Information Technology for Management

Dr. Ebadati

Kharazmi University

Chapter 5: Cybersecurity, Risk Management, and Financial Crime

Learning Objectives

The Face and Future of Cyberthreats

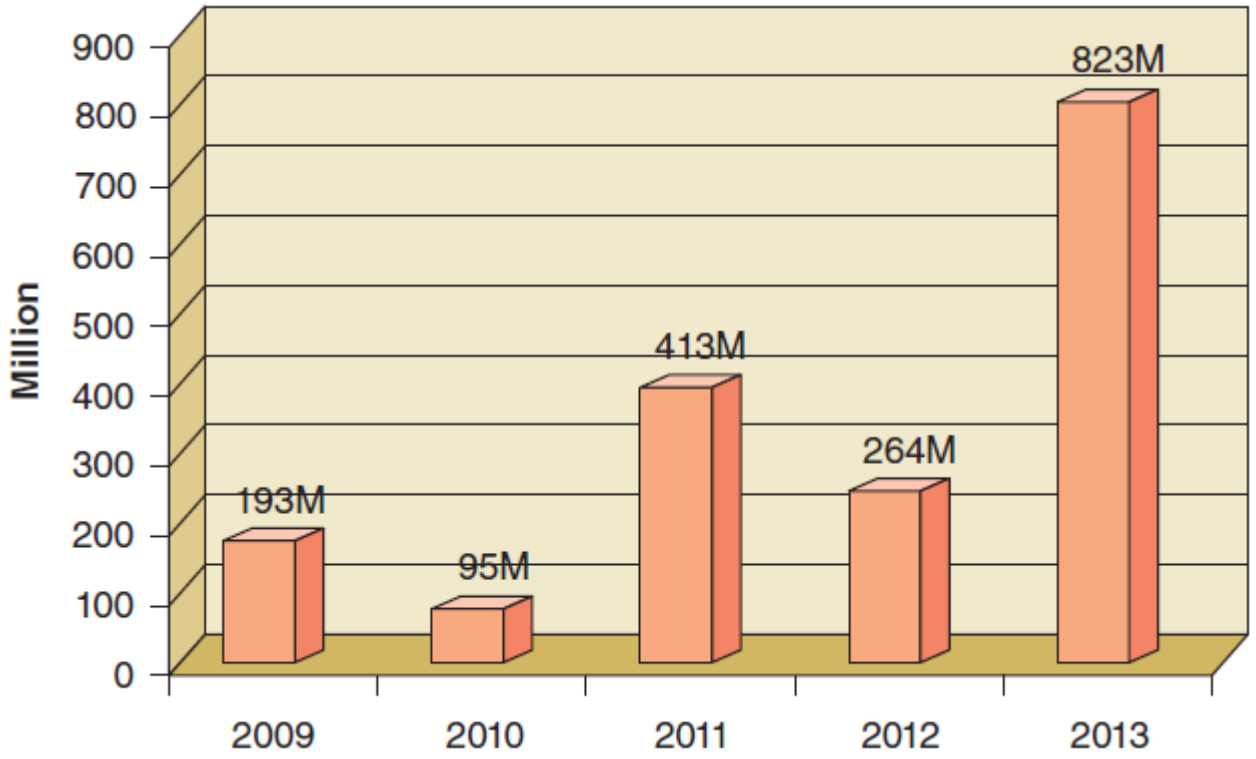


Figure 5.3 Number of reported data records breaches worldwide, 2009-2013.

The Face and Future of Cyberthreats

- Understanding the Scope of Breaches
  - **Adobe: 152 million** users account information
  - **eBay**: up to **145 million** records
  - **Michaels: 2.6 million** payment card numbers and expiration dates
  - **Target: 110 million** records
  - **Ubisoft: 58 million** records

The Face and Future of Cyberthreats

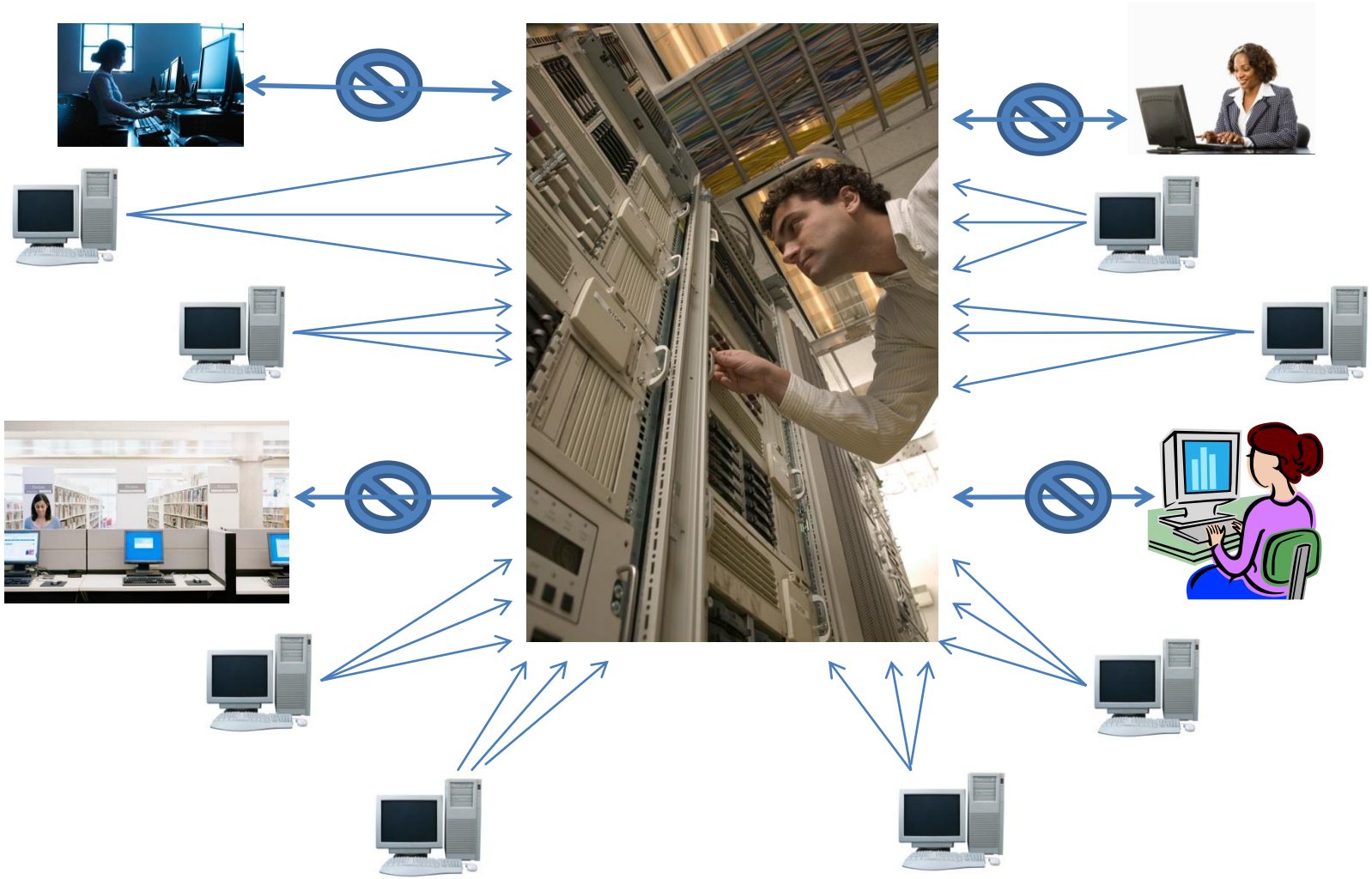
- Negligence
  - **Management not doing enough to defend against cyberthreats** and appear detached from the value of confidential data (even high-tech companies).
  - **The CIA and FBI have been hacked – nobody is safe.**
  - ***Critical Infrastructure* increasingly under attack**: **commercial** facilities, **defense industrial** base, transportation systems, national monuments and icons, banking and finance, and agriculture and food.

Critical infrastructure are systems and assets so vital to government that their incapacity or destruction would have a debilitating effect.

The Face and Future of Cyberthreats

- Battling Cyberthreats
  - **Distributed Denial-of-Service** (**DDoS**) attacks use **remote machines** (thousands or millions) to request service that keep organizations from providing a service over the Internet or crash a network or website.
  - Hackers, crime syndicates, militant groups, industrial spies, disgruntled employees, and hostile governments are some groups actively trying to gain profit, fame, revenge, promote ideology, wage warfare, terrorize, or disable targets.

The Face and Future of Cyberthreats



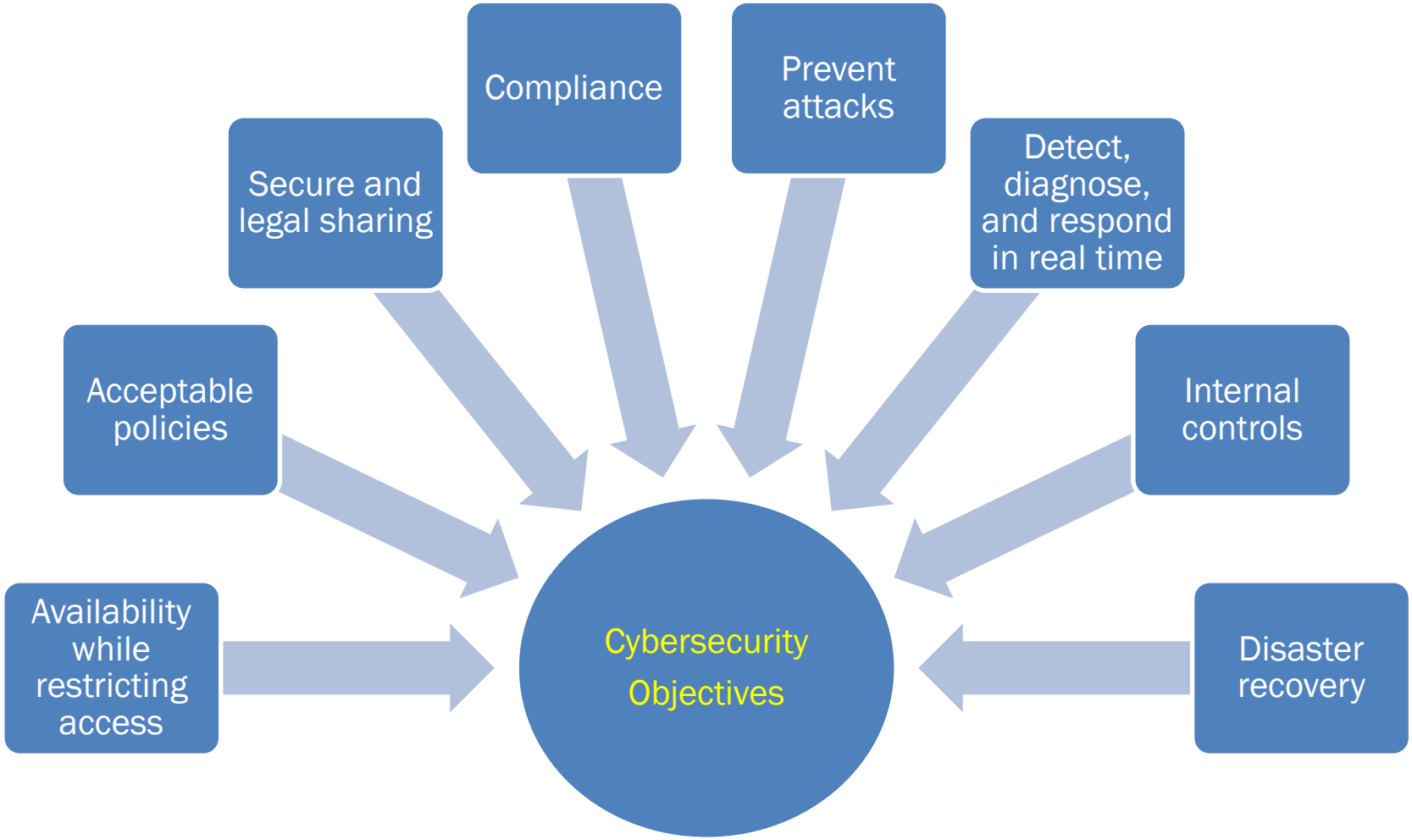
The Face and Future of Cyberthreats

- Vulnerabilities
  - Social Engineering (human hacking): **tricking users** or abusing human social norms into gaining advantage to a system or asset illicitly or legally, such as gaining **access to networks or accounts.**
  - **Bring Your Own Device (BYOD):** employees providing their own devices (mobile devices) for business purposes to reduce expenses through cut purchase and maintenance costs.

The Face and Future of Cyberthreats

- Advanced Persistent Threats (APT)
  - **Profit-motivated** cybercriminals often operate in stealth mode to continue long-term activities.
  - Hackers and hacktivists, commonly with personal agendas, carry out **high-profile attacks to further** their cause.
  - LulzSec, Anonymous, Combined Systems, Inc., and CIA find **poorly secured websites, steal information, and may post it online.**

The Face and Future of Cyberthreats



The Face and Future of Cyberthreats

1. Why was 2013 dubbed the "Year of the Breach"?

2013 has been dubbed the "Year of the Breach" because there were 2,164 reported data breaches that exposed an estimated 823 million records. Almost half of the 2013 breaches occurred in the United States, where the largest number of records were exposed—more than 540 million data records or 66 percent.

2. What causes or contributes to data breaches?

The main cause of a data breach is hacking, but the reason hacking is so successful is negligence—management not doing enough to defend against cyber-threats. Even high-tech companies and market leaders appear to be detached from the value of the confidential data they store and the threat that highly motivated hackers will try to steal them.

3. Why are cybercriminals so successful?

- *Answers may vary.* Current cybersecurity technologies and policies are simply not keeping pace with fast-evolving threats. Reasons for their success include:
- Defending yesterday. Relying on yesterday's cybersecurity practices is ineffective at combating today's threats.
- Bigger attack surface. The attack surface—consisting of business partners, suppliers, customers, and others—has expanded due to larger volumes of data flowing through multiple channels.
- Implementing before securing. Popular technologies like cloud computing, mobile, and BYOD (bring your own device) are implemented before they are secured.
- Not ready for next-generation cyberthreats. Few organizations are prepared to manage future threats. According to Gary Loveland, a principal in PwC's security practice, "What's needed is a new model of information security, one that is driven by knowledge of threats, assets, and the motives and targets of potential adversaries" (PWC, 2014).
- Unsafe cloud. While 47 percent of respondents use cloud computing, only 18 percent include provisions for cloud in their security policy.
- Unprepared for advanced persistent threats (APT). APTs require a new information-protection model that focuses on continuous monitoring of network activity and high-value information. Most U.S organizations lack these capabilities.
- Social engineering. Powerful IT security systems cannot defend against what appears to be authorized access. Robust data security is not the responsibility of IT alone, but the ongoing duty of everyone in an organization.

The Face and Future of Cyberthreats

4. What was the biggest data breach in history?

In October 2013 a data breach at Adobe exposed the account information of up to 152 million users—the largest data breach in history.

5. Describe the basic method of a distributed denial-of-service (DDoS) attack.

The textbook answer of "A distributed denial-of-service (DDoS) attack bombards a network or website with traffic (i.e., requests for service) to crash it and leave it vulnerable to other threats." actually describes any DoS attack. The difference between a DoS attack and a DDoS attack is the word, distributed – the attack originates from multiple sources.

6. What is a critical infrastructure? List three types of critical infrastructures.

Critical infrastructure is defined as "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.

Some examples are commercial facilities; defense industrial base; transportation systems; national monuments and icons; banking and finance; and agriculture and food.

7. What are the motives of hacktivists? A hacktivist is someone who does hacking as a way to protest for a cause.

8. What is the number one cause of data loss or breaches? Hacking is the number one cause of data loss.

The Face and Future of Cyberthreats

9. Why is social engineering a technique used by hackers to gain access to a network?

Social engineering, also known as human hacking, is tricking users into revealing their credentials and then using those credentials to gain access to networks or accounts. It is a hacker's clever use of deception or manipulation of people's tendency to trust, be helpful, or simply follow their curiosity. Powerful IT security systems cannot defend against what appears to be authorized access. Humans are easily hacked, making them and their social media posts high-risk attack vectors. For instance, it is often easy to get users to infect their corporate network or mobiles by tricking them into downloading and installing malicious apps or backdoors.

10. What are two BYOD security risks?

The user-owned device may become infected due to personal use, at home or mobile.

If an employee's device is lost, the company can suffer a data breach if the device is not encrypted.

11. Explain why APT attacks are difficult to detect.

APT is a stealth network attack in which an unauthorized person gains access to a network and remains undetected for a long time. Skilled hackers launch APT attacks to steal data continuously (e.g., daily) over months or year—rather than to cause damage that would reveal their presence. APTs require a new information-protection model that focuses on continuous monitoring of network activity and high-value information. Most U.S organizations lack these capabilities.

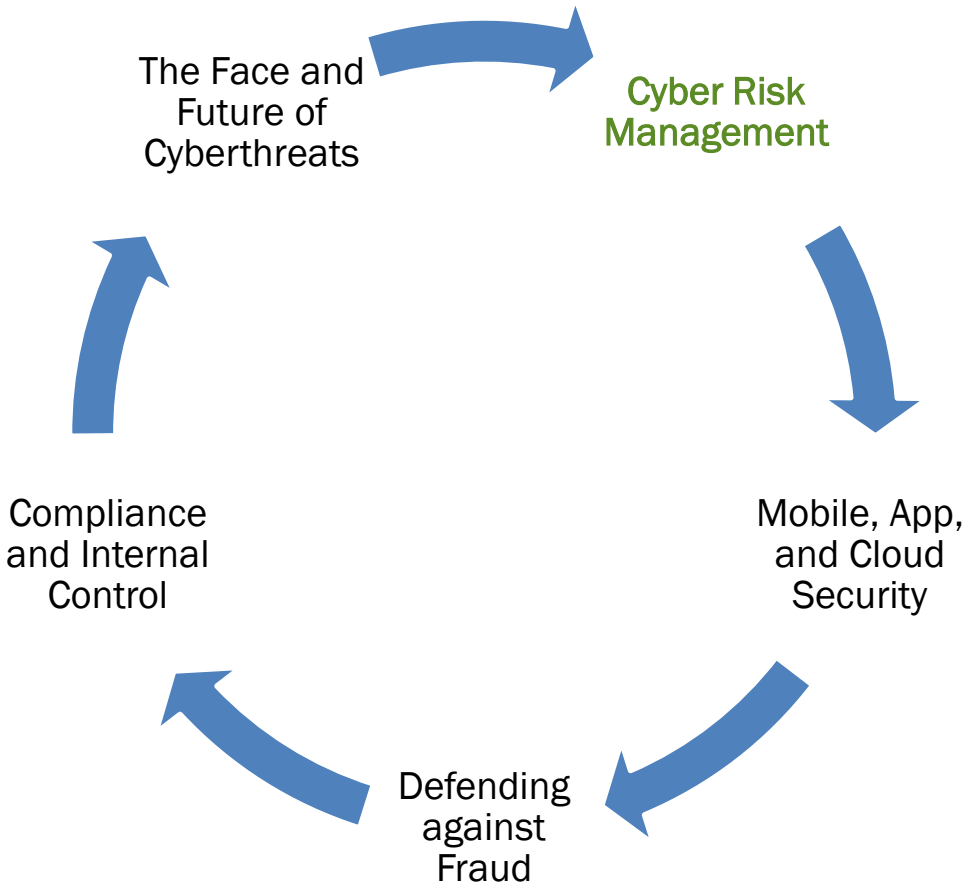
The Face and Future of Cyberthreats

12. What are the objectives of cybersecurity?

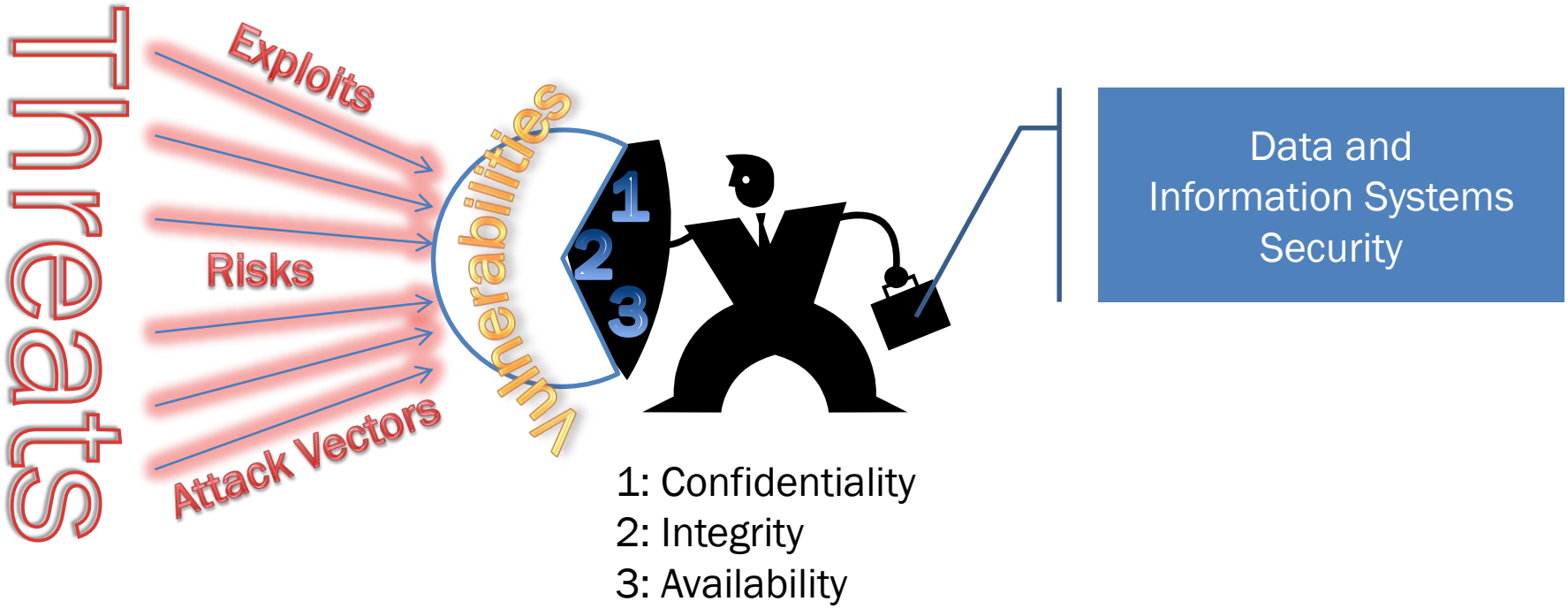
The objectives of cybersecurity are to:

- Make data and documents available and accessible 24/7 while simultaneously restricting access.
- Implement and enforce procedures and acceptable use policies (AUPs) for data, networks, hardware, and software that are company- or employee-owned, as discussed in the opening case.
- Promote secure and legal sharing of information among authorized persons and partners.
- Ensure compliance with government regulations and laws.
- Prevent attacks by having network intrusion defenses in place.
- Detect, diagnose, and respond to incidents and attacks in real time.
- Maintain internal controls to prevent unauthorized alteration of data and records.
- Recover from business disasters and disruptions quickly.

Learning Objectives



Cyber Risk Management



Three objectives of data and information systems security.

Cyber Risk Management

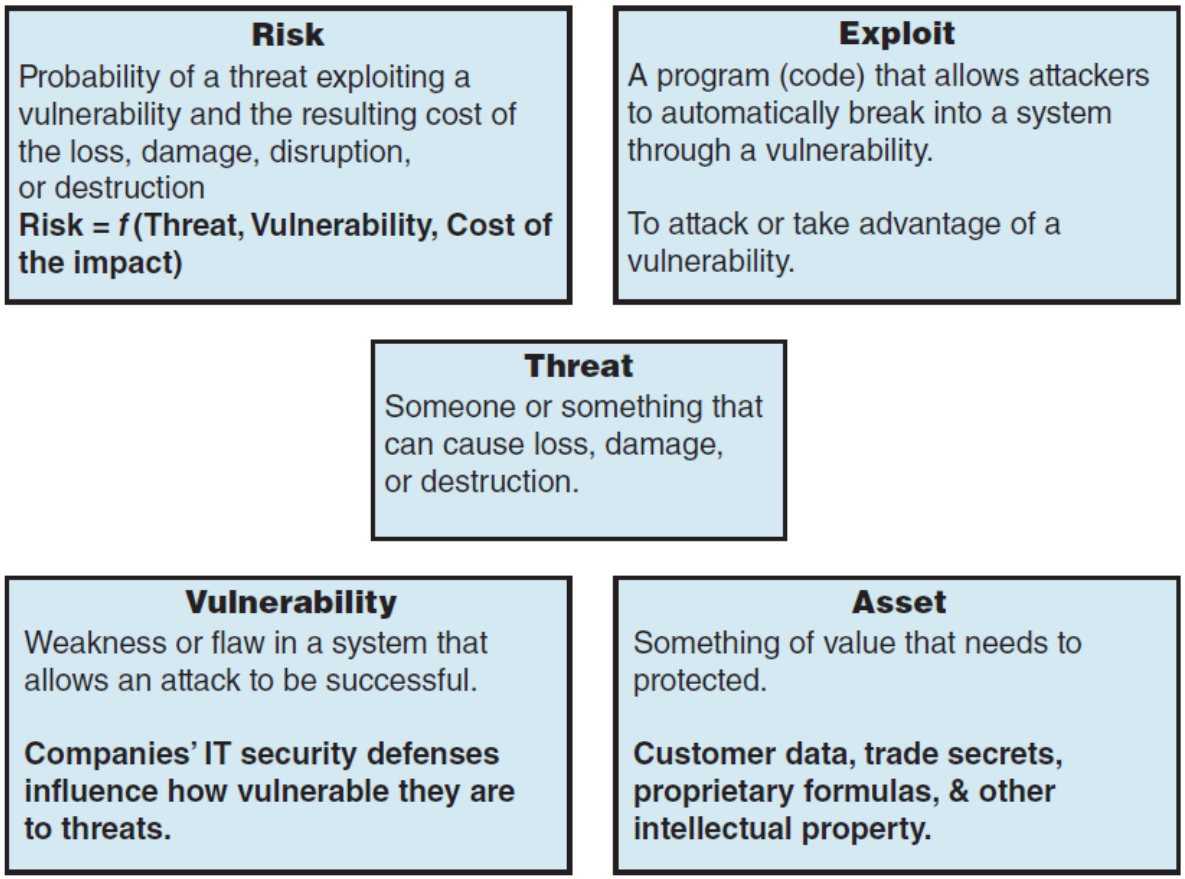


Figure 5.6 Basic IT security concepts.

Cyber Risk Management

- Attack Vectors
  - **Entry points for malware, hackers**, hacktivists, and organized crime including gaps, holes, weaknesses, flaws that expose an organization to intrusions or other attacks in:
    - Corporate networks
    - IT security defenses
    - User training
    - Policy enforcement
    - Data storage
    - Software
    - Operating systems
    - Applications
    - Mobile devices

Cyber Risk Management

- Contract Hacker
  - Industrialized method of **committing cybercrime:**
    - **Operations**
    - **Workforces**
    - **Support services**

Cyber Risk Management

- Password Vulnerabilities
  - **Weak passwords are guessable**, short, common, proper nouns or names, or a word in the dictionary:
    - 123456
    - password
  - **Strong passwords contain upper- and lowercase letter, numbers, and extended (special) characters** (!@#$%^...) **and** are **at least 8 characters** long:
    - Ur_x&e-w.5h
    - =p9M4&x!f26&zR

Cyber Risk Management

- Password Vulnerabilities
  - It is **hard to remember** randomly formatted strong passwords, so passphrases may help:

    Ex. I have worked on [system] at IBM since [date]

    converts into

    IhWo_OS2_aIBMs2008!

  - The system and date are variable adding complexity to an otherwise simple phrase that someone can actually remember.

Cyber Risk Management

- Phishing
  - Deceptive method of **stealing confidential information** by pretending to be a legitimate organization or trusted source, like John Wiley & Sons, Inc.
  - Messages include **links to fraudulent phish websites** that looks like the real one.
  - When the **user clicks the link to the phish site**, or a link on the phish site, they are prompted for confidential information like **credit card numbers, social security numbers, account numbers, or passwords.**

Cyber Risk Management

Defense-in-Depth

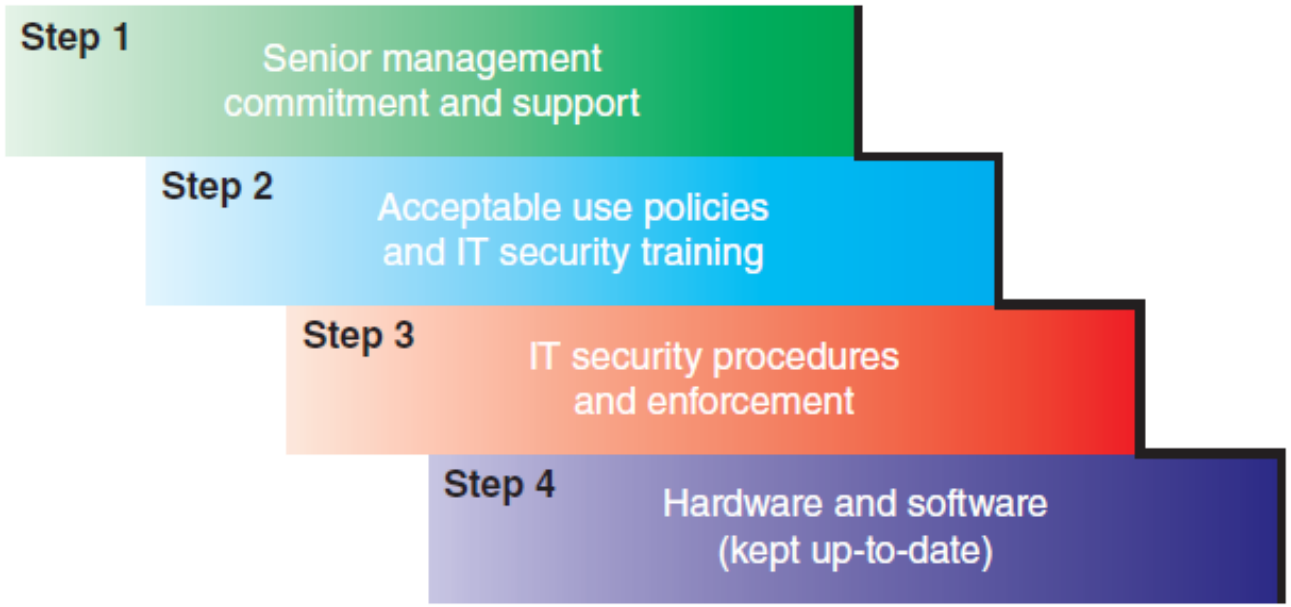


Figure 5.8 IT security defense-in-depth model.

Cyber Risk Management

- Threat Modeling
  - **Unintentional** threats:
    - **Human Error**
    - **Environmental Hazards**
    - **Computer System Failures**
  - **Intentional** threats:
    - **Theft**
    - **Inappropriate** Use
    - Deliberate **Manipulation**
    - **Strikes**, Riots, or **Damage**
    - **Malicious Damage,**
    - **Destruction**
    - **Various Abuses**

Cyber Risk Management

- **Malware**
  - **A computer program or code that can infect anything attached to the Internet** and is able to process the code that can **propagate**, or spread, to other machines or devices, or replicate, or make copies of itself.

WORMS

BOTNETS

ROOTKITS

VIRUSES

TROJANS

KEYLOGGERS

BACKDOORS

Cyber Risk Management

- Malware Reinfection, Signatures, Mutations, and Variants
  1. Malware is captured in backups or archives. Restoring the infected backup or archive also restores the malware.
  2. Malware infects removable media.
  3. Most antivirus (AV) software relies on signatures to identify and then block malware.

Cyber Risk Management

- Data tampering
  - A **common means of attack** that is overshadowed by other types of attacks.
  - **Refers to an attack during which someone enters false or fraudulent data** into a computer, or changes or deletes existing data.
  - Data tampering **is extremely serious because it may not be detected**; the method often used by insiders and fraudsters.

Cyber Risk Management

- Botnets
  - **A botnet is a collection of bots, which are malware-infected computers.**
  - Those infected computers, **called zombies, can be controlled and organized into a network of zombies** on the command of a remote botmaster (also called bot herder).

Cyber Risk Management

- Spear Phishing
  - **Spear phishers often target select groups of people** with something in common.
  - **Tricks users into opening an infected e-mail.**
  - **E-mails sent that look like the real** thing.
  - **Confidential information extracted**

  through seemingly legitimate Website requests for passwords, **user IDs, PINs, account numbers**, and so on.

Cyber Risk Management

- IT Defenses
  - **Antivirus** Software: designed to detect **malicious codes** and prevent users from downloading them.
  - **Intrusion Detection** Systems (**IDSs**): As the name implies, an IDS scans for unusual or suspicious traffic (***passive defense***).
  - Intrusion Prevention Systems (**IPSs**): An **IPS is designed to take immediate action**—such as blocking specific IP addresses—whenever a traffic-flow anomaly is detected (***active defense***).

Cyber Risk Management

1. What are threats, vulnerabilities, and risk?

- Threat: Someone or something that can cause loss, damage, or destruction.
- Vulnerability: Weakness or flaw in a system that allows an attack to be successful.
- Risk: Probability of a threat exploiting a vulnerability and the resulting cost of the loss, damage, disruption, or destruction. Risk = f (Threat, Vulnerability, Cost of the impact)

2. Explain the three components of the CIA triad.

- The CIA triad consists of three key cybersecurity principles: confidentiality, integrity, availability.
- Confidentiality: No unauthorized data disclosure.
- Integrity: Data, documents, messages, and other files have not been altered in any unauthorized way.
- Availability: Data is accessible when needed by those authorized to do so.

3. What is an attack vector? Give an example.

- Attack vectors are entry points for malware, hackers, hacktivists, and organized crime.
- *Answers may vary.* An example is anyone's improperly secured mobile device.

4. What is an exploit? Give an example.

- The term exploit has more than one meaning. An exploit is a hacker tool or software program used to break into a system, database, or device. An attack or action that takes advantage of a vulnerability is also called an exploit.
- *Answers may vary.* An example of the first is BlackPOS. An example of the second is a DDoS.

Cyber Risk Management

5. What is a contract hacker?

A contract hacker is a hacker available for hire and may supply complete hack attacks and 24/7 support through hacking help desks.

6. Give an example of a weak password and a strong password.

- *Answers may vary.* Some examples are: “1234546”, “password”, “mypassword”. Weak passwords are easily guessable, short, common, or a word in the dictionary.

- *Answers may vary.* They should contain some combination of upper- and lowercase letters, numbers, and/or punctuation marks, and be at least eight characters long.

7. How are phishing attacks done?

Phishing is a deceptive method of stealing confidential information by pretending to be a legitimate organization, such as PayPal, a bank, credit card company, or other trusted source. Phishing messages include a link to a fraudulent phish website that looks like the real one. When the user clicks the link to the phish site, he or she is asked for a credit card number, social security number, account number, or password. Successful attacks depend on untrained or unaware users responding to phishing scams.

8. What are the four steps in the defense-in-depth IT security model?

The four steps are:

- Step 1: Senior management commitment and support.
- Step 2: Acceptable use policies and IT security training.
- Step 3: IT security procedures and enforcement.
- Step 4: Hardware and software.

Cyber Risk Management

9. Define and give an example of an unintentional threat.

- Unintentional threats fall into three major categories: human error, environmental hazards, and computer system failures.
- Examples: *Answers may vary.*
- Human error can occur in the design of the hardware or information system. It can also occur during programming, testing, or data entry. Not changing default passwords on a firewall or failing to manage patches creates security holes. Human errors also include untrained or unaware users responding to phishing scams or ignoring security procedures.
- Environmental hazards include volcanoes, earthquakes, blizzards, floods, power failures or strong fluctuations, fires (the most common hazard), defective air conditioning, explosions, radioactive fallout, and water-cooling system failures. In addition to the primary damage, computer resources can be damaged by side effects, such as smoke and water. Such hazards may disrupt normal computer operations and result in long waiting periods and exorbitant costs while computer programs and data files are recreated.
- Computer systems failures can occur as the result of poor manufacturing, defective materials, and outdated or poorly maintained networks. Unintentional malfunctions can also happen for other reasons, ranging from lack of experience to inadequate testing.

10. Define and give an example of an intentional threat.

- Intentional threats are those where the individual(s) have intention to do harm or some illegal activity.
-
- Examples of intentional threats include data theft; inappropriate use of data (e.g., manipulating inputs); theft of mainframe computer time; theft of equipment and/or programs; deliberate manipulation in handling, entering, processing, transferring, or programming data; labor strikes, riots, or sabotage; malicious damage to computer resources; destruction from viruses and similar attacks; and miscellaneous computer abuses and Internet fraud.

Cyber Risk Management

11. List and define three types of malware.

- *Answers may vary.*
- Viruses, worms, trojans, rootkits, backdoors, botnets, and keyloggers are types of malware.
- Most viruses, trojans, and worms are activated when an attachment is opened or a link is clicked.
- Remote access trojans, or RATS, create an unprotected backdoor into a system through which a hacker can remotely control that system.

12. What are the risks caused by data tampering?

- *Answers may vary.*
- Data tampering refers to an attack during which someone enters false or fraudulent data into a computer, or changes or deletes existing data. Data tampering is extremely serious because it may not be detected. This introduces dirty data with all of its inherent issues.

13. Define botnet and explain its risk.

A botnet is a collection of bots, which are malware-infected computers. Infected computers, called zombies, can be controlled and organized into a network of zombies on the command of a remote botmaster. Embedding a botnet agent within thousands or even millions of computers increases processing power of the attack to that of a supercomputer. Zombies can be commanded to monitor and steal personal or financial data—acting as spyware. Botnets are used to send spam and phishing e-mails and launch DDoS attacks. Botnets are extremely dangerous because they scan for and compromise other computers, and then can be used for every type of crime and attack against computers, servers, and networks.

Cyber Risk Management

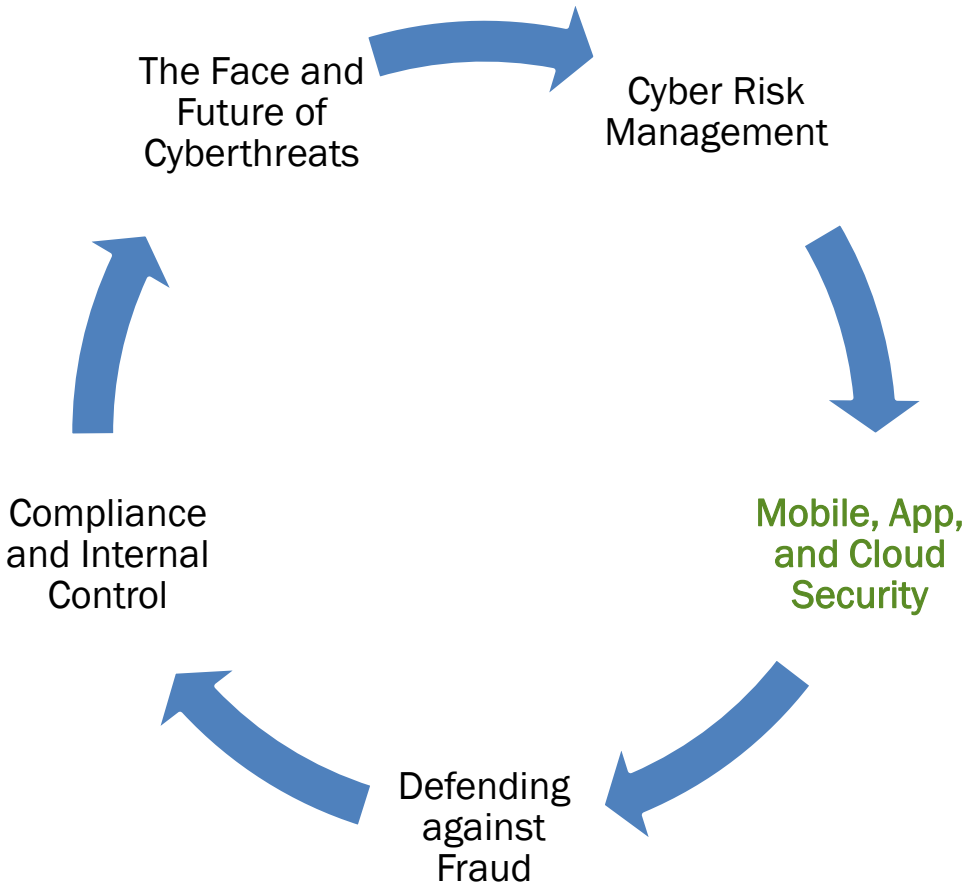
14. Explain spear phishing.

- Spear phishers often target select groups of people with something in common—they work at the same company, bank at the same financial institution, or attend the same university. The scam e-mails appear to be sent from organizations or people the potential victims normally receive e-mails from, making them even more deceptive.
-
- Spear phish creators gather information about people's companies and jobs from social media or steal it from computers and mobile devices, and then use that same information to customize messages that trick users into opening an infected e-mail. They then send e-mails that look like the real thing to targeted victims, offering all sorts of urgent and legitimate-sounding explanations as to why they need your personal data. Finally, the victims are asked to click on a link inside the e-mail that takes them to a phony but realistic-looking website, where they are asked to provide passwords, account numbers, user IDs, access codes, PINs, and so on.

15. What are the functions of an IDS and IPS?

- An Intrusion Detection System (IDS) scans for unusual or suspicious traffic. An IDS can identify the start of a DoS attack by the traffic pattern, alerting the network administrator to take defensive action, such as switching to another IP address and diverting critical servers from the path of the attack.
-
- An Intrusion Prevention System (IPS) is designed to take immediate action—such as blocking specific IP addresses—whenever a traffic-flow anomaly is detected. An application-specific integrated circuit–based (ASIC) IPS has the power and analysis capabilities to detect and block DDoS attacks, functioning somewhat like an automated circuit breaker.

Learning Objectives



Mobile, App, and Cloud Security

- CLOUD COMPUTING AND SOCIAL NETWORK RISKS
  - Provide a **single point of failure and attack** for organized criminal networks.
  - **Critical, sensitive, and private information is at risk**, and like previous IT trends, such as wireless networks, the goal is connectivity, often with little concern for security.
  - **As social networks increase their services, the gap between services and information security also increases.**

Mobile, App, and Cloud Security

- Patches and Service Packs
  - When new vulnerabilities are found in **operating systems, applications**, or wired and wireless networks, **patches** are released by the vendor or security organization.
  - **Service packs** are used **to update and fix vulnerabilities** in its operating systems.

Mobile, App, and Cloud Security

- Consumerization of Information Technology (COIT)
  - Practices that move **enterprise data and IT assets to employees' mobiles** and the **cloud**, creating a new set of **tough IT security challenges.**
  - **Widely used apps** sometimes operate **outside of the organization's firewall.**
  - **Enterprises take risks with BYOD** practices that they never would consider taking with conventional computing devices.

Mobile, App, and Cloud Security

- New Attack Vectors
  - BYOD: **Hackers steal secrets from employees' mobile** devices without a trace.
  - **New vulnerabilities are created when personal and business data and communications are mixed** together.
  - All **cybersecurity** controls can be rendered **useless** by an **employee-owned device.**
  - **Unacceptable** delays or additional investments may be caused by **unsupported devices.**

Mobile, App, and Cloud Security

- Mobile Biometrics
  - Voice Patterns
  - Fingerprint Analysis

The Face and Future of Cyberthreats

- **Mobile Computing Responses**
  - Detecting and destroying malicious apps “in the wild” is **rogue app monitoring** that may include major app stores.
  - If infected, lost, or stolen, **mobile devices** can be equipped with a “kill switch”, a means of erasing their memory **remotely** called **remote wipe capability.**

The Face and Future of Cyberthreats

- Do-Not-Carry!
  - U.S. companies, government agencies, and organizations may impose rules that assume mobile technologies will inevitably be compromised:
    - **Only "clean" devices** are allowed to be brought **inside**
    - **Devices are forbidden from connecting while abroad**
    - Some **individuals carry no electronics on trips** for compliance

Business Process Management and Improvement

1. How do social networks and cloud computing increase vulnerability?

Social networks and cloud computing increase vulnerabilities by providing a single point of failure and attack for organized criminal networks. Critical, sensitive, and private information is at risk, and like previous IT trends, such as wireless networks, the goal is connectivity, often with little concern for security.

2. Why are patches and service packs needed?

They are needed to keep software up to date and protected as fully as possible. When new vulnerabilities are found in operating systems, applications, or wired and wireless networks, patches are released by the vendor or security organization. Patches, sometimes called service packs, are software programs that users download and install to fix a vulnerability.

3. What is consumerization of information technology (COIT)?

Consumerization of information technology (COIT) is a trend where users are obtaining for personal use an increasing amount of information technology (e.g., personal mobile devices, such as smartphones and tablets, and powerful home PCs and laptops) which often is mobile, unsecured, and in some cases, better than that provided by their employer.

Business Process Management and Improvement

4. Why does BYOD raise serious and legitimate areas of concern?

BYOD raises serious and legitimate areas of concern. Hackers break into employees' mobile devices and leapfrog into employers' networks—stealing secrets without a trace. New vulnerabilities are created when personal and business data and communications are mixed together. All cybersecurity controls—authentication, access control, data confidentiality, and intrusion detection—implemented on corporate-owned resources can be rendered useless by an employee-owned device. Also, the corporation's mobile infrastructure may not be able to support the increase in mobile network traffic and data processing, causing unacceptable delays or requiring additional investments.

5. What are two types of mobile biometrics?

Two types of biometrics which can be implemented on mobile devices are voice and fingerprint.

6. Explain rogue app monitoring.

Rogue app monitoring is a type of defense to detect and destroy malicious apps in the wild. Several vendors offer 24/7 monitoring and detection services to monitor major app stores and shut down rogue apps to minimize exposure and damage.

Business Process Management and Improvement

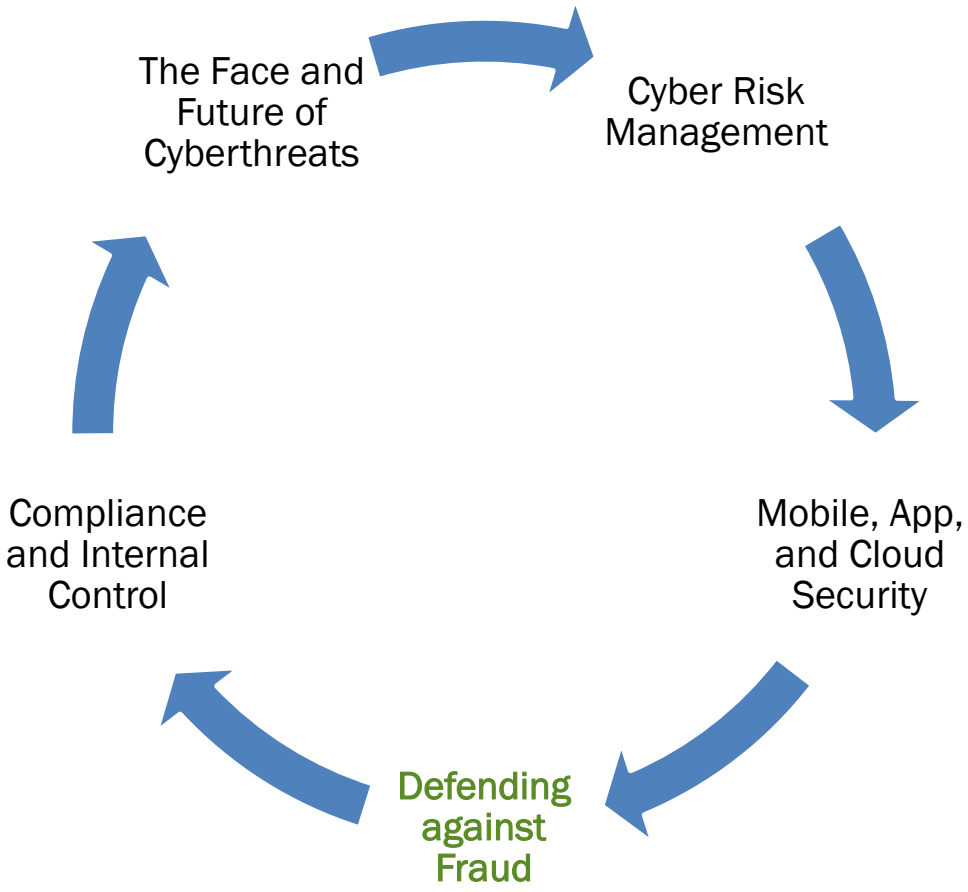
7. Why is a mobile kill switch or remote wipe capability important?

A mobile kill switch or remote wipe capability is needed in the event of loss or theft of a device.

8. What are the purposes of do-not-carry rules?

The purposes of do-not-carry rules are to prevent compromise, not only of the device but of the company and/or government network, as a response to mobile security threats. Travelers can bring only "clean" devices and are forbidden from connecting to the government's network while abroad.

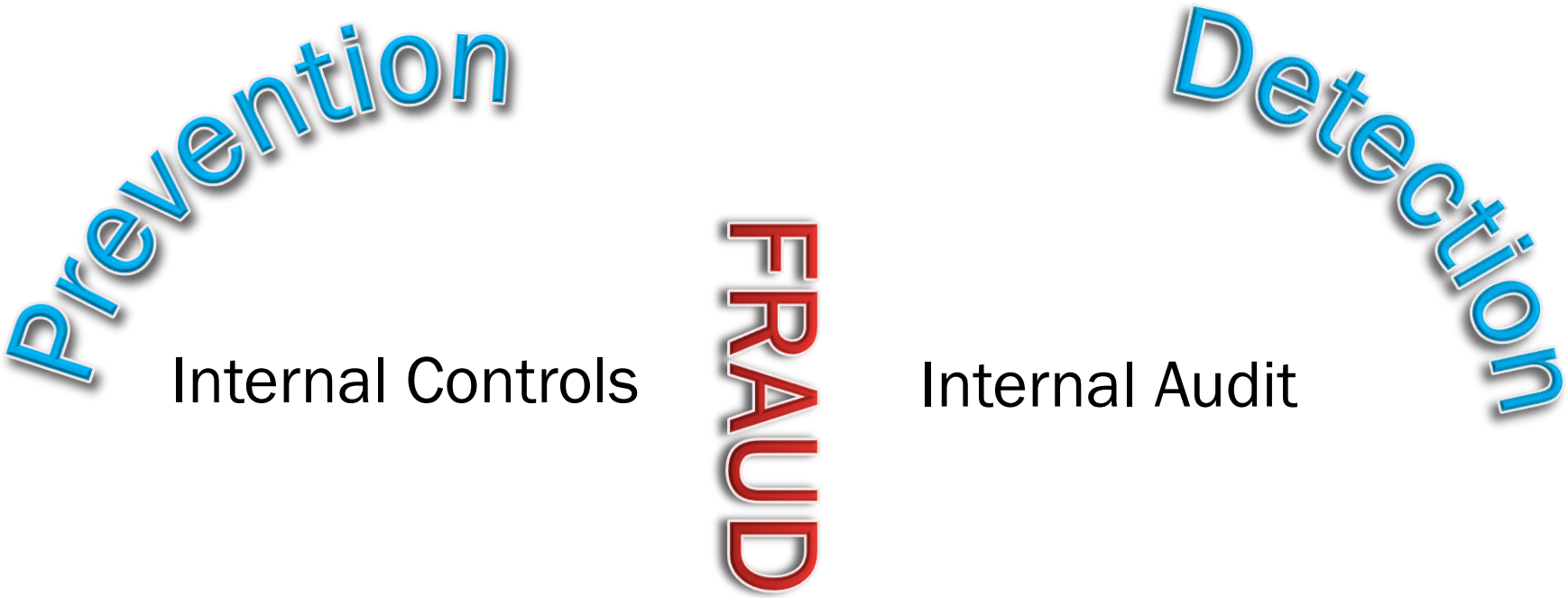
Learning Objectives



Defending against Fraud

- CRIME
  - **Violent** Crime involves **physical threat or harm.**
  - **Nonviolent Crime uses deception**, confidence, and **trickery** by abusing the power of their position or by taking advantage of the trust, ignorance, or laziness of others, otherwise known as **Fraud.**
- FRAUD
  - Occupational fraud refers to the deliberate **misuse of the assets** of one's employer for personal gain.

Defending against Fraud



Defending against Fraud

- Intelligent Analysis
  - Forms insider profiling to find **wider patterns of criminal networks.**
- Anomaly Detection
  - **Audit trails** from key systems and personnel records used to **detect anomalous patterns**, such as **excessive hours worked**, deviations in patterns of **behavior**, copying **huge amounts of data**, **attempts to override controls**, unusual transactions, and inadequate documentation about a transaction.

Defending against Fraud

- Identity Theft
  - **Social Security** and **credit card numbers** are **stolen** and used by thieves by:
    - **Stealing wallets**
    - **Dumpster digging**
    - **Bribery**
    - **Employee theft**
    - **Data Breaches**
    - **Ignorance or purposeful irresponsibility**

Defending against Fraud

1. What are the two categories of crime?

Crime can be divided into two categories depending on the tactics used to carry out the crime: violent and nonviolent.

2. Explain fraud and occupational fraud.

- Fraud is nonviolent crime because fraudsters use deception, confidence, and trickery. Fraudsters carry out their crime by abusing the power of their position or by taking advantage of the trust, ignorance, or laziness of others.
- Occupational fraud refers to the deliberate misuse of the assets of one's employer for personal gain.

3. What defenses help prevent internal fraud?

The single-most effective fraud prevention tactic is making employees know that fraud will be detected by IT monitoring systems and punished, with the fraudster possibly turned over to the police or FBI. The fear of being caught and prosecuted is a strong deterrent. IT must play a visible and major role in detecting fraud.

Defending against Fraud

4. What are two red flags of internal fraud?

Answers may vary. Internal fraud may be indicated by anomalous patterns, such as excessive hours worked, deviations in patterns of behavior, copying huge amounts of data, attempts to override controls, unusual transactions, and inadequate documentation about a transaction.

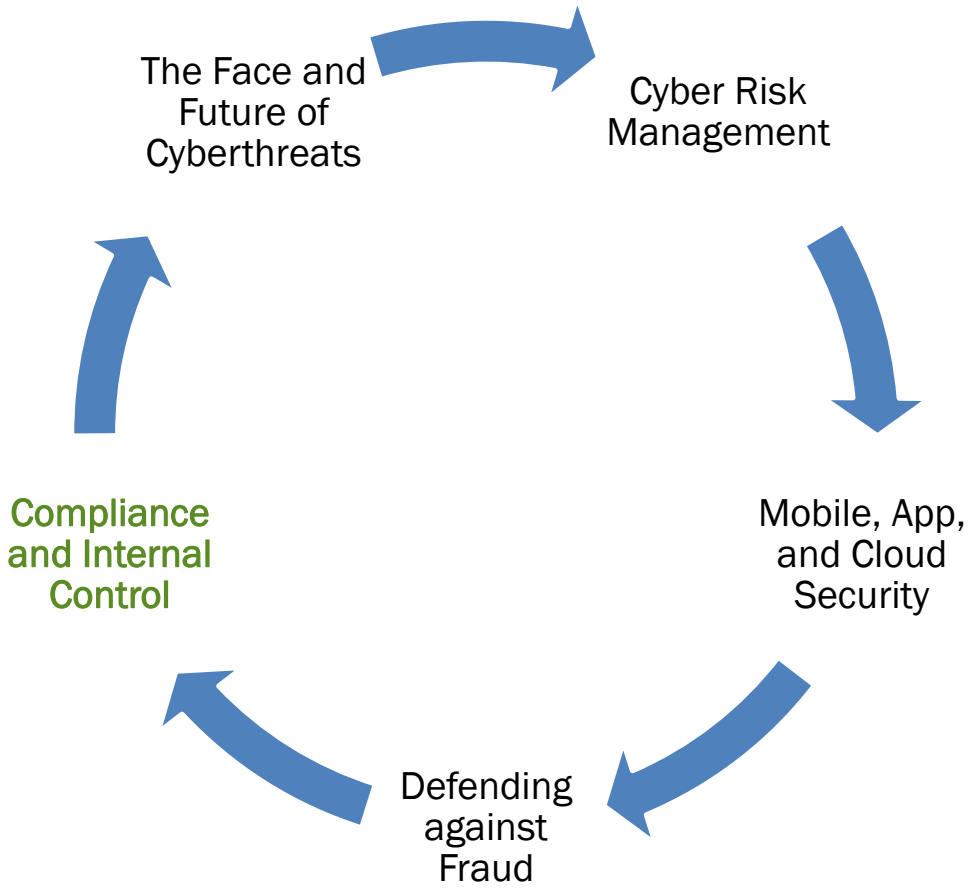
5. Explain why data on laptops and computers need to be encrypted.

Encryption is a part of a defense-in-depth approach to information security. The basic principle is that when one defense layer fails, another layer provides protection. For example, if a wireless network's security was compromised, then having encrypted data would still protect the data, provided that the thieves could not decrypt it.

6. Explain how identity theft can occur.

Criminals have always obtained information about other people—by stealing wallets or dumpster digging. But widespread electronic sharing and databases have made the crime worse. A variety of cybercrime, including the use of botnets, have been used to steal identities.

Learning Objectives



Compliance and Internal Control

- Internal Controls (IC)
  - A **process to ensure that sensitive data are protected** and accurate designed to achieve:
    - **Reliability of financial reporting**, to protect investors
    - **Operational efficiency**
    - **Compliance with laws**
    - **Regulations and policies**
    - **Safeguarding** of assets

Compliance and Internal Control

- Regulatory Complications
  - Sarbanes-Oxley Act (**SOX**), Gramm-Leach-Bliley Act (**GLBA**), Federal Information Security Management Act (**FISMA**), USA PATRIOT Act, and many others depending on industry, corporate filing, and operating location.
  - **Frameworks to address compliance:**
    - **Enterprise Risk Management** (**ERM**)
    - **Control Objectives for Information and Related Technology (COBIT)**
    - **Payment Card Industry Data Security Standard (PCI DSS)**

Compliance and Internal Control

- Controls are Regulated Because…
  - Approximately **85 percent of occupational fraud could have been prevented if proper IT-based internal controls had been designed**, implemented, and followed.
  - Prosecution reduces the likelihood of any employee adopting an "***I can get away with it***" **attitude.**

Compliance and Internal Control

- Defense Strategies
  1. Prevention and deterrence
  2. Detection
  3. Contain the damage
  4. Recovery
  5. Correction
  6. Awareness and compliance
- Defense Strategy Controls
  - General controls & Application controls

Compliance and Internal Control

- Authentication
  - Provides a means of **ensuring** that the user is **who** s/he claims to be.
- Biometrics
  - An **automated method of verifying the identity** of a person, based on physical or behavioral characteristics using systems that match the characteristic against a stored profile.

Compliance and Internal Control

- Biometrics – Authentication Factors
  - Something you are **saying, seeing, touching**…
  - Something **you know**…
  - Something **you have**…

Compliance and Internal Control

- Disaster Recover v. Business Continuity
  - DR is a **backup plan that ensures a business can recover** after a **major disruption**, but over an extended timeline.
  - BC refers to **maintaining business functions or restoring them** quickly after a major disruption.

  Fires, earthquakes, floods, power outages, malicious attacks, and other types of disasters are reasons businesses should have a business continuity plan.

Compliance and Internal Control

- **Auditing Web Sites**
  - A good preventive measure to manage the legal risk by reviewing content of the site, which may offend people or be in **violation of copyright** laws or other regulations (e.g., privacy protection).

Compliance and Internal Control

- **Cost-Benefit Analysis**
  - Measuring **expect losses is critical in understanding** the business impact of a disruption. Expected loss can be calculated as:

$$\text{Expected Loss} = P_1 * P_2 * L$$

where

- P_1 = **probability of attack** (estimate, based on judgment)
- P_2 = **probability of attack being successful** (estimate, based on judgment)
- L = **loss occurring** if attack is successful

Compliance and Internal Control

- **Cost-Benefit Analysis**

  Example:

  P_1 (.02) * P_2 (.10) * L ($1,000,000)

  Expected loss from this occurrence is

  (.02) * (.10) = .002 * 1,000,000 = $2,000

Compliance and Internal Control

- Business Impact Analysis (BIA)
  - **Estimates the consequences of disruption of a business** function and collects data to develop recovery strategies with potential loss scenarios first identified during the risk assessment.
  - Some examples:
    - **Lost sales and income**
    - **Delayed sales or income**
    - **Increased expenses** (e.g., overtime labor, outsourcing, expediting costs, etc.)
    - **Regulatory fines**

Compliance and Internal Control

1. Why are internal controls needed?

- The internal control environment is the work atmosphere that a company sets for its employees. Internal control (IC) is a process designed to achieve:
- Reliability of financial reporting, to protect investors
- Operational efficiency
- Compliance with laws
- Regulations and policies
- Safeguarding of assets

2. What federal law requires effective internal controls?

The Sarbanes-Oxley Act (SOX) requires companies to set up comprehensive internal controls.

3. Why do the SEC and FTC impose huge fines for data breaches?

The SEC and FTC impose huge fines for data breaches to deter companies from underinvesting in data protection.

4. What are the two types of controls in a defense strategy?

Answers may vary. The major categories of general controls are physical controls, access controls, data security controls, communication network controls, and administrative controls.

Compliance and Internal Control

5. Explain authentication and two methods of authentication.

- Authentication, also called user identification, is proving that the user is who he claims to be and is a part of access control.
- *Answers may vary.* Authentication methods include:
- Something only the user knows, such as a password
- Something only the user has, for example, a smart card or a token
- Something only the user is, such as a signature, voice, fingerprint, or retinal (eye) scan; implemented via biometric controls, which can be physical or behavioral

6. What are biometric controls? Give an example.

- A biometric control is an automated method of verifying the identity of a person, based on physical or behavioral characteristics. Most biometric systems match some personal characteristic against a stored profile.
- *Answers may vary.* The most common biometrics are a thumbprint or fingerprint, voice print, retinal scan, and signature.

7. Why do organizations need a business continuity plan?

Organizations need a business continuity plan to maintain or quickly restore business functions when there is a major disruption. The plan covers business processes, assets, human resources, business partners, and more. Fires, earthquakes, floods, power outages, malicious attacks, and other types of disasters hit data centers. Like insurance, it is a cost without a return on the investment unless and until a disaster happens.

8. Why should websites be audited?

Auditing a website is a good preventive measure to manage the legal risk. Legal risk is important in any IT system, but in Web systems it is even more important due to the content of the site, which may offend people or be in violation of copyright laws or other regulations (e.g., privacy protection).

Compliance and Internal Control

9. How is expected loss calculated?

- Expected loss is calculated as:
- Expected loss = P1 x P2 x L
- where
- P1 = probability of attack (estimate, based on judgment)
- P2 = probability of attack being successful (estimate, based on judgment)
- L = loss occurring if attack is successful

10. Explain business impact analysis.

- A business impact analysis (BIA) estimates the consequences of disruption of a business function and collects data to develop recovery strategies. The BIA identifies both operational and financial impacts resulting from a disruption. Several examples of impacts to consider include (Ready.gov, 2014):
- Lost sales and income
- Delayed sales or income
- Increased expenses (e.g., overtime labor, outsourcing, expediting costs, etc.)
- Regulatory fines
- Contractual penalties or loss of contractual bonuses
- Customer dissatisfaction or defection
- Delay of new business plans
- These costs and losses should be compared with the costs for possible recovery strategies. The BIA report should prioritize the order of events for restoration of the business, with processes having the greatest operational and financial impacts being restored first.

موفق باشید