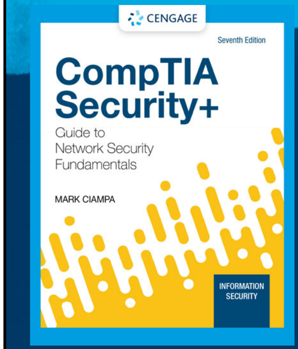


CENGAGE

Seventh Edition

CompTIA Security+

Guide to Network Security Fundamentals

MARK CIAMPA

INFORMATION SECURITY

Module 1
Introduction to Security

Background

- Why is it important for all computer users, not just IT professionals, to understand the importance of network and computer security

- Security Problem- 50 years ago and now?

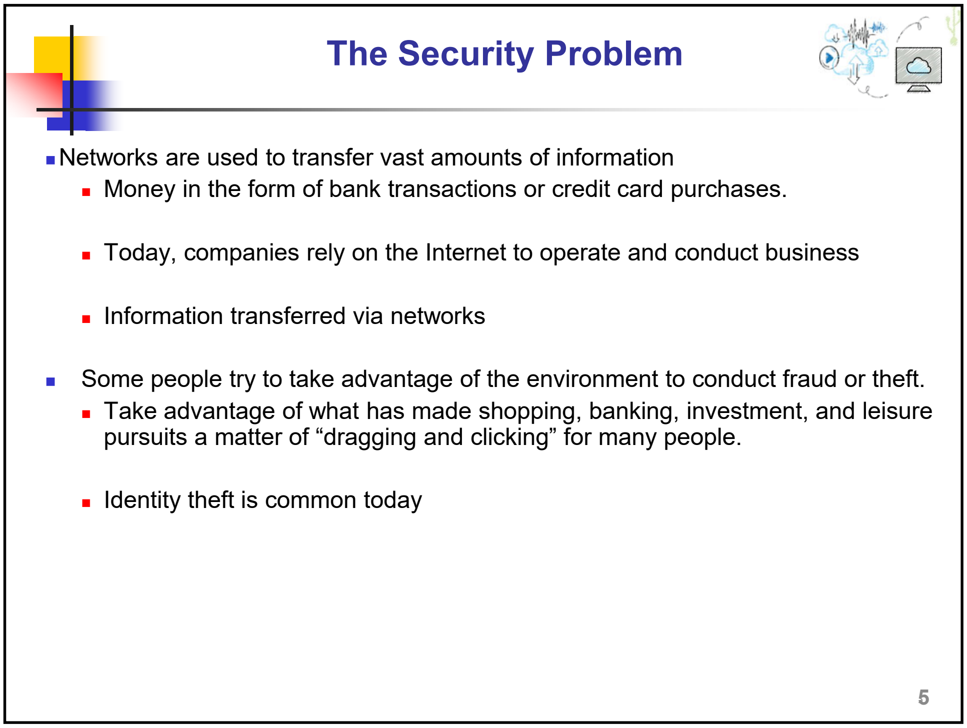
Module Objectives

- By the end of this module, you should be able to:
  - Define information security and explain why it is important
  - Identify threat actors and their attributes
  - Describe the different types of vulnerabilities and attacks
  - Explain the impact of attacks

The Security Problem

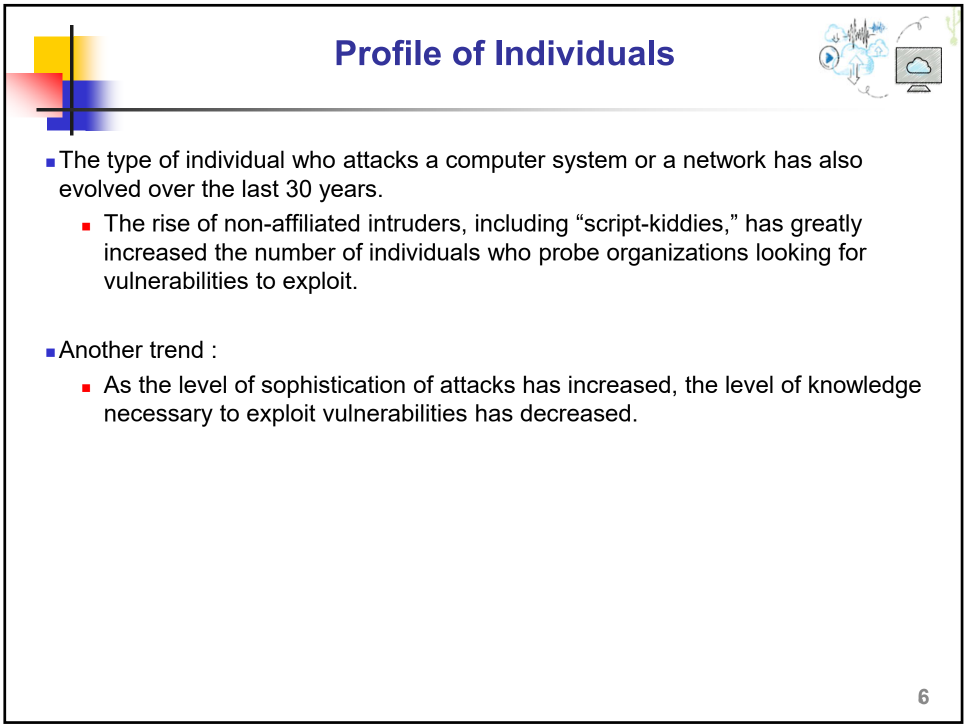
- **Fifty years ago:**
  - Computers and data were uncommon.
  - Computer hardware was a high-value item and security was mainly a physical issue.

- **Now:**
  - PC's- Ubiquitous and portable, making them much more difficult to secure physically.
  - Computers are connected to the Internet.
  - The value of the data on computers often exceeds the value of the equipment.



The Security Problem

- Networks are used to transfer vast amounts of information
  - Money in the form of bank transactions or credit card purchases.
  - Today, companies rely on the Internet to operate and conduct business
  - Information transferred via networks
- Some people try to take advantage of the environment to conduct fraud or theft.
  - Take advantage of what has made shopping, banking, investment, and leisure pursuits a matter of “dragging and clicking” for many people.
  - Identity theft is common today



Profile of Individuals

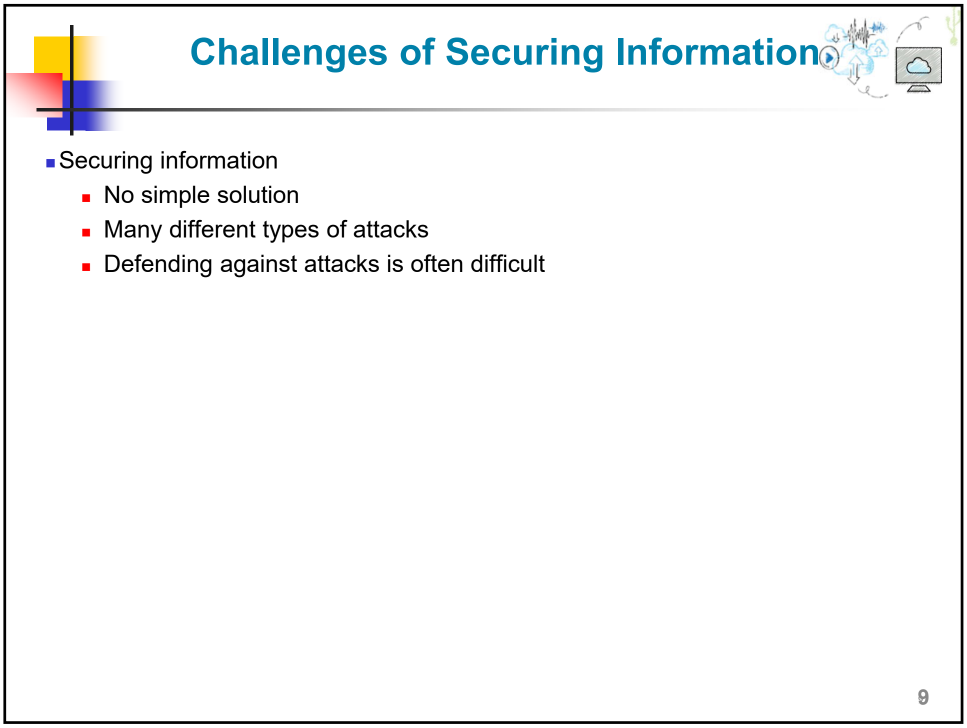
- The type of individual who attacks a computer system or a network has also evolved over the last 30 years.
  - The rise of non-affiliated intruders, including “script-kiddies,” has greatly increased the number of individuals who probe organizations looking for vulnerabilities to exploit.
- Another trend :
  - As the level of sophistication of attacks has increased, the level of knowledge necessary to exploit vulnerabilities has decreased.

Today’s Security Attacks

- Examples of recent attacks
  - Remotely controlling a car
  - Tampering with aircraft systems
  - Yahoo accounts compromised by attackers
  - USB flash drive malware/U S B Killer
  - Stolen data from the European Space Agency
  - IRS fraud
  - Hyatt Hotels Corporation hacked

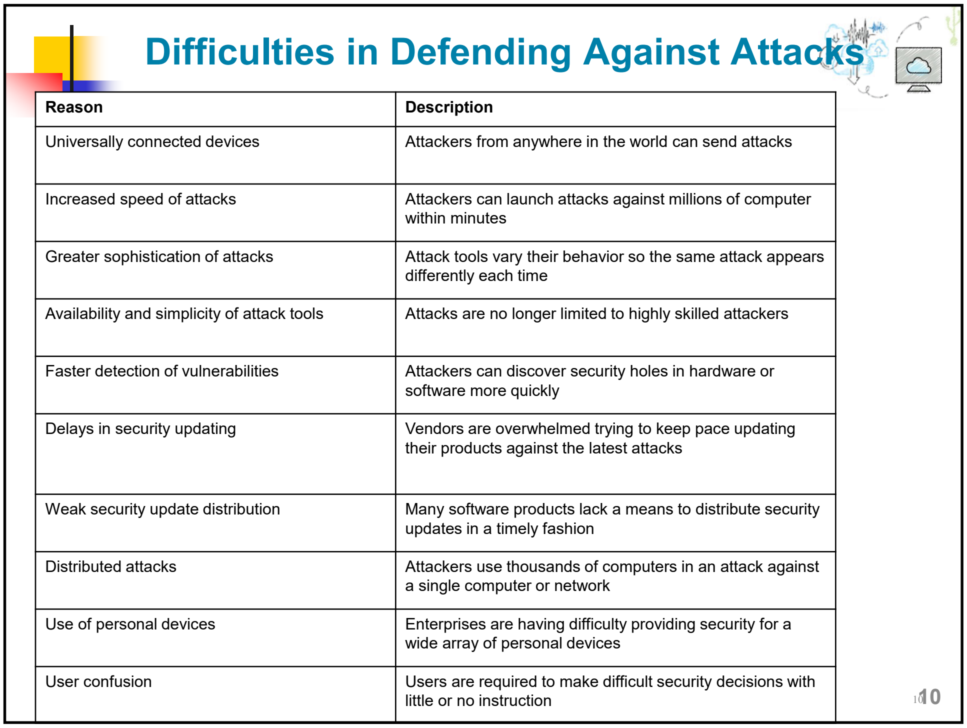
Reasons for Successful Attacks

- Widespread vulnerabilities
- Configuration issues
- Poorly designed software
- Hardware limitations
- Enterprise-based issues



Challenges of Securing Information

- Securing information
  - No simple solution
  - Many different types of attacks
  - Defending against attacks is often difficult



Difficulties in Defending Against Attacks

Reason	Description
Universally connected devices	Attackers from anywhere in the world can send attacks
Increased speed of attacks	Attackers can launch attacks against millions of computer within minutes
Greater sophistication of attacks	Attack tools vary their behavior so the same attack appears differently each time
Availability and simplicity of attack tools	Attacks are no longer limited to highly skilled attackers
Faster detection of vulnerabilities	Attackers can discover security holes in hardware or software more quickly
Delays in security updating	Vendors are overwhelmed trying to keep pace updating their products against the latest attacks
Weak security update distribution	Many software products lack a means to distribute security updates in a timely fashion
Distributed attacks	Attackers use thousands of computers in an attack against a single computer or network
Use of personal devices	Enterprises are having difficulty providing security for a wide array of personal devices
User confusion	Users are required to make difficult security decisions with little or no instruction

As the attacks and the types of attacks continue to increase, the need for trained security personnel also increases.

11

12

What is Information Security?

- Before defense is possible, one must understand:
  - Exactly what security is?
  - How security relates to information security?
  - The terminology that relates to information security?

Understanding Security

- Security is:
  - To be free from danger is the goal
  - The process that achieves that freedom

- As security is increased, convenience is often decreased
  - The more secure something is, the less convenient it may become to use

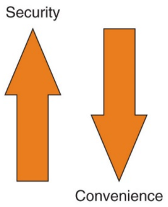
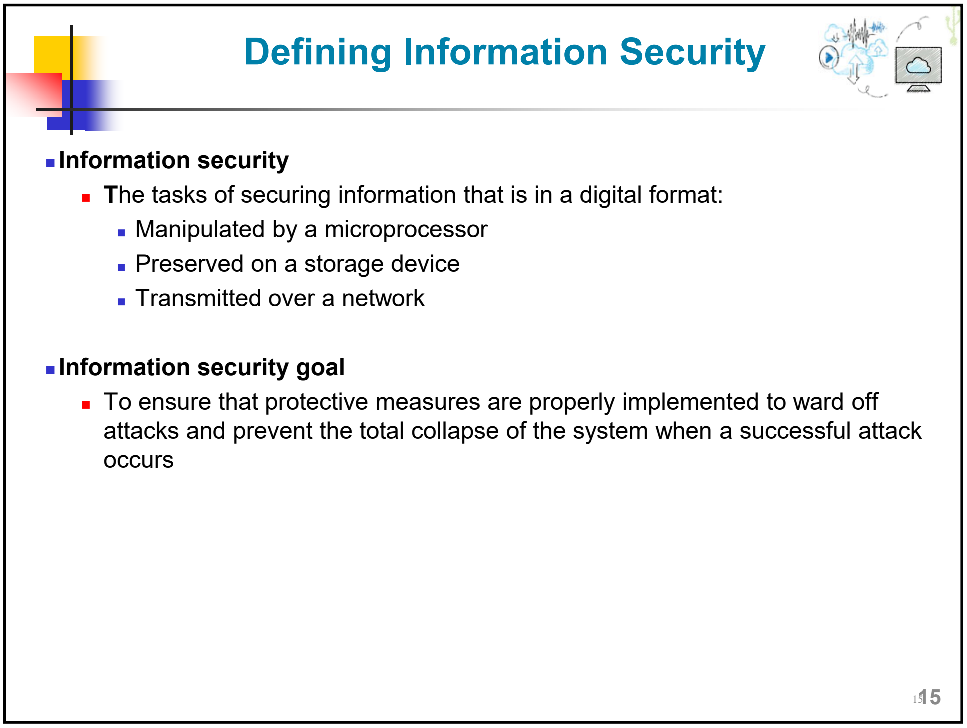


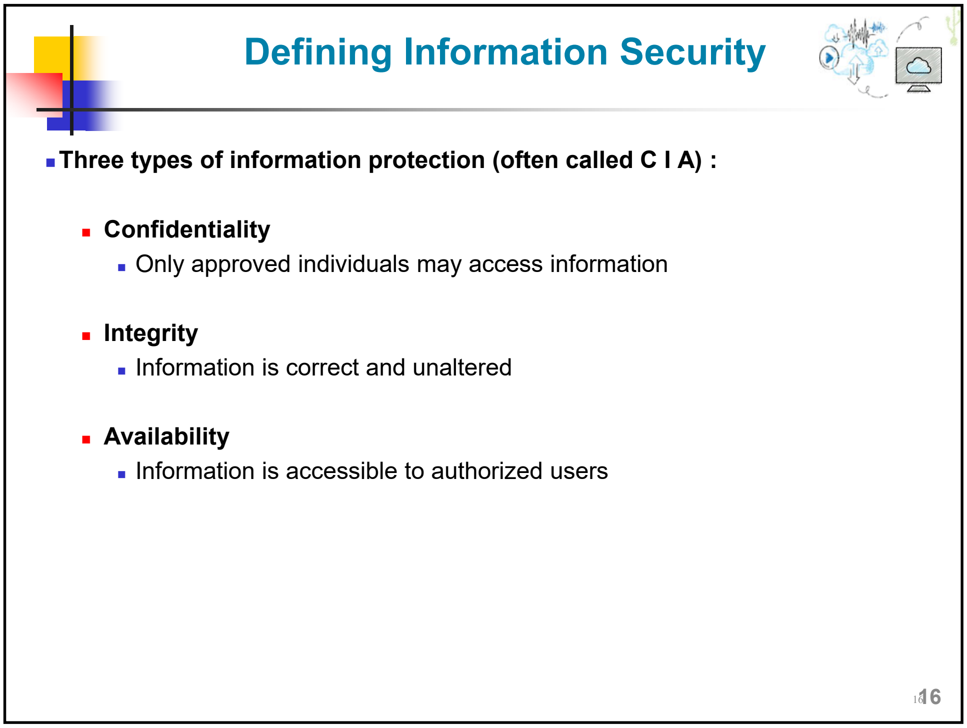
Figure 1-2 Relationship of security to convenience



Defining Information Security

- **Information security**
  - The tasks of securing information that is in a digital format:
    - Manipulated by a microprocessor
    - Preserved on a storage device
    - Transmitted over a network
- **Information security goal**
  - To ensure that protective measures are properly implemented to ward off attacks and prevent the total collapse of the system when a successful attack occurs

15



Defining Information Security

- **Three types of information protection (often called C I A) :**
  - **Confidentiality**
    - Only approved individuals may access information
  - **Integrity**
    - Information is correct and unaltered
  - **Availability**
    - Information is accessible to authorized users

16

Defining Information Security

- Information security is achieved through a process that is a combination of three entities:
  - Information and the hardware
  - Software
  - Communications

- These entities are protected in three layers:
  - Products
  - People
  - Policies and procedures

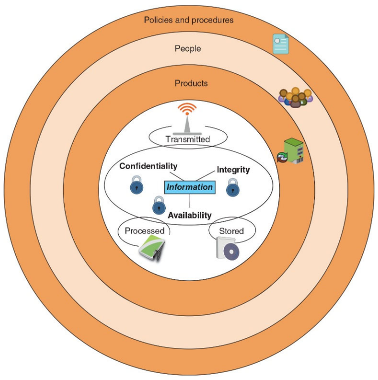
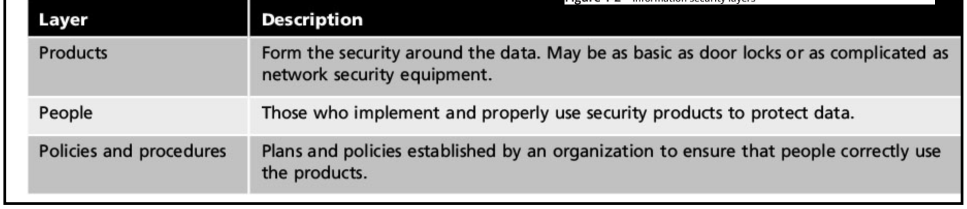


Figure 1-2 Information security layers



Layer	Description
Products	Form the security around the data. May be as basic as door locks or as complicated as network security equipment.
People	Those who implement and properly use security products to protect data.
Policies and procedures	Plans and policies established by an organization to ensure that people correctly use the products.

Information Security Terminology

- **Asset**
  - Item that has value

- **Threat**
  - Type of action that has the potential to cause harm

- **Threat actor**
  - An individual or entity with capapility to carry out a threat
  - Responsible for cyber incidents against the technology equipment of enterprises and users
  - The generic term *attacker* is also commonly used

Information Security Terminology (3 of 4)

- **Vulnerability**
  - Flaw or weakness that allows a threat agent to bypass security
- **Threat vector**
  - The means by which an attack can occur
- **Risk**
  - A situation that involves exposure to some type of danger
- **Risk response techniques**:
  - **Accept** – risk is acknowledged but no steps are taken to address it
  - **Transfer** – transfer risk to a third party
  - **Avoid** – identifying risk but making the decision to not engage in the activity
  - **Mitigate** – attempt to address risk by making the risk less serious

Information Security Terminology (2 of 4)

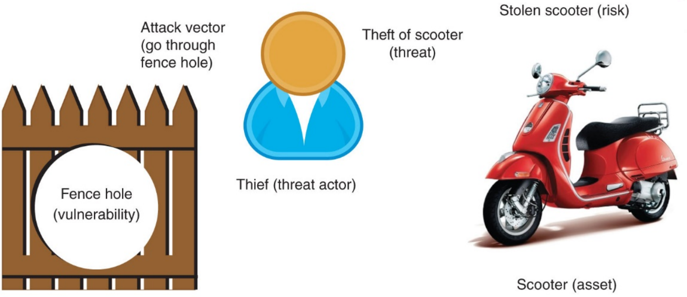

Attack vector (go through fence hole)
Theft of scooter (threat)
Stolen scooter (risk)
Fence hole (vulnerability)
Thief (threat actor)
Scooter (asset)

Figure 1-4 Information security components analogy

Term	Example in Ellie's scenario	Example in information security
Asset	Scooter	Employee database
Threat	Steal scooter	Steal data
Threat agent	Thief	Attacker, hurricane
Vulnerability	Hole in fence	Software defect
Threat vector	Climb through hole in fence	Access web server passwords through flaw in operating system
Threat likelihood	Probability of scooter stolen	Likelihood of virus infection
Risk	Not purchase scooter	Not install wireless network

Who Are the Attackers?

- **Hacker -** person who uses computer skills to attack computers
  - **Black hat hackers**
    - Violate computer security for personal gain and the goal is to inflict malicious damage
  - **White hat hackers**
    - Goal to expose security flaws, not to steal or corrupt data
  - **Gray hat hackers**
    - Goal is to break into a system without owner's permission, but not for their own advantage
    - Publically disclose the vulnerability

Script Kiddies

- **Script kiddies**
  - Individuals who want to attack computers yet they lack the knowledge of computers and network needed to do so
  - Download automated hacking software (scripts) from websites
  - Over 40 percent of attacks require low or no skills

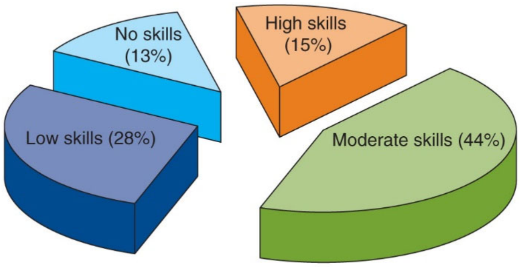
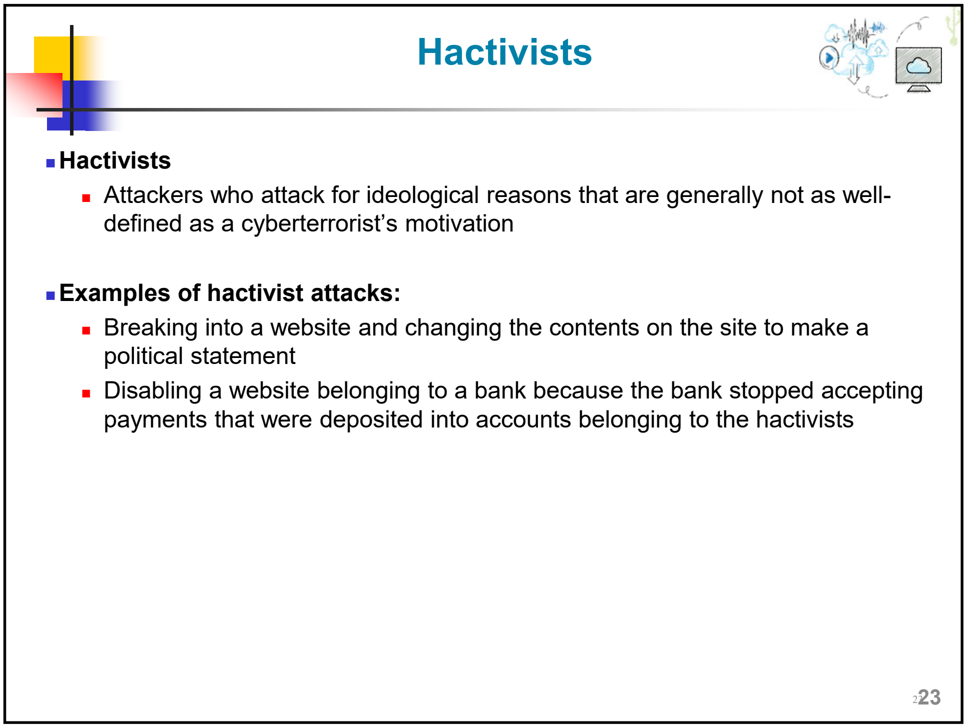


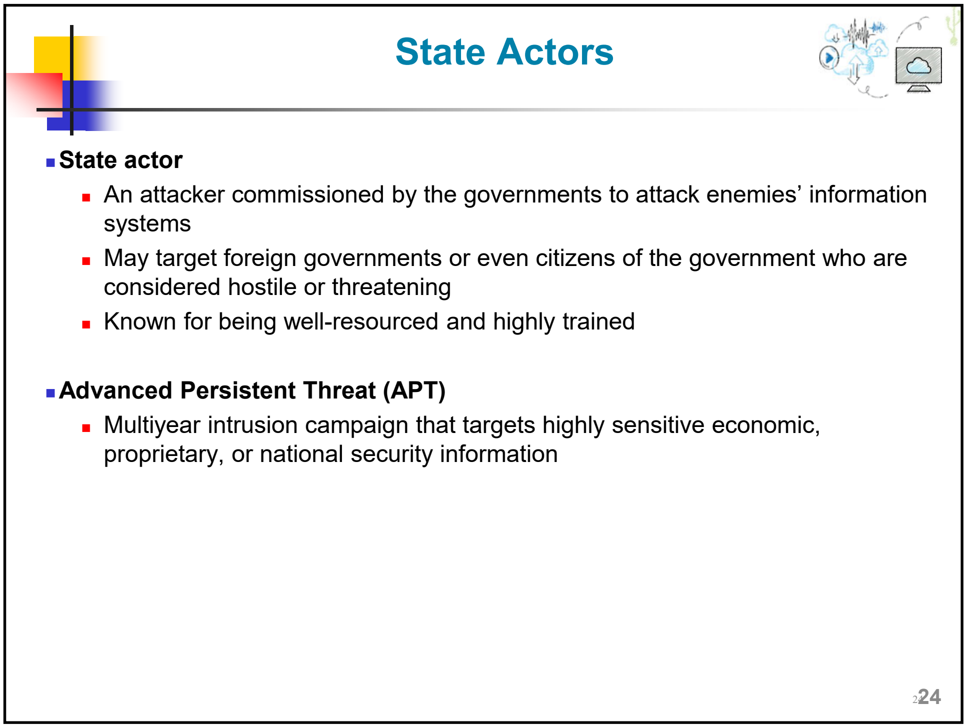
Figure 1-5 Skills needed for creating attacks



Hactivists

- **Hactivists**
  - Attackers who attack for ideological reasons that are generally not as well-defined as a cyberterrorist's motivation

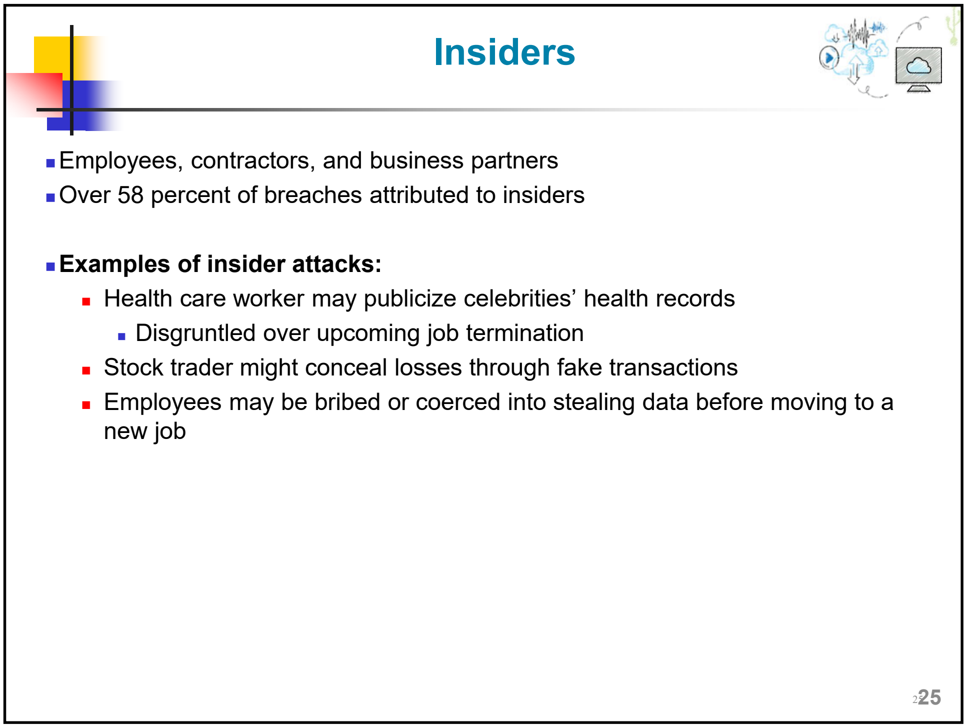
- **Examples of hactivist attacks:**
  - Breaking into a website and changing the contents on the site to make a political statement
  - Disabling a website belonging to a bank because the bank stopped accepting payments that were deposited into accounts belonging to the hactivists



State Actors

- **State actor**
  - An attacker commissioned by the governments to attack enemies' information systems
  - May target foreign governments or even citizens of the government who are considered hostile or threatening
  - Known for being well-resourced and highly trained

- **Advanced Persistent Threat (APT)**
  - Multiyear intrusion campaign that targets highly sensitive economic, proprietary, or national security information

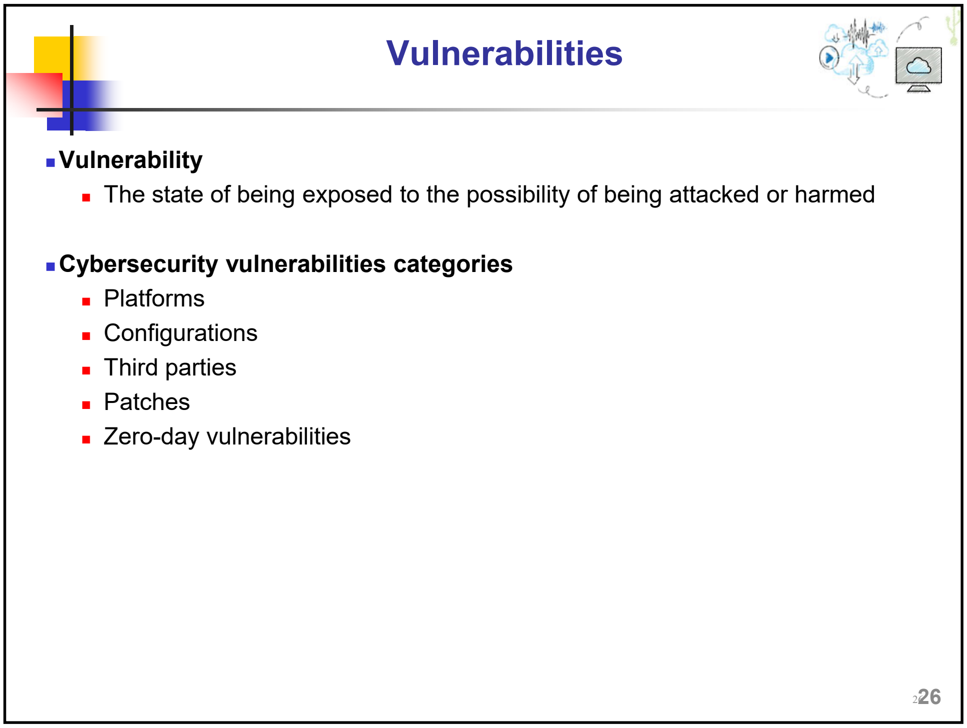


Insiders

- Employees, contractors, and business partners
- Over 58 percent of breaches attributed to insiders

- **Examples of insider attacks:**
  - Health care worker may publicize celebrities’ health records
    - Disgruntled over upcoming job termination
  - Stock trader might conceal losses through fake transactions
  - Employees may be bribed or coerced into stealing data before moving to a new job

25



Vulnerabilities

- **Vulnerability**
  - The state of being exposed to the possibility of being attacked or harmed

- **Cybersecurity vulnerabilities categories**
  - Platforms
  - Configurations
  - Third parties
  - Patches
  - Zero-day vulnerabilities

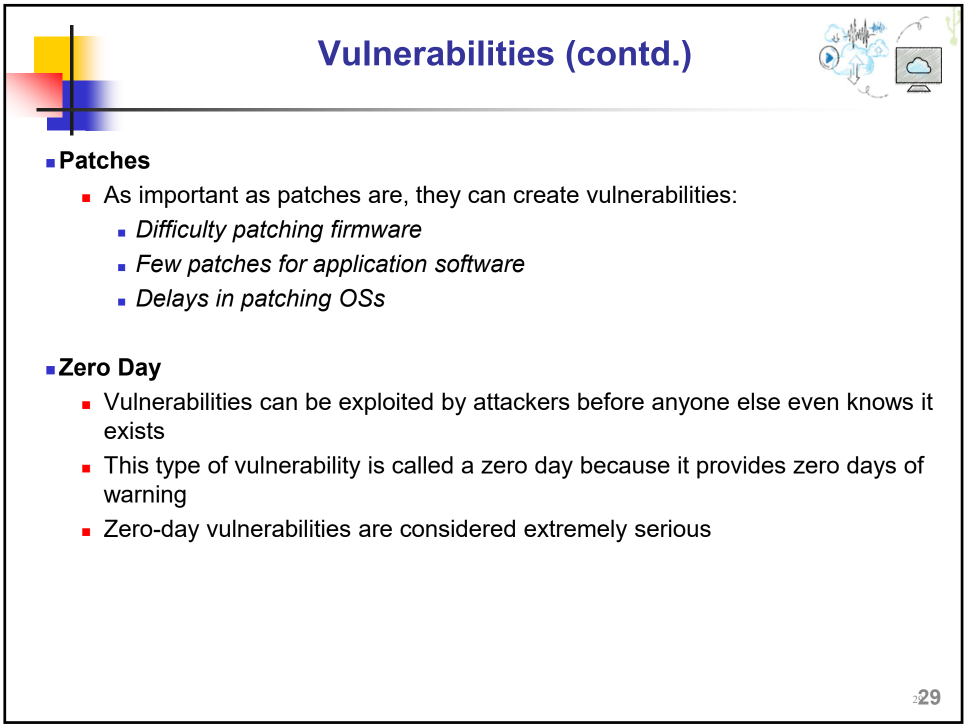
26

Vulnerabilities (contd.)

- **Platforms**
  - A computer platform is a system that consists of the hardware device and an OS that runs software
  - All platforms have vulnerabilities to some degree, some platforms have serious vulnerabilities including:
    - Legacy platforms
    - On-premises platforms
    - Cloud platforms
- **Configuration settings**
  - Often not properly implemented
  - Results in weak configurations

Vulnerabilities (contd.)

- **Third Parties**
  - Almost all businesses use external entities known as third parties
    - Examples : outsourced code development, data storage facilities
  - **Vendor management**
    - The process organizations use to monitor and manage the interactions with all of their external third parties
  - **System integration**
    - Connectivity between the organization and the third party
  - One of the major risks of third-party system integration involves the principle of the weakest link

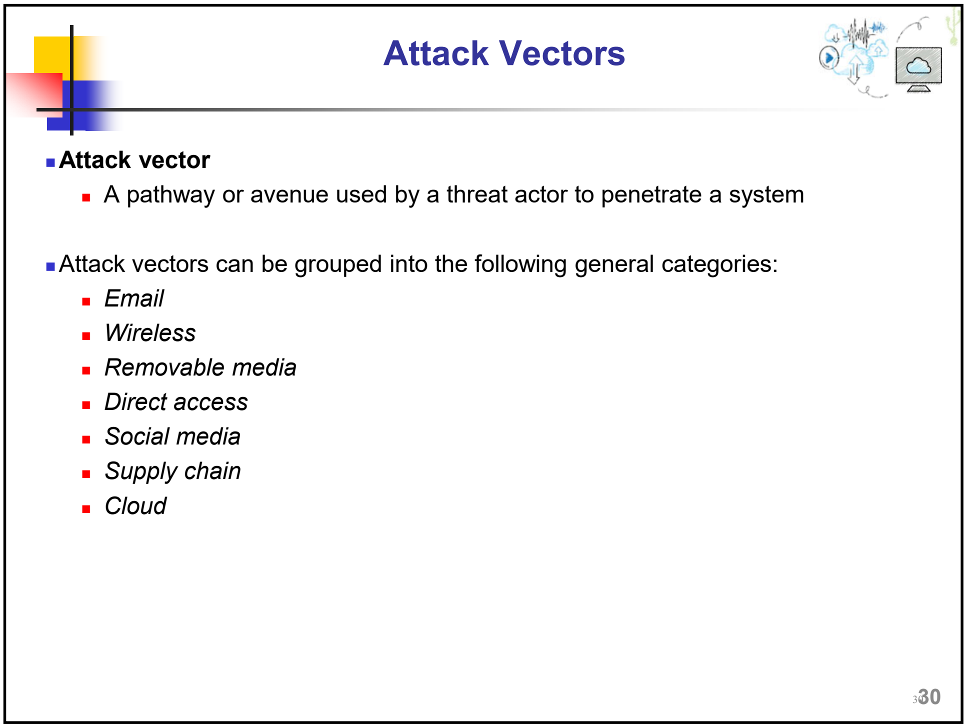


Vulnerabilities (contd.)

- **Patches**
  - As important as patches are, they can create vulnerabilities:
    - *Difficulty patching firmware*
    - *Few patches for application software*
    - *Delays in patching OSs*

- **Zero Day**
  - Vulnerabilities can be exploited by attackers before anyone else even knows it exists
  - This type of vulnerability is called a zero day because it provides zero days of warning
  - Zero-day vulnerabilities are considered extremely serious

29

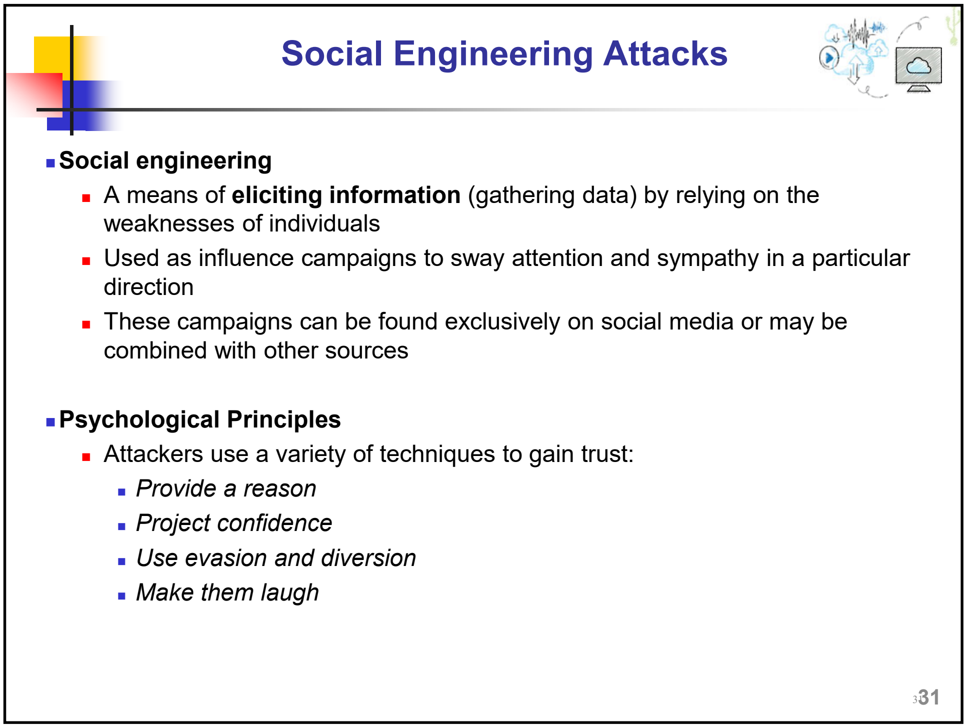


Attack Vectors

- **Attack vector**
  - A pathway or avenue used by a threat actor to penetrate a system

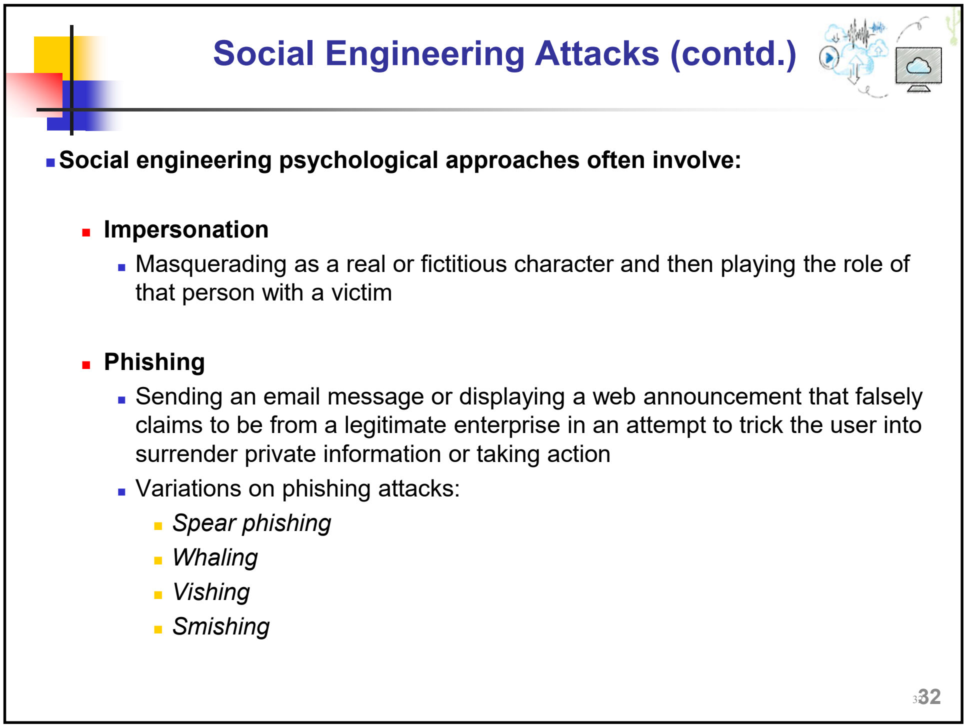
- Attack vectors can be grouped into the following general categories:
  - *Email*
  - *Wireless*
  - *Removable media*
  - *Direct access*
  - *Social media*
  - *Supply chain*
  - *Cloud*

30



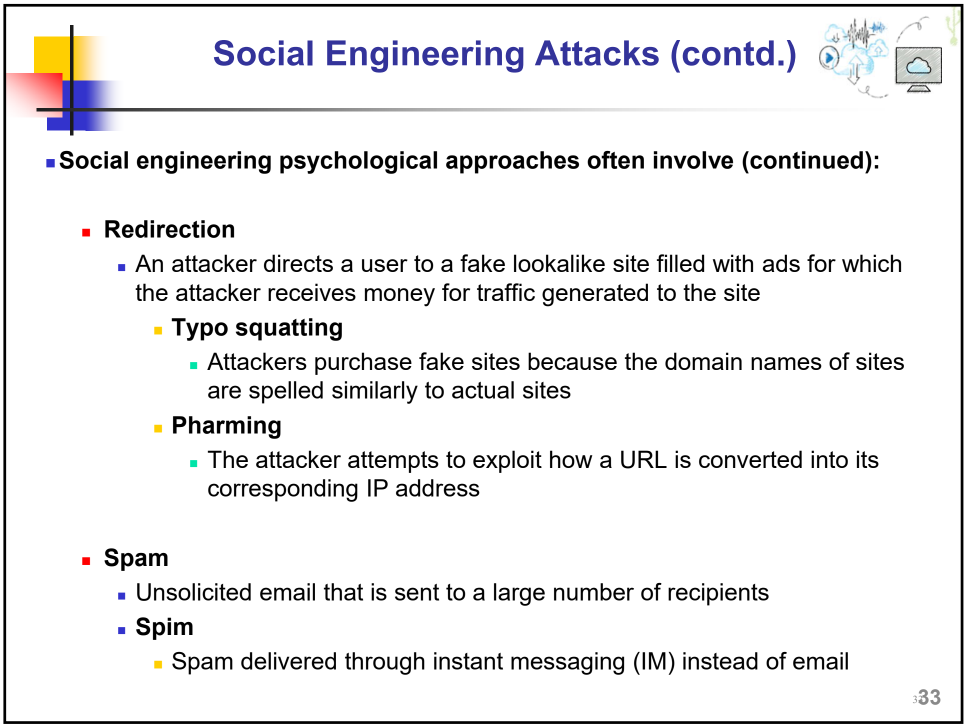
Social Engineering Attacks

- **Social engineering**
  - A means of **eliciting information** (gathering data) by relying on the weaknesses of individuals
  - Used as influence campaigns to sway attention and sympathy in a particular direction
  - These campaigns can be found exclusively on social media or may be combined with other sources
- **Psychological Principles**
  - Attackers use a variety of techniques to gain trust:
    - *Provide a reason*
    - *Project confidence*
    - *Use evasion and diversion*
    - *Make them laugh*



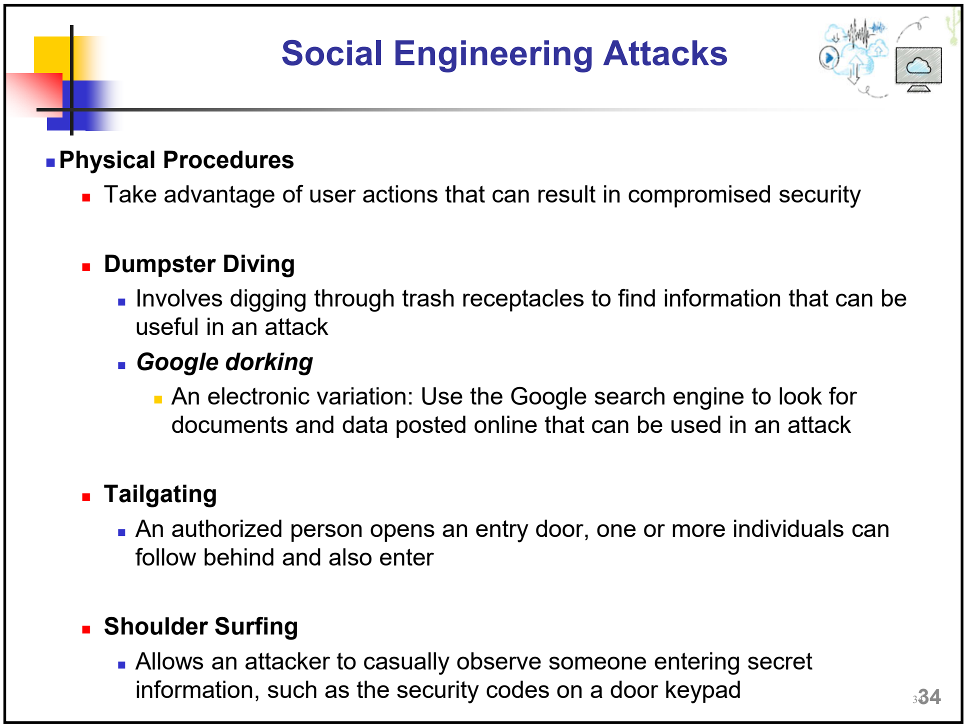
Social Engineering Attacks (contd.)

- **Social engineering psychological approaches often involve:**
  - **Impersonation**
    - Masquerading as a real or fictitious character and then playing the role of that person with a victim
  - **Phishing**
    - Sending an email message or displaying a web announcement that falsely claims to be from a legitimate enterprise in an attempt to trick the user into surrender private information or taking action
    - Variations on phishing attacks:
      - *Spear phishing*
      - *Whaling*
      - *Vishing*
      - *Smishing*



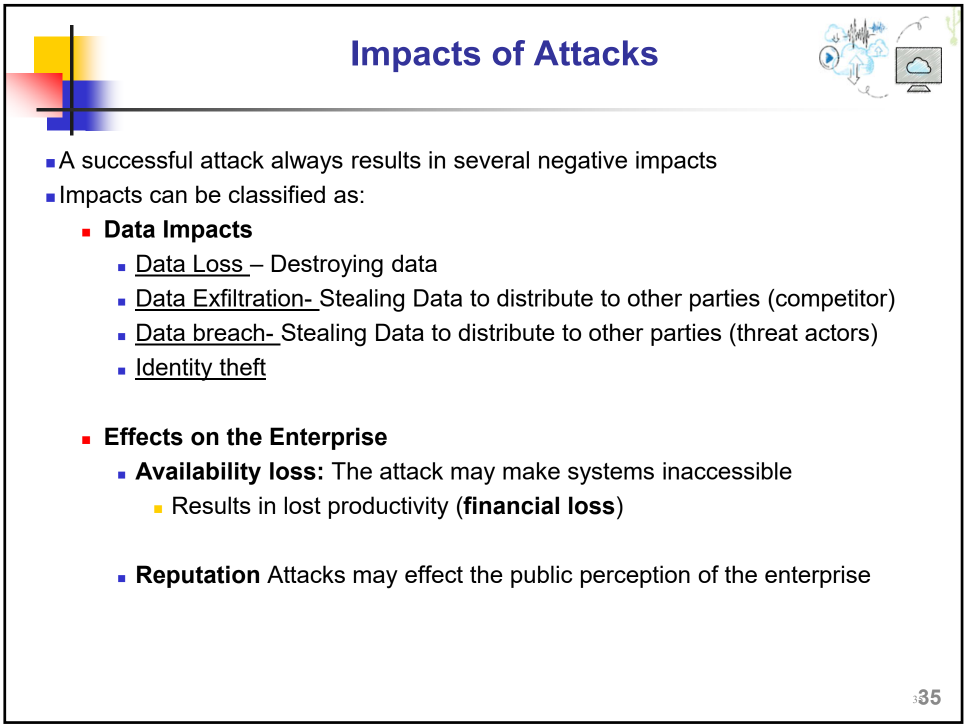
Social Engineering Attacks (contd.)

- **Social engineering psychological approaches often involve (continued):**
  - **Redirection**
    - An attacker directs a user to a fake lookalike site filled with ads for which the attacker receives money for traffic generated to the site
      - **Typo squatting**
        - Attackers purchase fake sites because the domain names of sites are spelled similarly to actual sites
      - **Pharming**
        - The attacker attempts to exploit how a URL is converted into its corresponding IP address
  - **Spam**
    - Unsolicited email that is sent to a large number of recipients
    - **Spim**
      - Spam delivered through instant messaging (IM) instead of email



Social Engineering Attacks

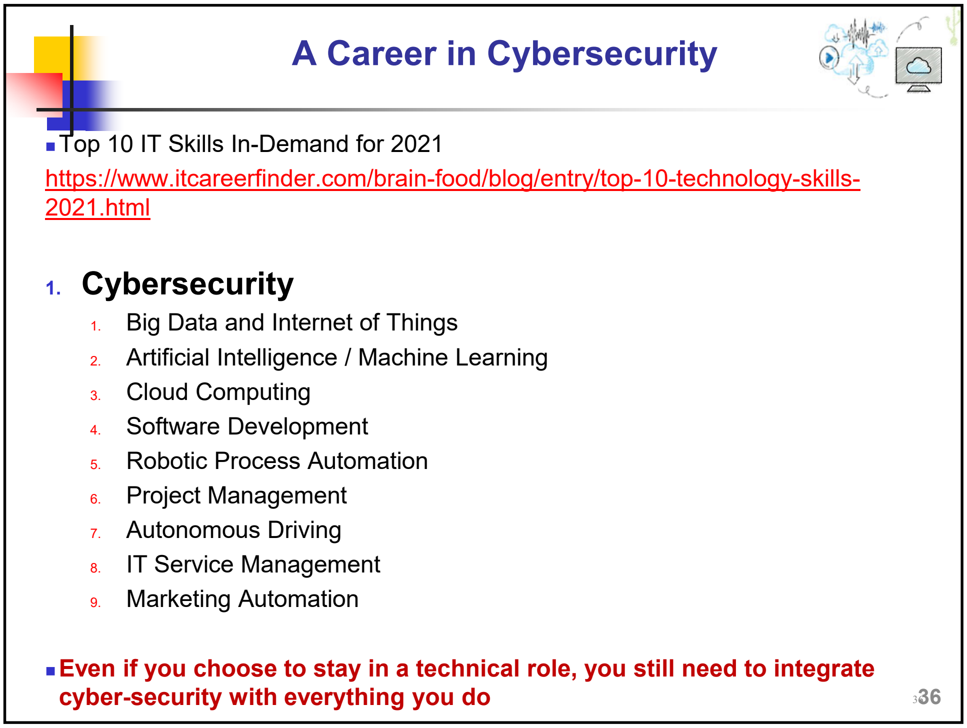
- **Physical Procedures**
  - Take advantage of user actions that can result in compromised security
  - **Dumpster Diving**
    - Involves digging through trash receptacles to find information that can be useful in an attack
    - ***Google dorking***
      - An electronic variation: Use the Google search engine to look for documents and data posted online that can be used in an attack
  - **Tailgating**
    - An authorized person opens an entry door, one or more individuals can follow behind and also enter
  - **Shoulder Surfing**
    - Allows an attacker to casually observe someone entering secret information, such as the security codes on a door keypad



Impacts of Attacks

- A successful attack always results in several negative impacts
- Impacts can be classified as:
  - **Data Impacts**
    - Data Loss – Destroying data
    - Data Exfiltration- Stealing Data to distribute to other parties (competitor)
    - Data breach- Stealing Data to distribute to other parties (threat actors)
    - Identity theft
  - **Effects on the Enterprise**
    - **Availability loss:** The attack may make systems inaccessible
      - Results in lost productivity (**financial loss**)
    - **Reputation** Attacks may effect the public perception of the enterprise

35



A Career in Cybersecurity

- Top 10 IT Skills In-Demand for 2021

https://www.itcareerfinder.com/brain-food/blog/entry/top-10-technology-skills-2021.html

1. **Cybersecurity**
   1. Big Data and Internet of Things
   2. Artificial Intelligence / Machine Learning
   3. Cloud Computing
   4. Software Development
   5. Robotic Process Automation
   6. Project Management
   7. Autonomous Driving
   8. IT Service Management
   9. Marketing Automation

- **Even if you choose to stay in a technical role, you still need to integrate cyber-security with everything you do**

36

Self-Assessment

Rate your competence of the following module objectives on a scale of 1 to 5 where 5 indicates you have full confidence in your competence of that objective and 1 indicates you have very little to no confidence in your competence of that objective.

1. Define information security and explain why it is important

2. Identify threat actors and their attributes

3. Describe the different types of vulnerabilities and attacks

4. Explain the impact of attacks

URL available in the the Module page on Blackboard

Assignment

- Interesting Difficult
- Proposed Quiz Questions

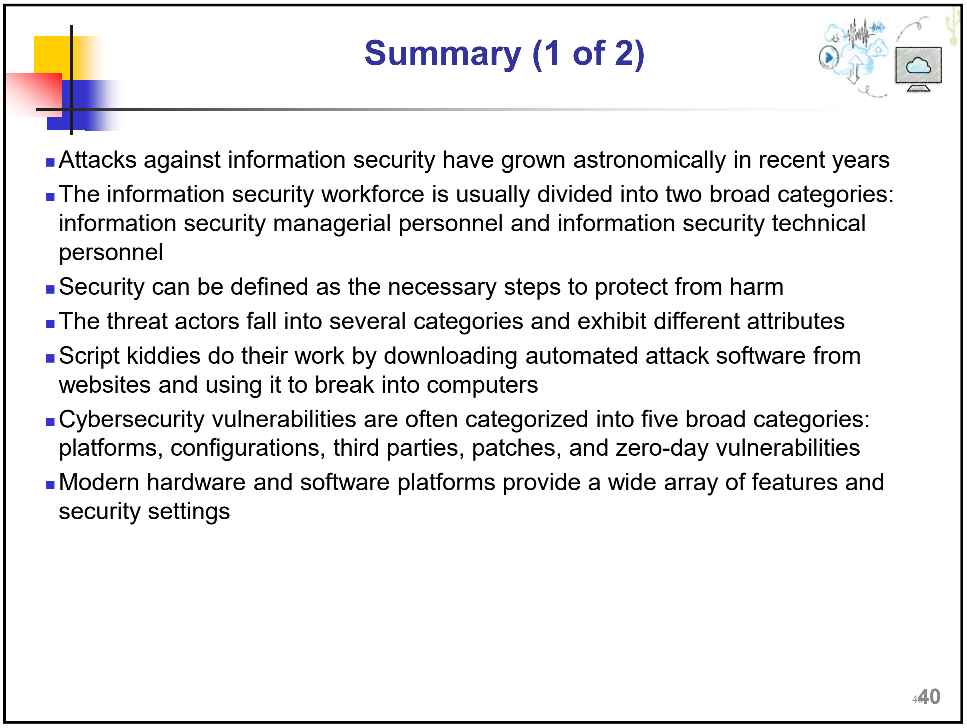
38

- **Available on Blackboard: Today. 11:59 pm**
- **Closing Date: Sunday, Jan 13, 11:59 pm**

Coming Up

- Tuesday:

39



Summary (1 of 2)

- Attacks against information security have grown astronomically in recent years
- The information security workforce is usually divided into two broad categories: information security managerial personnel and information security technical personnel
- Security can be defined as the necessary steps to protect from harm
- The threat actors fall into several categories and exhibit different attributes
- Script kiddies do their work by downloading automated attack software from websites and using it to break into computers
- Cybersecurity vulnerabilities are often categorized into five broad categories: platforms, configurations, third parties, patches, and zero-day vulnerabilities
- Modern hardware and software platforms provide a wide array of features and security settings

Summary (contd.)

- An attack vector is a pathway or avenue used by a threat actor to penetrate a system
- Social engineering is a means of eliciting information by relying on the weaknesses of individuals
- A successful attack always results in several negative impacts: data loss, data exfiltration, data breach, and identity theft