DR Chapter 1 - IT DR PLan

Table of Contents

1.0 | Disaster Recovery Plan Guide

The IT Disaster Recovery Plan (DRP) is based on the following facts:

- That a contract is in place with the alternate data center provider which adequately covers the infrastructure and services defined in the contract.
- That the IT DRP addresses the recovery of the IT capability of the business. It does not provide for the recovery of other departments or areas of the business possibly affected by the same event.
- That the level of the plan detail is based on the premise that sufficient and knowledgeable IT staff will execute the recovery actions.
- That the IT DRP is designed to recover from a worst-case event; that computer operations from the corporate data center has been suspended, interrupted, or destroyed.
- That the worst-case scenario extends from 8 hours to an undetermined time such as days, weeks, or months.
- That the mission critical applications and data are replicated continually to the alternate data center.
- That if a cyber-attack occurred and data was corrupted at the corporate data center, that data is replicated to the alternate data center. If a cyber-attack corrupted data in both the corporate and alternate data center, VTL (virtual tape library) data would be used to restore systems and data. RTO (Recovery Time Objective) and RPO (Recovery Point Objective) will be adversely affected.
- That similar and like equipment are already in place at the alternate data center allowing for the immediate recovery once a disaster has been declared.
- While operating at the alternate data center, the quality of service provided to users and computer equipment will be degradated due to limited available resources.

1.1 | IT Disaster Recovery Plan Overview

Wells Enterprises, Inc.'s Information Technology's Disaster Recovery Plan has been created to deal with outages resulting from events such as:

- System, hardware, network, data, and software failures
- Natural disasters such as tornadoes, floods, and severe storms
- Sabotage or major security breaches such as cyber-attacks that require operational shutdown
- Man-made disasters such as power outages, hazardous material spills, and terrorist attacks
- Recovering from an extended corporate data center outage event

Each section of the Disaster Recovery Plan has been designed to provide as much information and preparation as is required to recover from a loss of service.

The IT Disaster Recovery Plan is designed to identify and to mitigate risks associated with Wells Enterprises, Inc.'s computer and telecommunication resources. The process ensures efficient and effective resumption of vital business functions in the event of a major interruption.

Due to the growing dependence on information technologies to support essential business processes, business growth and change, the following methodology is used in the development of the IT Disaster Recovery Plan:

- Risk assessment evaluating the potential risks associated with Wells Enterprises Inc. that could cause an IT Disaster Recovery Plan declaration
- Business Impact Analysis (BIA) Summary systematic process to determine and evaluate the potential effects of an interruption to critical business operations as a result of an event that disrupts business operations
- Business Continuity the capability of a business to continue delivery of products or services at acceptable predefined levels following a disruptive event
- Recovery Plan Testing and Exercising perform periodic disaster recovery tests to ensure that Wells Enterprises Inc.'s IT Disaster Recovery Plan produces the required results
- Awareness and Training Updating processes and maintaining an up-to-plan IT DRP is crucial to the 'plan'. Training new employees is a key component to the plan

1.2 | Risk Assessment

The topics listed below identify potential risks to Wells' Enterprises, Inc. Information Technology arena. Risks are categorized by probability and impact. Typically, low probability risks have the highest impact. For example, a flood has a low probability of occurring but has a high impact should one happen.

Through risk assessments Wells has addressed vulnerabilities and created mitigation strategies that greatly reduce the impacts of those hazards. Depending on the impact of the threat, IT operations can be disrupted from a short time to an extended outage that requires operating from an alternate data center. A comprehensive plan utilizing a remote data center is addressed in Chapter 4.

Risks

Natural Threats	Probability	Impact
Tornado	Medium	High
Flooding	Low	High
Snow/Ice Storms	High	Low
Lightning/Thunderstorms	High	Low
Earthquake	Low	High

Facility Threats	Probability	Impact
Fire	Medium	High
Power	Low	High
Water Damage	Medium	High
Explosion	Medium	High
Electrical	Low	High

Social Threats	Probability	Impact
Terrorism	Low	High
Bombing	Low	High
Vandalism	Low	High

Personnel Threats	Probability	Impact
Pandemic Event	Low	High
Loss of Key People	Low	High

IT Threats	Probability	Impact
Data Center Loss	Low	High
Data Loss	Medium	High
Network Connectivity	Medium	High
Cyber Attack	Medium	High
Equipment Loss	Low	Medium

1.3 | Business Impact Analysis (BIA)

The Business Impact Analysis is the foundation of any Business Continuity Plan. The purpose of the BIA is to pinpoint the processes crucial to the continued operations and delivery of technologies to the organization.

The Business Impact Analysis is based on a worse-case, total outage of Wells' corporate data center and operating from the Security Institute on WITCC's campus.

Recovery Time Objective (RTO) and Recovery Point Objective (RPO) are two of the most important terms in the Business Impact Analysis.

- RTO - the targeted duration of time in which systems must be restored after a disaster or outage event.
- RTO designates the amount of "real time" that can pass before the disruption begins to seriously impede the flow of normal business operations.
- RPO – the amount of time between the last 'data save' and the amount of data that could be lost during a disaster event.
- RPO designates the variable "amount of data" that will be lost or will have to be re-entered during an outage event.

The following tiers and timeframes list the critical components and applications that need to be available before proceeding to the next tier level.

0 - 4 hours

- Pure storage - disk storage devices used to house company data
- Network - configuring hardware and settings that allow computer equipment to interact together
- Start all physical and virtual servers - but not the applications
- Oracle servers - single sign-on for Oracle, Apex, all that use Oracle SSO (single sign-on)
- Start IT tool servers - allows engineers to administer servers

4 - 8 hours

- Oracle applications – ERP system that manages and integrates production, inventory, and financial functions
- Oracle transportation management – system for managing interactions with trucking companies
- ASRS / EMS – south ice cream freezer automated inventory management
- EDI – exchange business critical data electronically in 'real-time' frequency
- Exchange email system – electronic mail system
- Ring Central - telephony system including messaging, video conferencing

- Bunnynet – Microsoft Sharepoint for Wells' employees
- Process control servers – plant automation
- Identity and access management – single sign-on

8 - 12 hours

- Oracle line side reconciliation – system for production lines around mixes and batching
- Yard management – system for tracking trailers and shag drivers
- Web sites – internal/external
- Door Security

12 - 24 hours

- Kronos – hourly employee time reporting and employee scheduling
- HCM & HR – payroll, benefits, training and other employee related processing and information
- Prescient – production scheduling, inventory planning and replenishment planning
- WHIMS / Plant floor data collection
- IVR – phone call in for tankers
- Consumer web sites
- Enterprise asset management scheduling

7 days

- Service desk – system to track support tickets
- Hyperion – analytical database application used for financial reporting
- Red Hat network – Linux operating system administration
- Veeam data retention – enterprise data backup system

Alternate Data Center

Wells Enterprises, Inc. has contracted with Long Lines for dedicated data center space to house its IT recovery capabilities.

The alternate data center is located on Western Iowa Tech Community College's campus:

```
Woodbury County E-911 Center
4647 Stone Boulevard
Building J
Sioux City, Iowa 51106
```

```
Long Lines - NOC (Business Hours) - 712-271-4662
Main Operation at Long Lines - 712-271-4000
Long Lines - On-Call (After Business Hours) - 712-271-4662
```

Wells Enterprises, Inc. has contracted with Woodbury County Emergency Services for classroom space if Wells needs to declare a disaster and activate the business from the alternate data center.

```
Woodbury County Emergency Management Coordinator - Rebecca Socknat (Primary)
Office:  712-222-4421   Email: rsocknat@woodburycountyiowa.gov
Woodbury County Emergency Management
601 Douglas Room 103
Sioux City, Iowa 51101
```

```
WITCC Contact - Tony Jasman (Secondary)
The Security Institute
4647 Stone Avenue, Lower Level
Sioux City, Iowa 51106
```

1.5 | Business Continuity

A business continuity program should not only address recovery - it should also address prevention.

Wells Enterprises, Inc. has enterprise level environments in place that will prevent events that can potentially cause outages and prevent data from being lost.

- Continual data replication to DR site
    - Mission critical data replicated to the DR site is as current as possible when an event happens that breaks the link between the corporate data center and the DR data center
    - Wells will be able to restore mission critical data almost to the point-in-time that the link failed
- Veeam backups
    - Mission critical data is replicated to the DR site based upon Service Level Agreement (SLA)
    - Veeam backups are used if the replicated data at the DR site cannot be used
- Pure snapshots
    - Create these snapshots before altering the VM configuration, data, etc. to preserve the image if the need to revert back should occur
    - Eliminates the backup window, decreases the amount of downtime associated with backup to zero
    - Recover applications in seconds
    - Keep the business online during migration, backup and other data center activitities
- Virtual machine snapshots
    - Snapshots can be created when the VM is active or powered off
    - The data includes all of the files that comprise the virtual machine (disks, memory, network interface cards, etc.)
    - Snapshots can revert a VM back to the point-in-time when a snapshot was created, saving the machine’s configuration if an upgrade or enhancement corrupted the machine
- High availability clusters
    - Are a group of computers that support server applications that can be utilized with minimal down-time
    - Use high-availability software which provides redundancies in clusters that provide continued service when system components fail
    - Build redundancy into a cluster eliminating single points of failure, including multiple network connections and data storage connected via storage area networks
- Enterprise class Cisco UCS* and Dell* hardware provides
    - High-availability
    - Redundancy

    - Clustering
    - Ability to create snapshots
- SAN environment
    - Redundant, high-performance network allowing each virtual machine to access share storage
    - Virtual SANs are scalable and provide ease of management
- Patching
    - Red Hat VM updates, Oracle patching, and Windows updates are key to keeping the hardware / software up-to-date
    - Helps with security measures that potentially eliminate or greatly reduce the effects of cyber-attacks
    - Keeping the hardware / software at the latest versions helps in problem determination when calling support services

1.6 | IT Security

IT Security provides a layer of protection from cyber-attacks and other security issues that can be very damaging and/or potentially destroy a business. Cyber-attacks have become an organization's largest threat according to the Business Continuity Institute 2016. Provisions are being made to address each of the security risks listed below. Preventing Cyber-attacks is a never ending endeavor and Wells must stay well ahead of those who may potentially attack our business.

- Loss or theft
  - Corporate asset reported lost or stolen including laptops, mobile devices, storage media, and compromised data
  - Attempted or successful destruction, corruption, or discloser of sensitive corporate information or Intellectual Property (IP)
- Compromised asset
  - Compromised host (root acccount, trojan, rootkit), network device, application, user account. This includes malware-infected hosts where an attacker is actively controlling the host
- Internal hacking
  - Reconnaissance or suspicious activity originating from inside the corporate network excluding malware
- External hacking
  - Reconnaissance or suspicious activity originating from outside the corporate network excluding malware
- Malware
  - A virus, worm, or botnet affecting multiple systems. This does not include compromised hosts that are being actively controller by an attacker via a backdoor or Trojan
- Denial of Service (DoS)
  - DoS, DDOS (Distributed), DRDoS (Distribution Reflection)
- Website
  - Website redirection, website defacement, or compromised URLs
- Social media
  - Compromised social media acccount or inappropriate posted comment
- Social engineering
  - Unsolicited email targeting in order to obtain information considered personal, confidential or sensitive, also including malicious links or attachments. This pertains to phone calls or physical contact attempted to obtain unauthorized information or access
- Policy violation
  - Intentional or unintentional behavior that falls outside the corporate security policies or standards, unapproved policies or standards, unapproved policy exceptions, or actions that

do not align with corporate code of conduct

- Unlawful activity
    - Computer-related incidents of a criminal nature, likely involving law enforcement, federal investigation, or loss prevention. This includes theft, fraud, human safety, or child pornography

1.7 | IT Disaster Recovery Summary

Disasters are a reality for which Wells Enterprises, Inc. needs to be well prepared. We plan for the worst and hope for the best. Disaster Recovery starts with sound planning and design. Replicating data to an alternate data center is an essential requirement for our Disaster Recovery plan. Being aware of disaster scenarios, preparing and testing to prevent them is critically important in protecting our data. To have an effective Disaster Recovery plan, we must be able to recover the business. The recovery process must function properly within a given timeframe defined by our Recovery Time Objective and Recovery Point Objective.

The need for thorough documentation exists within each Disaster Recovery plan. Having a step-by-step procedural document during an actual disaster event far outweighs trying to remember what to do and when to do it. A dynamic, up-to-date document defining the infrastucture, components, servers and virtual machines inventory is included in Wells' Disaster Recovery plan. The more dynamic information we can produce, the more robust our DR plan becomes.