# Security From The Ground Up

CHAPTER 1

## ABOUT THIS CHAPTER

This chapter introduces a basic approach to solving cybersecurity problems. We examine the approach in the context of a very small business. The chapter focuses on the following topics:

- Strategies for making security decisions
- An approach for identifying and prioritizing cybersecurity risks
- A process to identify security requirements
- The need to monitor and evaluate security measures continuously
- A review of ethical issues in cybersecurity practice

## 1.1 The Security Landscape

Cybersecurity problems can be small and local, or they can be international in scope, involving computers and organizations on every continent. We will start small with this case study:

### ALICE'S ARTS

*Alice operates a small store, "Alice's Arts," that sells unique clothing and fashion accessories. She enjoys running the store, but she must track her finances very carefully to remain in business. She uses a laptop computer to keep track of her expenses, pay bills, order merchandise, and manage her bank account. Her store also has a small point-of-sale (POS) computer. Although Alice learned a lot about computers in school, she spends as little time as possible on computer configuration and management. She prefers to spend her time with customers or looking for unusual, appealing, and low-cost merchandise to offer. Most of her advertising consists of social media interactions with her community of customers.*

Many small business owners recognize Alice's situation. She has a business to run, and the computer is a tool. Before POS computers, small shops used cash registers. The earliest cash registers were mechanical devices that kept the cash locked up and kept a

running total of sales. As electronics replaced earlier technologies, POS computers replaced cash registers. Other early computers in small businesses handled spreadsheets for inventory and expenses, and it printed letters or fliers. Security risks were local and physical. Old desktop machines were too heavy for a sneaky thief to carry away, although a well-equipped burglar might steal one. Alice's laptop, however, might even appeal to a shoplifter.

### Not Just Local Anymore

Thanks to the Internet and modern mobile technologies, Alice can order products from around the world for her local clients. She can also provide locally made products to international customers. In addition, Alice can arrange shipments, collect payments, and make payments without leaving her store.

Alice's global reach also places her at risk. Neighbors in her quiet town may not pose a risk to her business, but Internet-based criminals may threaten her at any distance. Her computer and her business are under constant attack. Malicious software, or ***malware***, exploits weaknesses in peoples' computers. Malware may damage hardware or software, or it may leak information to criminal groups. A ***worm*** is malware that constantly scans the Internet, searching for vulnerable computers. When the worm finds a weakness, it burrows into the vulnerable computer and establishes itself on that computer. The newly started worm begins its own search for vulnerable computers.

The earliest network worm programs were either experiments or high-tech forms of graffiti. Today, worms recruit computers for cybercrime. In some cases, the computers are forced to divulge their owners' secrets, like bank account and credit card passwords. In other cases, the computers become part of a cybercrime network or ***botnet***. The botnet's operator may use this brigade of computers to send "spam" email. Other botnets perform ***denial of service*** (DOS) attacks in which thousands of individual computers send overwhelming amounts of traffic at a victim computer, blocking the flow of legitimate traffic.

During the 2013 Christmas season, a cyberattack on Target Corporation's retail stores collected millions of customer credit cards. While such attacks may grab headlines, cyber criminals don't focus exclusively on large corporations. Surveys of cyberattacks in 2013 found that over two-thirds took place in businesses with 100 employees or less. In the United Kingdom (UK), a government-sponsored survey found that 87 percent (spelled out in text, p. 75) of small businesses surveyed had detected and reported cyberattacks.

### Not Just "Computers" Anymore

Cybersecurity used to be the exclusive realm of desktop and laptop computers, or company servers: problems that intrude on Web surfing or other traditional computer activities. Today, however, every electronic appliance contains a computer. Many connect through the Internet or other networks and even let us upload software application programs, or *apps*, to add features and capabilities.

This flexibility opens our products to cyberattacks. If we can upload software to our smartphone, video player, or even our wireless router, we can also upload malware.

Popular apps tend to be relatively safe, and smartphone vendors try to block most malware by distributing apps through a secure online store like the Google Play Store or the Apple App Store. This does not eliminate malware risks, but it reduces risks.

Computers have controlled large factories and vast electrical grids for decades. These systems rely on special computers to control motors, valves, and other devices in industrial applications. While some devices may be rugged forms of more familiar computers, others are specially designed supervisory control and data acquisition (SCADA) devices or programmable logic controllers (PLCs). Desktop malware may not represent a direct threat to SCADA or PLC-based equipment, but practical attacks exist on these systems. A cyberattack on a power grid or other key industrial resources could seriously disrupt the local economy and place lives at risk.

Modern automobiles rely on computer controls to optimize engine operation. They also use digital data and communications in many other aspects of their operation. This opens modern vehicles to cyber-based attacks. In 2010, researchers at the University of Washington and the University of California, San Diego, described malware attacks that could display incorrect speed, arbitrarily enable or disable the breaks, and disable the engine. Other researchers found it was possible to track individual vehicles through the wireless tire pressure sensors.

### 1.1.1 Making Security Decisions

Cybersecurity requires trade-offs. On the one hand, a good laptop computer can be very expensive and demands protection from risk. Whenever we bring it along, we risk theft or damage. Whenever we connect it to the Internet, we risk virus and worm infestation, not to mention phishing attacks and other forms of fraud. However, we only reap the benefits of ownership when we actually take advantage of what the computer can do.

Security decision-making falls into three categories:

1. **Rule-based decisions:** These are made for us by external circumstances or established, widely accepted guidelines (example: car ignition locks).
2. **Relativistic decisions:** These try to outdo others who are faced with similar security problems (example: the hunter's dilemma described later).
3. **Requirements-based decisions:** These are based on a systematic analysis of the security situation (example: the risk management framework described in the next section).

Some security decisions are made for us. For example, all modern automobiles include keys and locks for the ignition and doors. We rarely leave the keys in a car's ignition (Figure 1.1). Although this may seem like common sense, the behavior stems from public service advertising in the 1970s. At the time there was a barrage of ads commanding: "Lock the door. Take the keys." While most of us find it almost painful to leave keys in the ignition, others leave keys in the ignition as a habit, particularly in rural areas. Such people are more worried about a lost key than a stolen car.

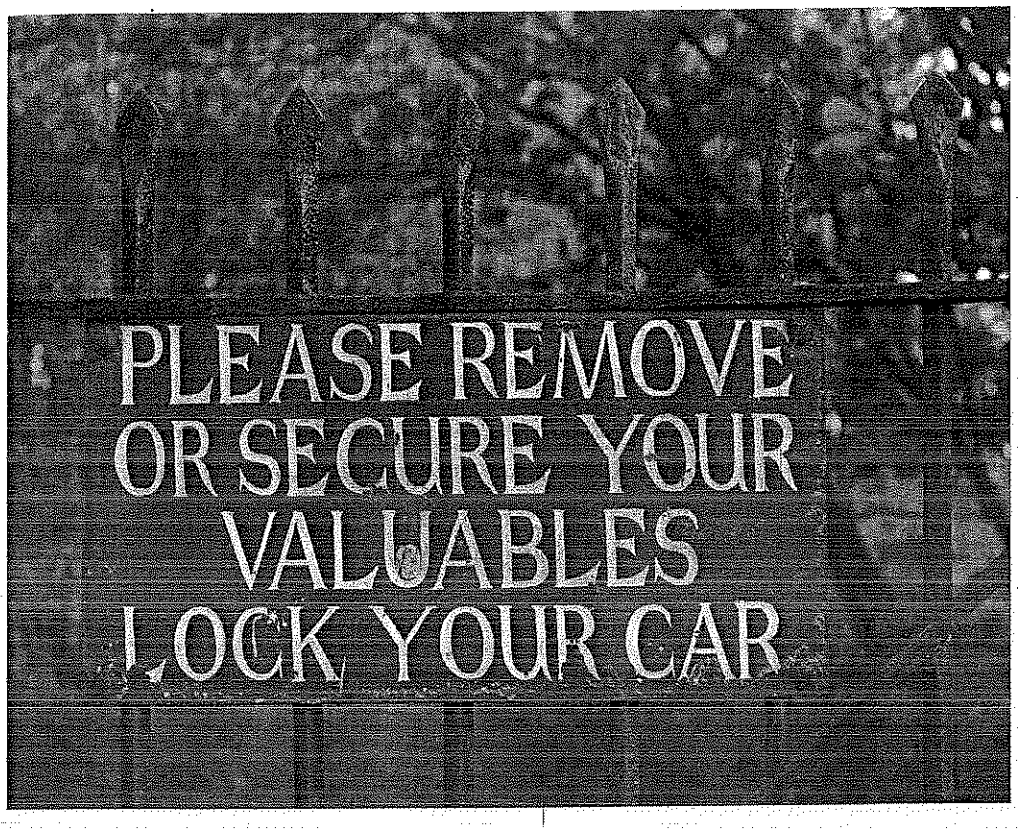




Figure 1.1

Rule-based security.

When we look at a friend's bike lock and then buy a more impressive model for ourselves, we are making a relativistic security decision. These decisions reflect the ***hunter's dilemma***: You are with a group of hunters who encounter an angry bear. The bear can run faster than you can, so how do you escape? Cynics and survivors point out that you don't have to outrun the bear; you only have to outrun another hunter.

This bit of cruel wisdom suggests that you don't have to defeat any attack, you simply have to be harder to catch (or rob) than your neighbor. In some cases, the security may be purely cosmetic: Many businesses install fake video cameras and hope that potential shoplifters will go elsewhere to steal merchandise. Relativistic security also leads to a phenomenon that security expert Bruce Schneier calls "security theater" in his 2003 book, *Beyond Fear*. Security theater refers to security measures intended to make potential victims feel safe and secure without regard to their effectiveness.

Security decisions made for us—or those based on one-upmanship—are not always the best ones. In a successful outing, all hunters return unscathed, and safe neighborhoods have as little theft as possible. Moreover, if you simply try to outdo your neighbor with a more elaborate version of the same security measures, you may both overlook a completely different threat. For example, a higher fence and a stronger lock will not protect your home from a clever bit of property fraud.

### Requirements-Based Security

In requirements-based security, we identify and prioritize our security needs in a ***risk assessment*** process. When we look for potential risks, we always find more than we can possibly protect against. We balance possible attacks against their impact on our activities, and we systematically prune our list of risks to those we can reasonably address. It is no sin to identify a risk and fail to defend against it, but we must justify that choice by comparing the security costs against the potential damage.

We generally start the process by asking, "What do we need to protect?" A flippant but useless answer might be "Let's protect our computer!" The computer doesn't need protection by itself. If so, we can leave it in a safety deposit box or seal it in a concrete vault.

Our first priority is to protect our activities, not our equipment. Alice relies on her own computer to track her store's finances, and she needs to do that regardless of what equipment she has. She needs to protect her working software and financial spreadsheets, as well as her equipment. Insurance might cover a theft, but it won't recreate her financial data. She needs to keep a ***backup copy*** of her software and data. The backup is a separate copy of her software and data that she keeps in a safe place, away from her computer. If her computer is stolen or damaged, she can use the backup copy to restore her valuable software and data.

Both rule-based and relativistic decisions often arise from ***security checklists***, which identify various security controls one might use. Longer and more-challenging checklists promote relativistic security: The more cautious users try to implement more measures than their peers. In requirements-based security, we can use our requirements to choose among competing checklists. If our requirements lead us to choose multiple checklists, the requirements may also help us prune the lists. We review each security control in a checklist and discard it if it doesn't really address our requirements.

## 1.1.2 Framework for Risk Management

There is no way to achieve 100 percent safety or to be secure against all possible risks. We always give up something—money, time, convenience, or flexibility—when we protect ourselves. We try to manage risk, not avoid it.

The Risk Management Framework (RMF) is a way to assess cybersecurity risks when developing large-scale computer systems. The National Institute of Standards and Technology (NIST), a part of the U.S. government, developed the framework. There are six steps in the framework:

1. **Categorize the information system:** identify its goals, security risks, and requirements.
2. **Select security controls:** identify existing controls and additional ones required.
3. **Implement security controls:** construct the system containing the controls.
4. **Assess security controls:** verify that the controls work as required.
5. **Authorize the information system:** approve the system for operation and deploy it.
6. **Monitor security controls:** watch for security incidents and address them; also review the environment for changes that affect security.

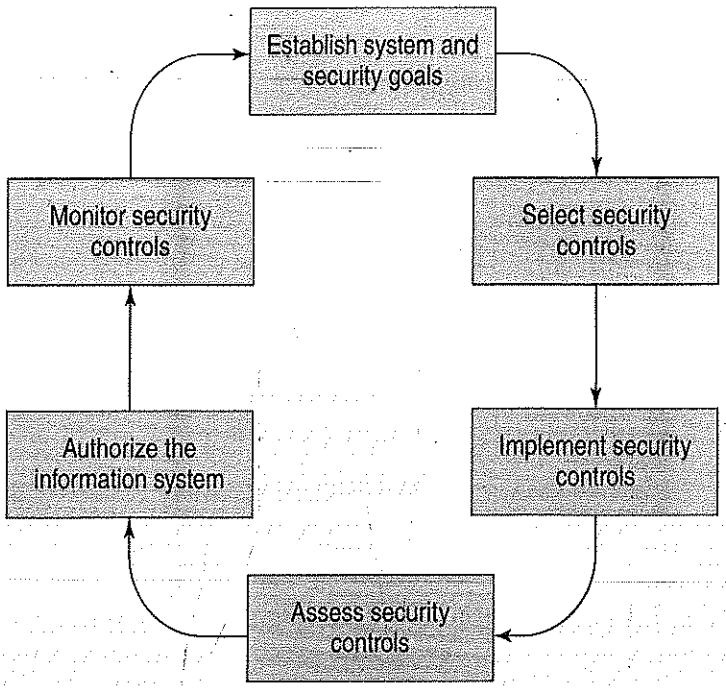


Figure 1.2

Risk management framework.

Figure 1.2 illustrates the RMF; this is based on a diagram produced by NIST. The steps appear to flow in an orderly manner from one to the next. In fact, many steps may take place simultaneously, especially among the first four steps. Step 5, the authorization step, must take place before we operate the system, but that is the only true sequence requirement.

Other steps, especially monitoring at Step 6, may uncover a problem that affects the other steps. We correct the problem by reexecuting that step whose assumptions have changed. If this is an early step, we need to reassess the subsequent steps to make sure that system is still safe to operate. Major changes require reauthorization at Step 5.

Alice needs to assess and manage her cyber risks, but she does not need this complex process. We will focus on a subset, the Proprietor's RMF (PRMF). There are only four steps, indicated by letters instead of numbers:

A. **Establish system and security goals:** identify the system's goals, security risks, and requirements. We perform a risk assessment and use it to produce a list of security requirements.
B. **Select security controls:** identify existing controls and additional ones required, and construct the system containing the controls. We use the security requirements to identify the controls we require.
C. **Validate the information system:** verify that the controls work as required, approve the system for operation, and deploy it. We test the system's controls against the security requirements to ensure that we address our risks.
D. **Monitor security controls:** watch for security incidents and address them; also review the environment for changes that affect security. The system must contain security controls that keep records of security-relevant operations and incidents.

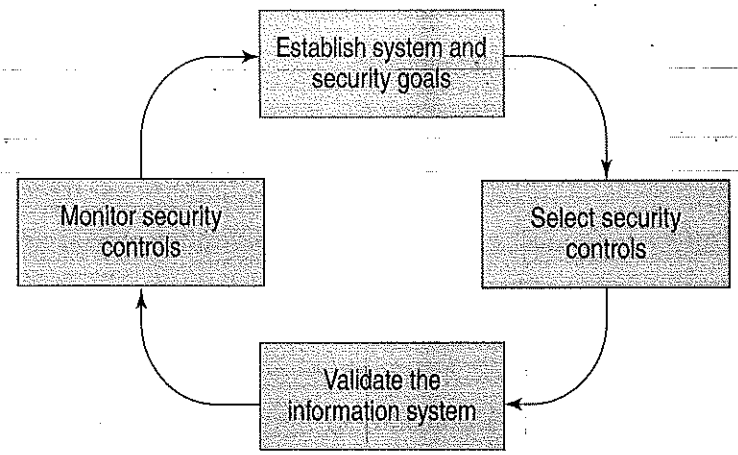


Figure 1.3

Proprietor's risk management framework—PRMF.

This process focuses on steps that everyone should take in managing risks. The full RMF uses a separate step to decide whether a system's deployment risk is worth the system's benefit; this makes sense in large organizations where major assets may be at stake. It makes less sense at a personal level when a system's sole owner/operator makes the decision.

Figure 1.3 illustrates the steps in the PRMF. The diagram includes dashed lines to show that results in one step may affect an earlier step, leading to repetition and reassessment of the system's security.

### Systems Engineering

Both forms of the RMF illustrate a ***systems engineering process:*** a way to plan, design, and build a complicated system. Companies that build complex technical products like operating systems, automobiles, or aircraft often follow a similar process.

These different processes share some crucial features:

- **Planning**—early phases lay out the project's expectations and requirements.
- **Trade-off analysis**—early phases compare alternative solutions against the project's requirements to ensure the best outcome.
- **Verification**—later phases verify that the implemented system meets requirements established in earlier phases.
- **Iteration**—if a later phase detects a problem with the results of earlier phases, then revisit the earlier phases to correct the problem.

These processes try to ensure that resources spent on a project yield the expected result. Large projects use a lot of resources and pose a serious risk: Enterprises can't afford to invest in a project only to have it fail. These steps help organize the work among a large team and track the project's progress.

The security process serves an additional purpose: It ensures that we have systematically reviewed the risks facing the system. When we rely purely on rules or on relativistic

security decisions, we assume that we all face the same risks. For example, several organizations have the following security rule:

*Never use a removable storage device in any company computer.*

Companies invoke this rule for many reasons. Recent computer malware, including Stuxnet and Conficker, have spread through infected storage drives. When an infected drive is plugged into a computer, a ***computer virus*** program would automatically start, and the virus would infect the computer's built-in storage. Companies may also lose vast amounts of sensitive company data or experience a large-scale privacy breach if someone copies the wrong information onto a removable drive.

In contrast, students use removable storage devices all the time, usually a flash drive that attaches to a universal serial bus (USB) connection. Some instructors recommend or require USB drives for particular courses. Does this expose students to an unnecessary security risk—or is that rule unnecessarily cautious? Many students' computers contain ***antivirus software*** that detects and removes virus programs from USB drives or other storage. If the students use antivirus software and avoid connecting their USB drive in risky situations, then the risk should be small. The security process allows us to identify risks that concern us and to avoid rules that don't really make us safer.

### Continuous Improvement: A Basic Principle

The security process and the systems engineering process find their origin in the concept of ***Continuous Improvement***. A process based on the Continuous Improvement principle never ends at the final step. Instead, any step in the process may suggest a change that will improve the result. To implement the change, we return to earlier steps in the cycle. Once we make the change, we continue the process.

Continuous Improvement is a ***basic principle*** of cybersecurity. We will encounter several such basic principles in this textbook. Security experts generally acknowledge these basic principles as fundamental building blocks for constructing and maintaining secure systems. When we encounter a principle in the textbook, it will be capitalized for emphasis.

## 1.2 Assessing Risks

The simplest way to address a security problem is the rule-based approach. Well-known risks often imply one or more specific security measures, often from a checklist. To defend against thieves walking through an open door, we put a lock on the door and keep it locked.

Alice can't leave her shop door locked during working hours. It remains unlocked so that customers may enter and leave. She must stay in the shop herself to help customers and to foil shoplifters or other thieves. If she needs a quick break, she closes the shop, locks the door, and leaves a sign saying "Back in 10 minutes."

Alice didn't perform a detailed risk assessment to arrive at this conclusion. She recognized the risks from her own shopping experiences and from working in other stores. Her experiences haven't really taught her rules of cybersecurity.

### Rule-Based Risk Assessment

One problem with Alice's situation is its scale: While attacks on her business may have an impact on her personally, its failure won't by itself have an impact on the local, regional, or national economy. Attacks on large private companies or on government agencies have broader impacts. This is why NIST developed the Risk Management Framework: to provide rules by which government agencies can assess their risks and construct a list of security requirements. Agencies apply the RMF to individual systems and to systems built of multiple systems. NIST has published a series of publications, including Federal Information Processing Standards (FIPS) and Special Publications (SP), to guide users of the RMF. Here are the key documents:

- SP 800-30, *Guide for Conducting Risk Assessments*
- SP 800-37, *Guide for Applying the Risk Management Framework to Federal Information Systems*
- FIPS 199, *Standards for Security Categorization of Federal Information and Information Systems*
- SP 800-60, *Guide for Mapping Types of Information and Information Systems to Security Categories*
- SP 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations*

The RMF begins with a high-level estimate of the impact caused by cybersecurity failures. This is called the ***security category***. FIPS 199 explains how a system's security category is defined, with SP 800-60 providing more detailed guidance. The RMF uses the system's security category to help select security controls from tables provided in SP 800-53.

The security category indicates the significance of security failures in terms of three general security properties, often called the *CIA properties*:

1. **Confidentiality:** The organization is obliged to keep some information confidential; how bad is the impact of confidential information being disclosed by the system?
2. **Integrity:** Computer systems misbehave or fail entirely if programs or data suffer undesired or unintended modifications; how bad is the impact of such modifications to this system?
3. **Availability:** Computer systems support the enterprise's ongoing operations. If this system isn't available, how bad is the impact?

The process estimates the potential impact of a failure on organizations or individuals. A four-point scale indicates the potential impact for each property:

- **Not applicable (NA):** The system handles public data, and disclosure has no impact. This only applies to the confidentiality property.
- **Low impact:** The failure has a noticeable impact on one or more of the agencies missions, or it causes minor damage to assets, minor financial loss, or minor injury to individuals.

- **Moderate impact:** The failure has a significant impact on mission effectiveness, or it causes significant damage to assets, significant financial loss, or significant injury to individuals that does not involve loss of life or life-threatening injuries.
- **High impact:** The failure has a severe or catastrophic impact that prevents the agency from performing one or more of its primary functions, or it causes major damage to assets, major financial loss, or severe injury to individuals that involves loss of life or life-threatening injuries.

The security category, or SC, is expressed by noting the impacts of failures in the three security properties. We express the SC in terms of a particular type of information or system, indicated below by *name:*

**SC name = {(confidentiality, impact), (integrity, impact), (availability, impact)}**

Let us look at a more specific example.

> *Amalgamated Widget, called "Amawig" for short, is a major manufacturer. It relies primarily on third-party distributors to sell its products. While it has a website, the site's purpose is to inform shareholders and to encourage potential customers to visit distributors to buy the products. A customer looking for an Amawig product through a Web search will see numerous sites describing its products, most of which belong to product distributors or retail outlets.*

Amawig's website provides publicity to company products and describes the company in general. Everything it provides is public information. The website is not the only one that provides access to Amawig products. In fact, a potential customer needs to go to a distributor or retailer to buy products in any case. To assess the 3 security properties:

1. **Confidentiality:** Not applicable, since all information is public.
2. **Integrity:** Low, since a site outage will not prevent customer sales.
3. **Availability:** Also low, since a site outage doesn't prevent customer sales.

Here is the resulting SC:

**SC Amawig Website = {(confidentiality, NA), (integrity, Low), (availability, Low)}**

Not all websites pose such a small risk. Let us reconsider the risks after Amawig expands its business. As part of a new product introduction, Amawig has decided to offer the product directly to customers via a new website and not sell it through distributors. The new sales site represents the only way to purchase that product. After six months, the new product represents a small, but significant, source of revenue. We need to reassess the three security properties:

1. **Confidentiality:** Moderate, since the website handles some electronic payment information from customers.
2. **Integrity:** Moderate, since the website handles some electronic payment information from customers, it specifies product prices, and it directs product shipments.

3. **Availability:** Moderate, since an interruption would visibly affect sales, but would not cause long-term damage to the company.

Here is the SC for the new website:

> **SC Amawig Sales Website = {(confidentiality, Moderate), (integrity, Moderate), (availability, Moderate)}**

Many companies use a single organization to manage their websites, or they even host all of their Web presence on a single site. What is the SC of the resulting website, if we combine both of Amawig's sites? According to FIPS 199, we examine each security property for each website and choose the highest impact value for each, with NA being the lowest. Since the sales site has a higher impact in each property, the combined site's SC is the same as the sales site's SC.

We establish the SC as part of the first step of the Risk Management Framework. SP 800-53 identifies security controls required in response to different impact values. This provides a rule-based approach to risk management. In smaller-scale systems, the required controls may map directly to available technical measures provided by the system's vendor. In larger-scale systems, the mapping might not be so simple, and the required controls may reflect security requirements to be met by a cooperating set of technical measures.

## 1.2.1 The Proprietor's Risk Management Framework

The NIST's RMF is well-documented and organized, but it doesn't really apply to Alice's situation. As sole proprietor of her business, she directly receives the benefits and troubles arising from her security measures, or lack thereof. The PRMF provides a more detailed and personalized assessment process than RMF's rule-based framework.

In this chapter, we look at Step A of the PRMF: We establish Alice's system and security goals. This yields a list of security requirements, a list that is sometimes called a ***security policy***. Later, we look at the problem of matching controls to those requirements. We perform Step A in three general parts: identifying risks, assessing risks, and identifying requirements. The process unfolds in six steps, as shown in Figure 1.4.

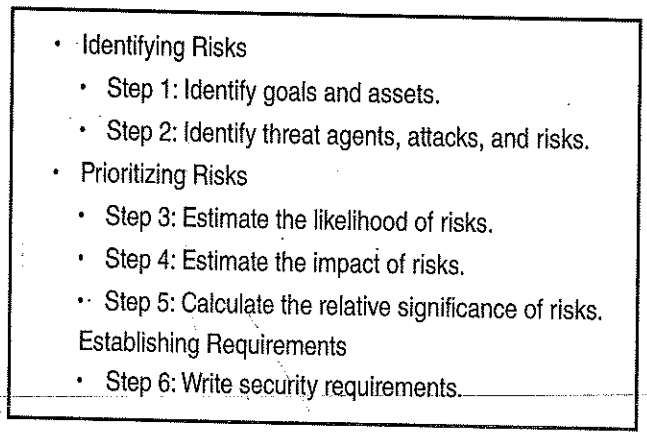


Figure 1.4

Details of PRMF Step A.

Cybersecurity risks can include a broad range of threats and potential events. In large-scale corporate or government environments, attacks can affect whole communities or regions. The RMF structures its risk assessment in those terms. If Alice's business fails, it will severely affect Alice and some of her business associates, but it shouldn't dislocate the area or regional economy. Alice needs to consider risks at a smaller scale than the RMF.

To identify Alice's risks, we look at her assets and threat agents. These reflect the potential attacks and defenses she will require. We produce our list of risks by studying these elements in the context of our assets and the boundaries we've built around them. Figure 1.5 illustrates the relationship of these elements.

Our first step is to identify the goals of the activity or enterprise that uses computing resources. These may be in terms of services rendered, things built and sold, transactions performed, and so on. These goals rely on particular computing assets, which may be computing equipment, data, or supported activities.

A ***threat agent*** is someone who is motivated to attack our assets. We don't identify threat agents by name; we identify them in terms of their behavior. Alice's shop faces two obvious threat agents: burglars and shoplifters. Shoplifters aren't likely to steal or damage Alice's computing assets, but a burglar could steal her equipment. Since Alice uses the Internet for online banking, merchandise ordering, and marketing, she also faces Internet-based threat agents.

An ***attack*** is an attempt by a threat agent to exploit the assets without permission. We call a threat agent an ***attacker*** when action replaces inclination and the attack actually takes place. If we have defined a security boundary, then an attack may be an attempt to breach the boundary. While thefts or acts of meddling may be attacks, we need to be more specific to perform a risk assessment. Typically, we identify attacks in terms of exploited vulnerabilities and broken defenses.

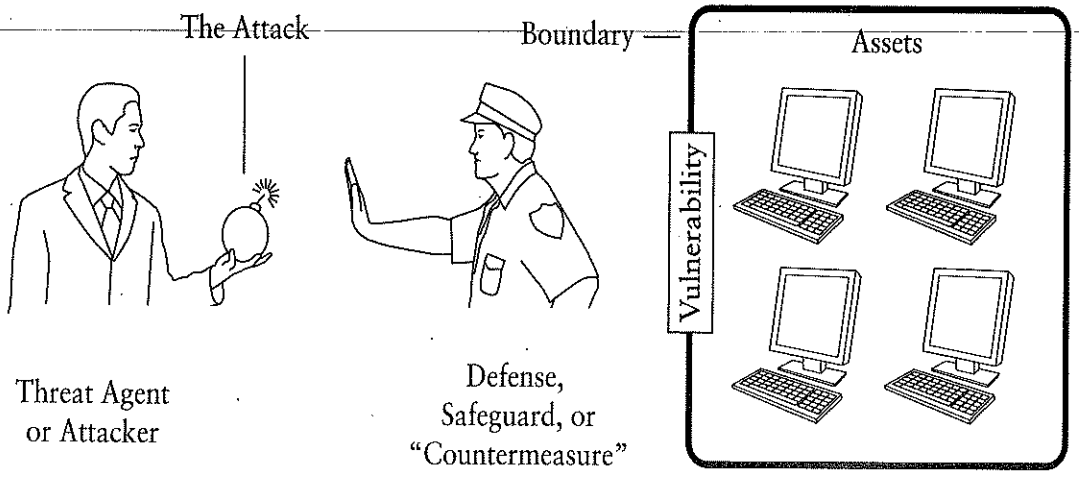


Figure 1.5

Elements of identifying risks.

A *vulnerability* is a weakness in the boundary that protects the assets from the threat agents. We often see this as an opening or other weakness in the boundary. For example, a door represents a vulnerability because it can admit thieves into Bob's suite.

A *defense,* safeguard, or countermeasure is a security measure intended to protect the asset. The boundary is the basic defense. Additional defenses often are associated with specific vulnerabilities. For example, a door lock is a defense intended to address the vulnerability posed by a door.

### Fine Points of Terminology

Threat agents and attackers both refer to people or other active entities; we distinguish them by what they *have* done, not what they might do. For example, Alice might think of customers in her store as threat agents: potential shoplifters. If a customer shoplifts, then the customer is in fact an attacker. A threat agent is a person who *might* attack our assets; an attacker *did* attack an asset.

A ***compromised system*** is one that is no longer safe to use following an attack. An attack may compromise a system by disabling security measures, which increases the risk of leaking confidential information. An attack may also install malware that bypasses security measures and allows the attacker to easily penetrate the system again or use it as a platform to attack other systems.

A ***botnet*** is a collection of compromised systems controlled remotely by the attacker. Botnets may contain thousands of computers. Each compromised system contains special software to allow the network's controller to give commands to the systems. Such systems often send the junk email we call "spam." By spreading the emails out among thousands of systems, the flood of email isn't detected as a flood.

## Hackers

The ***hacker*** has become an almost mythical figure in the computing community. The term originally arose in university research labs to refer to local experts with an almost uncanny understanding of computer systems. In the 1980s, the popular press used the term to identify people who attacked computers and other systems. A lexicon has developed to identify different people involved in attacking computer systems:

- **Script kiddy**—a person who uses an attack developed by another party to attack computers. The attack may be implemented using a "scripting language," so the attacker literally executes the script to attack the computer.
- **Cracker**—a person who has learned specific attacks on computer systems and can use those specific attacks. A cracker doesn't necessarily have the technical knowledge to modify the attacks and apply them to different types of targets.
- **Phone phreak**—a person who attacks telephone systems, usually to make long distance and international calls for free. John Draper (nicknamed "Captain Crunch") was a notorious phone phreak in the early 1970s.

- **Hacker**—a person with a high degree of knowledge and skill with computing systems, including the ability to attack them if so motivated. The term arose at Massachusetts Institute of Technology (MIT) in the 1950s and was applied to computer enthusiasts in the 1960s.
- **Black-hat hacker**—a person skilled in attacking computer systems, who uses those skills to attack a system. During the 1980s and 1990s, Kevin Mitnick became notorious for both phone phreaking and for computer break-ins. Following a prison term, Mitnick became a writer and consultant.
- **White-hat hacker**—a person skilled in attacking computer systems, who uses those skills as a security expert to help protect systems. Experts like Jeff Moss and Ray Kaplan have used their knowledge of hacking and the hacker community to bring such information to the security community.

Today, the term hacker is almost always used in the context of computer security, and the hacker is able to penetrate a system of interest. The term "black hat" or "white hat" indicates the hacker's motivation: whether he or she is inclined to attack or defend systems.

"Reformed" black-hat hackers pose a dilemma for the cybersecurity community. While their knowledge is often valuable, many companies will not hire a convicted felon to do security work, regardless of skill. There are a few well-known exceptions, including Mitnick and Frank Abagnale, the central character of the film *Catch Me if You Can* (2002).

## 1.2.2 Goals and Assets

When Alice hangs pictures in her store, she uses whatever hammer she finds in her toolbox. She's not especially aware of subtle differences between hammers and has no preference for one over another. Alice feels the same way about her computers. As long as they respond the way she expects, she doesn't care what she uses.

Alice's computers are not her only cyber assets. They probably aren't her most important cyber assets, since she can use substitute computers if necessary. Her principal cyber assets are the data files and services available through her computers. Even if Alice has insurance on her computers or can easily replace them some other way, she still needs her files, databases, and passwords.

### Identifying Goals

To identify assets, we first look at overall goals and objectives in a real-world context. Alice doesn't measure her store's success in terms of her computer's reliability. She measures it through customer visits, repeat visits, revenues, and profits.

To identify Alice's cyber risks, we first identify the cyber assets she uses to achieve those goals, directly or indirectly. The computer might not help her choose the item to show a particular customer, but it helps her stay in business and bring in items that will appeal to her customers. Her goals are to stay in business and offer appealing merchandise to her customers.

### Identifying Assets

Now that we have identified Alice's goals, we identify computing activities and resources that support those goals. We should strive for a complete list. If we omit any goals supported by her computer, then we won't identify risks associated with those goals. Here are examples of computing activities and resources to consider as Alice's assets:

- Computer hardware—naturally, each hardware item is itself an asset.
- Purchased software—each purchased software package can incur an expense if it is lost. At the least, it will cost Alice time to reinstall software if she must replace her computer hardware. There also may be extra purchase costs if the installation disks are lost.
- Operating system installation disk, if any
- Office software installation disk, if any
- Computer customization—it takes time to install and organize information on a computer in a way that works efficiently. Alice takes her desktop layout very seriously. This time must be spent if a computer is lost and replaced by a new one.
- Spreadsheets for tracking cash flow
- Online bank account and its credentials
- Online merchandise purchasing accounts and their credentials
- Social media accounts and their credentials

This list is sufficient for Alice's situation, even though the list is not necessarily complete. Every user needs to analyze goals individually or in terms of his or her organization. This asset list serves as an example.

## 1.2.3 Security Boundaries

Physical security is the foundation of all computer security. We need to keep our computing equipment physically protected from threat agents. If we can rely on the safety of the physical hardware, then we can focus our efforts on keeping the software secure. However, no amount of software security can redeem a system whose hardware has been compromised.

Boundaries are the essence of physical protection. A physical boundary establishes a container for our assets. We protect the assets from threat agents by denying them access to the container's contents. We measure the degree of protection by the strength of the boundary; we achieve strong protection if the boundary is very difficult to breach without permission.

### Least Privilege: A Second Basic Principle

Asset security depends on the people who can cross the boundary. In general, an asset is safer if we limit the number of people allowed inside its security boundary. If possible, we also restrict what each person may do to the asset. We call this ***Least Privilege***. We enforce Least Privilege when we give people as few privileges as possible regarding the assets we try to protect.

### Example: Boundaries in a Store

Figure 1.6 illustrates boundaries in and around Alice's Arts. While the front door is generally unlocked for customers, it forces them to pass near the sales counter when they enter or leave. Alice grants access to rooms inside the store as required by her customers or employees.

For example, Alice has given a set of keys to Nita, who works for her as a sales clerk. Nita is responsible for opening the store some mornings. Alice gave her a key to the front door and to the storage room in the back. These keys allow Nita to open the store and replenish items that are sold. Nita may even lock up the store if necessary while she runs an errand or is busy in the back. The keys do not unlock Alice's office. Nita is a trustworthy employee, but her job does not require access to Alice's office.

We'd like to exclude all threat agents from Alice's store, but there's no practical way to do that. While most customers are honest, a small number practice shoplifting. This is why Alice always has someone in the store while it is open and has placed the sales counter next to the door.

Boundary security has an obvious problem: Protecting the boundary is not the same as protecting the asset itself. Sometimes we can't help but grant access to a threat agent, regardless of how careful we might be. Nita herself may be a trustworthy employee, but Alice's next hire might not be. Alice keeps her computer locked in her office most of the time. She might move it out into the store when she is working there, but she always puts it away and locks it up if she's not in the store.

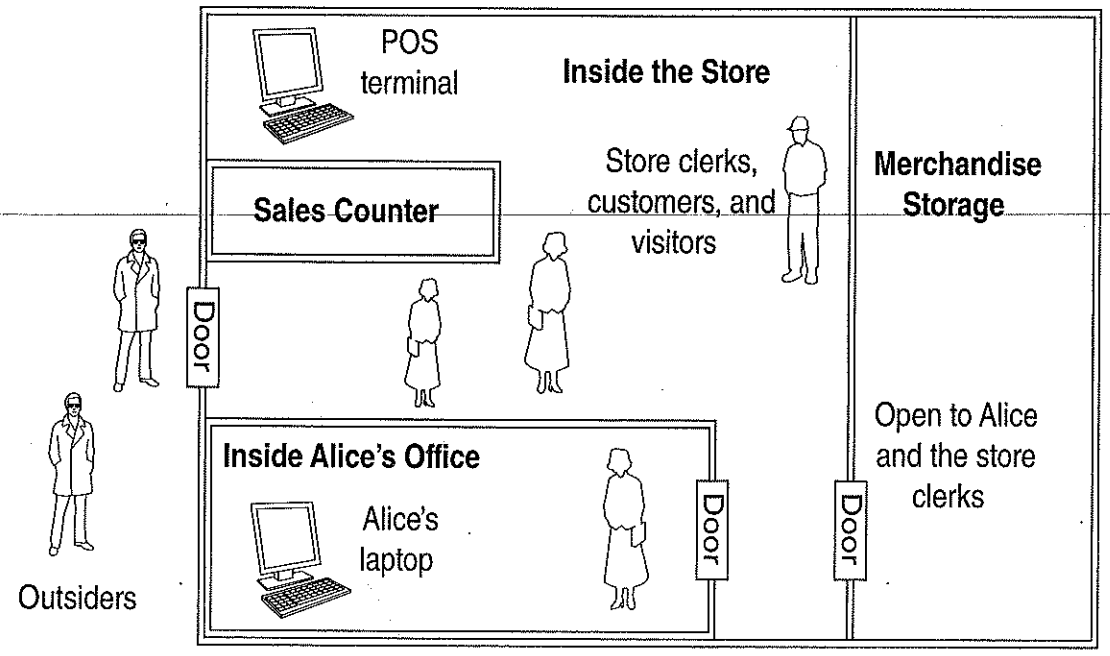


Figure 1.6

Physical boundaries in Alice's store.

### Analyzing the Boundary

Boundaries consist of two parts: the "walls" and the "doorways." The walls are fixed parts of the boundary that nobody can cross, not even those allowed inside. The doorways are the parts of the boundary that allow passage. The security challenge is to allow passage through the doors without letting any threat agents through. In computing, we often refer to the doorways as interfaces between the inside and the outside.

When analyzing security, a boundary poses four questions:

1. What must a threat agent do to breach a wall?
2. How do we control the doorways to exclude threat agents?
3. How can a threat agent pass through the doorway despite our protections?
4. We trust those we allow inside. Exactly what do we trust them to do—or not to do?

The point of the boundary is to keep the threat agents outside, away from our assets, and allow the trustworthy inside. The first question asks about the risk of breaching a wall. If it's practical for a threat agent to breach a wall, the risk assessment must include that risk in our assessment. In many cases, walls are strong enough not to be breached, and the risk is not important.

The second question asks how we control access to doorways. In a store, office, or home, the answer usually involves keys of some kind, either mechanical or electronic. In computing, we use special security controls built into our software. Our risk assessment identifies threat agents, and our security requirements identify whom we allow through the door. In Step B of the PRMF, our implementation shows *how* we control the door.

The third question considers the likelihood of an attacker breaking the access control or tricking it somehow. This leads to a trade-off between alternative security measures. A stronger or more sophisticated locking mechanism, or an armed guard, might further reduce the risk. The choice hinges whether the cost of an attack justifies the more expensive security measures.

### The Insider Threat

The fourth question asks about the ***insider threat***: What threat agents exist *inside* our security boundary? Although it is tempting to treat all threat agents as purely bad and anyone we trust as perfectly good, the world is not so simple. Some people are clearly threat agents in some cases but are trustworthy in others.

Alice must generally trust her clerks not to steal money from her. She can detect thefts from cash sales because her POS computer keeps track of the money collected. A clerk might steal cash one day and convince Alice that it was a mistake in making change, but large and repeated errors will cast suspicion on the clerk.

Like most stores, Alice's Arts has large glass windows and doors. A motivated burglar could definitely break some glass and steal some merchandise. Alice can't prevent such an attack, but she can detect it. She improves her security by installing an alarm to call for

help if a breach occurs. Alarms don't provide physical protection, but they pose a risk to the attacker: Can the attack succeed and the attacker withdraw to safety before someone answers the alarm? Many attackers rely heavily on stealth, and the alarm makes a stealthy attack less likely. The alarm might not deter all attackers, but it helps us recognize when attacks occur and helps motivate a rapid response.

## 1.2.4 Security Architecture

We often organize a security problem by defining boundaries and doorways in one sense or another. Alice uses with physical walls and doorways. Her "security architecture" consists of the security measures she applied and how they interact.

When we write a computer program, we establish boundaries when we put different functions into different procedures and files. We create doorways when we provide functions that different procedures may use. These decisions establish the structure of the program.

When we establish boundaries and doorways to address an information security problem, we produce an ***information security architecture***. Such an architecture often relies on boundaries *inside* the computer to protect important information and programs from error-prone or malicious programs.

Within a security architecture, we often find separate ***security domains***. Each domain is a place marked by security boundaries; each domain has its own set of security expectations. For example, if Alice's store is inside a shopping mall, then the separate stores represent different security domains. Alice's access rights to her own store do not grant her access rights to other stores. Each store has its own security expectations.

Separate domains may each require a separate security architecture. Each domain has its objectives and assets. Each domain has its policy for protecting and restricting actions. Each domain has its own trade-off to choose security over potential risk.

A ***security plan*** is a security architecture study that focuses on security requirements and implementation. The plan identifies appropriate security measures to protect against an identified set of security risks. The plan guides the builders to produce a secure system. Structurally, the plan focuses on security requirements and security controls. An effective plan includes security monitoring in its requirements and controls.

### Defense In Depth: A Third Basic Principle

Alice's store opens directly onto a public street. A burglar who breaches the front door has unfettered access to her merchandise. Alice's store might be safer as part of an enclosed shopping mall. The mall is closed to the public when the stores are closed. A burglar would then have to penetrate two separate, locked doors to reach Alice's merchandise. This makes the burglary more challenging and Alice's store less of a target.

Alice provides the best security for her mall store if she puts her own strong lock on the store's entrance. The store is Alice's own security domain. The mall's public area is another security domain. The mall managers keep the public area locked after hours and provide keys to store personnel. Alice can reach her store even after hours, and she can keep it locked against dishonest people working in other stores.

This provides *Defense in Depth* because Alice's store sits behind multiple security mechanisms. We also use the term *layered defense* because the separate security domains provide separate layers of protection. The innermost domain has the most restricted access, surrounded by another domain with less restriction, but that still enforces *some* access restriction.

To achieve genuine depth or layering, the access points or doorways must use truly independent security mechanisms. For example, some malls provide all the locks and keys for the stores. The locks are coordinated so that a special "master key" can open any door in the mall. The master key eliminates the separate security domains, undoing Defense in Depth.

## 1.3 Identifying Risks

To identify risks we look at threat agents and attacks: who attacks our assets and how the attacks might take place. We might also have information about vulnerabilities and defenses, but for now we only use it as extra information to help identify plausible attacks. For example, we might keep valuable articles in a room, like an office or storage locker. We need to identify threat agents and attacks that affect the assets stored in that room.

Based on news reports, stories, and personal experience, most of us should be able to identify threat agents and attacks. Here are examples of threat agents, attacks, and risks associated with a store's computer equipment:

- **Threat Agents**—thieves and vandals
- **Attacks**—theft, destruction, or damage associated with a break-in
- **Risks**—computer equipment stolen or damaged by thieves or vandals

If the assets are really valuable or an attack can cause really serious damage, then it's worthwhile to list every possible threat agent and attack. For example, banks analyze the risk of attacks through vault walls because their assets are quite valuable and portable. We decide whether to consider a particular type of attack, like those through walls, by looking at the rewards the attacker reaps with a difficult or unusual attack. The more difficult attacks may be less likely, so we balance the likelihood against the potential loss.

We develop the list of risks in three steps. First, we identify threat agents by identifying types of people who might want to attack our assets. Second, we identify the types of attacks threat agents might perform. Third, we build a ***risk matrix*** to identify the attacks on specific assets.

### Example: Risks To Alice's Arts

The rest of this chapter will use Alice's Arts as an example. We will perform the rest of PRMF Step A using Alice's list of assets developed in Section 1.2.2. The remainder of this section develops Alice's list of risks.

### 1.3.1 Threat Agents

We start our risk assessment by asking, "Who threatens our assets?" We might not be able to identify specific individuals, but we can usually identify categories of people. Those are our threat agents.

Natural disasters represent a well-known, nonhuman threat agent. Tornados, hurricanes, and other major storms can damage communications and power infrastructures. Major storms, like Katrina in 2005 and Sandy in 2012, destroyed communities and small businesses.

Other threat agents arise because some people act maliciously. We categorize such agents according to their likely acts and motivation: What might they do and why? For example, a thief will physically steal things and is probably motivated by a need for cash or possessions.

If our assets really face no threats from human threat agents, then our risk assessment is simple: We face nothing but natural disasters. In practice, even the smallest computer today is a target. Botnet operators happily collect ancient, underpowered desktops running obsolete software because they can exploit those computers.

Alice and her store face risks from specific threat agents. Someone might want to steal her computer or steal money from her online accounts. A competitor might want to interfere with her publicity on social media. Shoplifters and burglars also want to steal from her shop. Even her clerks might be tempted to steal. Petty thefts could put her out of business if they happen often enough. Door locks and a loud alarm may help protect her store when closed. Door locks on Alice's office area and her storage area may discourage her less-trustworthy clerks.

#### Identifying Threat Agents

We identify Alice's threat agents as a first step to identifying her risks. To identify human threat agents, we think about people in terms of their interest in attacking our assets (stealing, abusing, damaging, and so on). We don't try to profile a particular person like Jesse James or John Dillinger. Instead, we try to capture a particular motivation. Criminal threat agents won't hesitate to do us harm for their own benefit. Our friends and family, however, may be threat agents even if they aren't intending to harm us. A friend could accidentally do us a lot of harm when using an unprotected computer.

A threat agent list starts with classic threat agents, like thieves or vandals, and grows to incorporate stories we've heard in the news, from other people, or other sources. Here are features of a human threat agent:

- **Driven by a specific mission and/or specific goals**—The mission may be to make money, make news, or achieve some ideological victory. Revolutionary threat agents may seek a government overthrow, and your enterprise might be one of their perceived stepping-stones.
- **Interested in your assets and/or activities**—If your assets or activities can be exploited to forward the threat agent's mission or goals, then you are a possible target. Any computer on the Internet represents a potential asset in the cyber

underground, either to operate as part of a botnet or to be mined for sensitive data, like bank account passwords. A hotel, restaurant, or shop could be a terrorist target if it serves a person associated with, or who resides near, an important objective.

- **Has a distinct level of motivation**—When we look at lesser threat agents like friends, family members, colleagues, and employees, this balances their trustworthiness against their motivation to benefit at your expense. When we look at more significant threat agents, like criminal organizations, this notes whether or not agents stop short of taking human lives or causing similar levels of mayhem.
- **Has an established modus operandi (MO) at some level**—Different threat agents have different resources in terms of money, mobility, equipment, and manpower. This leads them to focus on particular types of attacks. Bank thieves and politically motivated terrorists may use guns and bombs, while botnet builders rely primarily on network-based attacks. Financially motivated agents always work in conjunction with a money stream.
- **Makes strategic decisions based on costs and benefits**—The difference between a benign and serious threat agent is whether or not the agent can leverage your enterprise in a practical manner. Innovative attacks are in fact rare; most threat agents prefer tried-and-true methods.

Here are categories of typical threat agents at the time of this book's publication:

- **Individual and petty criminals**—often individuals, and occasionally small groups, whose MO opportunistically targets vulnerable individuals or assets.
  - Petty thieves
  - Petty vandals
  - Con artists that prey on individuals or small businesses
  - Identity thieves that prey on individuals
  - Mass murderers
- **Criminal organizations**—an organized group that performs a coordinated criminal or terrorist activity.
  - Geographically limited examples include gangs or organized crime in a city or neighborhood.
  - Larger-scale organizations include drug cartels.
  - Terrorist groups may include groups like Al Qaeda that execute strategic gestures or localized militant groups like Al-Shabaab.

Cyber-criminal teams may reside in multiple countries and rely on others to convert stolen information into cash. Different teams may specialize in particular aspects of the crime. Here are examples:

- Collecting exploits and incorporating them into malware to use in a criminal activity—Malware authors often rent their creations to other teams for actual use. The alleged developer of the "Blackhole" exploit kit, a 27-year-old Russian, earned as much as $50,000 a month from renting the kit to other cyber criminals.

- Collecting databases of user information and offering them for sale—There are underground marketplaces that sell such information. After data breaches at Target Corporation in 2013, batches of cards were sold on an underground market for as much as $135 a card.
- Botnet herders—Each botnet is often subverted by similar malware, and each net is generally controlled by a particular individual or team. The botnet herder is in charge of the botnet. A herder may offer access to the botnet to other cyber criminals through underground marketplaces.
- Money-mule networks—When an attack manages to transfer money to a bank account somewhere, the money must be quickly converted to cash before the transfer can be reversed and the account closed. The money mule is a person who receives the money transfer, converts it to cash, and wires it to an accomplice in another country.

While some of these may be geographically limited, cybercrime organizations often span multiple countries. Many focus on specific parts of the operation, like exploit development, exploit tools, botnet management, login data collection, personal data collection, or conversion to cash through money mules. Here are some examples:

- **Hacktivists**—These threat agents are usually a loosely organized source of widespread attacks. Selected targets often reflect outrage at a political, social, or cultural phenomenon. The hacktivist group Anonymous, for example, has attacked Internet sites associated with copyright enforcement, fringe pornography, and Wall Street.
- **Nation-level competitors**—These threat agents serve to forward the interests of particular nations. These can include:
  - **Intelligence agents:** these are the traditional "spies," people who collect information on the behalf of competing countries.
  - **Technical collectors:** people and organizations who use remote sensing, surveillance, and intercepted communications to spy on other countries. The National Security Agency (NSA) intercepts communications on the behalf of the U.S. government.
  - **Military actors:** groups who use military force on behalf of a nation.
- **Business and personal associates**—People often interact with a broad range of others through their normal activities, and some of these people may be threat agents:
  - **Competitors:** people who are competing against us for some limited resource: a job, sales prospects, or other things.
  - **Suite/room/family/housemates:** people who share our living space.
  - **Malicious acquaintances:** people we know who would be willing to do us harm for their own benefit. This could include people who share our living space.
  - **Maintenance crew:** people who have physical access to our private living or working space. They might not usually intend to do us harm, but might do so if the benefit is large enough and the risk is small enough.

- **Administrators:** people who have administrative access to our computing resources. This may be limited to access to network resources or may include administrative access to our computer. As with maintenance people, administrators are rarely motivated to do harm to anyone in particular, but they might be tempted by easy prey.

- **Natural threats**—Actions of the natural environment may cause damage or loss, like severe weather or earthquakes.

A threat agent's level of motivation suggests the degree to which the agent is willing to do damage to achieve its goals. We use a five-level scale based on the risk levels in NIST's RMF:

- **Unmotivated**—not motivated to do harm.
- **Scant motivation**–limited skills and mild motivation—may exploit opportunities like unsecured doors, logged-in computers, or written-down passwords.
- **Stealth motivation**—skilled and motivated to exploit the system, but not to cause significant, visible damage. For example, a dishonest employee might steal small items from his or her employer's inventory if the item is hard to count accurately.
- **Low motivation**—will do harm that causes limited damage to assets. For example, a casual shoplifter rarely steals enough individually to put a store out of business.
- **Moderate motivation**—will do harm that causes significant damage to an enterprise or its assets, or injures a person, but does not cause critical injury. For example, a professional shoplifter could seriously hurt a store financially but would not threaten a clerk with a weapon.
- **High motivation**—will cause significant disruptions and even critical injuries to people to achieve objectives. This includes armed robbers, highly motivated terrorists, and suicide bombers.

In her quiet neighborhood, Alice is unlikely to encounter armed robbers, although any storekeeper might want to plan for that threat. Casual thieves and professional shoplifters pose the more likely threat. Depending on her situation, she may face threats with stealth motivation.

### Profiling A Threat Agent

An accurate risk assessment requires up-to-date profiles of the relevant threat agents. An up-to-date profile will always carry more accurate information than a textbook. The threat agents Alice probably faces might not change enough to affect her security strategy, but threat agents working against larger enterprises are always developing new techniques. Threat agent profiling becomes part of the risk assessment process.

We profile threat agents by studying their recent behavior. The threat agents worth studying have earned coverage in the public media. Large-scale news outlets cover some threat agents, while others are covered by industry-specific or technology-specific bloggers. Brian Krebs is one of several bloggers on computer security incidents, especially those involving malware or multinational cybercrime organizations. The Internet Storm

Center, Peter Neumann's Risks List, and Bruce Schneier's Cryptogram also serve as important resources for recent reports of cybersecurity incidents.

We use these sources to develop our profile of specific threat agents. A well-developed profile relies on data reported by one or more reliable sources. The profile describes four major elements of the threat agent:

1. **Goals:** Does the threat agent seek news coverage, financial gain, an ideological victory, or government overthrow? Financial goals are often achieved with less impact on the target than other goals.
2. **Typical MO:** Does the threat agent use physical attacks or cyberattacks; does the agent coordinate attacks somehow; does the agent kill people; will the agent be sacrificed? Modes of operation should also illustrate the leadership and command structure of the organization.
3. **Level of motivation:** How much harm is an agent willing to do to achieve its goals?
4. **Capabilities and logistical constraints:** How do financial costs, number of people, geographical limitations, operational complexity, or a need for special material or training affect the agent's choice of activities? Governmental actors and well-funded multinational enterprises may have significant capabilities.

The risk assessment for a large-scale system may require detailed profiles of the threat agents. Available time and resources may be the only limit on the content and level of detail. In other cases, the profiles simply highlight the threat agents' principal features. Organize a basic profile of a threat agent as follows:

- **Title**—Use a recognizable phrase to identify the threat agent.
- **Overview**—In one to two paragraphs, identify the threat agent in terms of newsworthy events and activities associated with that agent. The overview should identify specific examples of actions by that threat agent.
- **Goals**—In one paragraph, describe the goals of the threat agent. Illustrate this with specific examples from reports of the agent's activities.
- **Mode of operation**—In one paragraph, describe how the threat agent seems to choose targets and how operations are led. Add an additional paragraph to describe each specific type of operation the agent has used. Illustrate with specific examples from reliable sources.
- **Level of motivation**—Use the six-level scale described earlier to specify the level of motivation. Write a paragraph that gives examples of meeting that level of motivation. If the agent is motivated at a less than "high" level, try to show the agent avoiding higher degrees of damage.
- **Capabilities and constraints**—Describe the threat agent's logistical capabilities in one to three paragraphs. Use specific examples from reports to illustrate these capabilities.
- **References:**—Include the sources used to produce this profile. We want the highest-quality information we can find.

The best sources are primary sources: a writing of the author's own observations and experiences. A story from a large news outlet might say, "Cybersecurity experts uncovered a flaw in SSL." This is not a primary source. To use the primary source we must find out who the cybersecurity experts were and what they actually said.

In practice, we will use a lot of secondary sources. When a blogger describes a visit to a malicious website, we rely on the blogger's reputation for describing such things accurately. Malicious websites rarely persist for long, and responsible bloggers avoid publishing malware links. Vendor documentation is an authoritative source, even if it isn't a primary source.

A report in a newsletter or news outlet will usually identify its sources. When we track down such a source, we should find a report by someone who was closer to the actual event. Proximity should reduce errors in reporting. Wikipedia, on the other hand, makes a virtue of never being a primary source. At best, we might find decent sources in the article's list of references.

**Anonymous: A Sample Profile**

**Title:** Anonymous: A Hacktivist Group

*Overview*

While the name "Anonymous" has resonated in the Internet culture for decades, it became associated with a specific, if loosely coordinated, team of hacktivists in 2008. The group began a series of attacks on the Church of Scientology, targeting its fax machines and Internet servers. The attacks were coordinated using social media. In 2010, the group started attacking organizations associated with copyright enforcement, including the Recording Industry Association of America (RIAA) and the Motion Picture Association of America (MPAA). Later that year, attacks were expanded to include organizations that moved against Wikileaks following its publication of sensitive U.S. diplomatic cables. Members of Anonymous coordinated later attacks to support the Arab Spring, Occupy Wall Street, and gay rights.

*Goals*

Members of Anonymous try to suppress certain types of Internet behavior, many of which are also forms of suppression. The first attacks were retaliation for suppressing the distribution of certain videos by the Church of Scientology. Later attacks were against copyright enforcement groups (RIAA and MPAA) and child pornography sites. More recent attacks were against groups seen to oppose particular political movements, including the Arab Spring, Occupy Wall Street, and Wikileaks. The basic goal of an attack is to punish an organization for its behavior. A successful attack disrupts the organization enough to draw public attention to the attack.

*Mode of Operation*

Members of Anonymous deliberately eschewed hierarchies and leaders. The group used the "Internet relay chat" system, a primitive example of social media, to discuss issues of concern, identify targets, and propose acts of protest. Some participants stood in picket

lines or published protest pieces while others took action in the cyber domain. The group's large-scale actions were intended to arise from numerous individual actions.

For example, the attack on the Church of Scientology started with dozens of people sending faxes and hundreds of others transmitting thousands of Internet messages. In both cases, the flood used up supplies and temporarily overloaded equipment. As the disruption drew attention, it also drew additional participants. Subsequent operations used variants of the flooding attack.

*Level of Motivation: High Motivation*

As an organization, Anonymous strove to seriously disrupt totalitarian Arab regimes in Tunisia and Egypt. Their intent was to support the political unrest already brewing in the Arab Spring. Attacks on totalitarian rulers can easily involve loss of life on the part of participants, if not the targets. Many participants may have been driven by stealth motivation, but enough were highly motivated to pursue dangerous objectives.

*Capabilities and Constraints*

Successful actions relied on a large and willing community of participants. The size and enthusiasm of the community has varied over time. Moreover, attacks associated with Anonymous haven't required sophisticated technical skills. While this has left participation open to a larger, less-sophisticated community, it has also lured members into mass actions whose scale has caused damage and led to legal action. Investigators identified some participants and pursued criminal charges against them. In late 2009, a participant in the Scientology flooding attack was convicted under a U.S. computer crime law. While several more sophisticated attacks have been associated with Anonymous, they might be more accurately associated with similar but separate offshoots, like the group Lulzsec.

## References

Gabriella Coleman, "Anonymous: From the Lulz to Collective Action." Part of the "Politics in the Age of Secrecy and Transparency" Cluster (edited by Gabriella Coleman). *The New Everyday* (March 2011).

Nic Corbett, "Verona Man Admits Role in Attack on Church of Scientology's Websites," *New Jersey Star-Ledger*, Nov 17, 2009.

Quinn Norton, "2011: The Year Anonymous Took On Cops, Dictators and Existential Dread," Wired.com, Jan 11 2012.

## 1.3.2 Potential Attacks

We review threat agents to confirm that our assets are at risk and to identify their modes of operation. Next, we identify potential attacks that could use those modes of operation. We start with broad categories of attacks. Our basic categories arise from the CIA properties: What attacks arise when those properties fail?

- **Disclosure**—data that should be kept confidential is disclosed.
- **Subversion**—software has been damaged, or at least modified; injuring system behavior.

- Denial of service (DOS)—the use of computing data or services is lost temporarily or permanently, without damage to the physical hardware.

System subversion captures the essence of an integrity attack, but we also identify two other integrity attacks: forgery and masquerade. In *forgery,* the attacker constructs or modifies a message that directs the computer's behavior. In a *masquerade,* the attacker takes on the identity of a legitimate computer user, and the computer treats the attacker's behavior as if performed by the user.

Denial of service often arises from flooding attacks like those practiced by Anonymous against its targets. The system usually returns to normal service after a typical attack ends—not always, though. Fax attacks on the Church of Scientology intentionally used up fax paper and ink to make the machines unusable for a longer period. There are also "lockout" attacks in which the attacker triggers an intrusion defense that also blocks access by the target's system administrators.

Physical theft or damage poses the ultimate denial of service attack. Its physical nature gives it different properties from cyber-based DOS attacks. It requires different defenses. We treat it as a separate type of attack. Figure 1.7 summarizes our list of basic attacks.

We also distinguish between passive and active attacks. A ***passive attack*** simply collects information without modifying the cyber system under attack. Disclosure is the classic passive attack. An ***active attack*** either injects new information into the system or modifies information already there.

### The Attack Matrix

In a simple risk analysis, we can use the six general attack types and construct the risk matrix, described in the next section. If we need a more detailed analysis, we build an

- *Physical theft*— the computing resource itself is physically removed.
- *Denial of service (DOS)*— the use of computing data or services is lost temporarily or permanently, without damage to the physical hardware.
- *Subversion* — a program is modified to operate on the behalf of a threat agent.
- *Masquerade* — a person takes on the identity of another when using a computer.
- *Disclosure* — data that should be kept confidential is disclosed. This is the classic *passive* attack.
- *Forgery* — someone composes a bogus message and sends it to a computer. For example, a bogus order sends merchandise to the wrong recipient.

Figure 1.7

General types of attacks on information.

*attack matrix*. This yields a more specific set of attacks tied to our particular threat agents. The matrix lists threat agents along one axis and the general types of attacks on the other axis. For each agent and general attack, we try to identify more specific attacks that apply to our cyber assets.

Here is a list of Alice's threat agents, focusing on cyber threats:

- **Shoplifters**—people who visit her store and prefer to steal merchandise instead of paying for it. These are often crimes of opportunity and aren't intended to raise Alice's attention.
- **Malicious employees**—most employees she hires will probably be honest, but Alice has to anticipate the worst. Like shoplifting, employee crimes are often crimes of opportunity and rely on not being detected.
- **Thieves**—unlike shoplifters, these crimes won't be overlooked. A thief might be an armed robber or a burglar. In either case, Alice will know that a theft has occurred.
- **Identity thieves**—for some thieves, it is enough to steal a legitimate name and associated identity data like birth date or Social Security number, even if Alice herself doesn't have any money.
- **Botnet operators**—every computer has some value to a botnet, so attackers are going to try to collect Alice's computers into their botnet.

We construct Alice's attack matrix below. We compare the generic list of attacks in Figure 1.7 to Alice's threat agents, and we produce a more specific list of possible attacks. We use a table to ensure that we cover all possibilities. On one axis we list the generic attacks, and on the other we list the threat agents. Then we fill in the plausible cyberattacks (Table 1.1).

To fill in the table, we look at what motivates the threat agents, compare that against types of attacks, and identify specific kinds of attacks those agents might

**TABLE 1.1 Attack matrix for Alice's Arts**

| Possible Attacks | Shoplifters | Malicious Employees | Property Thieves | Identity Thieves | Botnet Operators |
|---|---|---|---|---|---|
| Physical loss | Shoplifting | Shoplifting, Robbing the till | Burglary, Armed robbery | | |
| Denial of service | | | Files lost | | Computer crash |
| Disclosure | | | | Password theft | |
| Subversion | | | | | Back door |
| Masquerade | | Social forgery | | Identity theft | |
| Forgery | | Embezzlement | | Bogus purchase | |

perform. This yields 12 specific attacks on Alice's store. The following is a brief description of each:

1. **Burglary:** someone steals Alice's laptop, POS terminal, or other computing items, like program disks or her USB drive.
2. **Shoplifting:** a customer or malicious employee steals from Alice's store without being detected, usually stealing merchandise. Portable computing equipment could also be stolen.
3. **Robbing the till:** a malicious employee steals money from the cash drawer used to collect customer payments; this cash drawer is also called "the till."
4. **Embezzlement:** a malicious employee takes advantage of Alice's trust to steal in some other way. For example, an employee might produce a bogus bill for purchased supplies; when Alice pays it, the money really goes to the employee.
5. **Armed robbery:** the thief confronts Alice or an employee with a weapon and demands that she hand over cash and/or other store assets.
6. **Social forgery:** someone sends false messages and makes false electronic statements masquerading as Alice, and those statements cause her personal damage or embarrassment.
7. **Password theft:** someone steals Alice's password. Alice realizes the theft took place before the password is misused.
8. **Bogus purchase:** someone poses as Alice to make a purchase using a credit card or other electronic financial instrument.
9. **Identity theft:** someone poses as Alice in one or more major financial transactions, like applying for a loan or credit card.
10. **Back door:** someone installs backdoor software in Alice's computer so the computer may take part in a botnet.
11. **Computer crash:** someone installs software in Alice's computer that causes the computer to crash.
12. **Files lost:** someone removes, erases, or otherwise damages some of Alice's files, making those files unusable. This includes physical loss of the device storing the files.

The list of potential attacks must be realistic and relevant. There should be documented examples of each attack, and those examples should indicate the type of damage that occurs. We focus on relevant attacks by building our list from Alice's threat agents.

**Remember:** The attack matrix is *optional*. We need to create a reasonable list of attacks. We can often use the generic attacks listed in Figure 1.7 instead. The attack matrix is useful if we face rapidly changing threat agents or if we need a more detailed analysis.

### 1.3.3 Risk Matrix

A risk is a potential attack against an asset. A risk carries a likelihood of occurring and a cost if it does occur. We identify risks by combining the list of assets and the list of attacks.

We use the attacks identified earlier in this chapter to construct this list. This may be the generic list of six attacks from Figure 1.7 or it may be the output of the attack matrix in Table 1.1. The risk matrix is a table to associate specific attacks with assets. We mark each attack that applies to each asset.

The risk matrix helps us focus on relevant attacks and eliminate attacks that don't apply to our assets. For example, physical theft will apply to physical computing devices and to software that is installed on specific devices. Fraudulent transactions will apply to resources associated with those transactions, like the server providing the defrauded service, or the bank supporting the fraudulent financial transaction.

The risk matrix lets us look for patterns among assets and attacks. We combine assets or attacks when they apply to a single, measurable risk. Earlier in this chapter we identified a list of nine cyber assets used in Alice's Arts. We will combine some of them to simplify the matrix even further. This yields a list of six assets:

1. Computer hardware and software
2. Software recovery disks
3. Computer customization
4. Spreadsheets
5. Online business and credentials
6. Social media and credentials

The list distinguishes between these assets because they pose different security concerns. Computer hardware and software represent the working collection of cyber assets contained in Alice's laptop and POS terminal. The recovery disk, customization, and spreadsheets represent different elements of those assets:

- **Third-party software**—represented by the recovery disks
- **Site-specific configuration**—represented by Alice's computer customization. This includes the files she installed, how she arranged them, and how she organized her desktop.
- **Working files**—represented by Alice's spreadsheets

We use different tools and strategies to preserve and protect these different cyber resources. It's relatively straightforward to save working files on a backup device. Site-specific configuration poses a challenge: It often resides in system files that are hard to reliably copy and restore. Third-party software poses a different challenge: Commercial software vendors may make it difficult to save a working copy of their application programs to reduce losses from software piracy.

Table 1.2 shows the risk matrix. Alice bought all of her computer equipment off-the-shelf, so disclosure poses no risk. Her arrangement of files, desktop, and so on reflects similar choices by others and poses no disclosure risk. Her spreadsheets contain business details, including employee salaries, and it's best to keep such information confidential. A subversion attack on Alice specifically would target her computer hardware and software.

**TABLE 1.2 Risk matrix for Alice's Arts**

| Assets | Disclosure | Subversion | Forgery | Masquerade | DOS | Physical damage |
|---|---|---|---|---|---|---|
| Computer hardware and software | | ☑ | | | ☑ | ☑ |
| Recovery disks | | | | | | ☑ |
| Computer customization | | | | | | ☑ |
| Spreadsheets | ☑ | | | | ☑ | ☑ |
| Online business and credentials | ☑ | | ☑ | ☑ | ☑ | |
| Social media and credentials | ☑ | | ☑ | ☑ | ☑ | |

Alice's local assets suggest other risks we can omit. Subversion, forgery, or masquerade of recovery disks could happen, but it's unlikely given the threat agents. Software subversion is usually part of a remote hacker attack, especially in a small retail store, and recovery disks aren't remotely accessible. Since subversion is supposed to apply to Alice's executable software, it doesn't apply to the other assets. A malicious employee could attack her computer customization or spreadsheets, but it doesn't fit the typical objectives of employees' attacks. Employees are most likely to steal tangible things and try to leave no obvious evidence. Changes to Alice's spreadsheets or computer customization won't give money to an employee; when Alice detects it, it causes extra work and inconvenience.

Both physical damage and denial-of-service (DOS) attacks could prevent Alice from using cyber resources. Alice could face DOS attacks due to power failures or outages at her Internet service provider (ISP). These could be accidental or intentional, but in both cases she must address the risks. Physical attacks include storm damage, vandalism, and theft.

When we look at attacks related to Alice's online activities, we must keep our security boundary in mind. While some of Alice's assets reside online, we won't analyze those online systems. We will focus on risks she can address within her security boundary. Alice can't personally counteract a DOS attack against her online resources, but she can take the risk into account. For example, if her credit card processor is offline, can she still sell merchandise? If not, how much will she lose?

In a masquerade against Alice's online accounts, the attacker transmits forged messages as if she were Alice. This may arise from disclosure of Alice's credentials or from other weaknesses in the online site. While we can identify separate, specific attacks on Alice's online sites that involve only forgery or disclosure or masquerade, we will treat them as a single "identity theft" risk.

This analysis yields a list of 11 risks to Alice's assets:

1. Physical damage to computer hardware and software
2. Physical damage to recovery disks

3. Physical damage to computer customization
4. Physical damage to spreadsheets
5. Denial of service for online business and credentials
6. Denial of service for social media and credentials
7. Subversion of computer hardware and software
8. Denial of service by computer hardware and software
9. Disclosure of spreadsheets
10. Identity theft of online business and credentials
11. Identity theft of social media and credentials

## 1.4 Prioritizing Risks

Alice is lucky: Larger enterprises are faced with a lot more risks. A really long list poses a challenge: Can we address all risks; if not, which do we address first? Naturally, we want to protect against the next attack, whatever it might be. We can't predict the future, so we must make our best guess.

We can aid our decision making by analyzing the risks and estimating their relative significance. The estimate compares the risks' relative costs over time. We estimate the impact of the risk's occurrence. We then estimate how often the risk might occur. To illustrate, we first calculate the significance of a shoplifter stealing Alice's laptop. Then we apply the same approach to all eleven of Alice's risks.

We calculate the significance in terms of both cost and time. We may calculate cost in terms of money, labor hours, or any other convenient metric. We use dollars here. Alice's laptop cost $1,000, and we assume that it faces a likelihood of theft once a month. Over the course of a year, the relative significance is $12,000 per year. Here is the calculation:

**Impact × Likelihood = Relative Significance**

Once the numbers and calculations are filled in, we identify the biggest risks by looking for the highest relative significance. The most significant risks are the ones that require our greatest attention. If we can't afford to protect against everything, we focus on the most significant risks.

### Estimating the Frequency of Individual Risks

Pick a time period (a day, a month, a year) and then estimate how often each type of attack might occur. Be sure to use the same time period for each type of attack. Use fractions or decimals as needed; if we are counting events per year and something bad occurs every 5 years, we still need to consider the risk. Table 1.3 estimates the rate of occurrence of certain crimes.

| TABLE 1.3 Example of crime rates | |
|---|---|
| Attack | Rate/Month |
| Armed robbery | 0.067 |
| Burglary | 0.402 |
| Larceny theft/shoplift | 1.176 |
| Fraud | 0.211 |
| Identity Theft | 0.049 |

We will use the rates given in Table 1.3 to estimate the frequency. These rates are based on national crime statistics in the United States and are scaled for a small store like Alice's. Like all estimates based on past experience, they don't predict the future. They simply give us a way to estimate the relative likelihood of the events.

According to Table 1.1, three threat agents might physically steal things from Alice's store: shoplifters, malicious employees, and armed robbers. The laptop is probably less accessible to shoplifters than other merchandise, but we'll assume that Alice took no significant steps to protect it. Employees probably won't steal the laptop for several reasons. While robbery is a definite possibility, it is less likely than theft by a highly motivated shoplifter.

Typical retail businesses expect a three percent rate of loss due to theft, damage, and other causes. Using statistics about shoplifting and losses, we estimate Alice's store will host 40 people who shoplift during a typical month. Most of these people shoplift as a bizarre hobby or compulsion. A handful of these are "professional" shoplifters who steal merchandise as a business. At least one professional will probably visit her shop every month. Let us assume that only a professional shoplifter steals business equipment like Alice's laptop. If we extrapolate the professionals' visits over an entire year, the statistics estimate a likelihood of 14.5 visits a year.

### Estimating the Impact of Each Risk

If a particular attack occurs, how much will it cost Alice to recover from it? As noted earlier, our estimate must include replacement cost, labor costs, the cost of lost opportunities, money spent on alternatives, and so on. We can estimate loss either in monetary terms or in terms of the time required to recover. In this case, we will estimate in terms of recovery time: the number of days it takes Alice to recover from a particular attack.

The laptop costs $1,000. Alice also spends an additional $50 in labor to acquire the replacement and reinstall her files. The monthly impact of its theft is a $1,050 expense to Alice.

We can also estimate the impact entirely in terms of labor hours. For example, it might take Alice 40 hours to earn the money to replace the laptop. She takes an additional two hours to acquire the replacement and reinstall her files. The impact is 42 hours.

### Calculating the Relative Significance of Risks

Once we have filled in the attack likelihoods and impacts, we compute the significance by multiplying these values together. The biggest risks have the highest numerical significance. A high significance means that a disruption is likely and that it will affect Alice's store for a long time. Other disruptions may be likely, but the effects won't be as profound.

### Relative Significance of Risks to Alice's Arts

Here we take the list of risks stated earlier in this chapter and calculate their relative significance. Below we review each risk and establish how we estimate its significance. Unless otherwise stated, we use the crime rates from Table 1.3 and calculate the impact on a monthly basis. The computed results appear in Table 1.4.

- **Subversion of computer hardware and software**—A subversion attack generally arises from a worm or virus infestation. The subversion itself might not cause direct damage. The infested computer might run imperceptibly slower. The real damages may arise from stolen online credentials, which we consider in other attacks. We will estimate a labor cost of six hours to restore a subverted computer, at $25 an hour, and that it occurs once a year.
- **Denial of service by computer hardware and software**—A power failure will generally bring Alice's computers to a halt. Customers on the U.S. power grid experience a failure approximately once a year, and the average failure lasts about two hours. An unexpected power failure, or even a fluctuation, may also damage computer equipment. We might estimate an annual failure that takes the store's POS device offline for two hours. If we estimate a net income of $25 per hour from individual sales, a two-hour outage costs $50.
- **Identity theft of online business and credentials**—According to the U.S. Bureau of Justice Statistics in 2013, 50 percent of identity theft attacks cost the victim $100

**TABLE 1.4 Calculating the impact**

| Computing Asset | Attack | Impact | Likelihood | Significance |
|---|---|---|---|---|
| Computer hardware and software | Physical damage | $1,000.00 | 1.1700 | $1,170.00 |
| Recovery disks | Physical damage | $200.00 | 1.1700 | $234.00 |
| Spreadsheets | Physical damage | $75.00 | 1.1700 | $87.75 |
| Computer customization | Physical damage | $25.00 | 1.1700 | $29.25 |
| Computer hardware and software | Subversion | $150.00 | 0.0833 | $12.50 |
| Online business and credentials | Denial of service | $25.00 | 0.3333 | $8.33 |
| Online business and credentials | Identity theft | $100.00 | 0.0490 | $4.90 |
| Computer hardware and software | Denial of service | $50.00 | 0.0833 | $4.17 |
| Spreadsheets | Disclosure | $75.00 | 0.0208 | $1.56 |
| Social media and credentials | Identity theft | $50.00 | 0.0208 | $1.04 |
| Social media and credentials | Denial of service | $25.00 | 0.0208 | $0.52 |

or less, and most attacks were on higher-income households. Alice's Arts does not support a high-income household.

- **Disclosure of spreadsheets**—The spreadsheets are confidential primarily because they contain salary information for employees. This may be open knowledge in a small store. However, we need to estimate it, so we will estimate that such a disclosure causes an employee to quit once every four years. Alice spends 3 hours of labor to replace the employee.
- **Identity theft of social media and credentials**—It is hard to predict the impact of this attack. We will estimate that Alice spends 2 hours of labor recovering from it once every four years.
- **Denial of service for social media**—Aside from personal entertainment value, Alice relies on social media to keep in touch with her local customer base. Her social media "advertising" tries to encourage customers to advertise for her. From time to time she may be prevented for a few hours—or days—from keeping watch on the social media, because she is in a location without Internet support. It is difficult to estimate how this might affect Alice's sales. We will estimate that Alice spends one hour of labor recovering from it once every four years.

The analysis, as well as the calculation, highlights both the greater risks and the lesser risks. Physical damage is the most significant risk. Loss of access to social media is the lowest risk. We will omit social media DOS from Alice's risk list.

When we calculate risk in terms of money we get simple and impressive numbers. However, those results are often misleading. Numbers by themselves carry a lot of authority, especially when they represent money. *Do not be fooled.* There are two reasons these numbers are misleading.

First, the numbers are nothing more than estimates. They are useful when comparing one to another, but don't rely on them in an absolute sense. An actual loss over time could be significantly less—or more—than this estimate.

Second, this calculation assumes that the risks and the attack events are independent of one another. This is nonsense. Some types of attacks, if successful, may increase the likelihood of further attacks. For example, shoplifters will steal more from a store that doesn't try to catch shoplifters. A burglary that breaks open the shop door after hours may give others the opportunity to steal remaining goods.

Our intent is to compare risks. The numerical values provide gross comparisons, and it's best to pay the most attention to the largest differences. Relatively small differences may not be significant.

## 1.5 Drafting Security Requirements

Security requirements complete the first step of both NIST's Risk Management Framework and the simplified PRMF. The requirements describe what we want the security measures to do. The list of requirements is sometimes called the ***security policy***.

We draft the security requirements to address the risks we identified. We then select security measures to implement those requirements. The requirements identify in general *what we want* for security, while the implemented security controls identify specifically *what we get* for security. For example, a household's security requirement might say: "We admit only family, friends, and trusted maintenance people to our house." The implementation says: "We have a lock on the door, we keep it locked, and we open the door only to admit people we know."

The list of security risks, requirements, and controls form the security plan. We draft the security requirements based on our list of risks. We then design the security system by selecting controls to implement those requirements. Once our design is complete, we review it to ensure that it implements all of the requirements.

Sometimes it is hard to tell if a statement represents a requirement or control. As we make statements that describe our system, some statements are more general and others are more specific; the more specific statements represent *implementation*. Some statements "set the stage" for other statements; those preparatory statements represent *requirements*.

### Writing Security Requirements

A well-written set of security requirements contains a series of individual statements. Each statement represents a single requirement. A well-written requirement has these five properties:

1. Each statement is numbered. This allows us to cross-reference the requirement statements to features of our implementation. A complicated policy might use outline numbering so that statements are arranged into sections and subsections.
2. Each statement uses the word "shall." This is part of many standards for writing requirements. We omit "shall" only if the requirement is somehow optional. In our examples, however, we won't have optional statements.
3. There should be a way to test the implementation to determine whether the requirement is true. When we test our implementation, the policy provides a list of features we must test.
4. Each statement identifies which prioritized risks the statement is intended to address.
5. Whenever possible, we phrase the statements in a positive and specific sense. In other words, requirements should describe what the system *does*, instead of talking about what it *doesn't do*. Although a few requirements may require global quantifiers like *all* or *any*, we should produce as few such statements as possible. It is harder (and less certain) to test and verify negative or global requirements.

To develop our requirements, we start with our prioritized list of risks. For each risk, we identify security requirements that, if achieved, will minimize or eliminate the risk.

### 1.5.1 Analyzing Alice's Risks

Alice's policy evolves directly from the risks. We identify how each risk might occur and we choose a general strategy to defend against that risk. As we analyze these risks, we focus on risks to Alice's information; we don't address other risks that apply to her personally or to other possessions of hers. To analyze a risk, we review it against the threat agents behind the risk.

1. **Physical damage to computer hardware and software**

The computer hardware Alice owns is all more-or-less portable, and she could carry the equipment with her. We want to focus our analysis on Alice's Arts, so we will assume the equipment resides in the store.

We start by physically securing the premises: *(1) Alice's Arts shall be locked up when no store employees (including Alice) are present.* This provides basic protection. We can't protect against all possible burglaries, though, so we include a requirement to reduce the impact of a successful burglary: *(2) There shall be insurance on the store's contents to cover the risks of theft, fire, or natural disasters.*

A POS terminal generally serves two purposes: it keeps a record of sales, and it contains a physically secure cash box. A thief could simply run into the store, overpower the clerk, grab the terminal, and carry it away. This leads to the requirement: *(3) The POS terminal shall be physically secured to the sales counter.* A burglar with time to work could still dislodge the terminal and carry it away, but this slows the thief down and reduces chances of success.

When it records the store's sales, the POS terminal also keeps a running tally of the amount of cash in the drawer. Alice or a trustworthy manager can compare the cash in the drawer against what the POS terminal expects. This helps detect dishonest clerks. Alice or her manager can reset the POS terminal's running total when they add or remove cash from the drawer. Clerks aren't allowed to make such changes: *(4) Alice or her trusted manager shall be able to adjust the POS terminal configuration.* Cash stored in the POS terminal also poses a large security risk; since it isn't a cyber risk, we won't analyze it here.

Laptops are popular targets for thieves and shoplifters. Alice's laptop is for her exclusive use and she doesn't share it with her clerks. The next requirement protects it when Alice isn't in the store: *(5) Alice's laptop shall be locked in her office when Alice is not in the store.* This also protects the laptop from tampering by store clerks.

2. **Physical damage to recovery disks**

If Alice suffers a hardware failure or theft, she needs to reinstall software from recovery disks. The software vendor generally provides these disks. Some vendors charge money to replace a lost recovery disk; some may demand the original purchase price. Alice needs to keep the recovery disks in a safe place, along with other backup copies: *(6) Alice shall have a secure, fireproof location separate from Alice's Arts for storing copies of her software (her "backup location"). (7) Alice shall keep her software recovery disks in her backup location when they are not in use.*

3. **Physical damage to computer customization**

This also arises from hardware failure or theft, but Alice needs to take the time to save this data for later recovery: *(8) Alice shall keep an up-to-date backup of her computer configurations for the POS terminal and the laptop, stored at her backup location.*

4. **Physical damage to spreadsheets**

This is a variant of the previous one. Alice's configurations might not change very often, but working files will change quite often: *(9) Alice shall keep an up-to-date backup of her laptop's working files, stored at her backup location.*

5. **Denial of service for online business and credentials**

If Alice's ISP connection fails, or her power fails, or her credit card processor drops offline, she still needs to transact business. She can lose access to her other bank accounts, her merchandise ordering accounts, and other services, but she must still be able to sell merchandise: *(10) Alice shall provide her clerks with a sales process that works correctly even if credit card processing or her POS terminal is offline.* Alice will simply accept the risk of being offline temporarily, as far as it affects her ability to order more merchandise or do online banking.

6. **Subversion of computer hardware and software**

This is primarily a risk arising from the Internet: Alice's equipment might be infected by a worm or virus, or it may accidentally download malware when visiting a website. This risk is too complicated to fully address here, but we will address the basic problems. Computer worms propagate by exploiting vulnerabilities in system software, and worms are blocked when those vulnerabilities were patched: *(11) Computers shall regularly check for system security updates and install those updates.*

Second, we are all familiar with antivirus software. The software searches a computer for files or other indicators of malicious software and disables that software: *(12) Computers shall contain and use antivirus software.* Antivirus software needs to be kept up-to-date, and that is covered by the previous requirement.

7. **Denial of service by computer hardware and software**

This may be caused by power failures; we provide partial relief with an uninterruptable power supply (UPS), which provides a temporary battery backup: *(13) There shall be an uninterruptable power supply for the store's computers.* Other mishaps could wipe out Alice's working files or part of her computer configuration. Although she may be able to recover from this, the time involved and the likelihood of the risk makes this worth avoiding. We addressed this through our earlier backup requirements.

8. **Disclosure of spreadsheets**

While spreadsheet disclosure poses a minor threat, it is a good place to start securing Alice's laptop from prying eyes. Like most people today, Alice has countless passwords. The security plan will identify certain passwords that Alice should protect in particular: *(14) Alice shall protect her most important passwords (her "critical passwords") from disclosure. (15) Critical passwords shall be hard to guess. (16) Alice's laptop shall*

*require a critical password before granting access to its resources.* Requirement 15 isn't really a positive requirement and will be hard to validate.

There is another important aspect of password use: leaving a computer unattended while logged in. If Alice leaves a shared server connection active while on a lab computer and leaves that computer, even briefly, another student could use that connection to copy Alice's files. This yields another requirement: *(17) Alice shall not leave a computer unattended if it is logged in using a critical password.*

9. **Identity theft of online business and credentials**

Alice needs to avoid identity theft, even though the average loss is alleged to be small: *(18) Passwords to bank and merchant websites shall be treated as critical passwords.*

10. **Identity theft of social media and credentials**

Alice's information on the social website is protected by a password. The estimated loss to social masquerade is relatively small, but Alice has decided to avoid the risk: *(19) Social media passwords shall be treated as critical passwords.*

### The Requirements

Now that we have analyzed Alice's high-priority risks, we extract the requirements from our analysis. As we draft our requirements, we review them against our five rules. We also ensure that all risks are addressed by at least one requirement. The result appears in Table 1.5.

As the lists of risks and requirements get longer, it becomes more challenging to process and cross-reference this information in textual form. Engineers often use spreadsheets or databases to maintain such information. While some may use a package like FileMaker or Microsoft Access, there also are specialized packages for requirements management ("Rational Doors," for example).

## 1.5.2 Monitoring Security Measures

Security measures are not implemented in a vacuum. Often they are just a delaying tactic, something to slow the attacker down while raising the alarm. Sometimes they only provide indications that trouble occurred and a record of the harm.

There are several ways to keep track of what happens to a computer. Most operating systems provide "logging" or "security auditing" services that keep track of significant events. These logging services can keep very detailed records. Detailed logging takes extra time and storage. By default, most systems only record the most significant events. A typical log indicates when a user logs in or logs out, and when major administrative or application programs are used. They also record obvious security events, like bad password entries or attempts to retrieve protected files. File systems often record key events for each file, including the date and time of creation, the last time it was examined, and the last time it was modified.

Years ago, typical system administrators turned off logging mechanisms to save resources; a detailed log requires extra computing time to create and a lot of hard disk space for storage. Separately, most file systems keep track of which files have been

**TABLE 1.5 Security requirements for Alice's Arts**

| # | Requirement | Risks |
|---|---|---|
| 1 | Alice's Arts shall be locked up when no store employees (including Alice) are present. | 1 |
| 2 | There shall be insurance on the store's contents to cover the risks of theft, fire, or natural disasters. | 1 |
| 3 | The POS terminal shall be physically secured to the sales counter. | 1 |
| 4 | Alice or her trusted manager shall be able to adjust the POS terminal configuration. | 1 |
| 5 | Alice's laptop shall be locked in her office when Alice is not in the store. | 1 |
| 6 | Alice shall have a secure, fireproof location separate from Alice's Arts for storing copies of her software (her "backup location"). | 2, 3, 4, 7 |
| 7 | Alice shall keep her software recovery disks in her backup location when they are not in use. | 2, 7 |
| 8 | Alice shall keep an up-to-date backup of her computer configurations for the POS terminal and the laptop, stored at her backup location. | 3, 7 |
| 9 | Alice shall keep an up-to-date backup of her laptop's working files, stored at her backup location. | 4, 7 |
| 10 | Alice shall provide her clerks with a sales process that works correctly, even if credit card processing or her POS terminal is offline. | 5 |
| 11 | Computers shall regularly check for system security updates and install those updates. | 6 |
| 12 | Computers shall contain and use antivirus software. | 6 |
| 13 | There shall be an uninterruptable power supply for the store's computers. | 7 |
| 14 | Alice shall protect her most important passwords (her "critical passwords") from disclosure. | 8, 9, 10 |
| 15 | Critical passwords shall be hard to guess. | 8, 9, 10 |
| 16 | Alice's laptop shall require a critical password before granting access to its resources. | 8 |
| 17 | Alice shall not leave a computer unattended if it is logged in using a critical password. | 8, 9, 10 |
| 18 | Passwords to bank and merchant websites shall be treated as critical passwords. | 9 |
| 19 | Social media passwords shall be treated as critical passwords. | 10 |

modified, and users can often use this feature to identify recent changes. This does not always tell us the entire story.

**An Incident:** A team of consultants visited a smaller *Fortune* 500 company to help them establish a computer security program. The company had some protections installed by rule, but very little else. The IT manager described an incident that occurred the night before: A person had connected to the main server over the Internet and located "the big spreadsheet" used to track and control the company's financial status. The

spreadsheet included every possible operational detail, including salaries of all employees. The IT manager was unhappy because the visitor had changed the access permissions so that anyone in the company could read or write "the big spreadsheet" and, in particular, look at the salaries.

The consultant sighed and asked, "Can you tell me if the visitor, or anyone else, has also *modified* the spreadsheet?"

The IT manager gasped. If someone *had* modified the spreadsheet, there would be no way to tell which cells had been changed. The spreadsheet had thousands of cells.

The IT manager was monitoring the site's Internet connection, and the monitor detected the break-in. This wasn't sufficient to identify all of the damage done, but at least people were alerted to the problem.

## 1.6 Ethical Issues in Security Analysis

Security analysis exists to improve system security. Students of security analysis must ensure that they themselves do not pose a risk to the systems they review. When an organization requests a security assessment, the security analyst's situation is clear:

- The analyst needs written authorization from the organization to verify that the assessment should take place.
- The analyst should use the appropriate tools to perform the assessment.
- When finished, the analyst should collect the results and report them to the appropriate people in the organization.

The assessment results could pose a risk to the organization, so they are treated as confidential. The results are shared only with the appropriate people in the organization. The analyst is obligated to protect all working notes and ensure that information about the analysis doesn't leak to others. When finished, the analyst should securely erase all information not needed for business purposes and take strong measures to prevent any details from leaking to others.

### Laws, Regulations, and Codes of Conduct

The guidance provided here may be affected by local laws and regulations, or by obligations to employers or other secrecy agreements. Here is a brief review of other obligations that might affect the handling and disclosure of security vulnerabilities.

- **Legal restrictions**—There are "antihacking" laws in some jurisdictions. In the United States, the Digital Millennium Copyright Act (DMCA) outlaws "circumvention" of technical measures intended to protect copyrighted data, often called *digital rights management* (DRM) mechanisms. The DMCA can make it a crime to find a vulnerability in a DRM technique and publish it.
- **National security information**—If the vulnerability involves a "classified" system, then the information may fall under defense secrecy restrictions. People who

handle such information sign secrecy agreements; violating such an agreement could even be treated as criminal espionage.

- **Nondisclosure agreements**—Employees and people working with sensitive information on the behalf of various enterprises or other organizations often sign an agreement not to disclose information the enterprise considers sensitive. Violations may lead to lost jobs and even lawsuits.
- **Codes of conduct**—Many professional organizations or holders of professional certifications agree to a professional code of conduct. Violators may lose their certification or membership. In practice, however, such codes of conduct aren't used punitively but instead try to reinforce accepted standards of just and moral behavior.

Legal and ethical obligations may push a security practitioner both toward secrecy and toward disclosure. Professional standards and even laws recognize an obligation to protect the public from danger. An extreme case often arises in medical science: When people get sicker during a drug trial, is it caused by the tested drug or by something else? The researchers may be obliged to keep their research secret because of agreements with the drug company. On the other hand, the drug company may be legally and morally liable if people die because they weren't informed of this newly discovered risk.

### 1.6.1 Searching for Vulnerabilities

With practice, it becomes easy to identify security weaknesses in everyday life. One sees broken fences, broken locks, and other security measures that are easy to circumvent. Such observations are educational when studying security. However, these observations can pose risks both to the security analyst and to people affected by the vulnerabilities.

In general, an analyst does not pose a danger by passively observing things and making mental notes of vulnerabilities. The risks arise if the analyst makes a more overt search for vulnerabilities, like searching for unlocked homes by rattling doorknobs. Police officers and other licensed security officers might do this, but students and other civilians should not engage in suspicious behavior.

For example, there are security scanning tools that try to locate computers on a network. Some of these tools also check computers for well-known vulnerabilities. Most companies that provide computer or network services require their users and customers to comply with an ***acceptable use policy*** (or AUP). Most network AUPs forbid using such tools, just as some towns might have laws against "doorknob rattling." Moreover, some tools may have unfortunate side effects, like the one in this example.

> **An Incident:** A security analysis team was scanning a network. Part of the scan was interpreted as attempts to log in as an administrative user on the main server computer. The numerous failed logins caused the system to "lock out" the administrative user. The system had to be restarted to reestablish administrative control.

Overt and systematic security scanning should take place only when it has been explicitly authorized by those responsible for the system. It is not enough to be a professional with a feeling of responsibility for security and the expertise to perform the scan.

In 1993, Randall Schwartz, a respected programming consultant and author of several books on programming, was working for an Intel Corporation facility in Oregon. Schwartz claimed to be concerned about the quality of passwords being used at the site, particularly by managers. Without formal authorization, Schwartz made a copy of a password file and used a "password cracking" program to extract the passwords.

Cybersecurity can't flourish as a grassroots effort. If upper management doesn't want to address security issues, we won't gain their trust and support by locating and announcing existing security weaknesses. Not only does this increase risks by highlighting weaknesses, it also carries an implicit criticism of management priorities. Security improves when the appropriate managers and system administrators apply resources to improve it. We must keep this in mind when we take on roles as managers and administrators.

## 1.6.2 Sharing and Publishing Cyber Vulnerabilities

Vulnerabilities are not necessarily found by security analysts working on behalf of a site or vendor. Many are found through a form of "freelance" security testing. Many people have earned a few minutes of fame and publicity by finding a security vulnerability, reporting it publicly, and seeing the report repeated in the national news. Others have found ways to profit financially from vulnerabilities.

The cybercrime community promotes an active trade in vulnerability information and in software to exploit those vulnerabilities. The most prized is a *zero-day* vulnerability or other flaw: One that hasn't been reported to the software's vendor or to the general public. Victims can't protect themselves against zero-day attacks, since the attack is new and unknown. The NSA has contributed to this by collecting zero-day vulnerabilities itself—and keeping them secret—to use in its intelligence-gathering and cyber-warfare operations. This poses a national security dilemma if an attacker could use the same vulnerabilities against targets in the United States.

Cyber vulnerabilities became a public issue in the 1990s as new Internet users struggled to understand the technology's risks. Initially, vulnerability announcements appeared in email discussion groups catering to security experts. Several such groups arose in the early 1990s to discuss newly uncovered vulnerabilities in computer products and Internet software. Many participants in these discussions believed that "full disclosure" of security flaws would tend to improve software security over time. Computer product vendors did not necessarily patch security flaws quickly; in fact, some did not seem to fix such flaws at all. Some computing experts hoped that the bad publicity arising from vulnerability reports would force vendors to patch security flaws promptly.

By the late 1990s, the general public had come to rely heavily on personal computers and the Internet, and security vulnerabilities had become a serious problem. Reports of security vulnerabilities often were followed by Internet-borne attacks that exploited those new vulnerabilities. This called into question the practice of full disclosure. Today, the general practice is as follows:

- Upon finding a vulnerability in a product or system, the finder reports the vulnerability to the vendor or system owner. The finder should provide enough information to reproduce the problem.
- The vendor should acknowledge the report within 7 days and provide the finder with weekly updates until the vendor has resolved the problem.
- The vendor and the finder should jointly decide how to announce the vulnerability.
- If the vendor and finder cannot agree on the announcement, the finder will provide a general announcement 30 days after the vendor was informed. The announcement should notify customers that a vulnerability exists and, if possible, make recommendations on how to reduce the risk of attack. The announcement should *not* include details that allow an attacker to exploit the vulnerability. Some organizations that handle vulnerabilities wait 45 days before making a public announcement.
- Publication of the details of the vulnerability should be handled on a case-by-case basis.

Although many organizations recognize these guidelines, they are not the final word on vulnerability disclosure. At the Black Hat USA 2005 Briefings, a security conference, security researcher Michael Lynn described a vulnerability in Cisco's Internet ***router*** products. Routers provide the backbone for moving messages on the Internet; they provide the glue to connect local networks and long-distance networks into a single, global Internet.

Lynn did not provide the details of how the vulnerability worked, but he did demonstrate the vulnerability to the audience at the conference. Cisco had released a patch for the vulnerability four months earlier. However, Lynn's presentation still unleashed a furor, including court actions and restraining orders. As Lynn noted in his talk, many routers on the Internet still would contain the vulnerability if their owners hadn't bothered to update the router software.

Although few student analysts are likely to uncover a vulnerability with widespread implications, many will undoubtedly identify weaknesses in systems they encounter every day. Students should be careful when discussing and documenting these perceived weaknesses.

Students who are analyzing systems for training and practice also should be careful. A student exercise that examines a real system could pose a risk if it falls into he wrong hands. Therefore, it is best to avoid discussing or sharing cybersecurity class work with others, except for fellow students in cybersecurity and the instructors.

Moreover, some countries and communities may have laws or other restrictions on handling security information. Be sure to comply with local laws and regulations. Even countries that otherwise guarantee free speech may have restrictions on sharing information about security weaknesses. In the United States, for example, the DMCA makes it illegal to distribute certain types of information on how to circumvent copyright protection mechanisms.

An ongoing discussion in the security community exists about whether, when, and how to announce security vulnerabilities. In the past, there was a tradition of openness and sharing in the Internet community that biased many experts toward full disclosure. Today, however, security experts tend to keep vulnerability details secret and, at most, share it with the owners of the vulnerable system. The challenge is to decide how much to tell, and when.

## 1.7 Resources

### IMPORTANT TERMS INTRODUCED

ACTIVE ATTACK
ADMINISTRATOR
ANTIVIRUS SOFTWARE
APP
ATTACK
ATTACK MATRIX
ATTACKER
AVAILABILITY
BACK DOOR
BACKUP COPY
BASIC PRINCIPLE
BLACK-HAT HACKER
BOTNET
CIA PROPERTIES
COMPROMISED SYSTEM
COMPUTER VIRUS
CONFIDENTIALITY
CONTINUOUS IMPROVEMENT
CRACKER
DEFENSE
DEFENSE IN DEPTH
DISCLOSURE
FORGERY
HACKER
HACKTIVIST
HIGH MOTIVATION
HUNTER'S DILEMMA
IDENTITY THEFT
INFORMATION SECURITY ARCHITECTURE
INSIDER THREAT
INTEGRITY
LAYERED DEFENSE
LEAST PRIVILEGE
LOW MOTIVATION
MALWARE
MASQUERADE
MODERATE MOTIVATION
PASSIVE ATTACK
PHONE PHREAK
RISK ASSESSMENT
RISK MATRIX
ROUTER
SCRIPT KIDDY
SECURITY CHECKLIST
SECURITY DOMAIN
SECURITY PLAN
SECURITY POLICY
SOCIAL FORGERY
STEALTH MOTIVATION
SUBVERSION
SYSTEMS ENGINEERING PROCESS
THREAT AGENT
UNMOTIVATED
VULNERABILITY
WHITE-HAT HACKER
WORM
ZERO-DAY

### ACRONYMS INTRODUCED (INCLUDING THE PREFACE)

ACM—Association for Computing Machinery
AUP—Acceptable use policy
CIA—Confidentiality, integrity, availability
CISSP—Certified information systems security professional
DMCA—Digital Millennium Copyright Act

DOS—Denial of service
DRM—Digital rights management
FIPS—Federal Information Processing Standard
ISP—Internet service provider
IT—Information technology
MIT—Massachusetts Institute of Technology
MO—Modus operandi
MPAA—Motion Picture Association of America
NIST—National Institute of Standards and Technology
NSA—National Security Agency
NA—Not applicable
PLC—Programmable logic controller
POS—Point of sale
PRMF—Proprietor's risk management framework
RIAA—Recording Industry Association of America
RMF—Risk management framework
SC—security category
SCADA—Supervisory control and data acquisition
SP—Special Publication
UK—United Kingdom
UPS—uninterruptable power supply
USB—Universal serial bus

## 1.7.1 Review Questions

R1. Describe the three strategies people often use to make security decisions.
R2. What is the hunter's dilemma?
R3. Explain the role of "reasoned paranoia" in the security process.
R4. Describe the six steps in NIST's risk management framework.
R5. Describe the four steps in the proprietor's risk management framework.
R6. How do the risk management frameworks compare to continuous quality improvement?
R7. What is the difference between *requirements* and *controls* in the security process?
R8. Describe the relationship between assets, boundaries, threat agents, vulnerabilities, attacks, and defenses.
R9. Identify some typical information assets.
R10. Explain the concept of Least Privilege.
R11. What are the four things to assess when looking at boundaries?
R12. Describe the three *security properties* of information (hint: "CIA").
R13. Explain the significant features we see in threat agents.
R14. Summarize the levels of motivation with which we assess threat agents.

R15. Describe the six general types of attacks on information. Which are passive attacks and which are active attacks?

R16. Explain the purpose and use of an attack matrix.

R17. Explain the purpose and use of a risk matrix.

R18. Explain the process for comparing the relative significance of different risks.

R19. List the five properties of a good security policy statement.

R20. Briefly describe the process for constructing a list of requirements from a list of assets, threat agents, and risks.

R21. Summarize the recommended ethical steps a security analyst takes when performing a security assessment.

R22. Summarize the recommended process for disclosing a security vulnerability.

## 1.7.2 Exercises

E2. Give examples of how individuals can act as vulnerabilities, defenses, or threats to an information system.

E3. Write a summary of how computers are used in your organization. The organization may be a particular portion of a larger site, like a school or college, or a department within the organization.

E4. Who do you call if something goes wrong with your computer? Provide contact information and a summary of which problems are covered by which contacts.

E5. Draw a diagram of the physical security boundary around your current living space. Identify possible points of entry. Describe how the physical boundary is kept secure if you are not present.

E6. Select a commercial space like a store or restaurant with which you are familiar. Draw a diagram of its physical security boundary. Identify possible points of entry or exit, including emergency exits. Describe the rules (the "policy") for opening, closing, and locking those entrances. Pay special attention to public, employee-only, and emergency exits, if any.

E8. Make a list of the really important tasks performed by your personal computer, as discussed in Section 1.2.2. If you do not own your own computer, describe one that you regularly use for class work. List the physical and information assets you rely upon to perform these tasks.

E9. Following the basic procedures described in Section 1.4, do a risk assessment of your own personal computer. Be sure to answer Exercise E8 first, and be sure that your risk assessment reflects your most important tasks and assets. Show the result as a list of risks.

| TABLE 1.6 Policy for Exercise E10 | | |
|---|---|---|
| # | Policy Statement | Risks |
| 1 | Bob is granted full access to all files on his computer. | 2 |
| 2 | Alice shall have full access to files she creates. | 2, 3 |
| 3 | Access shall never be granted to thieves. | 1 |
| 4 | Installation disks for proprietary software shall be kept in a locked drawer in Alice's room. | |
| 5 | The laptop shall regularly check for system security updates and install those updates. | |

E10. Table 1.6 lists five security policy statements. Compare the statements against the five properties of properly formed policy statements. For each statement, indicate which properties the statement fails to fulfill, if any.

E11. Write the first part of a security plan for your own cybersecurity assets or another small set of assets. The plan includes the following:

a. A list of security assets risks. This may reuse information produced in earlier assignments, as appropriate.

b. A list of security requirements for your assets.