3.2.2 MANAGING THE IT INFRASTRUCTURE

After understanding the basic tenets of how computers work and communicate, it is important to understand how they are managed. Security professionals are responsible for the assets of their companies, including assets intertwined with the IT network. They must therefore make sure IT is serving the organization's needs.

One mechanism IT professionals use for managing their work is the IT Infrastructure Library or ITIL (pronounced "eye-til"). This is a framework developed by the British Office of Government Commerce in the 1980s. It has since been adopted as an international standard for managing IT. The standard addresses the concept of a service-level agreement (SLA). This is the way one negotiates with IT professionals for the services an organization needs to have delivered.

Everything an organization desires, from regular to emergency services, must be codified in this way. Otherwise, when something is not working, IT professionals may not be able to meet the organization's needs. For example, if an organization does not specify the appropriate amount of bandwidth needed in both normal and emergency situations, the IT department may not create the appropriate configurations in their equipment to meet these needs. In an active shooter situation, five people might need access to the video server at once. If this need has not been addressed in advance, the necessary resources may not be available when the time comes.

Facilities requirements are also important from the perspective of the IT professional. IT professionals require physical security as well as appropriate environmental controls to make sure their systems are working appropriately. Humidity, vibration, and air conditioning are all important considerations for the IT practitioner. Additionally, physical security practitioners should consult with IT practitioners to make sure that appropriate intrusion detection systems, access control, and video surveillance are in place to protect the physical space around computer-based infrastructure.

This concern includes every place in which users can connect to the network or gain access to servers. If a person gains access to a physical computer or server, he can generally gain access to the data on it. Physical security practitioners should assume that if someone can gain access to the physical switch, he is close to getting to other resources on the network. All these areas must be appropriately secured.

3.2.3 REAL WORLD COMPUTER SYSTEMS

The most common type of network connection is to the Internet, and from a logical standpoint, it is the same whether one connects to the Internet from home or from a business. Once traffic enters the open Internet, it is impossible to know who, if anyone, is protecting the data.

Companies have addressed this in a multitude of ways. In some cases, companies pay telecommunications providers for private networks on which only their data travels. Multiple levels of privacy are available, but there are still risks.

One should not trust systems that are not under one's control, so it is prudent to place a device in between the Internet and the systems one needs to protect: a firewall. Firewalls for computers are like firewalls in cars. The intention is to keep a fire away from the inhabitants of the passenger compartment of the car in the event that the engine catches on fire. However, fires can still sometimes break through a firewall.

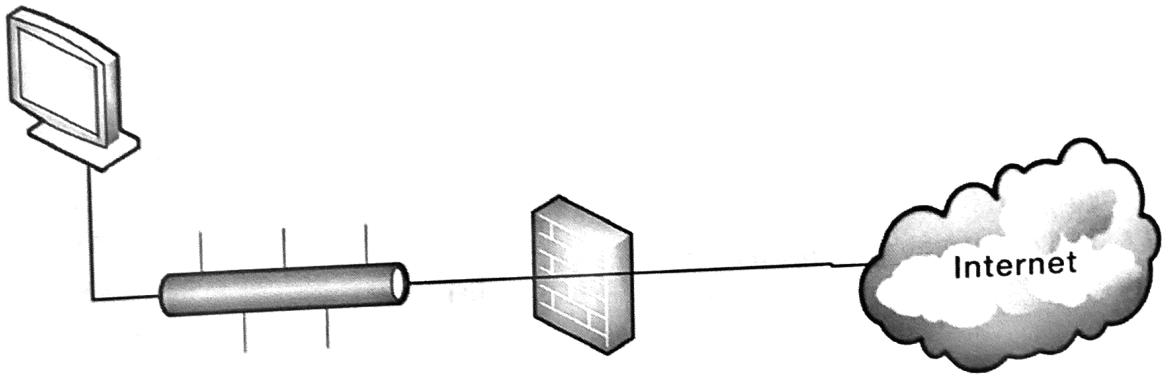

Figure 3-9
Firewall

Firewalls for computers allow only certain traffic to flow from a non-trusted network, like the Internet, to an internal network (where data is typically stored). They should be considered only one tool in the defense-in-depth arsenal.

If a company is truly concerned about the security of its data, over the open Internet or within a more private network, it can use a technology called virtual private network (VPN), which encrypts data from one point to another. For the data to be compromised, assuming the use of an adequate encryption algorithm, somebody has to know the secrets used to encrypt the data.

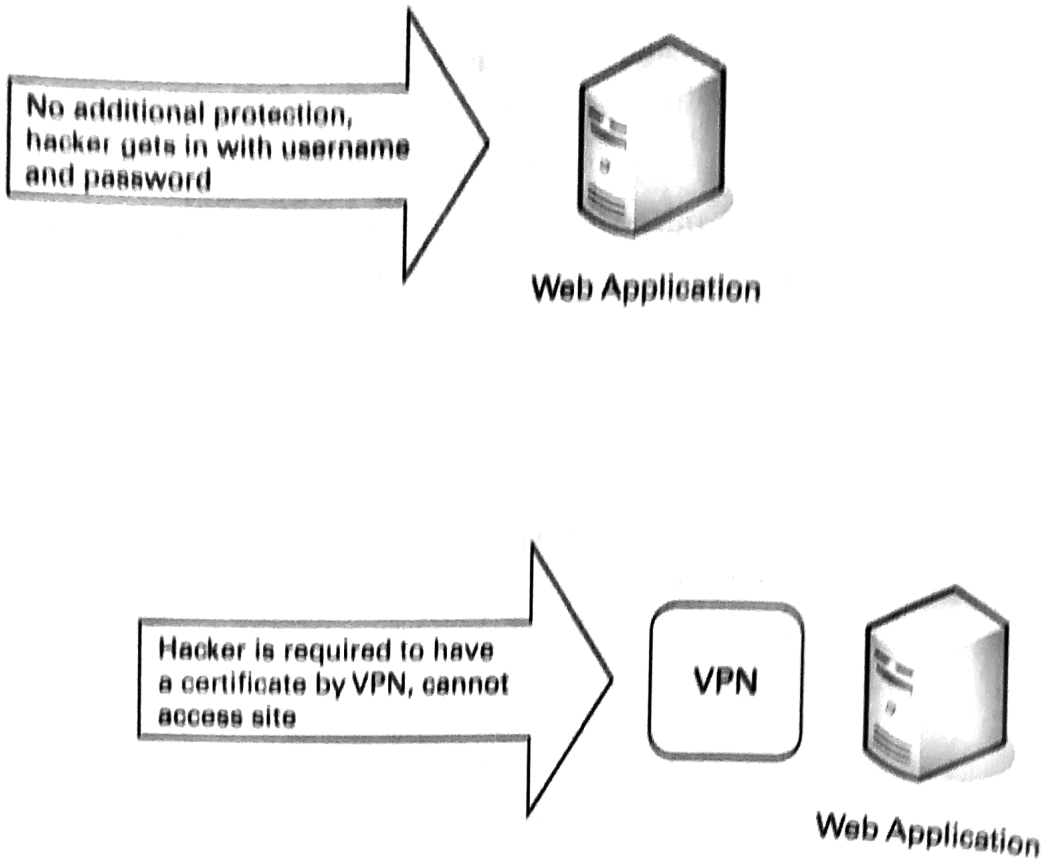

Figure 3-10
Virtual Private Network

An important issue in ISS is cloud computing, which enables companies to offer services without an investment in technology infrastructure. One appeal is that many IT concerns are managed by someone else. Unfortunately, cloud computing also raises data protection concerns.

Real Vulnerabilities: An E-Mail Example

E-mail has become the de facto standard communication mechanism in the corporate arena. Most interestingly, e-mail is directly available to the Internet. Someone can send e-mail directly to another person's mail server, and that mail server delivers it to the second person. In general, this is good; people like getting e-mail because it connects them to other people efficiently.