Review Questions

1. Why are information systems vulnerable to destruction, error, and abuse?

1.1 List and describe the most common threats against contemporary information systems.

The most common threats against contemporary information systems include: technical, organizational, and environmental factors compounded by poor management decisions.

1. Technical: Unauthorized access, introducing errors
2. Communications: Tapping, sniffing, message alternation, theft and fraud, radiation
3. Corporate servers: Hacking, viruses and worms, theft and fraud, vandalism, denial of service attacks
4. Corporate systems: Theft of data, copying data, alteration of data, hardware failure, and software failure. Power failures, floods, fires, or other natural disasters can also disrupt computer systems.
5. Poor management decisions: Poorly designed safeguards that protect valuable data from being lost, destroyed, or falling into the wrong hands.

Review Questions

1.2 Define malware and distinguish among a virus, a worm, and a Trojan horse.

• Malware (for malicious software) is any program or file that is harmful to a computer user. Thus, malware includes computer viruses, worms, Trojan horses, and also spyware programs that gather information about a computer user without permission.

• Virus: A program or programming code that replicates itself by being copied or initiating its copying to another program, computer boot sector or document.

• Worm: A self-replicating virus that does not alter files but resides in active memory and duplicates itself without human intervention.

• Trojan horse. A program in which malicious or harmful code is contained inside apparently harmless programming or data. A Trojan horse is not itself a virus because it does not replicate but is often a way for viruses or other malicious code to be introduced into a computer system.
1.3 Define a hacker and explain how hackers create security problems and damage systems.

A hacker is an individual who gains unauthorized access to a computer system by finding weaknesses in security protections used by Web sites and computer systems. Hackers not only threaten the security of computer systems, but they also steal goods and information, as well as damage systems and commit cybervandalism. They may intentionally disrupt, deface, or even destroy a Web site or corporate information system.

1.4 Define computer crime. Provide two examples of crime in which computers are targets and two examples in which computers are used as instruments of crime.

The Department of Justice defines computer crime as "any violations of criminal law that involve a knowledge of computer technology for their perpetration, investigation, or prosecution." Computer crime is defined as the commission of illegal acts through the use of a computer or against a computer system.

Computers as targets of crime:
1. Breaching the confidentiality of protected computerized data
2. Accessing a computer system without authority
3. Knowingly accessing a protected computer to commit fraud
4. Intentionally accessing a protected computer and causing damage, negligently or deliberately
5. Knowingly transmitting a program, program code, or command that intentionally causes damage to a protected computer
6. Threatening to cause damage to a protected computer

Computers as instruments of crime:
1. Theft of trade secrets
2. Unauthorized copying of software or copyrighted intellectual property, such as articles, books, music, and video
3. Schemes to defraud
4. Using e-mail for threats or harassment
5. Internationally attempting to intercept electronic communication
6. Illegally accessing stored electronic communications, including e-mail and voice mail
7. Transmitting or processing child pornography using a computer

1.5 Define identity theft and phishing and explain why identity theft is such a big problem today.

Identity theft is a crime in which an imposter obtains key pieces of personal information, such as social security identification number, driver's license number, or credit card numbers, to impersonate someone else. The information may be used to obtain credit, merchandise, or services in the name of the victim or to provide the thief with false credentials.

It is a big problem today as the Internet has made it easy for identity thieves to use stolen information because goods can be purchased online without any personal interaction. Credit card files are a major target of Web site hackers. Moreover, e-commerce sites are wonderful sources of customer personal information that criminals can use to establish a new identity and credit for their own purposes.

Phishing involves setting up fake Web sites or sending e-mail messages that look like those of legitimate businesses to ask users for confidential personal data. The e-mail instructs recipients to update or confirm records by providing social security numbers, bank and credit card information, and other confidential data either by responding to the e-mail message or by entering the information at a bogus Web site. New phishing techniques such as evil twins and pharming are very hard to detect.

1.7 Explain how software defects affect system reliability and security.

The software can fail to perform, perform erratically, or give erroneous results because of undetected bugs. A control system that fails to perform can mean medical equipment that fails or telephones that do not carry messages or allow access to the Internet. A business system that fails means customers are under- or over-billed. Or, it could mean that the business orders more inventory than it needs. Or an automobile's braking system may fail.

Major quality problems are the bugs or defects caused by incorrect design. The other problem is maintenance of old programs caused by organizational changes, system design flaws, and software complexity. Bugs in even mildly complex programs can be impossible to find in testing, making them hidden bombs.
2. What is the business value of security and control?

2.1 Explain how security and control provide value for businesses.

Security refers to the policies, procedures, and technical measures used to prevent unauthorized access, alteration, theft, or physical damage to information systems.

Controls consist of all the methods, policies, and organizational procedures that ensure the safety of the organization's assets; the accuracy and reliability of its account records; and operational adherence to management standards.

The business value of security and control:
1. Firms relying on computer systems for their core business functions can lose sales and productivity.
2. Information assets, such as confidential employee records, trade secrets, or business plans, lose much of their value if they are revealed to outsiders or if they expose the firm to legal liability.

3. What are the components of an organizational framework for security and control?

3.1 Define general controls and describe each type of general control.

General controls govern the design, security, and use of computer programs and the security of data files in general throughout the organization's information technology infrastructure. They apply to all computerized applications and consist of a combination of hardware, software, and manual procedures that create an overall control environment.

General controls include software controls, physical hardware controls, computer operations controls, data security controls, controls over implementation of system processes, and administrative controls.

3.2 Define application controls and describe each type of application control.

Application controls are specific controls unique to each computerized application. They include both automated and manual procedures that ensure that only authorized data are completely and accurately processed by that application.

Application controls can be classified as:
1. Input controls: Check data for accuracy and completeness when they enter the system. There are specific input controls for input authorization, data conversion, data editing, and error handling.
2. Processing controls: Establish that data are complete and accurate during updating.
3. Output controls: Ensure that the results of computer processing are accurate, complete, and properly distributed.

3.3 Describe the function of risk assessment and explain how it is conducted for information systems.

A risk assessment determines the level of risk to the firm if a specific activity or process is not properly controlled. Business managers working with information systems specialists can determine the value of information assets, points of vulnerability, the likely frequency of a problem, and the potential for damage. Controls can be adjusted or added to focus on the areas of greatest risk. An organization does not want to over-control areas where risk is low and under-control areas where risk is high.

Security risk analysis involves determining what you need to protect, what you need to protect it from, and how to protect it. It is the process of examining all of the firm’s risks, and ranking those risks by level of severity. This process involves making cost-effective decisions on what you want to protect. The old security adage says that you should not spend more to protect something than it is actually worth. Two elements of a risk analysis that should be considered are: (1) identifying the assets and (2) identifying the threats. For each asset, the basic goals of security are availability, confidentiality, and integrity. Each threat should be examined with an eye on how the threat could affect these areas. One step in a risk analysis is to identify all the things that need to be protected. Some things are obvious, like all the various pieces of hardware, but some are overlooked, such as the people who actually use the systems. The essential point is to list all things that could be affected by a security problem.
4. What are the most important tools and technologies for safeguarding information resources?

4.1 Name and describe three authentication methods.

Authentication refers to the ability to know that a person is who he or she claims to be. Some methods are described below:

1. What you know: Passwords known only to the authorized users.

2. What you have:
   - Token is a physical device that is designed to provide the identity of a single user
   - Smart card is a device that contains a chip formatted with access permission and other data.

3. What you are: Biometrics is based on the measurement of a physical or behavioral trait that makes each individual unique.

4.2 Describe the roles of firewalls, intrusion detection systems, and antivirus software in promoting security.

A firewall is a combination of hardware and software that controls the flow of incoming and outgoing network traffic. Firewalls prevent unauthorized users from accessing internal networks. They protect internal systems by monitoring packets for the wrong source or destination, or by offering a proxy server with no access to the internal documents and systems, or by restricting the types of messages that get through, for example, e-mail. Further, many authentication controls have been added for Web pages as part of firewalls.

Intrusion detection systems monitor the most vulnerable points or “hot spots” in a network to detect and deter unauthorized intruders. These systems often also monitor events as they happen to look for security attacks in progress. Sometimes they can be programmed to shut down a particularly sensitive part of a network if it receives unauthorized traffic.

Antivirus software is designed to check computer systems and drives for the presence of computer viruses and worms and often eliminates the malicious software, whereas antispyware software combats intrusive and harmful spyware programs. Often the software can eliminate the virus from the infected area. To be effective, antivirus software must be continually updated.

4.3 Describe the role of encryption and digital certificates in a public key infrastructure.

Digital certificates combined with public key encryption provide further protection of electronic transactions by authenticating a user’s identity. Digital certificates are data fields used to establish the identity of the sender and to provide the receiver with the means to encode a reply. They use a trusted third party known as a certificate authority to validate a user’s identity. Both digital signatures and digital certificates play a role in authentication. Authentication refers to the ability of each party to know that the other parties are who they claim to be.

11. eCommerce and eBusiness
Review Questions

1.1 List and describe the eight unique features of e-commerce.

- E-commerce technology is **ubiquitous**, meaning that it is available just about everywhere a computer can connect to the Internet.
- It has **global reach**, permitting commercial transactions to cross cultural and national boundaries far more conveniently and cost effectively than is true in traditional commerce.
- It operates according to **universal standards** shared by all nations around the world, whereas most traditional commerce technologies differ from one nation to the next.
- It provides information **richness**, enabling an online merchant to deliver to an audience of millions complex and rich marketing messages with text, video, and audio in a way not possible with traditional commerce technologies, such as radio, television, or magazines.
- It is **interactive**, meaning it allows for two-way communication between merchant and consumer and enables the merchant to engage a consumer in ways similar to a face-to-face experience but on a much more massive, global scale.
- It increases **information density** (the total amount and quality of information available to all market participants).
- It permits **personalization and customization**: Merchants can target their marketing messages to specific individuals by adjusting the message to a person’s name, interests, and past purchases.
- **Social technology** enables user content creation and distribution and supports social networks.

2.2 Name and describe the e-commerce revenue models.

There are six e-commerce revenue models:

- **Advertising** revenue: Generates revenue by attracting a large audience of visitors who can then be exposed to advertisements. It’s the most widely used revenue model in e-commerce.
- **Sales** revenue: Companies derive revenue by selling goods, information, or services to customers.
- **Subscription** revenue: A Web site offering content or services charges a subscription fee for access to some or all of its offerings on an ongoing basis.
- **Free/freemium** revenue: Basic services or content are free while advanced or special features cost extra.
- **Transaction fee** revenue: A company receives a fee for enabling or executing a transaction.
- **Affiliate** revenue: Sites that steer customers to an affiliate business receive a referral fee or percentage of the revenue from any resulting sales.

Review Questions

1.2 Define a digital market and digital goods and describe their distinguishing features.

Digital markets are said to be more “transparent” than traditional markets. The Internet has created a digital marketplace where millions of people are able to exchange massive amounts of information directly, instantly, and for free. Information asymmetry is reduced. Digital markets are very flexible and efficient, with reduced search and transaction costs, lower menu prices, and the ability to change prices dynamically based on market conditions. Digital markets provide many opportunities to sell directly to the consumer, bypassing intermediaries, such as distributors or retail outlets. Other features include delayed gratification, price discrimination, market segmentation, switching costs, and network effects.

Digital goods are goods that can be delivered over a digital network and include music, video, software, newspapers, magazines, and books. Once a digital product has been produced, the cost of delivering that product digitally is extremely low. New business models based on delivering digital goods are challenging bookstores, publishers, music labels, and film studios that depend on delivery of traditional goods.

2.1 Name and describe the principal e-commerce business models.

- **E-tailer**: Sells physical products directly to consumers or individual businesses.
- **Transaction broker**: Saves users money and time by processing online sale transactions and generates a fee each time.
- **Market creator**: Provides a digital environment where buyers and sellers meet, search for and display products, and establishes prices for those products; it can provide online auctions and reverse auctions.
- **Content provider**: Creates revenue by providing digital content, such as digital news, music, photos, or video over the Web.
- **Community provider**: Provides an online meeting place where people with similar interests can communicate and find useful information.
- **Portal**: Provides an initial point of entry to the Web along with specialized content and other services.
- **Service provider**: Provides Web 2.0 applications such as photo sharing, video sharing, and user-generated content as services. Provides other services such as online data storage and backup.