CIS-481: Introduction to Information Security

Module 5 – Incident Response and Contingency Planning

Exercise #9

Team: 5

Participants: Sam Martin, Charles Degboe, Nicholas Zhang, Abril Beascoechea, Ricardo Portillo

Logistics

A. Get together with other students on your assigned **Team** in person and/or virtually.

B. Discuss and complete this assignment in a collaborative manner. Don't just assign different problems to each teammate as that defeats the purpose of team-based learning and may impact your performance on assessments, especially with respect to the essay questions.

C. Choose a scribe to prepare a final document to submit via Blackboard for grading, changing the file name provided to denote the number of your assigned **Team**.

Problem 1 *(10 points)*

Refer to Figure 5-4 from the text and answer the following.

a) Explain each of the following key recovery measures: Recovery Point Objective (RPO), Recovery Time Objective (RTO), Work Recovery Time (WRT), and Maximum Tolerable Downtime (MTD). (*2 pts. each*)

Recovery Point Objective (RPO): This is the data/operations before the outage/disruption and after the last backup that is lost due to the outage and must be recovered. An organization's RPO can influence the frequency of data backups.

Recovery Time Objective (RTO): The maximum acceptable amount of time where the technology/systems can be unavailable before major negative impacts on other operations/services occur. Sometimes the WRT is added to this metric.

Work Recovery Time (WRT): This is the amount of time it takes to fully resume normal operations after technology systems are recovered. This usually includes many additional non-technical tasks.

Maximum Tolerable Downtime (MTD): This is the maximum amount of time where there is an active outage/system disruption that a system owner is willing to accept. Total recovery times must be lower than this value.

b) Is it possible to have an RTO of zero or nearly zero? What would be required to achieve near immediate recovery? (*2 pts.*)

It is possible to have an RTO of zero, it would require mechanisms that shorten the start-up time or provisions to make data available online at a failover site. This would also mean that recovery expenses would be much higher compared to systems with a longer RTO.

Problem 2 *(10 points)*

Classify each of the following occurrences as an *incident* or *disaster*. If an occurrence is a disaster, determine whether business continuity plans would be called into play. Briefly explain your reasoning for each. (*2 pts. each*)

a. A hacker breaks into the company network and deletes files from a server.

Classification: Incident

Explanation: This is an incident since it is about accessing unauthorizedly and deleting data. However, it represents an event with potentially huge impacts on data security and operations but might not exactly be a disruption of business activities in general.

b. A fire breaks out in the storeroom and sets off sprinklers on that floor. Some comp

Classification: Incident

Explanation: This is an incident since it is an event localized in space, like a fire, that damages some equipment such as computers. The impact is contained, and it's likely to be managed without invoking business continuity plans.

c. A tornado hits a local power station, and the company will be without power for three to five days.

Classification: Disaster

Explanation: This is a disaster because the natural event—the tornado—is causing huge disruption in power supply. Business continuity plans may be invoked to ensure that critical operations can carry on with alternate means of power supply.

d. Employees go on strike, and the company could be without critical workers for weeks.

Classification: Disaster

Explanation: This is a disaster since it involves an event related to labor—strike—that can have far-reaching consequences due to a shortage of critical workers. Business continuity plans may be activated to ensure that essential functions are maintained during the strike. Classification: Incident Explanation: This is an event in that it involves a labour-related event—strike, but the impact is mitigated by virtue of the fact that core operations can continue without fieldworkers. It may not be a case needing full activation of business continuity plans.

e. A disgruntled employee takes a critical server home, sneaking it out after hours.

Classification: Incident

Explanation: This is an incident involving unauthorized removal of equipment. While the server's removal is a concern, it might not lead to an immediate disaster scenario. However, data security and operational integrity need to be addressed promptly.

Problem 3 *(5 points)*

What is *digital forensics* and when is it used in a business setting?

Digital forensics is the methodical process of collecting, analyzing, and interpreting electronic data. There are multiple instances where this would be used in a business setting. The main way that is most applicable to this class, would be the use of digital forensics for security reasons. Digital forensics can be used to investigate fraud, harassment, or any other policy violations. Additionally, digital forensics may be used when analyzing non-crime events such as accidents and natural events that happen to a business.