PART I

Securing the Infrastructure

Infrastructure Security in the Real World

The following challenges will provide contextual reference points for the concepts you will learn in Part I. Because you have not yet read the chapters in Part I, the challenges in this chapter are designed to introduce you to the infrastructure security scenarios you'll face in the real world. In this chapter, you'll learn to:

- **Understand the relevance of infrastructure security**
- **Describe the functions, categories, subcategories, and reference structure of the NIST Cybersecurity Framework**
- **Apply the NIST Framework references to specific cybersecurity scenarios**

Security Challenges

The NIST Cybersecurity Framework was developed by the U.S. National Institute of Standards and Technology (NIST) to provide a set of independent guidelines that organizations can use to implement or upgrade their cybersecurity programs. Because the framework is a product-independent tool, it provides guidelines that any organization can tailor to meet its own cybersecurity needs.

The frameworks are divided into five functions (Identify, Protect, Detect, Respond, and Recover) that provide a top-level description of the cybersecurity development process. Each function is then divided into applicable categories that underpin the stated function. Each category is further divided into subcategories and implementation methodology. Finally, the subcategories are supported by lists of reference documents that contain the nuts and bolt of building the cybersecurity program.

This chapter will kickstart your thought processes for what you are about to learn in Part I. It contains two specific cybersecurity scenarios to which you will be asked to apply the NIST Framework in order to produce a cybersecurity solution that meets the desired objectives. In each case, you will be provided with specific subcategories to research, along with some guidance to help you produce your solutions.

In this first pass through the scenarios, you are expected to generate and record *general observations* about securing the infrastructure described, as you have not yet been introduced to the supporting material. As mentioned earlier, this is activity is designed to get your cybersecurity thought processes started.

In Chapter 5, you will return to these scenarios and use what you have learned in Chapters 2, 3, and 4 to revise your initial assessments. You will also compare your observations to those of professional security specialists who have provided their observations and solutions for these scenarios.

Infrastructure Security Scenario 1

You are in charge of planning and implementing a security system for a new electrical substation that will be built next to a new housing development. The substation is equipped with high-voltage electrical switching gear for the surrounding community. It is not manned on a full-time basis but does have a control building that houses instrumentation and communication equipment, as shown in Figure 1.1.

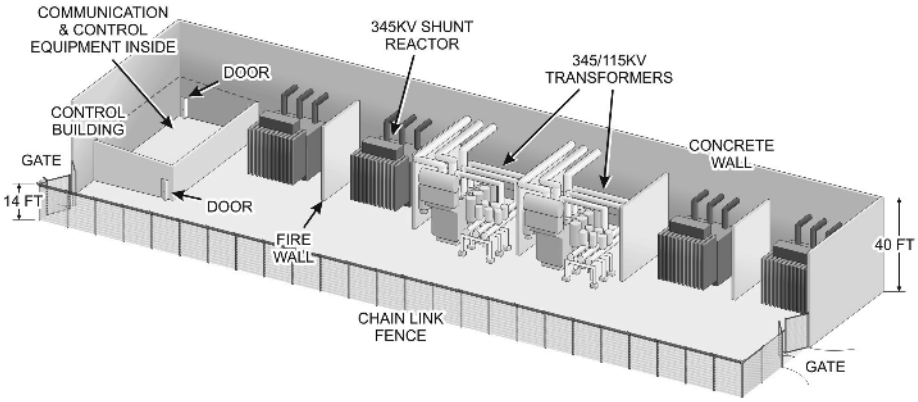

FIGURE 1.1 The Electrical Substation

The high-voltage switch gear accepts electrical power from different sources, which it then conditions and routes to the community users as needed.

The energy arrives on a set of different high-voltage supply lines and leaves the facility via different sets of distribution lines.

The monitoring devices and control systems in the substation communicate with different parts of the utility's transmission and distribution system to route electrical power where and when it is needed. These communication channels include wireless radio signals, signals transmitted across the power lines, and traditional network communications media.

Risk Assessment 1

From the information provided in this first scenario, consider the National Institute of Standards and Technology (NIST) functions detailed in this section and then record your observations as they relate to each category.

See Appendix C for the NIST Cyber Security Framework

A copy of the NIST Cyber Security Framework is available in Appendix C. These frameworks were developed by the U.S. National Institute of Standards and Technology to provide cybersecurity guidelines for Improving Critical Infrastructure Cybersecurity under executive order 13636. The ultimate goal of this initiative is to provide guidelines for the nation's critical infrastructure in business, industry, and utility organizations to reduce their cybersecurity risks.

Identify

Create an inventory of physical assets (devices and systems) within the substation (NIST ID.AM-1).

Understanding NIST References

NIST references include the function, the category, and the subcategory. In the example of ID.AM-1 mentioned earlier, the *function* is Identify (ID); the *category* is Asset Management (AM); and the *subcategory* is 1 (which is "physical devices and systems within the organization are inventoried"). To implement this portion of the Framework for the scenario presented, you may want to refer to an online copy of the designated *Reference* documents listed under this subcategory. The same is true of the following subcategories as well.

Protect

Describe in general how you might go about protecting the physical assets identified in the previous point (NIST PR.AC-2).

Detect

How would you know if someone or something was attempting to access, disable, degrade, or destroy one or more of the devices and/or systems in the substation? How could you detect anomalies and events that might impact the operation of the substation (NIST DE.CM-2, 8)?

Respond

How would you need to respond to the anomalies and events you've identified through the devices, systems, and steps you would implement in the previous point (NIST RS.AN-1, 2, 3)?

Recover

Which steps could be put in place to recover from actions intended to access, disable, degrade, or destroy the assets you previously identified (NIST RC.RP-1)?

Infrastructure Security Scenario 2

Your company is building a new corporate facility, as shown in Figure 1.2, to house its 5,000 headquarters employees. The facility will feature multiple floors. Some management personnel will use traditional offices with doors and windows, but the majority of the employees will work in open cubicles.

Each office and cubicle will be equipped with a telephone and network connection. In addition, many of the employees travel as part of their job roles and require portable computers. Other employees work with desktop personal computers.

The facility will house a cluster of computer servers and network devices that provide workflow and communications between all of the managers and employees. This architecture electronically manipulates, stores, and transmits all of the company's important business information and data. This includes product descriptions, accounting information, legal records, customer records, employee records, and the company's intellectual property.

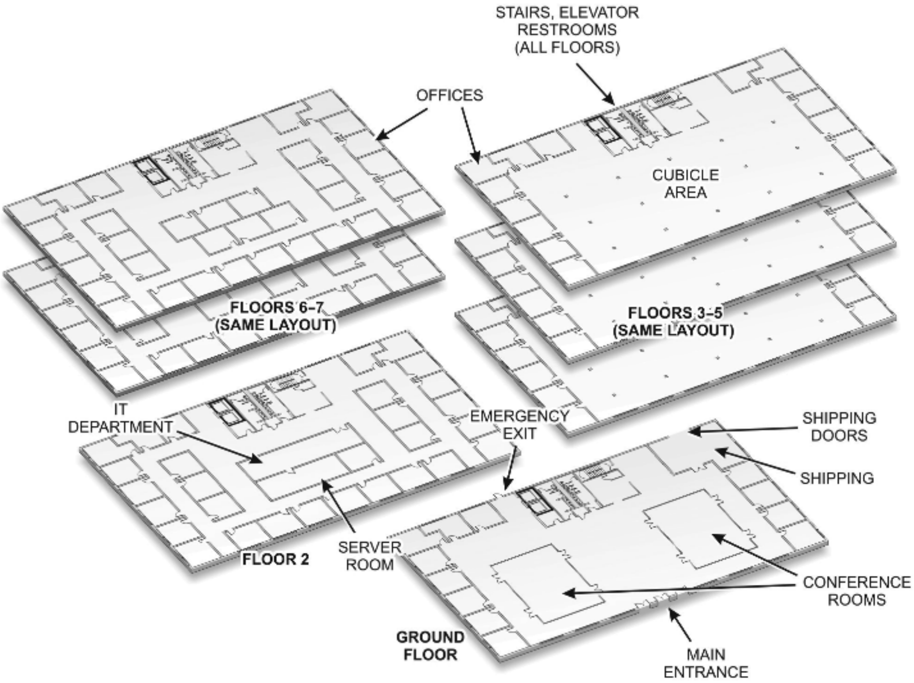

FIGURE 1.2 Headquarters Facility Plans

Risk Assessment 2

From the information provided in the second scenario, consider the NIST functions detailed in this section and then write your observations as they relate to each category.

Identify

Create an inventory of physical assets (devices and systems) within the organization (NIST ID.AM-1).

Create an inventory of cyber assets (software platforms and applications) within the organization (NIST ID.AM-2).

Prioritize the organization’s assets based on their criticality or value to the business functions of the organization (NIST ID.BE-3).

Identify any assets that produce dependencies or provide critical functions for any of the organization's critical services (NIST ID.BE-4).

Create a risk assessment of asset vulnerabilities identified (NIST ID.RA-1, 3).

Protect

Create a policy for managing access to authorized devices and resources based on the following items (NIST PR.AC-1).

Create a method for controlling physical access to secured assets (NIST PR.AC-2).

Create an action plan for informing and training general employees (NIST PR.AT-1).

Create a plan for helping privileged users understand their job roles and responsibilities (NIST PR.AT-2).

Detect

Which types of systems must be in place to identify occurrences of physical security breaches (NIST DE.CM-2)?

Which types of systems must be in place to monitor personnel activity to detect potential cybersecurity threats (NIST DE.CM-3)?

Respond

Which type of response plan might be necessary when general physical security is breached at the facility (NIST RS.AN-1, 2, 3)?

Considering the information kept on the company's servers, which type of response plan might be necessary when physical security is breached in the server room (NIST RS.CO-4, 5)?

Recover

Which type of recovery plan might be needed for general physical security breaches that occur at one of the cubicles in the facility (NIST RC.RP-1)?

Which items might a recovery plan include if server security is breached at the facility (NIST RC.CO-1, 2)?

Summary

Record your observations for the risk assessments presented in this chapter. In Chapter 5, you will compare these original thoughts and observations with those you will generate after reading Chapters 2, 3, and 4. You'll also be able to compare your answers to those of professional security specialists.