# **Chapter 1**

**Introduction to Security**

|  |
| --- |
| **At a Glance** |

#### Instructor’s Manual Table of Contents

* Overview
* Objectives
* Teaching Tips
* Quick Quizzes
* Class Discussion Topics
* Additional Projects
* Additional Resources
* Key Terms

|  |
| --- |
| Lecture Notes |

# **Overview**

Chapter 1 introduces security fundamentals that form the basis of the Security+ certification. It begins by examining the current challenges in computer security and why it is so difficult to achieve. It then describes information security in more detail to illustrate why it is important. Finally, the chapter looks at who is responsible for these attacks and what the fundamental defenses against attackers are.

# **Chapter Objectives**

* Explain the challenges of securing information
* Define information security and explain why it is important
* Identify the types of threat actors that are common today
* Describe how to defend against attacks

# **Teaching Tips**

**Challenges of Securing Information**

1. Explain that there is no simple solution to securing information. This can be seen through the different types of attacks that users face today, as well as the difficulties in defending against these attacks.

**Today’s Security Attacks**

1. Describe some recent security attacks, such as the following:
	1. A reporter drove a Jeep Cherokee while two security researchers 10 miles away remotely connected to it and started manipulating its controls.
	2. United Airlines passenger who tampered with the Seat Electronic Box to connect to other system on the plane.
	3. Half a billion Yahoo accounts were compromised by attacker who gained unauthorized access to its web servers.
	4. USB Killer device.
	5. WINVote voting machine vulnerabilities .
	6. VTech accounts that included information on 6.4 million children were hacked .
	7. IRS Get Transcript program was hacked.
2. Mention that security statistics bear witness to the continual success of attackers:
	1. From 2005-2017 over 907 million electronic data records in the U.S. had been breached.

|  |  |
| --- | --- |
| ***Teaching*** ***Tip*** | Phishing Web sites are well known for suddenly appearing and then disappearing to reduce the risk of being traced. The average time a site is online is only four days according to the APWG ([www.antiphishing.org](http://www.antiphishing.org)). |

|  |  |
| --- | --- |
| ***Teaching*** ***Tip*** | The US-CERT security bulletin is available at [www.us-cert.gov/cas/bulletins/](http://www.us-cert.gov/cas/bulletins/). |

**Reasons for Successful Attacks**

1. Discuss the following reasons behind successful attacks:
	1. Widespread vulnerabilities
	2. Configuration issues
	3. Poorly designed software
	4. Hardware limitations
	5. Enterprise-based issues

**Difficulties in Defending against Attacks**

1. Describe the following difficulties in defending against attacks:
	1. Universally connected devices
	2. Increased speed of attacks
	3. Greater sophistication of attacks
	4. Availability and simplicity of attack tools
	5. Faster detection of vulnerabilities
	6. Delays in security updating
	7. Weak security update distribution
	8. Distributed attacks
	9. Use of personal devices
	10. User confusion
2. Table 1-2 summarizes these difficulties.

**What Is Information Security?**

1. Mention that knowing why information security is important today and who the attackers are is beneficial. Point out that knowing the terminology used can be helpful when creating defenses for computers.

**Understanding Security**

1. Explain that security can be considered as a state of freedom from a danger or risk. This state or condition of freedom exists because protective measures are established and maintained.
2. Use Figure 1-2 to help explain the relationship between security and convenience. Point out that as security is increased, convenience is often decreased.

**Defining Information Security**

1. Define information security as the tasks of guarding information that is in a digital format. It ensures that protective measures are properly implemented. Information security cannot completely prevent attacks or guarantee that a system is totally secure.
2. Explain that information security is intended to protect information that has value to people and organizations. That value comes from the characteristics of the information:
	1. Confidentiality
	2. Integrity
	3. Availability

|  |  |
| --- | --- |
| ***Teaching*** ***Tip*** | The confidentiality, integrity, and availability of information is known as CIA. |

1. Explain that information security is achieved through a combination of three protections. Use Figure 1-3 and Table 1-3 to illustrate your explanation.
2. Emphasize that information security is that which protects the integrity, confidentiality, and availability of information on the devices that store, manipulate, and transmit the information through products, people, and procedures.

**Information Security Terminology**

1. Define the following information security terms:
	1. Asset
	2. Threat
	3. Threat actor
	4. Vulnerability
	5. Attack vector
	6. Attack surface
	7. Risk
2. Use Figure 1-4 and Table 1-5 to illustrate the terminology above.
3. Discuss and define the different options available when dealing with risks.
4. Acceptance
5. Transference
6. Risk avoidance
7. Mitigation

**Quick Quiz 1**

1. Which protection ensures that only authorized parties can view the information?
2. Confidentiality
3. Integrity
4. Accounting
5. Availability

Answer: A

1. Which of the following terms best describes ensuring that data is accessible to authorized users?
	* 1. Integrity
		2. Accounting
		3. Availability
		4. BYOD

Answer: C

1. A(n) \_\_\_\_ is defined as something that has a value.

Answer: asset

1. A situation that involves exposure to some type of danger is known as which of the following?
2. vector
3. risk
4. threat
5. asset

Answer: B

1. Addressing a risk by making it less serious is known as which of the following?
2. acceptance
3. transference
4. avoidance
5. mitigation

Answer: D

**Understanding the Importance of Information Security**

1. Mention that the main goals of information security are to prevent data theft, thwart identity theft, avoid the legal consequences of not securing information, maintain productivity, and foil cyberterrorism.
2. Explain that security is often associated with theft prevention. The theft of data is one of the largest causes of financial loss due to an attack. Individuals are often victims of data thievery.
3. Mention that identity theft involves using someone’s personal information to establish bank or credit card accounts that are then left unpaid, leaving the victim with the debts and ruining their credit rating.
4. Explain that a number of federal and state laws have been enacted to protect the privacy of electronic data, including the following:
	1. The Health Insurance Portability and Accountability Act of 1996 (HIPAA)
	2. The Sarbanes-Oxley Act of 2002 (Sarbox)
	3. The Gramm-Leach-Bliley Act (GLBA)
	4. Payment Card Industry Data Security Standard (PCI DSS)
	5. State notification and security laws

|  |  |
| --- | --- |
| ***Teaching*** ***Tip*** | In 2008, California extended its data breach notification law to encompass incidents including electronic medical and health insurance information. |

1. Explain that cleaning up after an attack diverts resources such as time and money away from normal activities. Use Table 1-6 to illustrate your explanation.
2. Define cyberterrorism as attacks by terrorist groups using computer technology and the Internet. Utility, telecommunications, and financial services companies are considered prime targets of cyberterrorists.

**Who Are the Threat Actors?**

1. Explain that the term threat actor, in a generic sense, is used to describe individuals who launch attacks against other users and their computers.
2. Explain that threat actors of today have a more focused goal of financial gain: to exploit vulnerabilities that can generate income.
3. Point out that the characteristic features of different groups of threat actors can vary widely:
	1. Sophisticated
	2. Funding and resources
	3. External or internal to the enterprise
	4. Intent and motivation
4. Today threat actors are recognized in more distinct categories, such as script kiddies, hactivists, nation state actors, insiders, and others.

|  |  |
| --- | --- |
| ***Teaching*** ***Tip*** | Security vulnerabilities, however, can be exposed in ways other than attacking another computer without the owner’s consent, and most security professionals would not refer to themselves as hackers. |

**Script Kiddies**

1. Define script kiddies as individuals that want to break into computers to create damage. They download automated hacking software (scripts) from Web sites and use it to break into computers.
2. Point out that script kiddies can acquire entire exploit kits from other attackers. It takes little skill to be a script kiddie.

#### Hactivists

1. Mention that hactivists are a group strongly motivated by ideology. They are likely to break into a website and change the contents as a means of making a political statement.
2. Point out that it is estimated that there are thousands of hacktivist groups worldwide supporting a wide variety of causes.

#### Nation State Actors

1. Define nation state actors as individuals hired by governments to launch computer attacks against the country’s foes.
2. Mention that a new class of attacks called Advanced Persistent Threat (APT) have been created. Further explain that these attacks uses innovative attack tools and once a system is infected it silently extracts data over an extended period.

**Insiders**

1. Mention that one of the largest information security threats to a business actually comes from an unlikely source: its employees, contractors and business partners.
2. Describe some of the reasons an employee would break into their company’s computer, including:
	1. Disgruntled employees may be intent on retaliating against the company
	2. Industrial espionage
	3. Blackmailing

**Other Threat Actors**

1. Use Table 1-7 to discuss the characteristics of the different types of attackers mentioned in this section of the text.

**Defending Against Attacks**

1. Mention that although multiple defenses may be necessary to withstand an attack, these defenses should be based on five fundamental security principles: layering, limiting, diversity, obscurity, and simplicity.

**Layering**

1. Mention that information security must be created in layers.
2. Explain that one defense mechanism may be relatively easy for an attacker to circumvent. Instead, a security system must have layers, making it unlikely that an attacker has the tools and skills to break through all the layers of defenses.
3. Explain that a layered approach (also called defense-in-depth) can also be useful in resisting a variety of attacks. Layered security provides the most comprehensive protection.

**Limiting**

1. Mention that limiting access to information reduces the threat against it.
2. Explain that only those who must use data should have access to it. In addition, the amount of access granted to someone should be limited to what that person needs to know.
3. Mention that some ways to limit access are technology-based, while others are procedural.

|  |  |
| --- | --- |
| ***Teaching*** ***Tip*** | What level of access should users have? The best answer is the least amount necessary to do their jobs, and no more. |

**Diversity**

1. Explain that layers must be different (diverse) so that if attackers penetrate one layer, they cannot use the same techniques to break through all other layers.
2. Using diverse layers of defense means that breaching one security layer does not compromise the whole system.

**Obscurity**

1. Explain that an example of obscurity is not revealing the type of computer, operating system, software, and network connection that a computer uses. An attacker who knows that information can more easily determine the weaknesses of the system.
2. Mention that obscuring information can be an important way to protect information.

**Simplicity**

1. Explain that information security is by its very nature complex. Complex security systems can be hard to understand, troubleshoot, and feel secure about.
2. Mention that as much as possible, a secure system should be simple for those on the inside to understand and use. Complex security schemes are often compromised to make them easier for trusted users to work with. Keeping a system simple from the inside but complex on the outside can sometimes be difficult but reaps a major benefit.

**Frameworks and Reference Architectures**

1. Explain that industry-standard frameworks and reference architectures provide a resource of how to create a secure IT environment.
2. Point out to students that various frameworks/architectures are specific to a particular sector (industry-specific frameworks) such as the financial industry.
3. Discuss how some of the framework/architectures are domestic while others are worldwide (national vs. international).

**Quick Quiz 2**

1. \_\_\_\_\_\_\_ is a generic term used to describe individuals who launch attacks against other users and their computers.

Answer: Threat actors

1. The motivation of which type of threat actor may be defined as ideology, or attacking for the sake of their principles or beliefs?
2. script kiddies
3. hactivists
4. nation state actors
5. insiders

Answer: B

1. Attackers who do their work by downloading automated attack software from websites and use it to perform malicious acts are known as which of the following?
2. script kiddies
3. hactivists
4. nation state actors
5. insiders
6. Answer: A
7. In which fundamental security principle would only those personnel who must use data have access to it?
8. layering
9. limiting
10. diversity
11. obscurity

Answer: B

1. Which fundamental security principle involves not revealing the type of computer, version of operating system, or brand of software that is used?
2. layering
3. limiting
4. diversity
5. obscurity

Answer: D

# **Class Discussion Topics**

1. What are the differences between hactivists and state-sponsored attackers?
2. Ask students to explain why creating a defense-in-depth is a good strategy when creating a secure IT environment.

# **Additional Projects**

1. Ask your students to read more about phishing scams and write a report with a series of guidelines to recognize them and other fraudulent e-mails.

Nessus is a widely used free vulnerability scanner tool used by many security experts. Ask your students to read more about Nessus and write a report summarizing its more important features.

# **Additional Resources**

1. FTC – Computer Security

<http://www.consumer.ftc.gov/topics/computer-security>

1. Fight Spam on the Internet!

<http://spam.abuse.net/>

1. How to recognize phishing e-mail messages, links, or phone calls

<http://www.microsoft.com/security/online-privacy/phishing-symptoms.aspx>

1. Anti-Phishing Working Group

<http://www.antiphishing.org/>

1. SANS' Information Security Reading Room

<http://www.sans.org/reading_room/>

1. Zero day initiative

<http://www.zerodayinitiative.com/>

**Key Terms**

* **accept**
* **administrative controls**
* **Advanced Persistent**
* **Threat (APT)**
* **architecture/design**
* **weaknesses**
* **asset**
* **attributes**
* **availability**
* **avoid**
* **competitors**
* **confidentiality**
* **control diversity**
* **default configurations**
* **defense-in-depth**
* **end-of-life system**
* **external**
* **funding and resources**
* **hactivists**
* **improper error**
* **handling**
* **improper input handling**
* **improperly configured**
* **accounts**
* **industry-specific**
* **frameworks**
* **industry-standard**
* **frameworks**
* **insiders**
* **integrity**
* **intent and motivation**
* **internal**
* **international**
* **lack of vendor support**
* **layered security**
* **misconfiguration**
* **mitigate**
* **nation state actors**
* **national**
* **new threat**
* **non-regulatory**
* **open-source intelligence**
* **organized crime**
* **race condition**
* **reference architectures**
* **regulatory**
* **resource exhaustion**
* **risk**
* **risk response**
* **techniques**
* **script kiddies**
* **sophisticated**
* **system sprawl**
* **technical controls**
* **threat**
* **threat actor**
* **transfer**
* **undocumented assets**
* **untrained users**
* **user training**
* **vendor diversity**
* **vulnerability**
* **vulnerable business**
* **processes**
* **weak configuration**
* **zero day**