, addresses, phone numbers, Social Security numbers, and so on. Also, your customer files may contain your customers' credit card numbers.

- Hackers who break into your network may be looking to plant a Trojan horse program on your server, enabling them to use your server for their own purposes. For example, someone may use your server to send thousands of unsolicited spam email messages. The spam won't be traced back to the hackers; it'll be traced back to *you*.
- Not everyone on the network knows enough about how Windows and the network work to be trusted with full access to your network's data and systems. A careless mouse click can wipe out a directory of network files. One of the best reasons for activating your network's security features is to protect the network from mistakes made by users who don't know what they're doing.

The Three Pillars of Cybersecurity

There are three pillars that you must consider as part of your cybersecurity plan. They're like the legs of a three-legged stool — if one fails, the whole thing comes crashing down. The three pillars of cybersecurity are

- **Prevention technology:** The first pillar of cybersecurity is technology that you can deploy to prevent bad actors from penetrating your network and stealing or damaging your data. This technology includes firewalls that block unwelcome access, antivirus programs that detect malicious software, patch management tools that keep your software up to date, and antispam programs that keep suspicious email from reaching your users' inboxes.

  Chapter 20 addresses firewalls and antivirus software, while Chapter 21 shows you how to employ antispam software.
- **Recovery technology:** The second pillar of cybersecurity is necessary because the first pillar isn't always successful. Successful cyberattacks are inevitable, so you need to have technology and plans in place to quickly recover from them when you do. You can learn more about recovery technology in Chapters 22 and 23.