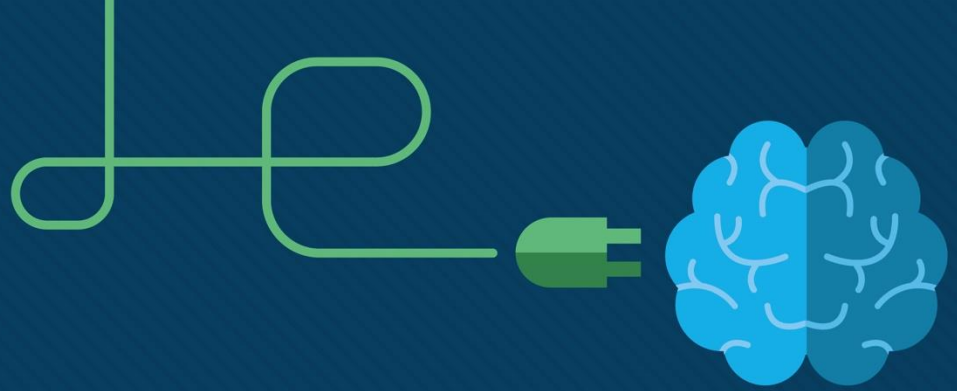
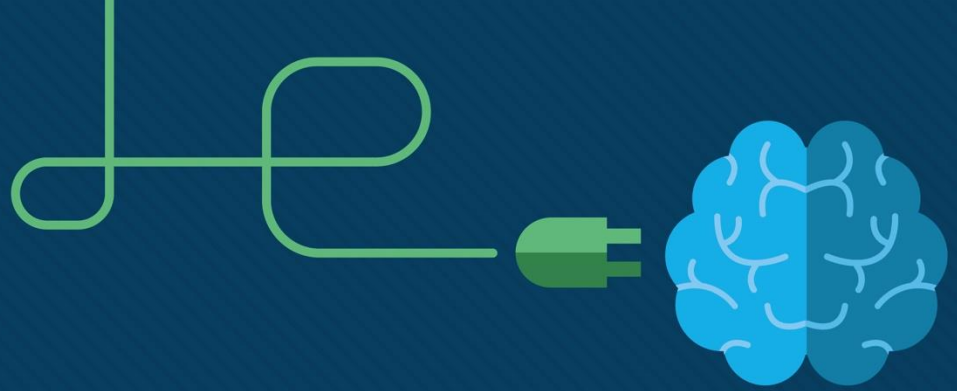


Chapter 1: The Need for Cybersecurity

Introduction to Cybersecurity v2.1



Chapter 1: The Need for Cybersecurity

Introduction to Cybersecurity v2.1

Chapter 1 - Sections & Objectives

- 1.1 Personal Data
  - Explain the characteristics and value of personal data.
    - Define personal data.
    - Explain why personal data is profitable to hackers.
- 1.2 Organization Data
  - Explain the characteristics and value of data within an organization.
    - Describe types of data used by governments and organizations.
    - Describe the impact of a security breach.
- 1.3 Attackers and Cybersecurity Professionals
  - Explain the characteristics and motives of cyber attackers and the legal and ethical issues for cybersecurity professionals.
    - Describe the characteristics and motives of an attacker.
- 1.4 Cyberwarfare
  - Explain the characteristics and purpose of cyberwarfare.
    - Describe cyberwarfare.

1.1 Personal Data

Introduction to Personal Data

- What is Cybersecurity?
  - Protection of networked system and data from unauthorized use or harm
- Your Online and Offline Identity
  - Offline Identity
    - Your identity that interacts on a regular basis at home, school or work
  - Online Identity
    - Your identity while you are in cyberspace
    - Should only reveal a limited amount of information about you
    - Username or alias
      - Should not include any personal information
      - Should be appropriate and respectful
      - Should not attract unwanted attention

Introduction to Personal Data

- Your Data
  - Medical Records
    - electronic health records (EHR) – physical, mental, and other personal information
    - prescriptions
  - Education Records
    - Grades, test scores, courses taken, awards and degrees rewarded
    - Attendance
    - Disciplinary reports
  - Employment and Financial Records
    - Income and expenditures
    - Tax records – paycheck stubs, credit card statements, credit rating and banking statement
    - Past employment and performance

Introduction to Personal Data

- Where is Your Data?
  - Medical records: doctor's office, insurance company
  - Store loyalty cards
    - Stores compile your purchases
    - Marketing partner uses the profiles for target advertisement
  - Online pictures: friends, strangers may also have a copy
- Your Computer Devices
  - Data storage and your portal to your online data
  - List some example of your computing devices

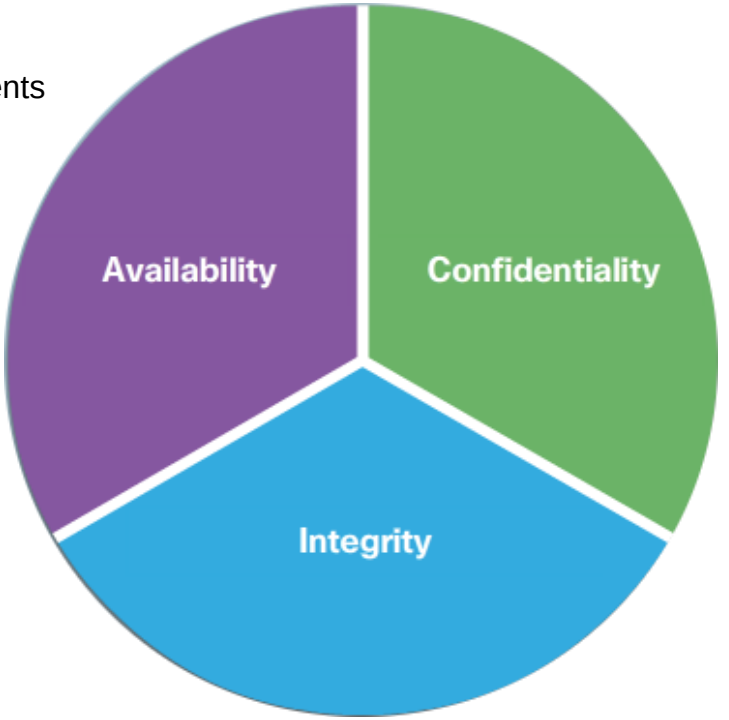
Personal Data as a Target

- How do the criminals get your money?
  - Online credentials
    - Gives thieves access to your accounts
  - Creative schemes
    - Trick into wiring money to your friends or family
- Why do they want your identity?
  - Long-term profits
  - Medical benefits
  - File a fake tax return
  - Open credit card accounts
  - Obtain loans

1.2 Organizational Data

Introduction to Organizational Data

- Types of Organizational Data
  - Traditional Data
    - Personnel – application materials, payroll, offer letter, employee agreements
    - Intellectual – patents, trademarks, product plans, trade secrets
    - Financial – income statements, balance sheets, cash flow statements
  - Internet of Things and Big Data
    - IoT – large network of physical objects, such as sensors
    - Big Data – data from the IoT
- Confidentiality, Integrity and Availability
  - Confidentiality – privacy
  - Integrity – accuracy and trustworthiness of the information
  - Availability – information is accessible



Lab – Compare Data with a Hash

Networking Academy

Lab – Compare Data with a Hash

Objectives

Use a hashing program to verify the integrity of data.

Background / Scenario

It is important to understand when data has been corrupted or it has been tampered with. A hashing program can be used to verify if data has changed, or if it has remained the same. A hashing program performs a hash function on data or a file, which returns a (usually much shorter) value. There are many different hash functions, some very simple and some very complex. When the same hash is performed on the same data, the value that is returned is always the same. If any change is performed on the data, the hash value returned will be different.

Note: You will need installation privileges and some knowledge of the process to install Windows programs.

Required Resources

- PC with Internet access

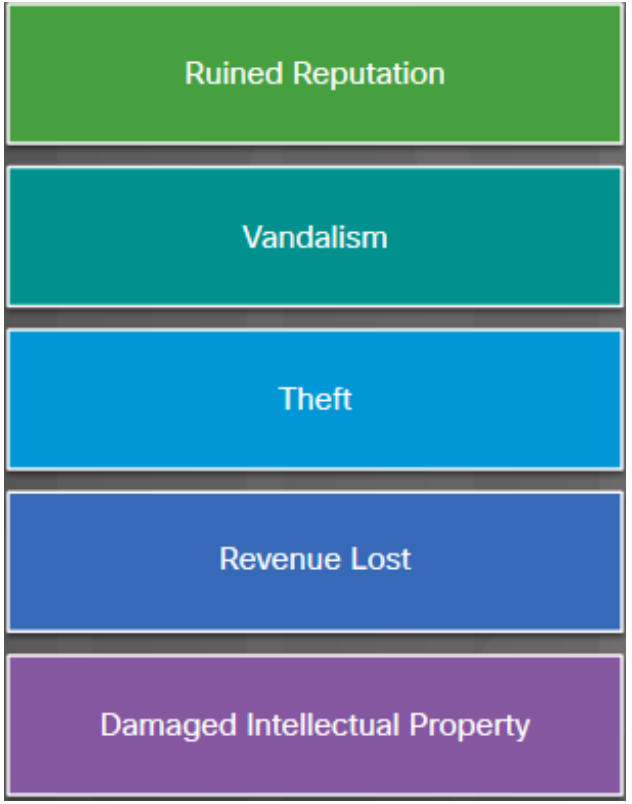
Step 1: Create a Text file

a. Search your computer for the Notepad program and open it.

b. Type some text in the program.

The Impact of a Security Breach

- The Consequences of a Security Breach
  - Not feasible to prevent every attack
  - Attackers will always find new ways
  - Ruined reputation, vandalism, theft, revenue lost, damaged intellectual property
- Security Breach Example - LastPass
  - An online password manager
  - Stolen email addresses, password reminders, and authentication hashes
  - Requires email verification or multi-factor authentication when logging in from an unknown device
  - Users should use complex master password, change master password periodically, and beware of phishing attacks



The Impact of a Security Breach

- Security Breach Example - Vtech
  - Vtech is a high tech toy maker for children
  - exposed sensitive information including customer names, email addresses, passwords, pictures, and chat logs.
  - Vtech did not safeguard information properly
  - Hackers can create email accounts, apply for credits, and commit crimes using the children's information
  - Hackers can also take over the parents' online accounts
- Security Breach Example - Equifax
  - Equifax is a consumer credit reporting agency.
  - Attackers exploited a vulnerability in web application software.
  - Equifax established a dedicated web site with a new domain name that allowed nefarious parties to create unauthorized websites for phishing scheme

Lab – What Was Taken?

Networking Academy

Lab – What was Taken?

Objectives

Search for and read about a few recent occurrences of security breaches.

Background / Scenario

Security breaches occur when individuals or applications are trying to gain unauthorized access to data, applications, services, or devices. During these breaches, the attackers, whether they are insiders or not, attempt to obtain information that they could use for financial gains or other advantages. In this lab, you will explore a few security breaches to determine what was taken, what exploits were used, and what you can do to protect yourself.

Required Resources

- PC or mobile device with Internet access

Security Breach Research

a. Use the two provided links to security breaches from different sectors to fill out the table below.

b. Search for a few additional interesting breaches and record the findings in the table below.

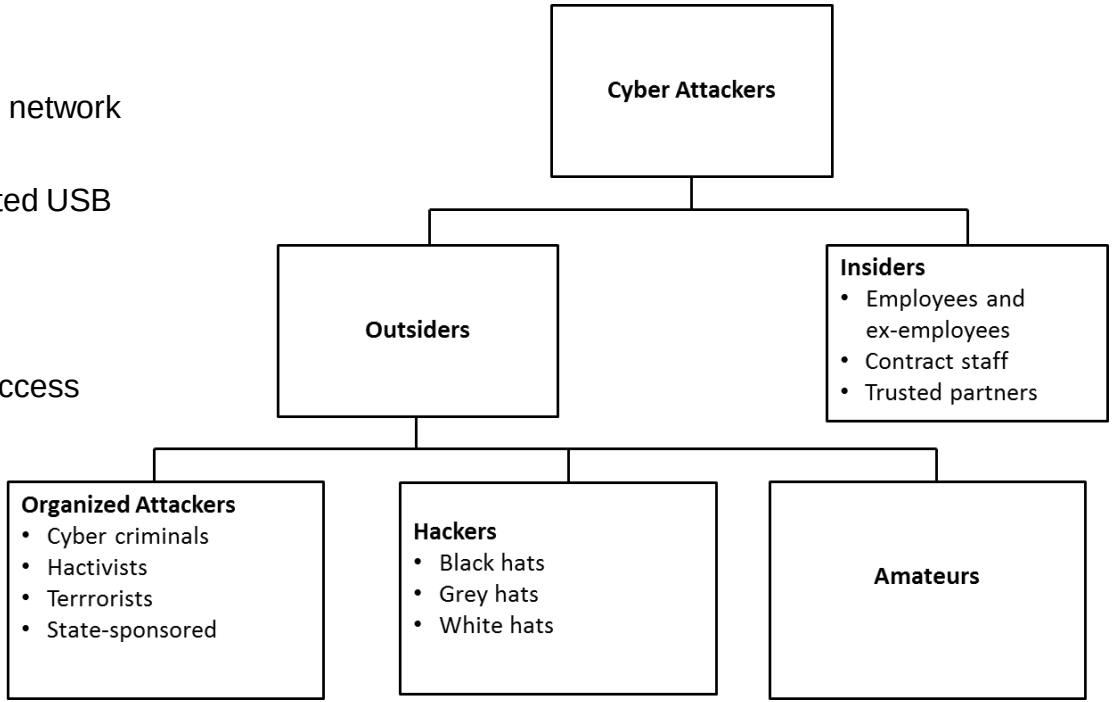
1.3 Attackers and Cybersecurity Professionals

Types of Attackers

- Amateurs
  - Script kiddies with little or no skill
  - Using existing tools or instructions found online for attacks
- Hackers - break into computers or networks to gain access
  - White hats – break into system with permission to discover weaknesses so that the security of these systems can be improved
  - Gray hats – compromise systems without permission
  - Black hats - take advantage of any vulnerability for illegal personal, financial or political gain
- Organized Hackers - organizations of cyber criminals, hacktivists, terrorists, and state-sponsored hackers.

Internal and External Threats

- Internal Security Threats
  - Can be an employee or contract partner
    - Mishandle confidential data
    - Threaten the operations of internal servers or network infrastructure devices
    - Facilitate outside attacks by connecting infected USB media into the corporate computer system
    - Accidentally invite malware onto the network through malicious email or websites
    - Can cause great damage because of direct access
- External Security Threats
  - exploit vulnerabilities in network or computing devices
  - use social engineering to gain access



1.4 Cyberwarfare

What is Cyberwarfare

- What is Cyberwarfare?
  - Conflict using cyberspace
  - Stuxnet malware
    - Designed to damage Iran's nuclear enrichment plant
    - Used modular coding
    - Used stolen digital certificates

The Purpose of Cyberwarfare

- Use to gain advantage over adversaries, nations or competitors
  - Can sabotage the infrastructure of other nations
  - Give the attackers the ability to blackmail governmental personnel
  - Citizens may lose confidence in the government's ability to protect them.
  - Affect the citizens' faith in their government without ever physically invading the targeted nation.

1.5 Chapter Summary

Summary

- Define personal data.
- Explain the characteristics and value of personal data.
- Explain the characteristics and value of data within an organization.
- Describe the impact of security breach.
- Describe the characteristics and motives of an attacker.
- Describe the legal and ethical issues facing a cybersecurity professional.
- Explain the characteristics and purpose of cyberwarfare.


CISCO