INFO 1400

Koffka Khan

Tutorial 8
1. A fully digital firm produces only digital goods or services.
Answer: FALSE

2. There are four major business functions: Sales and marketing; manufacturing and production; finance and accounting; and information technology.
Answer: FALSE

3. The use of information systems because of necessity describes the business objective of
   a) survival.
   b) improved business practices.
   c) competitive advantage.
   d) improved flexibility.
Answer: A
4. The average number of tickets sold daily online is an example of
   a) input.
   b) raw data.
   c) meaningful information.
   d) feedback.
   Answer:  C

5. In a hierarchical organization, the upper levels consist of
   a) managerial and professional employees.
   b) managerial, professional, and technical employees.
   c) professional and operational employees.
   d) managerial, professional, and operational employees.
   Answer:  B
6. You would use an MIS to help decide whether to introduce a new product line.
Answer: FALSE

7. A transaction processing system is a computerized system that performs and records the daily routine transactions necessary to conduct business.
Answer: TRUE

8. Which type of system would you use to change a production schedule if a key supplier was late in delivering goods?
   a) ESS
   b) TPS
   c) MIS
   d) DSS
Answer: B
9. Which systems are typically a major source of data for other systems?
   a) transaction processing systems
   b) management information systems
   c) executive support systems
   d) decision-support systems

Answer: A

10. The term "management information systems" designates a specific category of information systems serving
    a) integrated data processing throughout the firm.
    b) transaction process reporting.
    c) employees with online access to historical records.
    d) middle management functions.

Answer: D
11. A firm can be said to have competitive advantage when they have higher stock market valuations than their competitors.

Answer: TRUE

12. A transparent marketplace means that there is high product differentiation.

Answer: FALSE

13. The interaction between information systems and organizations is influenced
   a) primarily by the decision making of middle- and senior-managers.
   b) by many factors, including structure, politics, culture, and environment.
   c) by two main microeconomic forces: capital and labor.
   d) primarily by the organization's business processes and culture.

Answer: B
14. How does the technical view of organizations fall short of understanding the full impacts of information systems in a firm?
   a) It sees information systems as a way to rearrange the inputs and outputs of the organization.
   b) It sees capital and labor as primary production factors.
   c) It sees the inputs and outputs, labor and capital, as being infinitely malleable.
   d) It sees the organization as a social structure similar to a machine.

Answer: C

15. Business processes are collections of
   a) informal practices and behaviors.
   b) formalized and documented practices.
   c) routines.
   d) rights and privileges.

Answer: C
16. A cookie is a small file containing information about you and your Web activities that is deposited on your hard disk by a Web site.
Answer: TRUE

17. P3P encrypts or scrambles e-mail or data so that it cannot be read illicitly.
Answer: FALSE

18. The use of computers to combine data from multiple sources and create electronic dossiers of detailed information on individuals is called
   a) profiling.
   b) phishing.
   c) spamming.
   d) targeting.
Answer: A
19. The feature of social institutions that means mechanisms are in place to determine responsibility for an action is called
   a) due process.
   b) accountability.
   c) the courts of appeal.
   d) the judicial system.

   Answer: B

20. Immanuel Kant's Categorical Imperative states that
   a) if an action cannot be taken repeatedly, then it is not right to be taken at any time.
   b) one should take the action that produces the least harm or incurs the least cost.
   c) one can put values in rank order and understand the consequences of various courses of action.
   d) if an action is not right for everyone to take, it is not right for anyone to take.

   Answer: D
21. N-tier computing is a multi-tier, load-balancing scheme for Web-based applications in which significant parts of Web site content, logic, and processing are performed by smaller, less expensive servers located nearby the user.

Answer: TRUE

22. Like an ASP, a Web hosting service provides shared applications to subscribed users, but does this through a Web portal.

Answer: FALSE

23. Which type of infrastructure services provides voice and video connectivity to employees, customers, and suppliers?
   a) networking
   b) telephone
   c) VOIP
   d) telecommunications

Answer: D
24. A client computer networked to a server computer, with processing split between the two types of machines, is called a(n)
   a) service-oriented architecture.
   b) on-demand architecture.
   c) multi-tiered client/server architecture.
   d) two-tiered client/server architecture.
   Answer: D

25. Interpretations of Moore's law assert that
   a) computing power doubles every 18 months.
   b) transistors decrease in size 50% every two years.
   c) data storage costs decrease by 50% every 18 months.
   d) none of the above.
   Answer: A
26. A DBMS separates the logical and physical views of data.
   Answer: TRUE

27. A data warehouse is typically comprised of several smaller data marts.
   Answer: FALSE

28. The data dictionary serves as an important data management tool by
    a) assigning attributes to the data.
    b) creating an inventory of the data elements contained in the database.
    c) presenting data as end users or business specialists would perceive them.
    d) maintaining data in updated form.
   Answer: B
29. The most prominent data manipulation language today is
   a) Access.
   b) DB2.
   c) SQL.
   d) Crystal Reports.
   Answer: C

30. DBMSs typically include report-generating tools in order to
   a) retrieve and display data.
   b) display data in an easier-to-read format.
   c) display data in graphs.
   d) perform predictive analysis.
   Answer: B
INFO1400 Information Technology Fundamentals
Assignment 2 Presentations: 10 minutes per group

Present 1: Group 30
   Jozette Hector, Kerron Clement, Alycia Huggins, Nathaniel Holder
   Netflix

Present 2: Group 35
   Navin Narine, Robert V. Phillip, Darius Mc Connie
   Wal-Mart

Present 3: Group 23
   Kirron Lewis Zahrah Hosein Urban Stephens Rosella Latiff
   Wrigley

Present 4: Group 2
   Marcus Gopaul Kirby Sylvester Richard Balliram Curtis Griffith
   ILLUMINAT

Present 5: Group 11
   Candace-Lynn Jane Mahabir Kevin Sampath Jeremy Ramgoolie
   Ricardo Henry
   IBM
1. Is cyberwarfare a serious problem? Why or why not?

Cyberwarfare poses a unique and daunting set of challenges for security experts, not only in detecting and preventing intrusions but also in tracking down perpetrators and bringing them to justice. The most prominent threats so far include:

1. Successful attacks on the FAA airline system, including one in 2006 that partially shut down air traffic data systems in Alaska.
2. Intruders successfully penetrated the Pentagon’s $300 billion Joint Strike Fighter project and stole several terabytes of data related to design and electronics systems.
3. Cyberspies infiltrated the U.S. electrical grid in April 2009 and left behind software programs whose purpose is unclear.
4. In Iraq, insurgents intercepted Predator drone feeds using software downloaded from the Internet.
5. An act of cyberwar against a critical resource such as the electric grid, financial system, or communication systems would likely be devastating.
Case Study: Are We Ready for Cyberwarfare?

2. Assess the management, organization, and technology factors that have created this problem.

Management: For cybercriminals, the benefit of cyberwarfare is that they can compete with traditional superpowers for a fraction of the cost of other types of warfare. Because more and more modern technological infrastructure will rely on the Internet to function, cyberwarriors will have no shortage of targets at which to take aim. Users of targeted systems are still too careless about security and don’t do enough to help protect sensitive systems.

Organization: The U.S. has no clear policy about how the country would respond to a catastrophic level of a cyberattack. Even though the U.S. Congress is considering legislation to toughen cybersecurity standards, the standards will likely be insufficient to defend against attacks. The organization of U.S. cybersecurity is messy, with no clear leader among intelligence agencies.

Technology: While the U.S. is currently at the forefront of cyberwarfare technologies, it’s unlikely to maintain technological dominance because of the relatively low cost of the technologies needed to mount these types of attacks. Secret surveillance software can be installed on unprotected systems and can access files and e-mail thus spreading itself to other systems. Tracing identities of specific attackers through cyberspace is next to impossible, making deniability of suspected intruders simple.
Case Study: Are We Ready for Cyberwarfare?

3. What solutions have been proposed? Do you think they will be effective? Why or why not?

Proposed solutions include the following along with an assessment of their effectiveness:

1. Congress is considering legislation that would require all critical infrastructure companies to meet newer, tougher cybersecurity standards. As cyberwarfare technologies develop and become more advanced, the standards imposed by this legislation will likely be insufficient to defend against attacks.

2. Secretary of Defense Gates ordered the creation of Cybercom, the first headquarters designed to coordinate government cybersecurity efforts. It was activated in May 2010. It will coordinate the operation and protection of military and Pentagon computer networks. It will coordinate efforts to restrict access to government computers and protect systems that run the stock exchanges, clear global banking transactions, and manage the air traffic control system. Its ultimate goal will be to prevent catastrophic cyberattacks against the U.S. Some insiders suggest that it might not be able to effectively organize the governmental agencies without direct access to the President, which it currently lacks.

3. Because spy agencies like the CIA are prohibited by law from acting on American soil, some people are proposing to entrust some of the cyberwarfare work to private defense contractors. There is no effective way for a domestic agency to conduct computer operations without entering prohibited networks within the U.S. or even conduct investigations in countries that are American allies. Preventing terrorist or cyberwar attacks may require examining some email messages from other countries or giving intelligence agencies more access to networks or Internet service providers.
Case Study: Are We Ready for Cyberwarfare?

4. Are there other solutions for this problem that should be pursued? What are they?

It’s unclear as to how strong the United States’ offensive capabilities for cyberwarfare are. The government closely guards this information, almost all of which is classified. But former military and intelligence officials indicate that our cyberwarfare capabilities have dramatically increased in sophistication in the past year or two. Because tracking cybercriminals has proven so difficult, it may be that the best defense is a strong offense.
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.
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
Review Questions

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.
Review Questions

2.2 Describe the relationship between security and control and recent U.S. government regulatory requirements and computer forensics.

Legal actions requiring electronic evidence and computer forensics also require firms to pay more attention to security and electronic records management. Computer forensics is the scientific collection, examination, authentication, preservation, and analysis of data held on or retrieved from computer storage media in such a way that the information can be used as evidence in the court of law. It deals with the following problems:

1. Recovering data from computers while preserving evidential integrity
2. Securely storing and handling recovered electronic data
3. Finding significant information in a large volume of electronic data
4. Presenting the information to a court of law

Recent U.S. government regulatory requirements include:

1. Health Insurance Portability and Accountability Act (HIPAA)
2. Gramm-Leach-Bliley Act
3. Sarbanes-Oxley Act

These laws require companies to practice stringent electronic records management and adhere to strict standards for security, privacy, and control.
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.
Review Questions

3.4 Define and describe the following: Security policy, acceptable use policy, and identity management.

A security policy consists of statements ranking information risks, identifying acceptable security goals, and identifying the mechanisms for achieving these goals. The security policy drives policies determining acceptable use of the firm’s information resources and which members of the company have access to its information assets.

An acceptable use policy (AUP) defines acceptable uses of the firm’s information resources and computing equipment, including desktop and laptop computers, wireless devices, telephones, and the Internet. The policy should clarify company policy regarding privacy, user responsibility, and personal use of company equipment and networks. A good AUP defines unacceptable and acceptable actions for each user and specifies consequences for noncompliance.

Identity management consists of business processes and software tools for identifying valid system users and controlling their access to system resources. It includes policies for identifying and authorizing different categories of system users, specifying what systems or portions of systems each user is allowed to access, and the processes and technologies for authenticating users and protecting their identities.
3.5 Explain how MIS auditing promotes security and control.

Comprehensive and systematic MIS auditing organizations determine the effectiveness of security and controls for their information systems. An MIS audit identifies all of the controls that govern individual information systems and assesses their effectiveness. Control weaknesses and their probability of occurrence will be noted. The results of the audit can be used as guidelines for strengthening controls, if required.
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 Explain how encryption protects information.

Encryption, the coding and scrambling of messages, is a widely used technology for securing electronic transmissions over the Internet and over Wi-Fi networks. Encryption offers protection by keeping messages or packets hidden from the view of unauthorized readers. Encryption is crucial for ensuring the success of electronic commerce between the organization and its customers and between the organization and its vendors.
4.4 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.
4.5 Distinguish between fault-tolerant and high-availability computing, and between disaster recovery planning and business continuity planning.

Fault-tolerant computer systems contain redundant hardware, software, and power supply components that can back the system up and keep it running to prevent system failure. Some systems simply cannot be allowed to stop, such as stock market systems or some systems in hospitals. Fault-tolerant computers contain extra memory chips, processors, and disk storage devices to backup a system and keep it running. They also can use special software routings or self-checking logic built into their circuitry to detect hardware failures and automatically switch to a backup device.

High-availability computing, though also designed to maximize application and system availability, helps firms recover quickly from a crash. Fault tolerance promises continuous availability and the elimination of recovery time altogether. High-availability computing environments are a minimum requirement for firms with heavy electronic commerce processing requirements or for firms that depend on digital networks for their internal operations.

Disaster recovery planning devises plans for the restoration of computing and communications services after they have been disrupted by an event such as an earthquake, flood, or terrorist attack. Disaster recovery plans focus primarily on the technical issues involved in keeping systems up and running, such as which files to back up and the maintenance of backup computer systems or disaster recovery services.

Business continuity planning focuses on how the company can restore business operations after a disaster strikes. The business continuity plan identifies critical business processes and determines action plans for handling mission-critical functions if systems go down.
4.6 Identify and describe the security problems posed by cloud computing.

Accountability and responsibility for protection of sensitive data reside with the company owning that data even though it’s stored offsite. The company needs to make sure its data are protected at a level that meets corporate requirements. The company should stipulate to the cloud provider how its data is stored and processed in specific jurisdictions according to the privacy rules of those jurisdictions. The company needs to verify with the cloud provider how its corporate data is segregated from data belonging to other companies and ask for proof that encryption mechanisms are sound. The company needs to verify how the cloud provider will respond if a disaster strikes. Will the cloud provider be able to completely restore the company’s data and how long will that take? Will the cloud provider submit to external audits and security certifications?
Review Questions

4.7 Describe measures for improving software quality and reliability.

Using software metrics and rigorous software testing are two measures for improving software quality and reliability.

Software metrics are objective assessments of the system in the form of quantified measurements. Metrics allow an information systems department and end users to jointly measure the performance of a system and identify problems as they occur. Metrics must be carefully designed, formal, objective, and used consistently. Examples of software metrics include:

1. Number of transactions that can be processed in a specified unit of time
2. Online response time
3. Number of known bugs per hundred lines of program code

Early, regular, and thorough testing will contribute significantly to system quality. Testing can prove the correctness of work but also uncover errors that always exist in software. Testing can be accomplished through the use of:

1. Walkthroughs: A review of a specification or design document by a small group of people
2. Coding walkthroughs: Once developers start writing software, these can be used to review program code.
3. Debugging: When errors are discovered, the source is found and eliminated