

Business Continuity and Disaster Recovery Planning

MFA Panel

May 11, 2004

NYC

Agenda

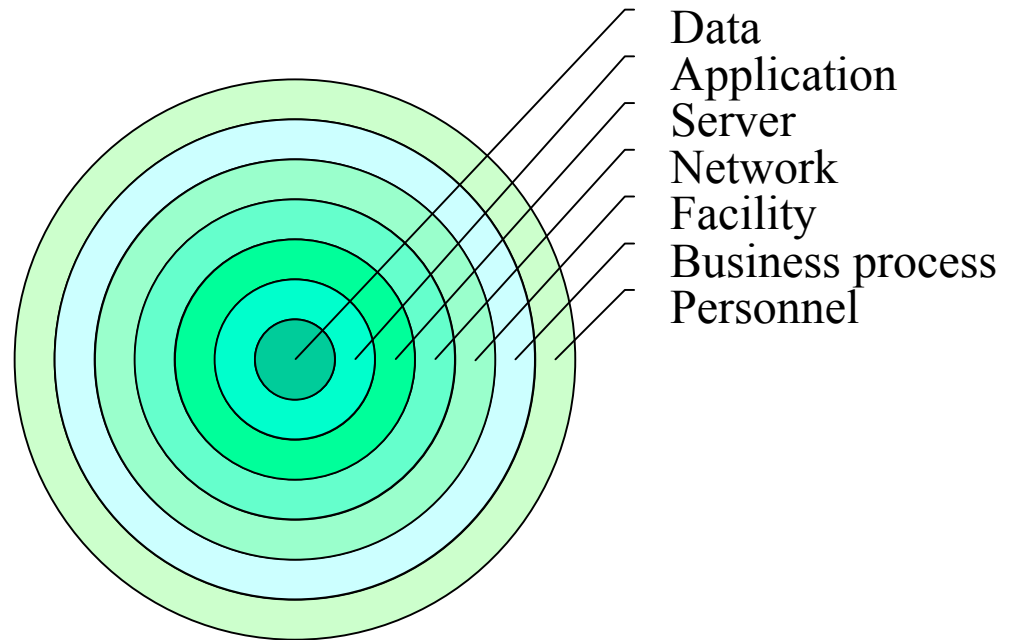
- Compelling events
- Recovery metrics and cost balancing
- Contingency plan evolution
- Disaster Recovery Planning
- Data Center

Compelling Events

- Regulation
- Growing dependency chains
- Wear and tear
- Sabotage and terrorism

Growing Dependency Chain

- Practice
- Provider
- Electronic exchange
- Patient
- Accounting
- Bank
- Technology



Lessons of September 11

- Ignored the potential for wide-spread disaster including disruption of multiple sites
- Business concentrations intensified the impact of disruptions
 - Geographic
 - Critical market functions, e.g., clearing and settlement of funds, securities, and contracts
 - Telecommunications vulnerabilities
- Interdependence among financial-system participants
 - Some customers were affected by actions of institutions with which they did not even do business, e.g., funds could not be delivered because of operational problems of other institutions

Agenda

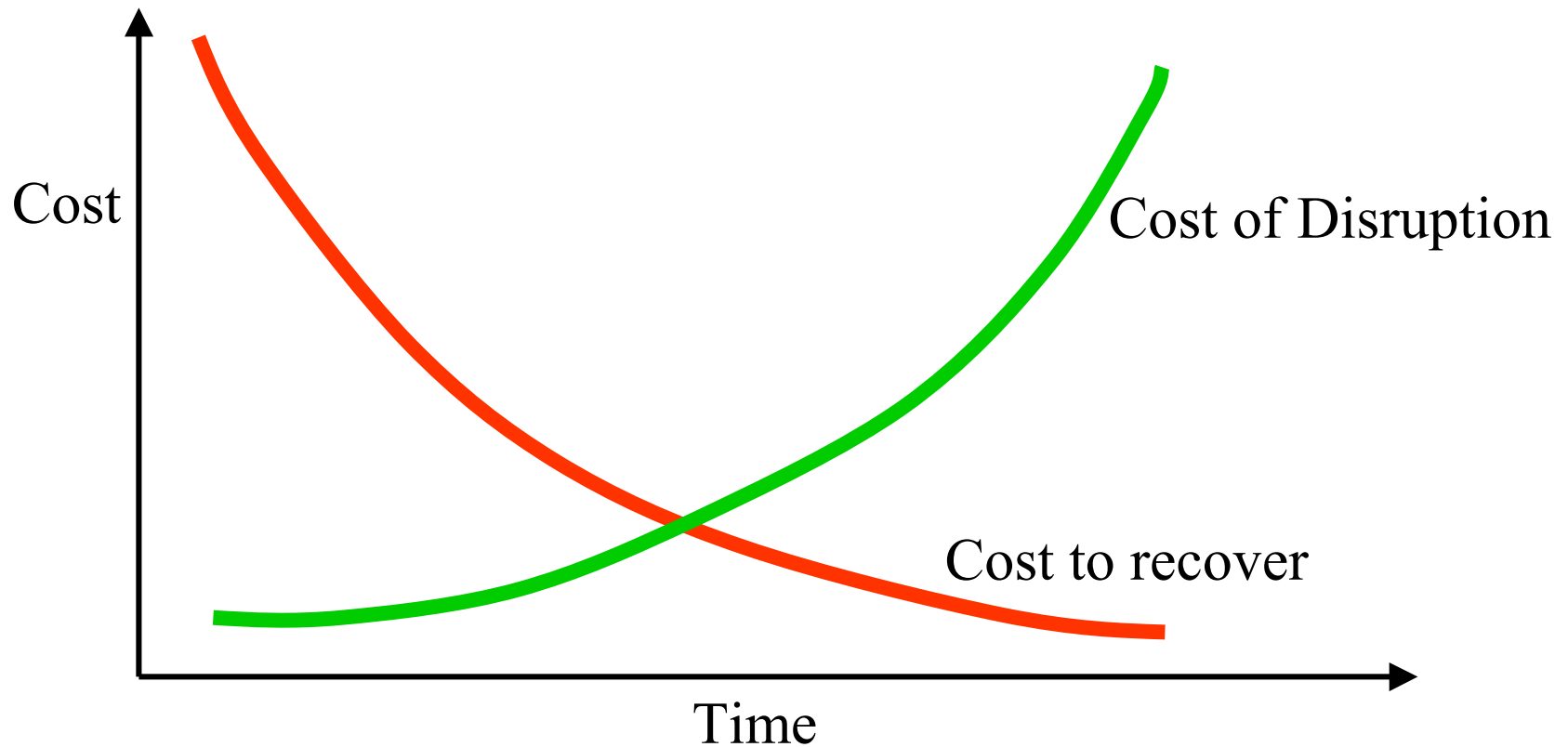
- Compelling events
- **Recovery metrics and cost balancing**
- Contingency plan evolution
- Disaster Recovery Planning
- Data Center

Steps for Financial Institutions

- Tactical steps
 - Enhance security, update communications plans, improve real-time data backup
- Strategic steps
 - Migrate from traditional active-backup site pair to ‘split-operations’ model
 - Diversify telecommunications methods and vendors
 - Respond to client expectation for consistent, coordinated, and transparent business continuity planning

Recovery Cost Balancing

How long can you afford the system to be down?



Disaster Recovery Metrics

- MTTR – Mean time to recover
- ADL – Allowable data loss
- Retention – How long backups are stored

DR Levels

	Static Data	Dynamic Data	MMTR	ADL	Retention
Entry	Email Documents	None	1 Day	1 Day	Days or Weeks
Mid	Application Servers	Databases	Minutes or Hours	Minutes or Hours	Months or Years
Enterprise	Any	Any	zero	zero	Unlimited (WORM)

Agenda

- Compelling events
- Recovery metrics and cost balancing
- **Contingency plan evolution**
- Disaster Recovery Planning
- Data Center

Contingency Plan Evolution

Primary
Business
Operations

Backup
Business
Operations

Primary
Data Center

Backup
Data Center

- Only the primary site is active
- Requires identical copies of technology and up-to-date data
- Relies on relocating staff

Split
Business
Operations

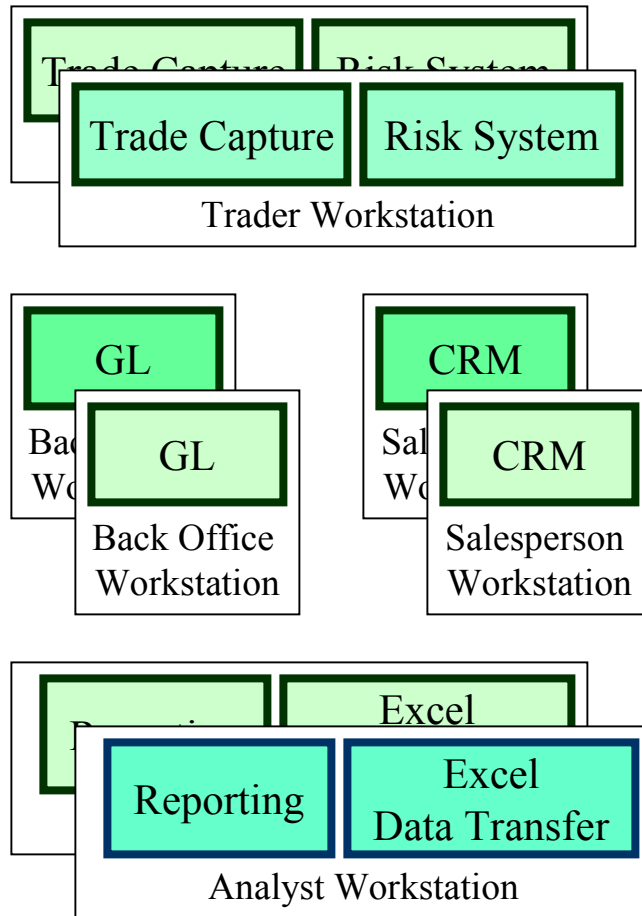
Split
Business
Operations

Split
Data Center

Split
Data Center

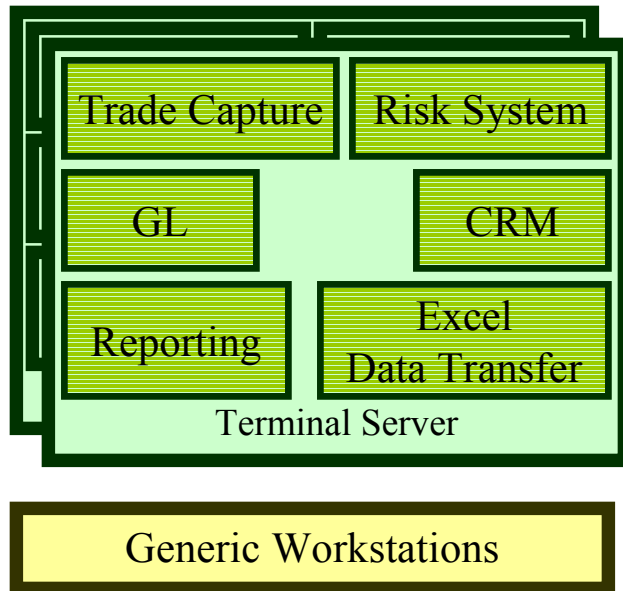
- All sites are active performing some of the functions
- More expensive

Distributed Data Centers



	Distributed
Data Center	Partial
Functionality	Partial
Points of Failure	Multiple
Dependencies	Multiple
Work Location	Location dependent
Redundancy	Complex Expensive

Centralized Data Center



	Distributed	Centralized
Data Center Functionality	Partial	Complete
Points of Failure	Multiple	Single
Dependencies	Multiple	Few
Work Location	Location dependent	Generic
Redundancy	Complex Expensive	Simple Inexpensive

Agenda

- Compelling events
- Recovery metrics and cost balancing
- Contingency plan evolution
- **Disaster Recovery Planning**
- Data Center

IT Contingency Planning

- Develop contingency planning policy
- Conduct business impact/downtime tolerance analysis
- Identify preventive controls
- Develop recovery strategies
- Test and train
- Maintain

Types of Contingency Plans

Plan	Purpose	Scope
Business Continuity	Sustaining business operations while recovering from disruption	Addresses business processes; IT addressed only on its support for business
Business Process Recovery	Procedures for recovering operations immediately following a disaster	As above
Continuity of Operations	Procedures and capabilities to sustain essential strategic functions at an alternate site for up to 30 days	The most mission-critical subset of organization; not IT focused
Continuity of Support/IT Contingency	Procedures and capabilities for recovering a major application or general support system	Addresses IT systems disruptions, not business process focused
Crisis Communications	Procedures for disseminating status reports	Communications with personnel; not IT
Cyber Incident Response	Procedures to detect, respond to, and limit consequences of malicious cyber incident	Focused on information security and responses to incidents affecting systems
Disaster Recovery	Procedures to facilitate recovery of capabilities at an alternate site	IT-focused, limited to major disruptions with long-term effects
Occupant Emergency	Procedures to minimize loss of life or injury and protect property damage in response to physical threat	Focuses on personnel and property, not business or IT

Disaster Recovery & Security Plan

- Security assessment
 - External Penetration Testing,
 - Internal Security Assessment,
 - Operational Analysis
- Business impact analysis
 - Analyze the risk of disaster in specific areas of the business. Include natural disasters, the risk of sabotage, physical violence, and cyber crime.
 - Define the impact of potential disasters on your organization.
- Documentation
 - Detailed network diagrams, including operating systems, equipment functionality, applications/users supported, and vendors utilized.
 - Enumerate applications, including information about installation, licensing, security, and passwords.
 - Identify services, including cable, DSL, satellite, phones, outsourcing, etc.
- Detailed planning

Detailed Disaster Recovery Plan

1. Prioritization list to order pieces of the network (hardware) and applications and services must be restored first in the event of a disaster.
2. Define hot/cold site requirements.
3. Key contact and organizational chart. Include vendors, consultants, media, insurance, and other stakeholders.
4. Organize recovery teams. Divide the recovery process into various objectives and create teams who will be responsible for meeting these objectives.

Offsite Storage Facility Selection

- **Geography** – distance and the likelihood to be affected by the same disaster
- **Accessibility** –operating hours and the time to retrieve the data
- **Security** – capabilities and employee confidentiality
- **Environment** – structural and environmental conditions (humidity, fire-prevention, temperature, power management)
- **Cost** – cost of shipping, operational fees, disaster response services

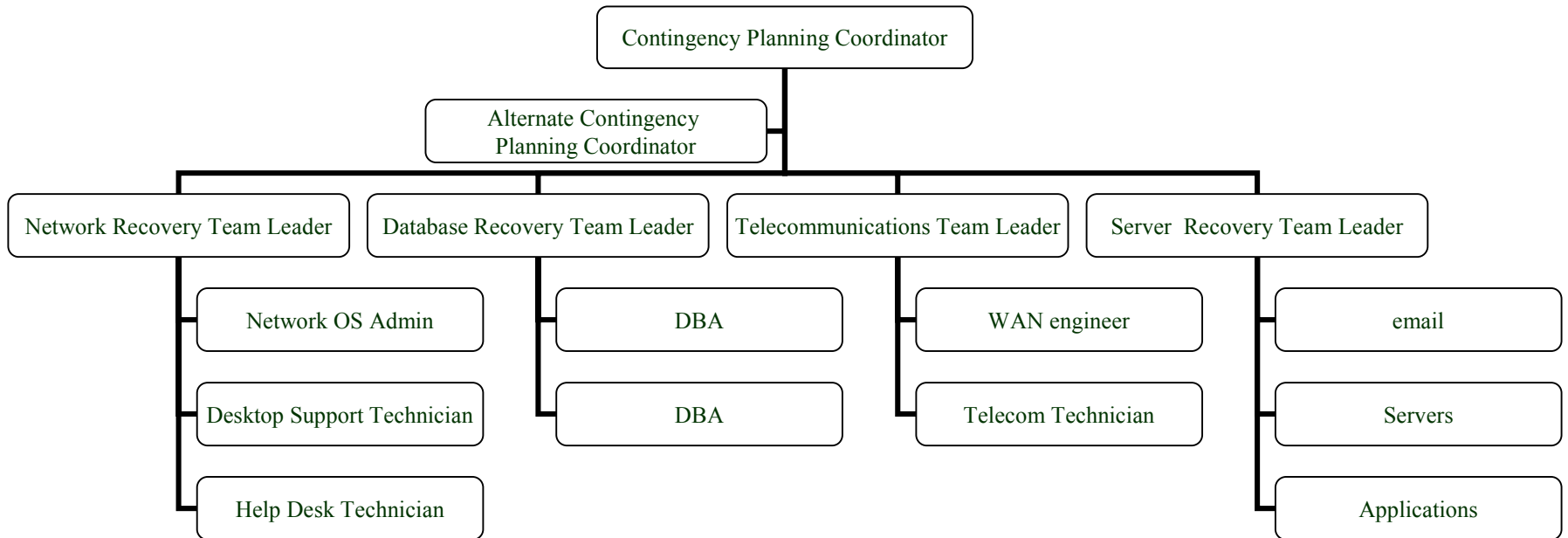
Alternate Site

- Cold
 - Adequate space and infrastructure
 - No IT or office automation equipment
- Warm
 - Often used for another function, which is displaced temporarily to accommodate the disrupted system
- Hot
 - Configured with all system hardware, infrastructure, and support personnel
- Mirrored
 - Fully redundant infrastructure, systems, and data

Selecting Right Team

- Leaders and knowledge
 - Caveat: too many leaders can spoil the best a plan.
- Calming yet responsive people
- Discipline: will they stick to the plan and know not to interfere?
- Decision makers
 - Can they be decisive given the facts not the fiction?
 - Can they be relied upon to speak up when adjustments are needed?
- Team players
 - Will they go into crisis mode to get the job done?
- Strong administrators
 - Who will support you without getting under your feet or second-guessing and who will record every detail so it can be counted as legal evidence?

Sample Call Tree



External Penetration Testing

- Discovery = gathering relevant information
 - Sources include whois databases, search engines, and other publicly available sites.
 - Details collected include domain names, host names, and network boundaries, i.e., firewalls, routers, and intrusion detection systems.
- Enumeration = extract information about each component.
 - Use netcat, banners, and anonymous connections.
- Vulnerability mapping = map system attributes against vulnerabilities
- Exploitation = perform a controlled attack to verify results by exploiting the vulnerabilities identified in the mapping phase

Scheduled Vulnerability Scans

- Regularly scheduled network vulnerability scans can detect these new vulnerabilities so you can take corrective action before an attack occurs.
- Automated scans on a predetermined schedule.
 - Commercial and Open Source scanning tools
- Reporting
 - Pro-active alerts when a vulnerability is detected –
 - Next business day delivery of an alert report.
 - Monthly or Quarterly reports
 - date and time of tests,
 - vulnerabilities detected,
 - configuration changes,
 - and corrective actions required

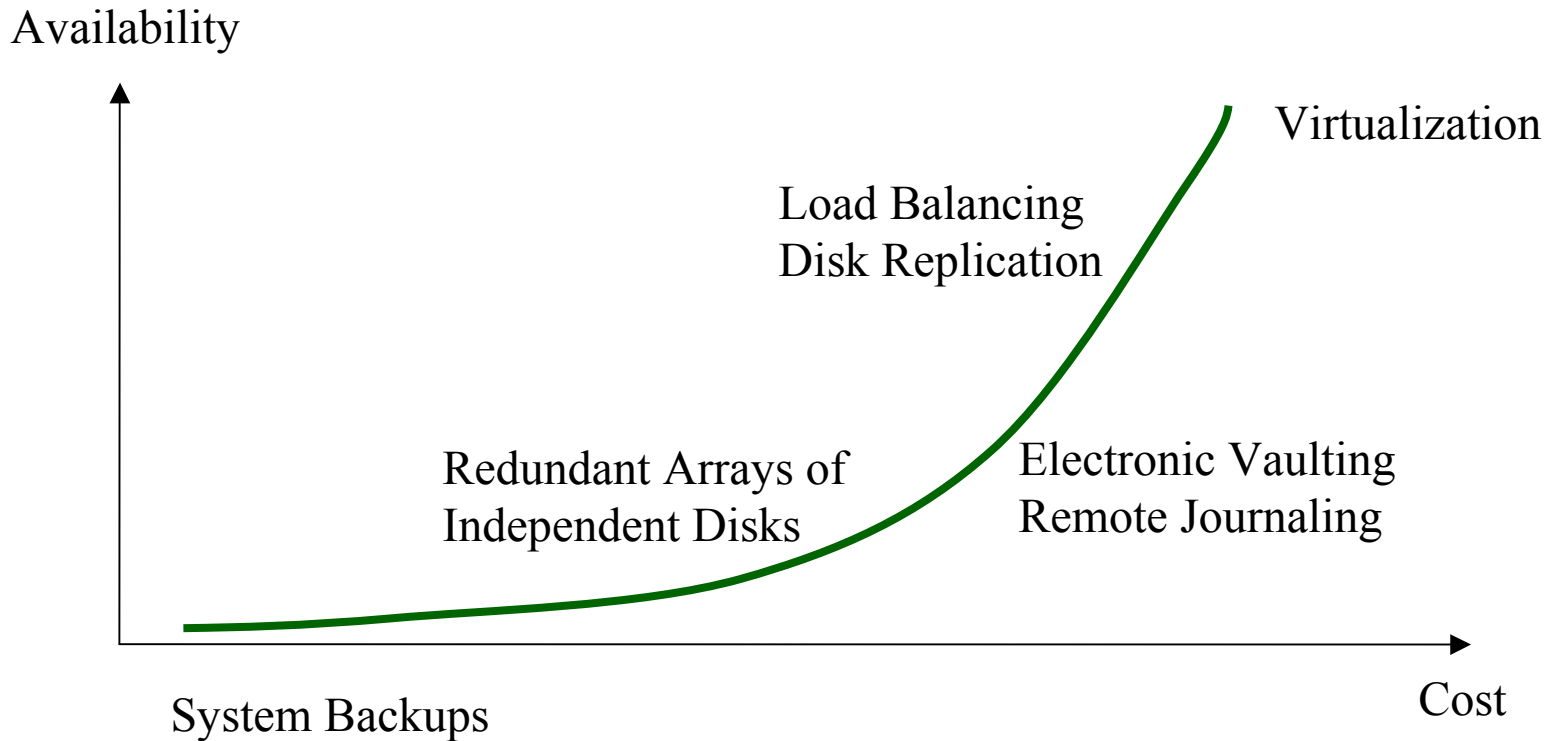
Internal Security Assessment

- Determine vulnerabilities that may result from
 - poor configuration,
 - gaps in security,
 - out-dated service patches
- Identify performance issues due to poor configuration

Disaster Recovery Plan Operational Analysis

- Policies, practices, procedures
- Physical security
- Network practices
- Critical services
- Help desk
- Passwords/usernames and account policies
- Internet use
- e-mail and anti-virus deployment
- Connectivity issues
- Backup data storage
- File storage
- Equipment/system documentation review

Server Contingency Solutions

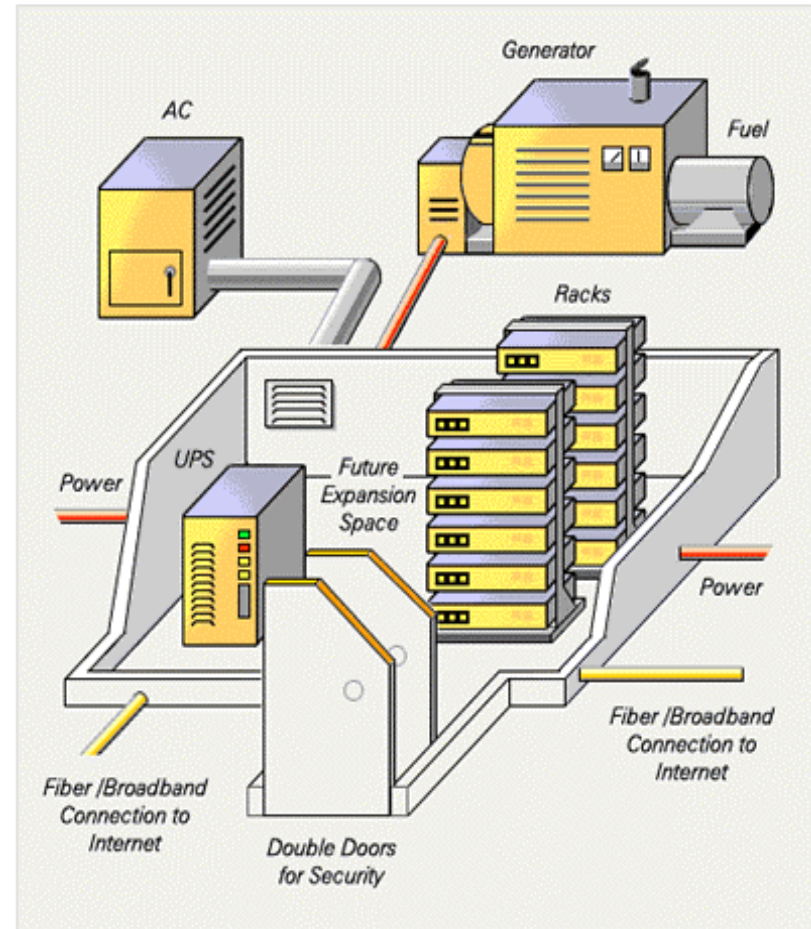


Agenda

- Compelling events
- Recovery metrics and cost balancing
- Contingency plan evolution
- Disaster Recovery Planning
- Data Center

Data Center

- The data center facility ~ 35,000 Square Feet
- Disaster recovery is facilitated by two redundant secondary sites
- Comprehensive backups are performed nightly to both sites
- The data center is built upon multiple dedicated OC192 back bone
- Redundant power and network architecture
- Sophisticated and multi-faceted security systems
- High-tech fire suppression
- Highly trained staff is available on site 24x7



Amenities and Network Architecture

Amenities

- Reinforced concrete masonry with brick
- State of the art 19" & 23" Wright line cabinets
- Each cabinet is equipped with 2-110v, 20-amp redundant circuits along with 2 power strips containing 8 receptacles each
- 10/100 FE line of GigE line as needed

Network Architecture

- Multiple OC 192's, 48's going to various cities
- Redundant paths into the building allow for fail over
- MFN owns 1 AS number thus international transit is not seen as a network hop

Fire Suppression and Power Supply

Fire Suppression

- VESDA system detects and dry action piping
- Pre action water system (no water in pipes)
- Zoned sprinkler heads work independently
- Air sampler system for smoke monitoring; upon smoke detection, water will begin flowing through the pipes.
- Once the heat melts the specific sprinkler tip (165 degrees) the water will be dispersed

Power Supply

- Multiple Diesel Generators
- Inertial Flywheel during change to backup power



Security Systems

- 24/7 Security on site
- CCTV cameras used to monitor internal and external activities
- Data Center activity is stored on tape
- All persons entering must show government issued picture ID. Picture and name cross checked with access list
- On-site key control system to manage access to customer cabinets

