Solution Manual for Experiencing MIS 6th Edition by Kroenke

Boyle ISBN 0133939138 9780133939132

Chapter 1 The Importance of MIS

1 -4. Abstract reasoning.

a. Define abstract reasoning , and explain why it is an important skill for business professionals.

b. Explain how a list of items in inventory and their quantity on hand is an abstraction of a physical inventory.

c. Give three other examples of abstractions commonly used in business.

d. Explain how Jennifer failed to demonstrate effective abstract reasoning skills. e. Can people increase their abstract reasoning skills? If so, how? If not, why not?

1 -5. Systems thinking.

a. Define systems thinking , and explain why it is an important skill for business professionals.

b. Explain how you would use systems thinking to explain why Moore's Law caused a farmer to dig up a field of pulpwood trees. Name each of the elements in the system and explain their relationships to each other.

c. Give three other examples of the use of systems thinking with regard to consequences of Moore 's Law.

d. Explain how Jennifer failed to demonstrate effective systems-thinking skills. e. Can people improve their systems-thinking skills? If so, how? If not, why not?

1 -6. Collaboration.

a. Define collaboration , and explain why it is an important skill for business professionals.

b. Explain how you are using collaboration to answer these questions. Describe what is working with regard to your group's process and what is not working.

c. Is the work product of your team better than any one of you could have done separately? If not, your collaboration is ineffective. If that is the case, explain why. d. Does the fact that you cannot meet face to face hamper your ability to collaborate? If so, how?

e. Explain how Jennifer failed to demonstrate effective collaboration skills. f. Can people increase their collaboration skills? If so, how? If not, why not?

1 -7. Experimentation.

a. Define experimentation , and explain why it is an important skill for business professionals.

b. Explain several creative ways you could use experimentation to answer this question.

c. How does the fear of failure influence your willingness to engage in any of the ideas you identified in part b?

d. Explain how Jennifer failed to demonstrate effective experimentation skills.

e. Can people increase their willingness to take risks? If so, how? If not, why not?

1 -8. Job security.

a. State the text 's definition of job security .

b. Evaluate the text's definition of job security. Is it effective? If you think not, offer a better definition of job security.

c. As a team, do you agree that improving your skills on the four dimensions in Collaboration Exercises 1-4 through 1-7 will increase your job security?

d. Do you think technical skills (accounting proficiency, financial analysis proficiency, etc.) provide job security? Why or why not? Do you think students in 1990 would have answered this differently? Why or why not?

Information System Security is a very important task for most of the organizations and individual users of the internet; following are the problems which arise due to lack of proper security policies.

• **THREAT:** A threat is a person or organization trying to access or steal sensitive personal information or data or assets from users without the user permissions. This unauthorized access of user information is usually done without the user's knowledge.

• **For example:** A user is doing a bank transaction online, the user provides his/her bank account details and login credentials over the web to access his bank account. If any intruder captures these data details and accesses the user account without the user knowledge, such an illegal access of data causing a loss to the user is called as a threat.

• **VULNERABILITY:** it is the gateway point through which individual data or assets are accessed by intruders or threats, that is the chance given to the threats to access information.

• **For example:** for the same example when the user provides the login credentials to access the account online, data is transmitted over the web, this transfer of data over the internet is the vulnerable point allowing threats to access the user information.

• **SAFEGUARD:** these are the protection policies employed by the website owners or organizations to protect their data and assets from illegal access. These methods are not always effective.

• **For example:** when an individual is transferring information over the web, a safeguard protect this information and hides it from being accessed by intruders or threats.

• **TARGET:** the data or asset that is being illegally accessed by the threat is called as the target.

• **For example:** in the above example the login credentials of the user bank account is the target of the threat or intruder.

The different sources of threats are:

• **Human Errors:** these threats are caused by individuals like employees or customers, employees accidental deleting or misplacing customer details or records.

• **Computer Crimes:** this threat is caused by intruders, hackers trying to access information over the web illegally, installing viruses on individual computers trying to corrupt user systems, phishing etc.

• **Natural events and disasters:** these threats are caused due to natural calamities like fire accidents, floods, earthquakes.

The different types of losses:

• **Unauthorized Data Disclosure:** Sensitive data or information of a user or organization when accessed by unauthorized people creates a loss to the organization or to the users. That is disclosure of data can be done either accidentally or intentionally, when an employee accidentally sends an email containing his clients sensitive information to the entire team or friends. An intruder accessing organization trade secrets illegally. Phishing, spoofing, hacking, sniffing all these activities try to access data illegally.

• **Incorrect Data Modification:** this security loss occurs when an organizations data or user's data has been modified incorrectly, data modifications which occur due to human errors that is an employee trying to modify customer data following a procedure which is incorrectly designed, or modifying data by performing calculation errors. Sometimes intruders illegally try to access data and modify its contents.

• **Faulty Service:** when services provided by the organization or a system halt or crash due to incorrect system operations. Incorrect system operations can occur either due to incorrect code or incorrect procedures designed to run the systems. Sometimes the system operation raise fault as intruders try to modify the system code.

• **Denial of Service:** this type of security loss occurs when there is an error in the procedure code or the procedures are not compiling to provide services, this could happen due to human error or by an intruder blocking the services provided by the procedure.

• **Loss of Information:** this type of loss may occur due to human error, theft of information, natural disasters crashing the system databases.

There are several threats and each threat results in different kind of loss to the Information System

Threats due to Human Error and their Loss:

• Human errors are usually procedural mistakes, incorrect coding of procedures, system errors, errors in developing the code, errors in deploying the code, errors in installing the procedures, sometime human errors occur accidentally.

• All these threats due to human errors result in the following losses, Unauthorized data disclosure, Incorrect data modification, faulty service, denial of service and loss of infrastructure.

Threats due to Computer Crime and their loss:

• The different types of cybercrimes are phishing, pretexting, spoofing, sniffing, hacking, theft, Usurpation, denial of service attacks.

• The loss which occur due to cybercrimes are, sensitive data being disclosed publicly, incorrect data modification due to unauthorized access of data, faulty services, denial of service, loss of infrastructure.

Threats due to Natural Disaster and their loss:

• The loss due to natural disaster are data being disclosed during recovery, incorrect recovery of data, improper restoration of services resulting in faulty services, loss of property

Example for Threat over the Web
• A Hacker wants to access your credit card details and wants to employ a Trojan on your PC and sends a fake email stating that the last transaction made by the user was incorrect and will be reverted. To complete the last transaction the user made they ask the user to visit a site provide the details requested, the user is provided with a link.

• If proper Safeguard is employed by the user like antivirus, firewalls and malwares as soon as the user clicks on the link no loss of information occurs and the safeguard protects the user PC and information.

• If ineffective safeguard techniques are used there is loss of information and the computer may be affected by virus.

• The user using a proper safeguard and who follows procedures tries to type the correct IP address of the website he last visited where he has done his credit card transaction and verifies his transaction details before providing his credit card details.

Estimating the Cost to Implement Information System Security:

The cost required to implement or to provide security to information systems is difficult to estimate due to the following factors:

• Organizations or users cannot exactly estimate the loss which occurred due to cybercrime in monetary terms. Though the cost of the data or asset lost can be estimated for that instance, but lost data or information related to an organization is related to many customers and sometimes related to organization trade secrets that has many liabilities and is difficult to estimate.

• The amount of man hours required to back up and restore the lost information cannot be estimated exactly if proper risk management facility is not available.

• Though the cost required to purchase efficient safeguards can be estimated, but not all the safeguards employed work effectively.

Goal of Information System Security:

The main goal of information security is to protect data or information related to organizations or users from being accessed and used illegally. Information system security aims to provide Confidentiality, Availability, and Integrity of data or information to its users.

• Confidentiality means controlling and preventing unauthorized access of data when the data is stored on a disk or when the data is being transmitted.

• Integrity is to maintain consistence in the data stored, loss which occurs due to incorrect data modifications must be reduced, illegal modifications of data is not allowed.

• Availability making sure that the data or information is accessible for the right users in right time, this goal tries to protect the data from the loss that occurs due to faulty services and denial of service.

• The main important goal of information security systems is to balance between the risk due to loss of information and the cost to implement security measures or safeguards to protect the data from threats.

• The organizations should select appropriate safeguards techniques suitable for their project system in the provided budget, these safeguards must reduce the risks which occur due to threats or loss.