Chapter 6: Information Systems Security

David T. Bourgeois

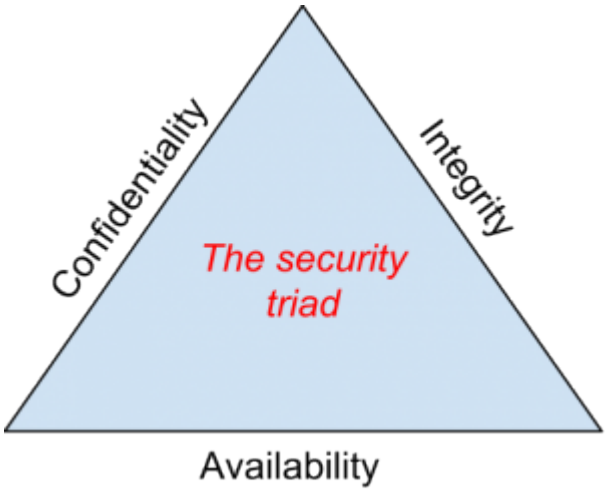
Learning Objectives

Upon successful completion of this chapter, you will be able to:

- identify the information security triad;
- identify and understand the high-level concepts surrounding information security tools; and
- secure yourself digitally.

Introduction

As computers and other digital devices have become essential to business and commerce, they have also increasingly become a target for attacks. In order for a company or an individual to use a computing device with confidence, they must first be assured that the device is not compromised in any way and that all communications will be secure. In this chapter, we will review the fundamental concepts of information systems security and discuss some of the measures that can be taken to mitigate security threats. We will begin with an overview focusing on how organizations can stay secure. Several different measures that a company can take to improve security will be discussed. We will then follow up by reviewing security precautions that individuals can take in order to secure their personal computing environment.



The security triad

The Information Security Triad: Confidentiality, Integrity, Availability (CIA)

Confidentiality

When protecting information, we want to be able to restrict access to those who are allowed to see it; everyone else should be disallowed from learning anything about its contents. This is the essence of confidentiality. For example, federal law requires that universities restrict access to private student information. The university must be sure that only those who are authorized have access to view the grade records.

Integrity

Integrity is the assurance that the information being accessed has not been altered and truly represents what is intended. Just as a person with integrity means what he or she says and can be trusted to consistently represent the truth, information integrity means information truly represents its intended

meaning. Information can lose its integrity through malicious intent, such as when someone who is not authorized makes a change to intentionally misrepresent something. An example of this would be when a hacker is hired to go into the university's system and change a grade.

Integrity can also be lost unintentionally, such as when a computer power surge corrupts a file or someone authorized to make a change accidentally deletes a file or enters incorrect information.

Availability

Information availability is the third part of the CIA triad. *Availability* means that information can be accessed and modified by anyone authorized to do so in an appropriate timeframe. Depending on the type of information, *appropriate timeframe* can mean different things. For example, a stock trader needs information to be available immediately, while a sales person may be happy to get sales numbers for the day in a report the next morning. Companies such as Amazon.com will require their servers to be available twenty-four hours a day, seven days a week. Other companies may not suffer if their web servers are down for a few minutes once in a while.

Tools for Information Security

In order to ensure the confidentiality, integrity, and availability of information, organizations can choose from a variety of tools. Each of these tools can be utilized as part of an overall information-security policy, which will be discussed in the next section.

Authentication

The most common way to identify someone is through their physical appearance, but how do we identify someone sitting behind a computer screen or at the ATM? Tools for authentication are used to ensure that the person accessing the information is, indeed, who they present themselves to be.

Authentication can be accomplished by identifying someone through one or more of three factors: something they know, something they have, or something they are. For example, the most common form of authentication today is the user ID and password. In this case, the authentication is done by confirming something that the user knows (their ID and password). But this form of authentication is easy to compromise (see sidebar) and stronger forms of authentication are sometimes needed. Identifying someone only by something they have, such as a key or a card, can also be problematic. When that identifying token is lost or stolen, the identity can be easily stolen. The final factor, something you are, is much harder to compromise. This factor identifies a user through the use of a physical characteristic, such as an eye-scan or fingerprint. Identifying someone through their physical characteristics is called biometrics.

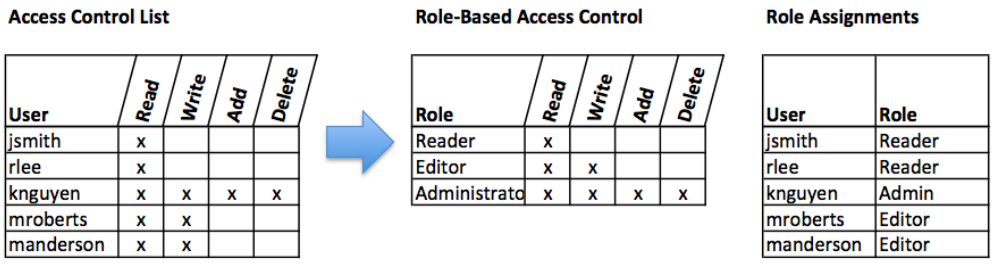
A more secure way to authenticate a user is to do multi-factor authentication. By combining two or more of the factors listed above, it becomes much more difficult for someone to misrepresent themselves. An example of this would be the use of an RSA SecurID token. The RSA device is something you have, and will generate a new access code every sixty seconds. To log in to an information resource using the RSA device, you combine something you know, a four-digit PIN, with the code generated by the device. The only way to properly authenticate is by both knowing the code *and* having the RSA device.

Access Control

Once a user has been authenticated, the next step is to ensure that they can only access the information resources that are appropriate. This is done through the use of access control. Access control determines which users are authorized to read, modify, add, and/or delete information. Several different access control models exist. Here we will discuss two: the access control list (ACL) and role-based access control (RBAC).

For each information resource that an organization wishes to manage, a list of users who have the ability to take specific actions can be created. This is an access control list, or ACL. For each user, specific capabilities are assigned, such as *read*, *write*, *delete*, or *add*. Only users with those capabilities are allowed to perform those functions. If a user is not on the list, they have no ability to even know that the information resource exists.

ACLs are simple to understand and maintain. However, they have several drawbacks. The primary drawback is that each information resource is managed separately, so if a security administrator wanted to add or remove a user to a large set of information resources, it would be quite difficult. And as the number of users and resources increase, ACLs become harder to maintain. This has led to an improved method of access control, called role-based access control, or RBAC. With RBAC, instead of giving specific users access rights to an information resource, users are assigned to roles and then those roles are assigned the access. This allows the administrators to manage users and roles separately, simplifying administration and, by extension, improving security.



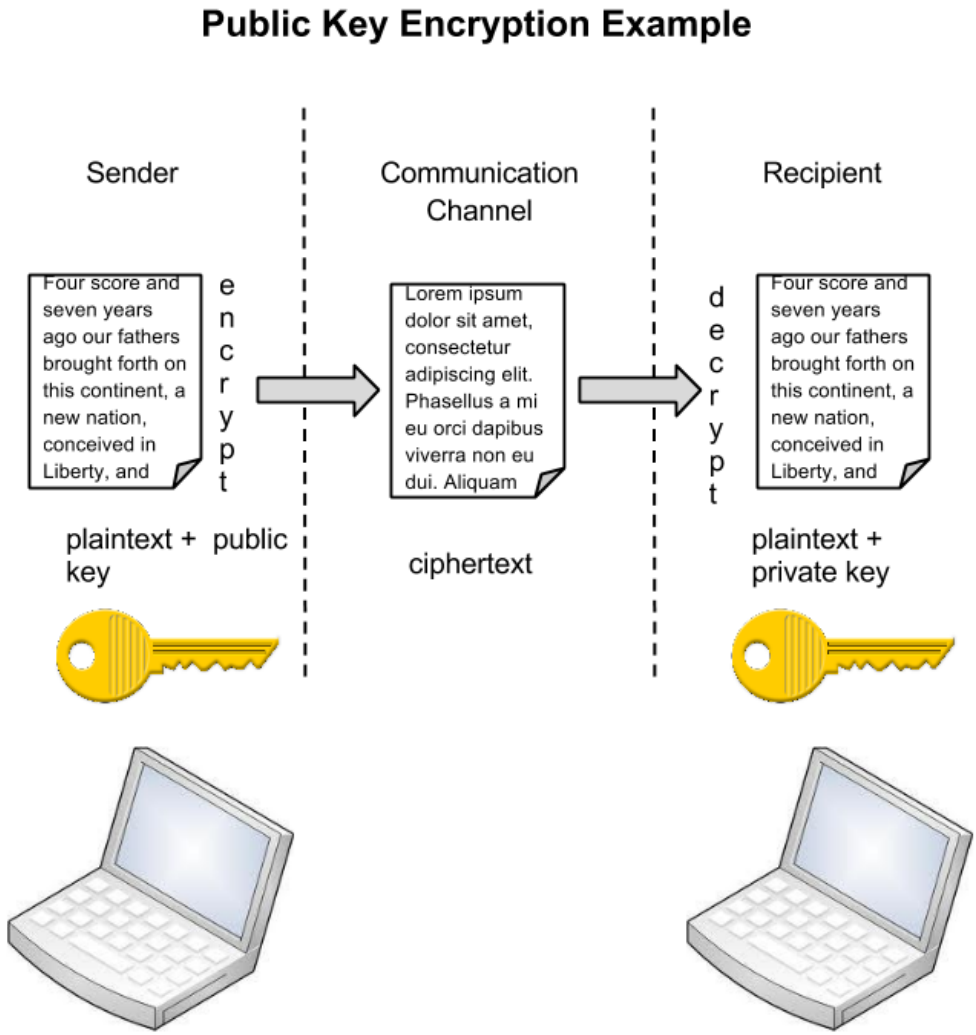
Comparison of ACL and RBAC (click to enlarge)

Encryption

Many times, an organization needs to transmit information over the Internet or transfer it on external media such as a CD or flash drive. In these cases, even with proper authentication and access control, it is possible for an unauthorized person to get access to the data. Encryption is a process of encoding data upon its transmission or storage so that only authorized individuals can read it. This encoding is accomplished by a computer program, which encodes the plain text that needs to be transmitted; then the recipient receives the cipher text and decodes it (decryption). In order for this to work, the sender and receiver need to agree on the method of encoding so that both parties can communicate properly. Both parties share the encryption key, enabling them to encode and decode each other's messages. This is called symmetric key encryption. This type of encryption is problematic because the key is available in two different places.

An alternative to symmetric key encryption is public key encryption. In public key encryption, two keys are used: a public key and a private key. To send an encrypted message, you obtain the public key, encode the message, and send it. The recipient then uses the private key to decode it. The public key can be given to anyone who wishes to send the recipient a message. Each user simply needs one private key and

one public key in order to secure messages. The private key is necessary in order to decrypt something sent with the public key.



Public key encryption (click for larger diagram)

Sidebar: Password Security

So why is using just a simple user ID/password not considered a secure method of authentication? It turns out that this single-factor authentication is extremely easy to compromise. Good password policies must be put in place in order to ensure that passwords cannot be compromised. Below are some of the more common policies that organizations should put in place.

- Require complex passwords. One reason passwords are compromised is that they can be easily guessed. A recent study found that the top three passwords people used in 2012 were *password*, *123456* and *12345678*.[1] A password should not be simple, or a word that can be found in a dictionary. One of the first things a hacker will do is try to crack a password

1. "Born to be breached" by Sean Gallagher on Nov 3 2012. *Arstechnica*. Retrieved from http://arstechnica.com/information-technology/2012/11/born-to-be-breached-the-worst-passwords-are-still-the-most-common/ on May 15, 2013.

by testing every term in the dictionary! Instead, a good password policy is one that requires the use of a minimum of eight characters, and at least one upper-case letter, one special character, and one number.

- Change passwords regularly. It is essential that users change their passwords on a regular basis. Users should change their passwords every sixty to ninety days, ensuring that any passwords that might have been stolen or guessed will not be able to be used against the company.
- Train employees not to give away passwords. One of the primary methods that is used to steal passwords is to simply figure them out by asking the users or administrators. *Pretexting* occurs when an attacker calls a helpdesk or security administrator and pretends to be a particular authorized user having trouble logging in. Then, by providing some personal information about the authorized user, the attacker convinces the security person to reset the password and tell him what it is. Another way that employees may be tricked into giving away passwords is through e-mail phishing. Phishing occurs when a user receives an e-mail that looks as if it is from a trusted source, such as their bank, or their employer. In the e-mail, the user is asked to click a link and log in to a website that mimics the genuine website and enter their ID and password, which are then captured by the attacker.

Backups

Another essential tool for information security is a comprehensive backup plan for the entire organization. Not only should the data on the corporate servers be backed up, but individual computers used throughout the organization should also be backed up. A good backup plan should consist of several components.

- A full understanding of the organizational information resources. What information does the organization actually have? Where is it stored? Some data may be stored on the organization's servers, other data on users' hard drives, some in the cloud, and some on third-party sites. An organization should make a full inventory of all of the information that needs to be backed up and determine the best way back it up.
- Regular backups of all data. The frequency of backups should be based on how important the data is to the company, combined with the ability of the company to replace any data that is lost. Critical data should be backed up daily, while less critical data could be backed up weekly.
- Offsite storage of backup data sets. If all of the backup data is being stored in the same facility as the original copies of the data, then a single event, such as an earthquake, fire, or tornado, would take out both the original data and the backup! It is essential that part of the backup plan is to store the data in an offsite location.
- Test of data restoration. On a regular basis, the backups should be put to the test by having some of the data restored. This will ensure that the process is working and will give the organization confidence in the backup plan.

Besides these considerations, organizations should also examine their operations to determine what effect downtime would have on their business. If their information technology were to be unavailable for any sustained period of time, how would it impact the business?

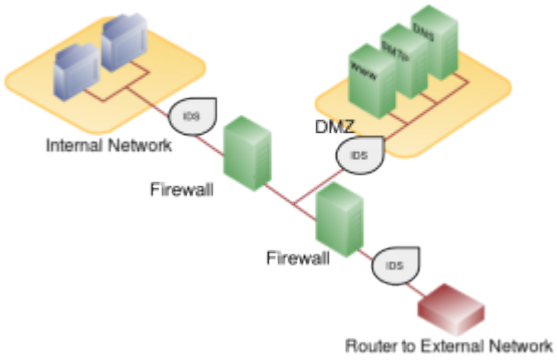
Additional concepts related to backup include the following:

- Universal Power Supply (UPS). A UPS is a device that provides battery backup to critical components of the system, allowing them to stay online longer and/or allowing the IT staff to shut them down using proper procedures in order to prevent the data loss that might occur from a power failure.
- Alternate, or "hot" sites. Some organizations choose to have an alternate site where an exact replica of their critical data is always kept up to date. When the primary site goes down, the alternate site is immediately brought online so that little or no downtime is experienced.

As information has become a strategic asset, a whole industry has sprung up around the technologies necessary for implementing a proper backup strategy. A company can contract with a service provider to back up all of their data or they can purchase large amounts of online storage space and do it themselves. Technologies such as storage area networks and archival systems are now used by most large businesses.

Firewalls

Another method that an organization should use to increase security on its network is a firewall. A firewall can exist as hardware or software (or both). A hardware firewall is a device that is connected to the network and filters the packets based on a set of rules. A software firewall runs on the operating system and intercepts packets as they arrive to a computer. A firewall protects all company servers and computers by stopping packets from outside the organization's network that do not meet a strict set of criteria. A firewall may also be configured to restrict the flow of packets leaving the organization. This may be done to eliminate the possibility of employees watching YouTube videos or using Facebook from a company computer.



Network configuration with firewalls, IDS, and a DMZ. Click to enlarge.

Some organizations may choose to implement multiple firewalls as part of their network security configuration, creating one or more sections of their network that are partially secured. This segment of the network is referred to as a DMZ, borrowing the term *demilitarized zone* from the military, and it is where an organization may place resources that need broader access but still need to be secured.

Intrusion Detection Systems

Another device that can be placed on the network for security purposes is an intrusion detection system, or IDS. An IDS does not add any additional security; instead, it provides the functionality to identify if the network is being attacked. An IDS can be configured to watch for specific types of activities and then alert security personnel if that activity occurs. An IDS also can log various types of traffic on the network for analysis later. An IDS is an essential part of any good security setup.

Sidebar: Virtual Private Networks

Using firewalls and other security technologies, organizations can effectively protect many of their information resources by making them invisible to the outside world. But what if an employee working from home requires access to some of these resources? What if a consultant is hired who needs to do work on the internal corporate network from a remote location? In these cases, a virtual private network (VPN) is called for.

A VPN allows a user who is outside of a corporate network to take a detour around the firewall and access the internal network from the outside. Through a combination of software and security measures, this lets an organization allow limited access to its networks while at the same time ensuring overall security.

Physical Security

An organization can implement the best authentication scheme in the world, develop the best access control, and install firewalls and intrusion prevention, but its security cannot be complete without implementation of physical security. Physical security is the protection of the actual hardware and networking components that store and transmit information resources. To implement physical security, an organization must identify all of the vulnerable resources and take measures to ensure that these resources cannot be physically tampered with or stolen. These measures include the following.

- Locked doors: It may seem obvious, but all the security in the world is useless if an intruder can simply walk in and physically remove a computing device. High-value information assets should be secured in a location with limited access.
- Physical intrusion detection: High-value information assets should be monitored through the use of security cameras and other means to detect unauthorized access to the physical locations where they exist.
- Secured equipment: Devices should be locked down to prevent them from being stolen. One employee's hard drive could contain all of your customer information, so it is essential that it be secured.
- Environmental monitoring: An organization's servers and other high-value equipment should always be kept in a room that is monitored for temperature, humidity, and airflow. The risk of a server failure rises when these factors go out of a specified range.
- Employee training: One of the most common ways thieves steal corporate information is to steal employee laptops while employees are traveling. Employees should be trained to secure their equipment whenever they are away from the office.

Security Policies

Besides the technical controls listed above, organizations also need to implement security policies as a form of administrative control. In fact, these policies should really be a starting point in developing an overall security plan. A good information-security policy lays out the guidelines for employee use of the information resources of the company and provides the company recourse in the case that an employee violates a policy.

According to the SANS Institute, a good policy is "a formal, brief, and high-level statement or plan that embraces an organization's general beliefs, goals, objectives, and acceptable procedures for a specified subject area." Policies require compliance; failure to comply with a policy will result in disciplinary action. A policy does not lay out the specific technical details, instead it focuses on the desired results. A security policy should be based on the guiding principles of confidentiality, integrity, and availability.[2]

A good example of a security policy that many will be familiar with is a web use policy. A web use policy lays out the responsibilities of company employees as they use company resources to access the Internet. A good example of a web use policy is included in Harvard University's "Computer Rules and Responsibilities" policy, which can be found here.

A security policy should also address any governmental or industry regulations that apply to the organization. For example, if the organization is a university, it must be aware of the Family Educational Rights and Privacy Act (FERPA), which restricts who has access to student information. Health care organizations are obligated to follow several regulations, such as the Health Insurance Portability and Accountability Act (HIPAA).

A good resource for learning more about security policies is the SANS Institute's Information Security Policy Page.

Sidebar: Mobile Security

As the use of mobile devices such as smartphones and tablets proliferates, organizations must be ready to address the unique security concerns that the use of these devices bring. One of the first questions an organization must consider is whether to allow mobile devices in the workplace at all. Many employees already have these devices, so the question becomes: Should we allow employees to bring their own devices and use them as part of their employment activities? Or should we provide the devices to our employees? Creating a BYOD ("Bring Your Own Device") policy allows employees to integrate themselves more fully into their job and can bring higher employee satisfaction and productivity. In many cases, it may be virtually impossible to prevent employees from having their own smartphones or iPads in the workplace. If the organization provides the devices to its employees, it gains more control over use of the devices, but it also exposes itself to the possibility of an administrative (and costly) mess.

Mobile devices can pose many unique security challenges to an organization. Probably one of the biggest concerns is theft of intellectual property. For an employee with malicious intent, it would be a very simple process to connect a mobile device either to a computer via the USB port, or wirelessly to the corporate network, and download confidential data. It would also be easy to secretly take a high-quality picture using a built-in camera.

When an employee does have permission to access and save company data on his or her device, a different security threat emerges: that device now becomes a target for thieves. Theft of mobile devices (in this case, including laptops) is one of the primary methods that data thieves use.

So what can be done to secure mobile devices? It will start with a good policy regarding their use. According to a 2013 SANS study, organizations should consider developing a mobile device policy that addresses the following issues: use of the camera, use of voice recording, application purchases, encryption at rest, Wi-Fi autoconnect settings, bluetooth settings, VPN use, password settings, lost or stolen device reporting, and backup. [3]

2. SANS Institute. "A Short Primer for Developing Security Policies." Accessed from http://www.sans.org/security-resources/policies/Policy_Primer.pdf on May 31, 2013.

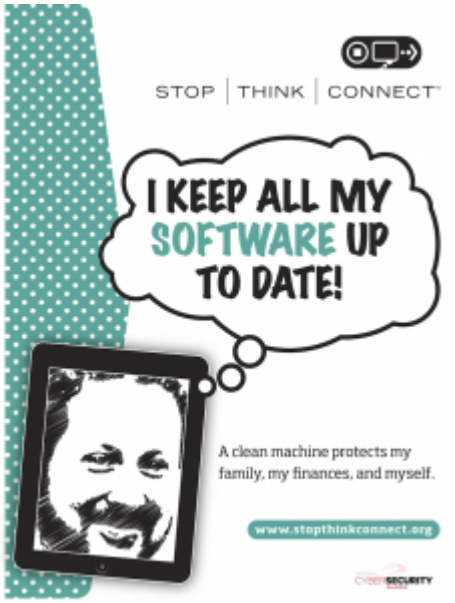
Besides policies, there are several different tools that an organization can use to mitigate some of these risks. For example, if a device is stolen or lost, geolocation software can help the organization find it. In some cases, it may even make sense to install remote data-removal software, which will remove data from a device if it becomes a security risk.

Usability

When looking to secure information resources, organizations must balance the need for security with users' need to effectively access and use these resources. If a system's security measures make it difficult to use, then users will find ways around the security, which may make the system more vulnerable than it would have been without the security measures! Take, for example, password policies. If the organization requires an extremely long password with several special characters, an employee may resort to writing it down and putting it in a drawer since it will be impossible to memorize.

Personal Information Security

We will end this chapter with a discussion of what measures each of us, as individual users, can take to secure our computing technologies. There is no way to have 100% security, but there are several simple steps we, as individuals, can take to make ourselves more secure.



Poster from Stop. Think. Connect. Click to enlarge. (Copyright: Stop. Think. Connect. http://stopthinkconnect.org/resources)

- Keep your software up to date. Whenever a software vendor determines that a security flaw has been found in their software, they will release an update to the software that you can download to fix the problem. Turn on automatic updating on your computer to automate this process.
- Install antivirus software and keep it up to date. There are many good antivirus software packages on the market today, including free ones.
- Be smart about your connections. You should be aware of your surroundings. When connecting to a Wi-Fi network in a public place, be aware that you could be at risk of being spied on by others sharing that network. It is advisable not to access your financial or personal data while attached to a Wi-Fi hotspot. You should also be aware that connecting USB flash drives to your device could also put you at risk. Do not attach an unfamiliar flash drive to your device unless you can scan it first with your security software.
- Back up your data. Just as organizations need to back up their data, individuals need to as well. And the same rules apply: do it regularly and keep a copy of it in another location. One simple solution for this is to set up an account with an online backup service, such as Mozy or Carbonite, to automate your backups.

3. Taken from SANS Institute's Mobile Device Checklist. You can review the full checklist at www.sans.org/score/checklists/mobile-device-checklist.xls.

- Secure your accounts with two-factor authentication. Most e-mail and social media providers now have a two-factor authentication option. The way this works is simple: when you log in to your account from an unfamiliar computer for the first time, it sends you a text message with a code that you must enter to confirm that you are really you. This means that no one else can log in to your accounts without knowing your password *and* having your mobile phone with them.
- Make your passwords long, strong, and unique. For your personal passwords, you should follow the same rules that are recommended for organizations. Your passwords should be long (eight or more characters) and contain at least two of the following: upper-case letters, numbers, and special characters. You also should use different passwords for different accounts, so that if someone steals your password for one account, they still are locked out of your other accounts.
- Be suspicious of strange links and attachments. When you receive an e-mail, tweet, or Facebook post, be suspicious of any links or attachments included there. Do not click on the link directly if you are at all suspicious. Instead, if you want to access the website, find it yourself and navigate to it directly.

You can find more about these steps and many other ways to be secure with your computing by going to Stop. Think. Connect. This website is part of a campaign that was launched in October of 2010 by the STOP. THINK. CONNECT. Messaging Convention in partnership with the U.S. government, including the White House.

Summary

As computing and networking resources have become more and more an integral part of business, they have also become a target of criminals. Organizations must be vigilant with the way they protect their resources. The same holds true for us personally: as digital devices become more and more intertwined with our lives, it becomes crucial for us to understand how to protect ourselves.

Study Questions

1. Briefly define each of the three members of the information security triad.
2. What does the term *authentication* mean?
3. What is multi-factor authentication?
4. What is role-based access control?
5. What is the purpose of encryption?
6. What are two good examples of a complex password?
7. What is pretexting?
8. What are the components of a good backup plan?
9. What is a firewall?
10. What does the term *physical security* mean?

Exercises

1. Describe one method of multi-factor authentication that you have experienced and discuss the pros and cons of using multi-factor authentication.
2. What are some of the latest advances in encryption technologies? Conduct some independent research on encryption using scholarly or practitioner resources, then write a two- to three-page paper that describes at least two new advances in encryption technology.
3. What is the password policy at your place of employment or study? Do you have to change passwords every so often? What are the minimum requirements for a password?
4. When was the last time you backed up your data? What method did you use? In one to two pages, describe a method for backing up your data. Ask your instructor if you can get extra credit for backing up your data.
5. Find the information security policy at your place of employment or study. Is it a good policy? Does it meet the standards outlined in the chapter?
6. How are you doing on keeping your own information secure? Review the steps listed in the chapter and comment on how well you are doing.