CHAPTER

What is Information Security? 1

CHAPTER OUTLINE

The Basics of Information Security. DOI: http://dx.doi.org/10.1016/B978-0-12-800744-0.00001-4

INFORMATION IN THIS CHAPTER

- What is security?
- Models for discussing security issues
- Attacks
- Defense in depth

INTRODUCTION

Information security is a concept that becomes ever more enmeshed in many aspects of our society, largely as a result of our nearly ubiquitous adoption of computing technology. In our everyday lives, many of us work with computers for our employers, play on computers at home, go to school online, buy goods from merchants on the Internet, take our laptops to the coffee shop and check our e-mail, carry our smartphones on our hips and use them to check our bank balances, track our exercise with sensors in our shoes, and so on, ad infinitum.

Although this technology enables us to be more productive and allows us to access a host of information with only a click of the mouse, it also carries with it a host of security issues. If the information on the systems used by our employers or our banks becomes exposed to an attacker, the consequences can be dire indeed. We could suddenly find ourselves bereft of funds, as the contents of our bank account are transferred to a bank in another country in the middle of the night. Our company could lose millions of dollars, face legal prosecution, and suffer damage to its reputation because of a system configuration issue allowing an attacker to gain access to a database containing personally identifiable information (PII) or proprietary information. We see such examples appear in the media with disturbing regularity.

If we look back 30 years, such issues related to computer systems were nearly nonexistent, largely due to the low level of technology implementation and the few people who were using what was in place. Although technology changes at an increasingly rapid rate, and specific implementations arise on a seemingly daily

basis, much of the theory that discusses how we go about keeping ourselves secure changes at a much slower pace and does not always keep up with the changes to our technology. If we can gain a good understanding of the basics of information security, we are on a strong footing to cope with changes as they come along.

What is security?

Information security is defined as "*protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction*," according to US law [1]. In essence, it means we want to protect our data (whereever it is) and systems assets from those who would seek to misuse it.

In a general sense, security means protecting our assets. This may mean protecting them from attackers invading our networks, virus/worms, natural disasters, adverse environmental conditions, power failures, theft or vandalism, or other undesirable states. Ultimately, we will attempt to secure ourselves against the most likely forms of attack, to the best extent we reasonably can, given our environment.

When we look at what exactly it is that we secure, we may have a broad range of potential assets. We can consider physical items that we might want to secure, such as those of inherent value (e.g., gold bullion) or those that have value to our business (e.g., computing hardware). We may also have items of a more ethereal nature, such as software, source code, or data. In today's computing environment, we are likely to find that our logical assets are at least as valuable as, if not more than, our physical assets. Additionally, we must also protect the people who are involved in our operations. People are our single most valuable asset, as we cannot generally conduct business without them. We duplicate our physical and logical assets and keep backup copies of them elsewhere against catastrophe occurring, but without the skilled people to operate and maintain our environments, we will swiftly fail.

In our efforts to secure our assets, we must also consider the consequences of the security we choose to implement. There is a well-known quote that says, "The only truly secure system is one that is powered off, cast in a block of concrete and sealed in a lead-lined room with armed guards—and even then I have my doubts" [2]. Although we could certainly say that a system in such a state could be considered reasonably secure, it is surely not usable or productive. As we increase the level of security, we usually decrease the level of productivity. With the system mentioned in our quote, the level of security would be very high, but the level of productivity would be very near zero. The goal of a security plan is to find the balance between protection, usability, and cost.

Additionally, when securing an asset, system, or environment, we must also consider how the level of security relates to the value of the item being secured. We can, if we are willing to accommodate the decrease in performance, apply very high levels of security to every asset for which we are responsible. We can build a billion-dollar facility surrounded by razor wire fences and patrolled by armed guards and vicious attack dogs, and carefully place our asset in a hermetically

sealed vault inside . . . so that mom's chocolate chip cookie recipe will never come to harm, but that would not make much sense. In some environments, however, such security measures might not be enough. In any environment where we plan to put heightened levels of security in place, we also need to take into account the cost of replacing our assets if we do happen to lose them and make sure we establish reasonable levels of protection for their value. The cost of the security we put in place should never outstrip the value of what it is protecting.

When are we secure?

Defining the exact point at which we can be considered secure presents a bit of a challenge. Are we secure if our systems are properly patched? Are we secure if we use strong passwords? Are we secure if we are disconnected from the Internet entirely? From a certain point of view, all of these questions can be answered with a "no," so the real question is are we reasonably secure.

Even if our systems are properly patched, there will always be new attacks to which we are vulnerable. When strong passwords are in use, there will be other avenues that an attacker can exploit. When we are disconnected from the Internet, our systems can be physically accessed or stolen. In short, it is very difficult to define when we are truly secure. We can, however, turn the question around.

Defining when we are insecure is a much easier task, and we can quickly list a number of items that would put us in this state:

- Not patching our systems or not patching quickly enough
- Using weak passwords such as "password" or "12345678"
- Downloading infected programs from the Internet
- Opening dangerous e-mail attachments from unknown senders
- Using wireless networks without encryption that can be monitored by anyone

We could go on for some time creating such a list. The good thing is that once we are able to point out the areas in an environment that can cause it to be insecure, we can take steps to mitigate these issues. This problem is akin to cutting something in half over and over; there will always be some small portion left to cut again. Although we may never get to a state that we can definitively call "secure," we can take steps in the right direction.

Alert!

Compliance is a key aspect of any security program and should be coordinated across the organization. The bodies of law that define standards for security vary quite a bit from one industry to another and wildly from one country to another. Organizations that operate globally are very common at present, and we need to take care that we are not violating any such laws in the course of conducting business. We can see exactly such a case when we look at the differences in data

privacy laws between the United States and the European Union. When in doubt, consult legal counsel before acting.

Some bodies of law or regulations do make an attempt to define what secure is, or at least some of the steps we should take to be "secure enough." We have the Payment Card Industry Data Security Standard (PCI DSS) for companies that process credit card payments, the Health Insurance Portability and Accountability Act of 1996 (HIPAA) for organizations that handle health care and patient records, the Federal Information Security Management Act (FISMA) that defines security standards for many federal agencies in the United States, and a host of others. Whether these standards are effective or not is the source of much discussion, but following the security standards defined for the industry in which we are operating is generally considered to be advisable, if not mandated.

Models for discussing security

When we discuss security issues, it is often helpful to have a model or framework that we can use as a foundation or a baseline. This gives us a consistent set of terminology and concepts that we, as security professionals, can refer to when security issues arise.

The confidentiality, integrity, and availability triad

Three of the primary concepts in information security are confidentiality, integrity, and availability, commonly known as the confidentiality, integrity, and availability (CIA) triad, as shown in Figure 1.1. The CIA triad gives us a model by which we can think about and discuss security concepts, and tends to be very focused on security, as it pertains to data.

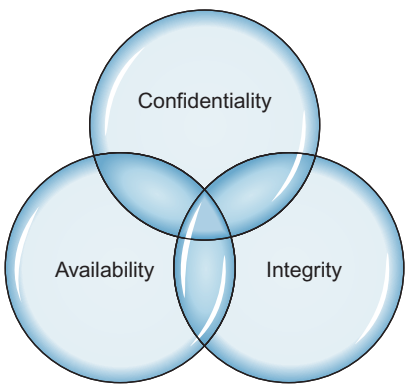

FIGURE 1.1

The CIA triad.

More advanced

The common notation for confidentiality, integrity, and availability is CIA. In certain materials, largely those developed by International Information Systems Security Certification Consortium (ISC^2) we may see this rearranged slightly as CAI where folks associate CIA with Central Intelligence Agency. No change to the concepts is implied in this rearrangement, but it can be confusing for those who do not know about it in advance. We may also see the CIA concepts expressed in their negative forms: disclosure, alteration, and denial (DAD).

Confidentiality

Confidentiality is a concept similar to, but not the same as, privacy. Confidentiality is a necessary component of privacy and refers to our ability to protect our data from those who are not authorized to view it. Confidentiality is a concept that may be implemented at many levels of a process.

As an example, if we consider the case of a person withdrawing money from an ATM, the person in question will likely seek to maintain the confidentiality of the personal identification number (PIN) that allows him, in combination with his ATM card, to draw funds from the ATM. Additionally, the owner of the ATM will hopefully maintain the confidentiality of the account number, balance, and any other information needed to communicate to the bank from which the funds are being drawn. The bank will maintain the confidentiality of the transaction with the ATM and the balance change in the account after the funds have been withdrawn. If at any point in the transaction confidentiality is compromised, the results could be bad for the individual, the owner of the ATM, and the bank, potentially resulting in what is known in the information security field as a breach.

Confidentiality can be compromised by the loss of a laptop containing data, a person looking over our shoulder while we type a password, an e-mail attachment being sent to the wrong person, an attacker penetrating our systems, or similar issues.

Integrity

Integrity refers to the ability to prevent our data from being changed in an unauthorized or undesirable manner. This could mean the unauthorized change or deletion of our data or portions of our data, or it could mean an authorized, but undesirable, change or deletion of our data. To maintain integrity, we not only need to have the means to prevent unauthorized changes to our data but also need the ability to reverse authorized changes that need to be undone.

We can see a good example of mechanisms that allow us to control integrity in the file systems of many modern operating systems such as Windows and Linux. For purposes of preventing unauthorized changes, such systems often implement permissions that restrict what actions an unauthorized user can perform on a given

file. Additionally, some such systems, and many applications, such as databases, can allow us to undo or roll back changes that are undesirable.

Integrity is particularly important when we are discussing the data that provides the foundation for other decisions. If an attacker were to alter the data that contained the results of medical tests, we might see the wrong treatment prescribed, potentially resulting in the death of the patient.

Availability

The final leg of the CIA triad is availability. Availability refers to the ability to access our data when we need it. Loss of availability can refer to a wide variety of breaks anywhere in the chain that allows us access to our data. Such issues can result from power loss, operating system or application problems, network attacks, compromise of a system, or other problems. When such issues are caused by an outside party, such as an attacker, they are commonly referred to as a denial of service (DoS) attack.

Relating the CIA triad to security

Given the elements of the CIA triad, we can begin to discuss security issues in a very specific fashion. As an example, we can look at a shipment of backup tapes on which we have the only existing, but unencrypted, copy of some of our sensitive data stored. If we were to lose the shipment in transit, we will have a security issue. From a confidentiality standpoint, we are likely to have a problem since our files were not encrypted. From an integrity standpoint, presuming that we were able to recover the tapes, we again have an issue due to the lack of encryption used on our files. If we recover the tapes and the unencrypted files were altered, this would not be immediately apparent to us. As for availability, we have an issue unless the tapes are recovered since we do not have a backup copy of the files.

Although we can describe the situation in this example with relative accuracy using the CIA triad, we might find that the model is more restrictive than what we need in order to describe the entire situation. An alternative model does exist that is somewhat more extensive.

The Parkerian hexad

The Parkerian hexad, named for Donn Parker and introduced in his book *Fighting Computer Crime*, provides us with a somewhat more complex variation of the classic CIA triad. Where the CIA triad consists of confidentiality, integrity, and availability, the Parkerian hexad consists of these three principles, as well as possession or control, authenticity, and utility [3], for a total of six principles, as shown in Figure 1.2.

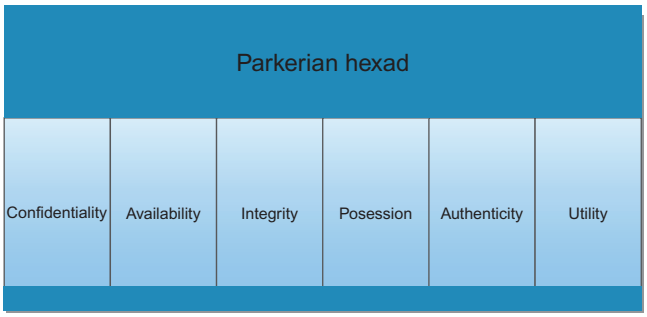

FIGURE 1.2

The Parkerian hexad.

Alert!

Although it is considered by some to be a more complete model, the Parkerian hexad is not as widely known as the CIA triad. If we decide to use this model in discussion of a security situation, we should be prepared to explain both the difference and benefits.

Confidentiality, integrity, and availability

As we mentioned, the Parkerian hexad encompasses the three principles of the CIA triad with the same definitions we just discussed. There is some variance in how Parker describes integrity, as he does not account for authorized, but incorrect, modification of data and instead focuses on the state of the data itself in the sense of completeness.

Possession or control

Possession or control refers to the physical disposition of the media on which the data is stored. This enables us, without involving other factors such as availability, to discuss our loss of the data in its physical medium. In our lost shipment of backup tapes, let us say that some of them were encrypted and some of them were not. The principle of possession would enable us to more accurately describe the scope of the incident; the encrypted tapes in the lot are a possession problem but not a confidentiality problem, and the unencrypted tapes are a problem on both counts. This is critical in today's environment where data can be on multiple devices and there could be numerous versions.

Authenticity

Authenticity allows us to talk about the proper attribution as to the owner or creator of the data in question. For example, if we send an e-mail message that is altered so as to appear to have come from a different e-mail address than the one from

which it was actually sent, we would be violating the authenticity of the e-mail. Authenticity can be enforced through the use of digital signatures, which we will discuss further in Chapter 5. A very similar, but reversed, concept to this is nonrepudiation. Nonrepudiation prevents someone from taking an action, such as sending an e-mail, and then later denying that he or she has done so. This is critical to e-commerce and is defined by the laws governing the transactions. We will discuss nonrepudiation at greater length in Chapter 5 as well.

Utility

Utility refers to how useful the data is to us. Utility is also the only principle of the Parkerian hexad that is not necessarily binary in nature; we can have a variety of degrees of utility, depending on the data and its format. This is a somewhat abstract concept, but it does prove useful in discussing certain situations in the security world. For instance, in one of our earlier examples, we had a shipment of backup tapes, some of which were encrypted and some of which were not. For an attacker, or other unauthorized person, the encrypted tapes would likely be of very little utility, as the data would not be readable. The unencrypted tapes would be of much greater utility, as the attacker or unauthorized person would be able to access the data.

Attacks

We may face attacks from a wide variety of approaches and vectors. When we look at what exactly makes up an attack, we can break it down according to the type of attack that it represents, the risk the attack represents, and the controls we might use to mitigate it.

Types of attack payloads

When we look at the types of attacks we might face, we can generally place them into one of four categories: interception, interruption, modification, and fabrication. Each category can affect one or more of the principles of the CIA triad, as shown in Figure 1.3. Additionally, the lines between the categories of attack and the particular effects they can have are somewhat blurry. Depending on the attack in question, we might argue for it to be included in more than one category or have more than one type of effect.

Interception

Interception attacks allow unauthorized users to access our data, applications, or environments, and are primarily an attack against confidentiality. Interception might take the form of unauthorized file viewing or copying, eavesdropping on phone conversations, or reading e-mail, and can be conducted against data at rest or in motion. Properly executed, interception attacks can be very difficult to detect.

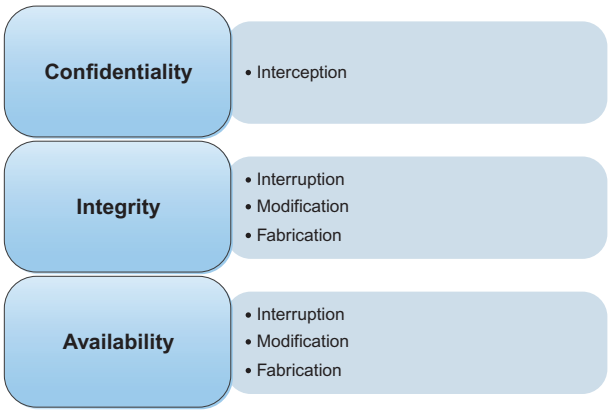

FIGURE 1.3

Categories of attack.

Interruption

Interruption attacks cause our assets to become unusable or unavailable for our use, on a temporary or permanent basis. Interruption attacks often affect availability but can be an attack on integrity as well. In the case of a DoS attack on a mail server, we would classify this as an availability attack. In the case of an attacker manipulating the processes on which a database runs in order to prevent access to the data it contains, we might consider this an integrity attack, due to the possible loss or corruption of data, or we might consider it a combination of the two. We might also consider such a database attack to be a modification attack rather than an interruption attack.

Modification

Modification attacks involve tampering with our asset. Such attacks might primarily be considered an integrity attack but could also represent an availability attack. If we access a file in an unauthorized manner and alter the data it contains, we have affected the integrity of the data contained in the file. However, if we consider the case where the file in question is a configuration file that manages how a particular service behaves, perhaps one that is acting as a Web server, we might affect the availability of that service by changing the contents of the file. If we continue with this concept and say the configuration we altered in the file for our Web server is one that alters how the server deals with encrypted connections, we could even make this a confidentiality attack.

Fabrication

Fabrication attacks involve generating data, processes, communications, or other similar activities with a system. Fabrication attacks primarily affect integrity but could be considered an availability attack as well. If we generate spurious

information in a database, this would be considered to be a fabrication attack. We could also generate e-mail, which is commonly called spoofing. This can be used as a method for propagating malware, such as we might find being used to spread a worm. In the sense of an availability attack, if we generate enough additional processes, network traffic, e-mail, Web traffic, or nearly anything else that consumes resources, we can potentially render the service that handles such traffic unavailable to legitimate users of the system.

Threats, vulnerabilities, and risk

In order to be able to speak more specifically on attacks, we need to introduce a few new items of terminology. When we look at the potential for a particular attack to affect us, we can speak of it in terms of threats, vulnerabilities, and the associated risk that might accompany them.

Threats

When we spoke of the types of attacks we might encounter, in the "Attacks" section earlier in this chapter, we discussed some of the things that have the potential to cause harm to our assets. Ultimately, this is what a threat is—something that has the potential to cause us harm. Threats tend to be specific to certain environments, particularly in the world of information security. For example, although a virus might pose a threat to a Windows operating system, the same virus will be unlikely to have any effect on a Linux operating system.

Vulnerabilities

Vulnerabilities are weaknesses that can be used to harm us. In essence, they are holes that can be exploited by threats in order to cause us harm. A vulnerability might be a specific operating system or application that we are running, a physical location where we have chosen to place our office building, a data center that is populated over the capacity of its air-conditioning system, a lack of backup generators, or other factors.

Risk

Risk is the likelihood that something bad will happen. In order for us to have a risk in a particular environment, we need to have both a threat and a vulnerability that the specific threat can exploit. For example, if we have a structure that is made from wood and we set it on fire, we have both a threat (the fire) and a vulnerability that matches it (the wood structure). In this case, we most definitely have a risk.

Likewise, if we have the same threat of fire, but our structure is made of concrete, we no longer have a credible risk, because our threat does not have a vulnerability to exploit. We can argue that a sufficiently hot flame could damage the concrete, but this is a much less likely event.

We will often have similar discussions regarding potential risk in computing environments, and potential, but unlikely, attacks that could happen. In such cases, the best strategy is to spend our time mitigating the most likely attacks. If we sink our resources in trying to plan for every possible attack, however unlikely, we will spread ourselves thin and will be lacking in protection where we actually need it the most.

Impact

Some organizations, such as the US National Security Agency (NSA), add an additional factor to the threat/vulnerability/risk equation, in the form of impact. If we consider the value of the asset being threatened to be a factor, this may change whether we see a risk as being present or not. If we revisit our example of lost backup tape and stipulate that the unencrypted backup tapes contain only our collection of chocolate chip cookie recipes, we may not actually have a risk. The data being exposed would not cause us a problem, as there was nothing sensitive in it, and we can make additional backups from the source data. In this particular case, we might safely say that we have no risk. Transversely if a company's critical proprietary information was compromised, they could end up going out of business.

Risk management

In order to compensate for risks that occur in our environment, the risk management process is very important to implement and follow. This program must be managed at the senior leader level of the organization and implemented by everyone (not just the technical staff). At a high level, we need to identify our important assets, identify the potential threats against them, assess the vulnerabilities that we have present, and then take steps to mitigate these risks, as shown in Figure 1.4.

Identify assets

One of the first and, arguably, one of the most important parts of the risk management process is identifying and categorizing the assets that we are protecting. If we cannot enumerate the assets that we have and evaluate the importance of each of them, protecting them can become a very difficult task indeed.

Although this may sound like an exceedingly simple task, in actuality in can be somewhat more complex a problem than it might seem to be on the surface. Particularly in larger enterprises, merely producing a list of all of the assets with which we are concerned may be troublesome. In many cases, various generations of hardware and devices may be present, assets from acquisitions of other companies may be lurking in unknown areas, and scores of unrecorded virtual hosts may be in use, any of which may be critical to the continued functionality of certain aspects of a business.

Once we have been able to identify the assets in use, deciding which of them is a critical business asset is another question entirely. If we ask the individual business or function to which the asset belongs, we will likely find it deemed to

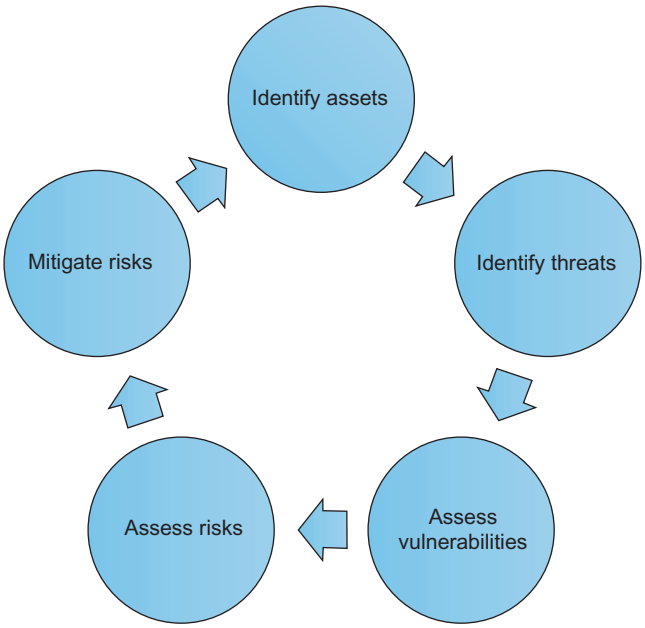

FIGURE 1.4

The risk management process.

be critical, whether it is critical to the functionality of the organization as a whole is another question entirely. Making an accurate determination of which assets are truly critical to conducting business will generally require the input of functions that make use of the asset, those that support the asset itself, and potentially other involved parties as well. Not all assets need to be protected equally, by determining where resources should be focused and cost can be reduced while security increased.

Identify threats

Once we have enumerated our critical assets, we can then begin to identify the threats that might affect them. It is often useful to have a framework within which to discuss the nature of a given threat, and the CIA triad or Parkerian hexad that we discussed earlier in this chapter serve nicely for this purpose. For instance, if we apply this to examining the threats that we might face against an application that processes credit card payments:

Confidentiality—If we expose data inappropriately, we have a potential breach
Integrity—If data becomes corrupt, we may incorrectly process payments
Availability—If the system or application goes down, we cannot process payments
Possession—If we lose backup media, we have a potential breach

Authenticity—If we do not have authentic customer information, we may process a fraudulent transaction
Utility—If we collect invalid or incorrect data, it has limited utility to us

While this is clearly a high level pass at assessing threats for this system, it does point out a few problem areas immediately. We need to be concerned with losing control of data, maintaining accurate data, and keeping the system up and running. Given this information, we can begin to look at areas of vulnerability and potential risk.

Assess vulnerabilities

When we look at assess vulnerabilities, we need to do so in the context of potential threats. Any given asset may have thousands or millions of threats that could impact it, but only a small fraction of these will actually be relevant. The issue of identifying these is narrowed considerably by looking at potential threats first, as we discussed in the previous section. In our example, we looked at potential threats against a system processing credit card transactions. Although this is at a high level, we can look at the issues that we identified and attempt to determine whether vulnerabilities exist in any of these areas as well:

Confidentiality—If we expose data inappropriately, we have a potential breach
Our sensitive data is encrypted at rest and in motion. Our systems are regularly tested by an external penetration testing company.
Integrity—If data becomes corrupt, we may incorrectly process payments
We carefully validate that payment data is correct as part of the processing workflow. Invalid data results in a rejected transaction.
Availability—If the system or application goes down, we cannot process payments
We do not have redundancy for the database on the back-end of our payment processing system.
Possession—If we lose backup media, we have a potential breach
Our backup media is encrypted and hand carried by a courier.
Authenticity—If we do not have authentic customer information, we may process a fraudulent transaction
Ensuring that valid payment and customer information actually belong to the individual conducting the transaction is difficult, we do not have a good way of doing this.
Utility—If we collect invalid or incorrect data, it has limited utility to us
To protect the utility of our data, we might checksum credit card numbers, ensure that the billing address and e-mail address are valid and perform other measures to ensure that our data is correct.

These examples are a very high level view of the process that we need to undertake but serve to illustrate the task. From here, we can again see a few areas of concern and can begin to evaluate the areas in which we may have risks.

Assess risks

Once we have identified the threats and vulnerabilities for a given asset, we can assess the overall risk. As we discussed earlier in this chapter, risk is the conjunction of a threat and a vulnerability. A vulnerability with no matching threat or a threat with no matching vulnerability do not constitute a risk.

For example, we looked at the following item as both a potential threat and an area of vulnerability:

> Availability—If the system or application goes down, we cannot process payments
>
> We do not have redundancy for the database on the back-end of our payment processing system.

In this case, we do have both a threat and a vulnerability that coincide, with the resulting risk being the loss of ability to process credit card payments due to a single point of failure on our database back-end. Once we work through our threats and vulnerabilities in this manner, we can then proceed toward mitigating these risks.

Mitigating risks

In order to help us mitigate risk, we can put measures in place to help ensure that a given type of threat is accounted for. These measures are referred to as controls. Controls are divided into three categories: physical, logical, and administrative.

Physical Physical controls are those controls that protect the physical environment in which our systems sit, or where our data is stored. Such controls also control access in and out of such environments. Physical controls logically include items such as fences, gates, locks, bollards, guards, and cameras, but also include systems that maintain the physical environment such as heating and air-conditioning systems, fire suppression systems, and backup power generators.

Although at first glance, physical controls may not seem like they would be integral to information security, they are actually one of the more critical controls with which we need to be concerned. If we are not able to physically protect our systems and data, any other controls that we can put in place become irrelevant. If an attacker is able to physically access our systems, he can, at the very least, steal or destroy the system, rendering it unavailable for our use in the best case. In the worst case, he will have access directly to our applications and data and will be able to steal our information and resources, or subvert them for his own use.

Logical and technical controls Logical controls, sometimes called technical controls, are those that protect the systems, networks, and environments that process, transmit, and store our data. Logical controls can include items such as passwords, encryption, logical access controls, firewalls, and intrusion detection systems.

Logical controls enable us, in a logical sense, to prevent unauthorized activities from taking place. If our logical controls are implemented properly and are successful, an attacker or unauthorized user cannot access our applications and data without subverting the controls that we have in place. This allows for multiple functions like

finance, human resources, and sales to all be run on one server, but none of them to have access to each other. If one is compromised they are not all compromised.

Administrative Administrative controls are based on rules, laws, policies, procedures, guidelines, and other items that are "paper" in nature. In essence, administrative controls set out the rules for how we expect the users of our environment to behave. Depending on the environment and control in question, administrative controls can represent differing levels of authority. We may have a simple rule such as "turn the coffee pot off at the end of the day," aimed at ensuring that we do not cause a physical security problem by burning our building down at night. We may also have a more stringent administrative control, such as one that requires us to change our password every 90 days.

One important concept when we discuss administrative controls is the ability to enforce compliance with them. If we do not have the authority or the ability to ensure that our controls are being complied with, they are worse than useless, because they create a false sense of security. For example, if we create a policy that says our business resources cannot, in any fashion, be used for personal use, we need to be able to enforce this. Outside of a highly secure environment, this can be a difficult task. We will need to monitor telephone and mobile phone usage, Web access, e-mail use, instant message conversations, installed software, and other potential areas for abuse. Unless we were willing to devote a great deal of resources for monitoring these and other areas, and dealing with violations of our policy, we would quickly have a policy that we would not be able to enforce. Once it is understood that we do not enforce our policies, we set ourselves up for misuse and even malicious activities.

Incident response

In the event that our risk management efforts fail, incident response exists to react to such events. Incident response should be primarily oriented to the items that we feel are likely to cause us pain as an organization, which we should now know based on our risk management efforts. Reaction to such incidents should be based, as much as is possible or practical, on documented incident response plans, which are regularly reviewed, tested, and practiced by those who will be expected to enact them in the case of an actual incident. The actual occurrence of such an emergency is not the time to (attempt to) follow documentation that has been languishing on a shelf, is outdated, and refers to processes or systems that have changed heavily or no longer exists.

The incident response process, at a high level, consists of:

- Preparation
- Detection and analysis
- Containment
- Eradication
- Recovery
- Post incident activity

Preparation

The preparation phase of incident response consists of all of the activities that we can perform, in advance of the incident itself, in order to better enable us to handle it. This typically involves having the policies and procedures that govern incident response and handling in place, conducting training and education for both incident handlers and those who are expected to report incidents, conducting incident response exercises, developing and maintaining documentation, and numerous other such activities.

The importance of this phase of incident response should not be underestimated. Without adequate preparation, it is extremely unlikely that response to an incident will go well and/or in the direction that we expect it to go. The time determines what needs to be done, who needs to do it, and how to do it, is not when we are faced with a burning emergency.

Detection and analysis

The detection and analysis phase is where the action begins to happen in our incident response process. In this phase, we will detect the occurrence of an issue and decide whether or not it is actually an incident so that we can respond to it appropriately.

The detection portion of this phase will often be the result of monitoring of or alerting based on the output of a security tool or service. This may be output from an Intrusion Detection System (IDS), Anti Virus (AV) software, firewall logs, proxy logs, alerting from a Security Information and Event Monitoring (SIEM) tool if program is internal or Managed Security Service Provider (MSSP) if program is external, or any of a number of similar sources.

The analysis portion of this phase is often a combination of automation from a tool or service, usually an SIEM, and human judgment. While we can often use some sort of thresholding to say that X number of events in a given amount of time is normal or that a certain combination of events is not normal (two failed logins followed by a success, followed by a password change, followed by the creation of a new account, for instance), we will often want human intervention at a certain point when discussing incident response. Such human intervention will often involve review of logs output by various security, network, and infrastructure devices, contact with the party that reported the incident, and general evaluation of the situation. This can be expensive if you're running a team of analysts 24×7 so automation of as many functions as possible is key.

When the incident handler evaluates the situation, they will make a determination regarding whether the issue constitutes an incident or not, an initial evaluation as to the criticality of the incident (if any), and contact any additional resources needed to proceed to the next phase.

Containment, eradication, and recovery

The containment, eradication, and recovery phase is where the majority of the work takes place to actually solve the incident, at least in the short term.

Containment involves taking steps to ensure that the situation does not cause any more damage than it already has, or to at least lessen any ongoing harm. If the problem involves a malware infected server actively being controlled by a remote attacker, this might mean disconnecting the server from the network, putting firewall rules in place to block the attacker, and updating signatures or rules on an Intrusion Prevention System (IPS) in order to halt the traffic from the malware.

During eradication, we will attempt to remove the effects of the issue from our environment. In the case of our malware infected server, we have already isolated the system and cut it off from its command and control network. Now we will need to remove the malware from the server and ensure that it does not exist elsewhere in our environment. This might involve additional scanning of other hosts in the environment to ensure that the malware is not present, and examination of logs on the server and activities from the attacking devices on the network in order to determine what other systems the infected server had been in communication with. With malware, particularly very new malware or variants, this can be a tricky task to ensure that we have properly completed. The adversary is constantly developing countermeasures to the most current security tools and methodologies. Whenever doubt exists as to whether malware or attackers have been truly evicted from our environment, we should err to the side of caution while balancing the impact to operations. Each event requires a risk assessment.

Lastly, we need to recover to a better state that were in which we were prior to the incident, or perhaps prior to the issue started if we did not detect the problem immediately. This would potentially involve restoring devices or data from backup media, rebuilding systems, reloading applications, or any of a number of similar activities. Additionally we need to mitigate the attack vector that was used. Again, this can be a more painful task than it initially sounds to be, based on potentially incomplete or unclear knowledge of the situation surrounding the incident and what exactly did take place. We may find that we are unable to verify that backup media is actually clean and free or infection, backup media may be bad entirely, application install bits may be missing, configuration files may not be available, and any of a number of similar issues.

Post incident activity

Post incident activity, as with preparation, is a phase we can easily overlook, but should ensure that we do not. In the post incident activity phase, often referred to as a postmortem (latin for after death), we attempt to determine specifically what happened, why it happened, and what we can do to keep it from happening again. This is not just a technical review as policies or infrastructure may need to be changed. The purpose of this phase is not to point fingers or place blame (although this does sometimes happen), but to ultimately prevent or lessen the impact of future such incidents.

Defense in depth

Defense in depth is a strategy common to both military maneuvers and information security. In both senses, the basic concept of defense in depth is to formulate a multilayered defense that will allow us to still achieve a successful defense should one or more of our defensive measures fail. In Figure 1.5, we can see an example of the layers we might want to put in place to defend our assets from a logical perspective; we would at the very least want defenses at the external network, internal network, host, application, and data levels. Given well-implemented defenses at each layer, we will make it very difficult to successfully penetrate deeply into our network and attack our assets directly.

One important concept to note when planning a defensive strategy using defense in depth is that it is not a magic bullet. No matter how many layers we put in place, or how many defensive measures we place at each layer, we will not be able to keep every attacker out for an indefinite period of time, nor is this the ultimate goal of defense in depth in an information security setting. The goal is to place enough defensive measures between our truly important assets and the attacker so that we will both notice that an attack is in progress and also buy ourselves enough time to take more active measures to prevent the attack from succeeding.

We can see exactly such a strategy in the theater release of the Batman movie, *The Dark Knight*, in 2008. The production company for the movie, Warner Bros., spent 6 months developing a multilayered defensive strategy to keep the movie from being pirated and placed on file-sharing networks for as long as possible. These measures included a tracking system to monitor who had access to copies of

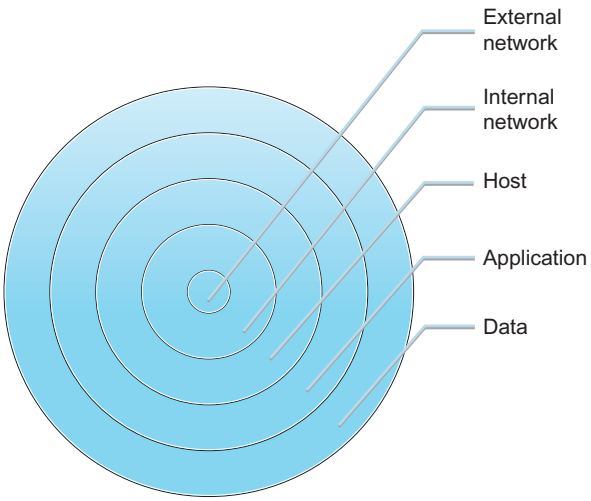

FIGURE 1.5

Defense in depth.

the movie at any given time, shipping the film reels in multiple parts separately to theaters in order to keep the entire movie from being stolen in shipping, monitoring movie theaters with night-vision equipment to watch for those attempting to record the movie in the theater, and other measures. Even with all the time and resources spent to prevent piracy of the movie, it was found on a file-sharing network 38 h after it was released [4]. For Warner Bros., this was considered a success, as the company was able to prevent the movie from being pirated for a long enough period that opening weekend sales were not significantly impacted.

Layers

When we look at the layers we might place in our defense in depth strategy, we will likely find that they vary given the particular situation and environment we are defending. As we discussed, from a strictly logical information security perspective, we would want to look at the external network, network perimeter, internal network, host, application, and data layers as areas to place our defenses. We could add complexity to our defensive model by including other vital layers such as physical defenses, policies, user awareness and training, and a multitude of others, but we will stay with a simpler example for the time being. As we progress through the book, we will return to the concept of defense in depth as we discuss security for more specific areas.

As we can see in Figure 1.6, some of the defenses we might use for each of the layers we discussed are listed. In some cases, we see a defensive measure listed in multiple layers, as it applies in more than one area. Just like the military has reconnaissance forces watching the front lines, they still have local patrols

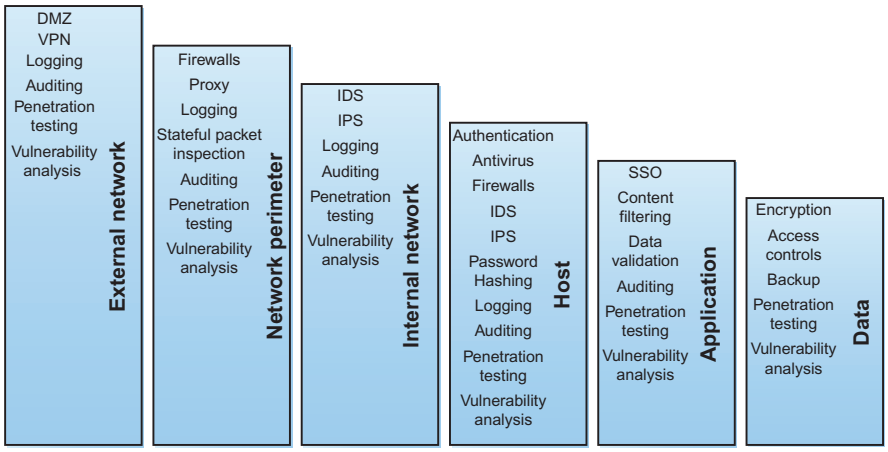

FIGURE 1.6

Defenses in each layer.

around the headquarters. As we move through the book, we will discuss each of these areas in greater detail, and the specific defenses we might want to use for each.

Information security in the real world

The concepts we discussed in this chapter are foundational to information security and are used on a regular basis in the course of normal information security tasks in many organizations. We will often find that security incidents are described in terms of their effects, such as breaches of confidentiality, or the authenticity of a given e-mail message.

Information security is a daily concern for organizations of any size, particularly those that handle any type of personal information, financial data, health-care data, educational data, or other types of data that are regulated by the laws of the country in which they operate. In the case of an organization that does not take the time to properly put itself on a good footing as relates to information security, the repercussions can be severe in the sense of reputational impact, fines, lawsuits, or even the inability to continue conducting business if critical data is irretrievably lost. In short, information security is a key component of the modern business world.

SUMMARY

Information security is a vital component to the era in which data regarding countless individuals and organizations is stored in a variety of computer systems, often not under our direct control. When discussing information security in a general sense, it is important to remember that security and productivity are often diametrically opposing concepts, and that being able to point out exactly when we are secure is a difficult task.

When discussing information security issues or situations, it is helpful to have a model by which to do so. Two potential models are the CIA triad, composed of confidentiality, integrity, and availability, and the Parkerian hexad, composed of confidentiality, integrity, availability, possession or control, authenticity, and utility.

When we look at the threats we might face, it is important to understand the concept of risk. We only face risk from an attack when a threat is present and we have a vulnerability which that particular threat can exploit. In order to mitigate risk, we use three main types of controls: physical, logical, and administrative.

Defense in depth is a particularly important concept in the world of information security. To build defensive measures using this concept, we put in place multiple layers of defense, each giving us an additional layer of protection. The idea behind defense in depth is not to keep an attacker out permanently but to delay him long enough to alert us to the attack and to allow us to mount a more active defense.

EXERCISES

1. Explain the difference between a vulnerability and a threat.
2. List six items that might be considered logical controls.
3. What term might we use to describe the usefulness of data?
4. Which category of attack is an attack against confidentiality?
5. How do we know at what point we can consider our environment to be secure?
6. Using the concept of defense in depth, what layers might we use to secure ourselves against someone removing confidential data from our office on a USB flash drive?
7. Based on the Parkerian hexad, what principles are affected if we lose a shipment of encrypted backup tapes that contain personal and payment information for our customers?
8. If the Web servers in our environment are based on Microsoft's Internet Information Server (IIS) and a new worm is discovered that attacks Apache Web servers, what do we not have?
9. If we develop a new policy for our environment that requires us to use complex and automatically generated passwords that are unique to each system and are a minimum of 30 characters in length, such as *!Hs4(j0qO$&zn1%2SK38cn^!Ks620!*, what will be adversely impacted?
10. Considering the CIA triad and the Parkerian hexad, what are the advantages and disadvantages of each model?

References

[1] US Government, Legal Information Institute, Title 44, Chapter 35, Subchapter 111, §3542, Cornell University Law School, <www.law.cornell.edu/uscode/44/3542.html> [accessed 20.09.13].
[2] Spafford E. Quotable spaf, Gene Spafford's personal pages, <http://spaf.cerias.purdue.edu/quotes.html>; 2009 [accessed 20.09.13].
[3] Parker D. Fighting computer crime. Wiley; 1998, ISBN: 0471163783.
[4] Chmielewski D. Secrecy cloaked "Dark Knight," Los Angeles Times, <http://articles.latimes.com/2008/jul/28/business/fi-darkknight28>; July 28, 2008 [accessed 20.09.13].