Cyber Snapshot

Exploring and Assessing Current Topics

MICHIGAN CYBER COMMAND CENTER (MC3)

March 13, 2020
CS-02-2020

Disaster Recovery Plan

OVERVIEW

A Disaster Recovery Plan (DRP) is a crucial tool used to aid in preparing for a disaster, as well as streamlining the handling of the incident by utilizing preplanned procedures. Disruptions can negatively impact an organization by temporarily interrupting operations, functions, and processes. The three types of disruptions are:

1. Non-Disaster (temporary malfunction or failure)
2. Disaster (sudden event resulting in long-term impact)
3. Catastrophe (disaster with wider and longer impact)

In terms of disaster causes, there are three types:

1. Technological Disaster (failure of a device)
2. Human-Caused Disaster (human intent or error)
3. Natural Disaster (the result of a natural hazard)

Business technology functions can be affected in the event of almost every disaster scenario. All aspects of the business network, from security to phones to computers to printers, if shutdown, can negatively impact an organization.

DRP DEVELOPMENT

Organizations should develop a DRP as part of a larger Business Continuity Plan (BCP). A BCP focuses on organizational function when a disruption occurs. It addresses and prioritizes all aspects affected by a disaster including technological components. When preparing for a BCP, a Business Impact Analysis (BIA) should be initiated. A BIA entails running an analysis on the impact of a disaster and producing a document that lists necessary business functions and resources according to criticality.

Image Source: fema.gov

A DRP should be developed based on an organization's priority functions and recovery time objectives, emphasizing the critical business functions necessary for fundamental operations. Information technology systems require multiple components to run and if one part of the "system" fails, the rest of the system may fail. Recovery strategies should be developed in the event of one or more systems failing.

The Michigan Cyber Command Center (MC3) recommends organizations form a committee to create, implement, test, and continually improve their DRP. It is imperative the organization's senior management support the DRP committee. It is also recommended the committee include a representative from senior management, each business unit, the organization's I.T., legal, security, and communications departments.

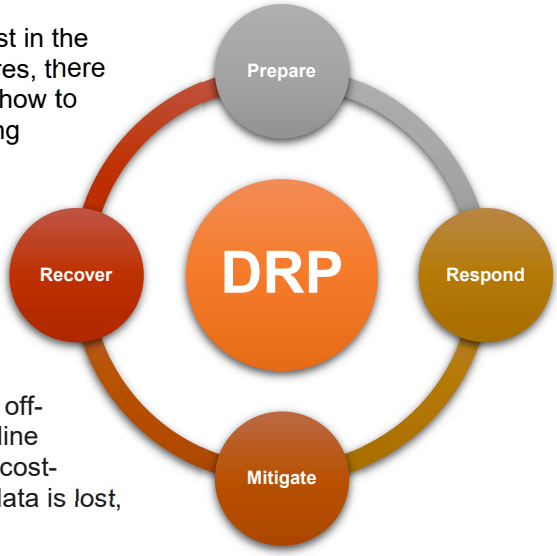
DRP COMPONENTS

Within a DRP, there should be two parts:

1. Higher-Level Recovery Strategies (identifying the order in which processes and functions are to be restored)
2. System-Level Recovery Strategies (identifying how particular systems will be restored)

A DRP should always refer to plans and procedures rather than individuals and must account for the interrelationships between processes and systems.

It is also important to document recovery plans so everyone can assist in the recovery process. Keeping in mind the possibility of technology failures, there should be printed copies of the DRP. The DRP must also document how to restore functionality to end-users. This should occur in stages, starting with the most critical infrastructure being restored first.



Similar to responding to a ransomware incident, it is crucial to backup data and test plans for restoration. Identify data on network servers, desktop computers, laptops, and wireless devices that need to be backed up. The plan should include regularly scheduled backups from all identified business computer equipment, including network and security appliance configuration files. The frequency of backups, security of the backups, and secure off-site storage should be addressed in the plan. Many vendors offer online data backup services including storage in the "cloud" which can be a cost-effective solution. Data should be backed up frequently to ensure if data is lost, it will not cripple the business.

In the event a site or facility is physically destroyed, operations may need to move off-site to a different location. An off-site location should be able to accommodate all required business technology functions. The off-site location should be geographically different as to not be affected by the same disaster which harmed the primary location. The DRP should specify how to move off-site and begin operating from the new location, as well as how to migrate back to the primary location when repairs and restoration have completed.

CYBER INCIDENT RESPONSE PLAN

Along with the DRP and BCP, the MC3 recommends organizations conduct contingency planning for a much larger range of potential hazards to include a plan for Cyber Incident Response. The MC3 recommends organizations develop an additional Cyber Incident Response plan in a similar matter to DRP, with a narrower focus to actions and procedures taken if under a cyberattack.

Any additional questions or concerns can be sent to mc3@michigan.gov or 1-877-MI-CYBER.

DRP PLANNING RESOURCES

NIST SP 800-34 Rev. 1: Contingency Planning Guide for Federal Information Systems
https://www.cisecurity.org/spotlight/cybersecurity-spotlight-disaster-recovery-plan-drp/
https://www.ready.gov/business/implementation/IT