Course Learning Outcomes for Unit VIII

Upon completion of this unit, students should be able to:

1. List the procedures for a disaster recovery plan.
2. Explain the importance of security training and awareness.

Reading Assignment

Chapter 13:
Business Continuity

Chapter 14:
Risk Mitigation

Click here to access the Chapter 13 Presentation.

Click here to access the Chapter 14 Presentation

Unit Lesson

This unit includes the critical importance of keeping an organization operational in the face of disaster, what business continuity is and its importance, ways to prevent disruptions through disaster recovery and how to protect resources with environmental controls, and see how incident response procedures are utilized when an unauthorized event, such as a security breach occurs. This unit also includes how organizations establish and maintain security in the face of risk, risks and steps to control them, security policies and the different types of policies that are used to reduce risk, and how training and awareness can help provide the user with the tools to maintain a secure environment within the organization (Ciampa, 2012).

First, let us define business continuity. According to Ciampa (2012), business continuity can be defined as "The ability of an organization to maintain its operations and services in the face of a disruptive event" (p. 489). Some examples of disruptive events include power outages, hurricanes, and tsunamis. The business continuity planning and testing steps include (1) creating preventative and recovery procedures, (2) testing procedures to determine if they are sufficient, and (3) identifying the exposure to threats. Succession planning determines in advance who is authorized to take over if key employees are incapacitated or die. The business impact analysis (BIA) analyzes the most important business functions and quantifies the impact of their losses, identifies threats through risk assessment, and determines impact of threats are realized.

Disaster recovery is a subset of business continuity planning and testing. Disaster recovery is also known as contingency planning and focuses on protecting and restoring information technology functions. Mean time to restore (MMTR) is used as a measurement and measures the average time needed to reestablish services. Disaster recovery activities include creating, implementing, and testing disaster recovery plans. A disaster recovery plan is a written document that details the process for restoring IT resources following a disruptive event. The plan is comprehensive in scope and is updated on a regular basis. The disaster recovery plan details restoration procedures, outlines emergency procedures, lists risks and procedures, and safeguards that reduced risk. The plan also defines the purpose and scope as well as the recovery team and their responsibilities. The plan also includes preparing for a disaster, emergency procedures, and restoration procedures. A disaster exercise objective tests the efficiency of the interdepartmental planning and coordination in managing a disaster. It also tests the current disaster recovery plan procedures and determines the strengths and weaknesses of the responses.

A single point of failure should be removed to ensure business continuity. A server plays a key role in the network infrastructure, and a crash of a single server can have devastating consequences. An organization should designate other servers in a cluster for redundancy. Maintaining electrical power is also essential when planning for redundancy. An uninterruptible power supply (UPS) is a device that can be used to handle this need. Three types of redundant sites are used when an organization is forced to use another location after some type of disaster: hot sites, cold sites, and warm sites. Data backups are also essential in a disaster recovery plan. It is best to have the storage location different from the main site such as another state. Fire damage could also serve as a constant threat. Electromagnetic fields are emitted from all computer systems and similar devices. A Faraday cage can be used to control this threat. Computer forensics is of interest and "attempts to retrieve information that can be used in the pursuit of a computer crime" (Ciampa, 2012, p. 517).

Several different types of terms are used in the context of information security: threat, threat agent, vulnerability, and risk. *Threats* have the potential to cause harm. *Threat agents* are people who have the power to carry out the threat. A flaw or weakness is considered a *vulnerability* and can allow a threat agent to bypass security. The *risk* is the likelihood that a threat agent will exploit the vulnerability. Risks are divided into several classifications. See Table 14-1 (page 436 in your textbook) below.

Risk category	Description	Example
Strategic	Action that affects the long-term goals of the organization	Theft of intellectual property, not pursuing a new opportunity, loss of a major account, competitor entering the market
Compliance	Following a regulation or standard	Breach of contract, not responding to the introduction of new laws
Financial	Impact of financial decisions or market factors	Increase in interest rates, global financial crisis
Operational	Events that impact the daily business of the organization	Fire, hazardous chemical spill, power blackout
Environmental	Actions related to the surroundings	Tornado, flood, hurricane
Technical	Events that affect information technology systems	Denial of service attack, SQL injection attack, virus
Managerial	Actions that are related to the management of the organization	Long-term illness of company president, key employee resigning

Table 14-1 Risk classifications *(Ciampa, 2012)*

Risk can be controlled by privilege, privilege management, privilege auditing, and change management. Change management consists of changes to the system architecture and changes to a file or document classification. Risk can also be controlled by incident management, security policies, and awareness and training.

Reference

Cengage Learning. (2012). Security+ [Photograph]. Retrieved from www.cengage.brain.com

Learning Activities (Non-Graded)

Define risk mitigation, and explain the importance of security training and awareness.

Non-graded Learning Activities are provided to aid students in their course of study. You do not have to submit them. If you have questions, contact your instructor for further guidance and information.