CIS-481: Introduction to Information Security
Module 5 – Incident Response and Contingency Planning
Exercise #9

Team: 3
Participants: Ashley Aguilera Rico, Raveen Bryant, Ryan Foster, Yen Hsieh Hsu, Abby Nguyen

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*)

RPO: The point in time prior to a disruption or system outage to which mission/business process data can be recovered after an outage (given the most recent backup copy of the data)

RTO: The maximum amount of time that a system resource can remain unavailable before there is an unacceptable impact on other system resources, supported mission/business processes, and the MTD.

WRT: The amount of effort (expressed as elapsed time) necessary to make the business function operational after the technology element is recovered (as identified with RTO). Tasks include testing and validation of the system.

MTD: The total amount of time the system owner or authorizing official is willing to accept for a mission/business process outage or disruption, including all impact considerations.

b) Is it possible to have an RTO of 0? What would be required to achieve near immediate recovery? (*2 pts.*)

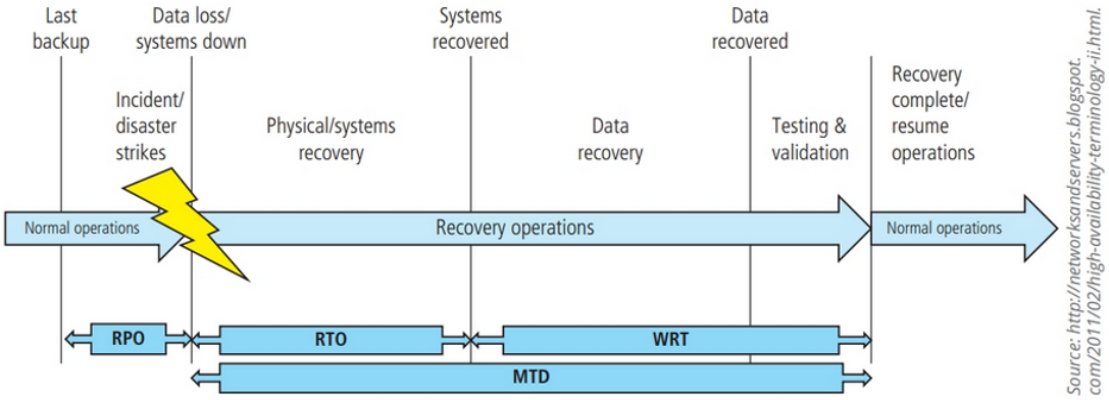

Figure 5-4 RTO, RPO, MTD, and WRT

It is possible to have an RTO of 0. To achieve near immediate recovery, a fully redundant alternative processing site will be required, which results in higher costs.

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.

   Incident: business continuity plans will be put into play where the deleted files will be restored using backups.

b. A fire breaks out in the storeroom and sets off sprinklers on that floor. Some computers are damaged, but the fire is contained.

   Incident: business continuity plan would not be needed because the fire was contained but still needed to find out the way to prevent the fire from breaking out again.

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

Disaster: business continuity plans will be needed to compensate for the days where the power is interrupted, and will have to use the plan to have alternative ways for the business to operate in that situation.

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

   Incident: business continuity plans will be needed as there are no workers for a prolonged period of time. The business will have to find ways to restore their operations and to get the workers back to work.

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

   Incident: business continuity plans will be needed as it is a critical server that the employee takes home, which may interrupt operations until the server is returned or restored. Law enforcement may have to be called in this situation as it is a crime.

Problem 3 *(5 points)*
What is *digital forensics* and when is it used in a business setting?

Digital forensics: Involves preservation, identification, extraction, documentation, and interpretation of digital media for evidentiary and root-cause analysis.

It is used in a business setting to look into incidents of a physical or information asset being attacked, as well as any policy or legal infractions committed by an employee, contractor, or outsider.