IN THIS CHAPTER

- Assessing the risk for security
- Determining your basic security philosophy
- Physically securing your network equipment
- Considering user account security
- Looking at other network security techniques
- Making sure your users are secure

Chapter 19

Welcome to Cybersecurity Network

As an IT professional, cybersecurity is the thing most likely to keep you awake at night. Consider the following scenarios:

- Your phone starts ringing like crazy at 3 o'clock one afternoon because no one anywhere on the network can access any of their files. You soon discover that your network has been infiltrated by *ransomware,* nefarious software that has encrypted every byte of data on your network, rendering it useless to your users until you pay a ransom to recover the data.
- Your company becomes a headline on CNN because a security breach has resulted in the theft of your customers' credit card information.
- On his last day of work, a disgruntled employee copies your company contact list and other vital intellectual property to a flash drive and walks away with it along with his Swingline stapler. A few months later, your company loses its biggest contract to the company where this jerk now works.