Chapter 1 Solutions

Review Questions

1. Identify the three main items that are utilized in achieving security objectives in order to protect our information and system

   policies, procedures and design

2. Identify and define three objectives that are key to achieving effective security architecture.

   Confidentiality—the efforts taken through policy, procedure, and design in order to create and maintain the privacy and discretion of information and systems.

   .*Integrity*— efforts taken through policy, procedure, and design to create and maintain reliable, consistent, and complete information and systems.

   Availability— the efforts taken through policy, procedures and design in order to create and maintain the accessibility of resources on a network.

3. List and define the different classifications created to clarify the difference between hackers and crackers.

   White hat— an ethical hacker; a hackers that uses their extensive experience and knowledge to test systems and provide security consultation to others.
   Grey hat— an individual or groups of individuals that waver between the classification of a hacker and a cracker. Grey hats sometimes act in good will and other times in malice.
   Black hat— someone who breaks into computer networks without authorization and with malicious intent.
   Hactivist— hackers and crackers who use their extensive experience and skill to use networks to share their ideologies regarding controversial social, political, and economic tips.
   Script Kiddie— amateur crackers that use programs and scripts written by other people to infringe upon a computer network system's integrity.

4. List six common errors that users make on a network. Give examples of each.

   Poor habits —leaving computers unlocked and unattended while using the restroom, attending meetings, going to lunch, or visiting colleagues.
   Password error— choosing easy to guess passwords, writing them down on post-its or in notebooks and storing them in plain sight, on desks, under keyboards, or on top of monitors.
   Disregard to company policy— visiting unauthorized websites and downloading unauthorized software in the process; attaching unauthorized equipment to their PC's, like USB (Universal Serial Bus) devices and external hard drives; logging into the company remotely using unapproved personal laptops and computers.
   Opening unknown e-mails —viewing risky attachments containing games, greeting cards, pictures, and macro files.
   Inappropriate Disclosure— giving out information over the phone and falling prey to social engineering.
   Procrastination— failing to report computer or network issues in a sufficient amount of time**.**

5. Explain three ways that the Internet can be used as a tool to compromise information security.

   Hijacking, malware, and spoofing

6. List the destructive tactics that uneducated computer users can run into when using e-mail.

   Attachments, phishing, and web-embedded HTML

7. Define the following: computer viruses, worms, Trojans, spyware, adware, and bots.

   Computer virus— a form of malware intended to spread from one computer to another without detection.

   Worm— self-replicating malware that is able to harness the power of networks and use this power in its attacks against them.

   Trojan (Trojan horse)— malware that disguises itself and its harmful code which often hide within enticing programs such as software updates, games, and movies.

   Spyware a— general term for any software that intentionally monitors and records a user's computer and/or internet activi—ties.

   Adware —a general term for software that uses typical malware intrusion techniques to obtain marketing data or advertise a product or service.

   Bot, or software robot— a form of malware that has the ability to perform a large array of automated tasks for an intruder at a remote location, ranging in severity from spamming a system to initiating DoS attacks on sytems.

8. List and define each phase in the process of creating and maintaining security architecture.

   Assessment and analysis—the identification of vulnerabilities, threats, and assets that exist within an environment's devices, resources, and vendor relationships.

   Design and modeling—the creation of policies and prototype security architecture that fit the needs of a business.

   Deployment—security policies, hardware, and tools defined in previous phases are put into place.

   Management and support— the ongoing support, maintenance, and assessment of the security architecture that was deployed in the previous phase.

9. List and describe the information that should be included in a security policy.

   Define the overall goals of the policy—shows a direct relationship to the overall business goals.

   Provide the scale of the security policy—which data, people, departments, facilities, and technology are included and protected by the policy.

   Define the roles and responsibilities—of all employees the roles of those involved in maintaining the security of the environment.

   Identify processes—includes processes for both prevention, detection, and reaction of security threats that include, but are not limited to, securing, updating, maintaining, managing and monitoring a network.

   *Handle non-compliance*t—he consequences for not complying with security policy.

10. Explain the difference between an update and an upgrade.

    An update is a change that is added to previously installed software or firmware, and an upgrade is

    a replacement for older versions of software or firmware.

11. List six questions you should ask when creating a backup management plan.

    What type of media should I use?

    Where is the backup to be placed?

    What should be backed up?

    How often should information be saved?

    What time of day or night should backup occur?

What type of backup should be completed?

12. Which backup media would be most appropriate for a large enterprise or network?

    Tape backup cassettes

13. Identify and explain the four options available for restoring your network in the event of a disaster.

    Cold site—is a facility that provides the basic necessities for rebuilding your network. A contract that involves a cold site would promise the use of a facility that provides water, power, air conditioning, or heat. This is the least expensive agreement that can be made.
    Warm site—a facility that contains the basic environmental concerns, as well as computers, connection hardware, and software devices necessary to rebuild a network system..
    Hot site— an exact replica of an organization's network, or a mirror site, that promises that the vendor will assume all responsibility for ensuring that the network is readily available in the event of a disaster.
    Shared site agreements— an arrangement between companies with similar, if not identical, data centers.

14. Explain the multi-layered nature of security.

    Answers may vary. If multiple layers of security are applied to a network, intruders will have a more difficult time accessing the network. If a single layer of security is compromised, the intruder will have to bypass the second or even third level to gain access to vital data.

15. Identify the layers within the multi-layered approach to security and give examples of each.

    Operational layer user awareness training, change management, patch and update management, backup management, disaster recovery, risk management

    Physical layer smart cards, locked doors, security monitoring equipment

    Design layer firewalls, proxy servers, intrusion detection systems, DMZ zones

    File layer/access controls encryption techniques, password policies, user and group rights

    Transport layer public and private keys, authentication, SSL

Case Studies

Case Study 1-1: Locating Recent Vulnerabilities

Answers may vary based on recent state of network vulnerability.

Case Study 1-2: Legal Privacy Compliancy

Compliance Laws may vary based on location.

Compliance Laws	Rules
Payment Card Industry (PCI) Data Security Standard (DSS),	Credit card companies- encrypt transmission of sensitive information (including visa cards) and end to end encryption of wireless
The Health Information Technology for Economic and Clinical Health (HITECH)	In the healthcare industry- must secure protected health information in transit, at rest, or in use. Data encryption must be so strong that it leaves information unable to be deciphered by unauthorized people or computers.

The Sarbanes-Oxley Act (SOX)	In public companies- CEO's and CFO's must ensure guaranteed no access, procedures, and controls to ensure no unauthorized access, that information is protected and separated from other information before it is widely disclosed. Must ensure CIA of data at rest and in motion.
Graham-Leach-Bliley Act	Financial institutions- must protect information by encrypting sensive consumer data when in transit on public networks.
The Basel II	Banks- must implement information methods that are strong, protect critical information traveling on the network, and ensure CIA of customer data and institutions data.
ISO 17799 Compliance	General template for all types of organizations to use, seen throughout the world as best practice for information technology groups that guarantee CIA.

Case Study 1-3: Understanding the Risk that Users Pose

Password restrictions, mandatory security training, unauthorized software not allowed, all hardware must be approved (storage devices, laptops, etc.), users not permitted on unauthorized websites, users are not permitted to download unfamiliar e-mail attachments or open unauthorized e-mails, do not write passwords down, users are not to share sensitive information or access to accounts, computer etc., lock PC while unattended.

Answers may vary.

Hands-On Projects

Hands-on Project 1-1: Assessing and Prioritizing Risks

Answers will vary.

Hands-on Project 1-2: Designing Your Security Defense

Answers will vary.

Hands-on Project 1-3: Implementing A Strategy

Answers will vary.