

CPIM

CENTER FOR PUBLIC INVESTMENT MANAGEMENT



A PROGRAM BROUGHT TO YOU BY:

JOSH MANDEL

TREASURER OF OHIO

SEC 120

Disaster Recovery & Business Continuity

Disaster Recovery

- What is a disaster?
 - The unplanned interruption of services caused by a failure of components such as networks, hardware, software or data loss.
 - The reason for failure could be:
 - Physical damage, flood, fire, long term power outage, cyber-event, etc.

Disaster Recovery

- What is Business Continuity?
 - The strategy or group of plans that ensure the critical and core business functions continue without interruption despite a disaster.

Disaster Recovery

- A typical disaster Scenario (if there is one!)
 - Winter Storm with ice
 - Power is out
 - Entire system is down for 1 week while power is restored
 - No ability to provide normal service because of dependency on 1 set of equipment
 - Not a long term issue, but your services will be impacted for longer than acceptable

Disaster Recovery

- What happens to an organization without proper DR and BC?
 - The business will usually fail.
 - 75% of businesses fail within three years of a natural disaster that do not have business continuity plans. -FEMA

<http://www.usfa.fema.gov/pdf/efop/efo47103.pdf>

Disaster Recovery

- What are the critical systems that need protection?
 - Email Servers
 - Database Servers
 - Application Servers
 - File Share Servers
 - VOIP systems
 - Anything that provides critical services

Disaster Recovery

- What about backups?
 - All critical systems should be backed up at the file level
 - File level backups are defined as technology that replicates exact copies of files that are critical to business
 - Spreadsheets, Word processing documents, finance records, etc.
 - File level backups are the last resort. They provide your critical files, but they won't restore the systems

Disaster Recovery

- ◉ What about backups?
 - How are traditional backups stored?
 - Physical media is the most common. Tapes or portable drives
 - These need to be stored off site so the in the event of a disaster they are not destroyed too! The site must be physically secured
 - Encrypt anything that is physical! AES 256 minimum
 - Cloud backups!
 - Backups are transferred to another server for storage
 - They are stored off site 100% of the time
 - A reliable and quick internet connection are required for these backups, including when you have to restore

Disaster Recovery

- ◉ What about backups?
 - How often should I back up?
 - Critical files- Every day!
 - Non Critical but necessary files- Do full, complete backups every month!
 - How much data loss can you tolerate?
 - Testing?
 - YES!!!
 - This cannot be stressed enough!
 - At least 4 times a year if not more

Disaster Recovery

- DR sites!
 - An alternative location to run critical systems from
 - Hot Site
 - A location that has all critical equipment necessary for continued operation of critical systems with little or no interruption of services during a disaster.
 - The most expensive, but the least amount of interruption to services
 - Data is usually replicated across a network link multiple times a day

Disaster Recovery

- ◉ DR sites!
 - An alternative location to run critical systems from
 - Warm Site
 - A location that has the systems in a basic state. Software may need to be installed and backups restored, but the infrastructure for systems is in place.
 - Some down time is expected
 - Backups must be available
 - Medium cost

Disaster Recovery

- DR sites!
 - An alternative location to run critical systems from
 - Cold Site
 - A location that is ready for system installation. The infrastructure is not currently present, but the location is ready to have systems moved in.
 - Down time is various
 - Backups and systems must be available
 - Least Cost

Disaster Recovery

- BC Sites!
 - Locations that are designed to house the other critical services and employees that may not be appropriate for a DR site
 - Employee office space
 - Face to Face services
 - Communications equipment

Disaster Recovery

- How are DR and BC sites different?
 - DR sites are typically datacenters where there is room for infrastructure equipment only
 - BC sites are typically office spaces that employees are housed at
 - This is not always the case. Hybrid office space and infrastructure space can be more affordable!
 - Depends on your needs

Disaster Recovery

- How long should I be able to operate from DR and BC sites?
 - Indefinitely. The key is that business and services are not interrupted, or if they are, minimally

Disaster Recovery

- Other things to keep at the ready
 - Contact lists for anyone deemed important
 - Service partners, employees, vendors, support lines, etc.
 - Any documents or manuals regarding the system
 - Anything you can not live without if the system is down

Disaster Recovery

- Where should I start?
 - If you don't have the know how, invest in it. Get training yourself, or contract/hire someone who already has it.
 - Create a DR plan!
 - Create and BC plan!
 - Implement them and test them!
 - Look for partnership opportunities with other entities! Don't reinvent the wheel

Disaster Recovery

- Where should I start?
 - [Ready.gov/business](https://www.ready.gov/business)
 - [Sba.gov/content/disaster-planning](https://www.sba.gov/content/disaster-planning)
 - [Fema.gov/small-business-toolkit-tools-and-resources-plan-prepare-and-protect](https://www.fema.gov/small-business-toolkit-tools-and-resources-plan-prepare-and-protect)