- **The human firewall:** The most important element of cybersecurity is what I call the *human firewall.* Technology can only go so far in preventing successful cyberattacks. Most successful attacks are the result of human error, when users open email attachments or click web links that they should have known were dangerous. So, in addition to providing technology to prevent attacks, you also need to make sure your users know how to spot and avoid suspicious email attachments and web links. (For more information, see the section "Securing the Human Firewall" later in this chapter.)

Two Approaches to Security

When you're planning how to implement security on your network, first consider which of two basic approaches to security you'll take:

- **Open door:** You grant everyone access to everything by default and then place restrictions just on those resources to which you want to limit access.
- **Closed door:** You begin by denying access to everything and then grant specific users access to the specific resources that they need.

In most cases, an open door policy is easier to implement. Typically, only a small portion of the data on a network really needs security, such as confidential employee records, or secrets, such as the Coke recipe. The rest of the information on a network can be safely made available to everyone who can access the network.

If you choose a closed door approach, you set up each user so that he has access to nothing. Then, you grant each user access only to those specific files or folders that he needs.

A closed door approach results in tighter security but can lead to the Cone of Silence Syndrome: Like how Max and the Chief can't hear each other but still talk while they're under the Cone of Silence, your network users will constantly complain that they can't access the information that they need. As a result, you'll find yourself often adjusting users' access rights. Choose a closed door approach only if your network contains a lot of sensitive information, and only if you're willing to invest time administrating your network's security policy.

You can think of an open door approach as an *entitlement model,* in which the basic assumption is that users are entitled to network access. In contrast, the closed-door policy is a *permissions model,* in which the basic assumption is that users aren't entitled to anything but must get permissions for every network resource that they access.