Technical Contingency Planning Considerations

Contingency Planning Guide for Federal Information Systems

Алиса Погодаева,
Adrian Cinal,
Oliwer Sobolewski,
Gabriel Wechta

April 12, 2022

Table of Contents

Introduction

Considered platform types

1. Client/server systems
2. Telecommunications systems
3. Mainframe systems

Perspective I - technical requirements when planning a system recovery strategy.
Perspective II - technology-based solutions for each type of system.

Common considerations

- Use of information gathered from the **BIA** process.
- Development of primary and alternate sites with **configured power management** systems and **environmental controls**.
- High availability (**99.9999%**) processes access to **alternate system resources**.

Maintenance of Data Security, Integrity, and Backup

Goal: keeping data **safe**, **accurate** on the system's primary storage devices and **eliminate loss of data from single drive failures**.

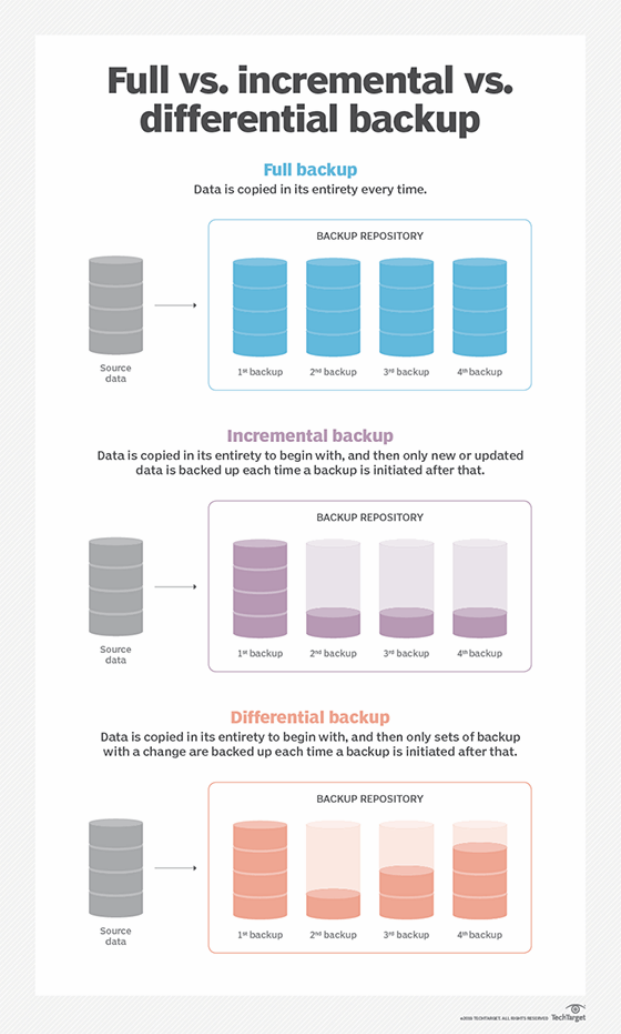
Data Security

Encryption - both onsite and offsite.
Keys - stored separately, but accessible to, the encrypted backup data.

Backups

Keeping backups allows for a ready access to backups during a contingency event.
Full - all files, lengthy time, unnecessary storage.
Differential - since the last **full** backup, smaller size, quicker.
Incremental - since the last **full or incremental** backup, smallest, quickest, require many backups to restore.

Backup types



3 types of backups.

Backup types

A **combination** of backup operations can be used depending on system configuration and recovery requirements.

How to design backup policy?

- **Where** and how will media be **stored**?
- How **quickly** are the backups to be **retrieved** in the event of an emergency?
- **How long** will the backup media be retained?
- What is the appropriate **backup medium** for the types of backups to be performed?

Backup solution factors:

- **Media lifetime expectations** (HDDs, DVDs, mag. tapes (6TB sic!))
- **Storage volume** (Software and **drivers** also)
- **Backup Software** (Timeshift)

Alternate Storage and Processing Facilities

Cold site

- **Basic infrastructure** and environmental controls available.
- **No** equipment or **telecommunications** established.
- Low cost, long recovery time.

Warm site

- **Basic infrastructure** and **sufficient telecommunications**.
- Equipment only to operate **critical** mission/business processes.
- Medium cost, shorter recovery time.

Hot site

- **Fully operational** equipment, able to quickly **take over** operations.
- The most current version of software, storage for the production data.
- High cost, full support, require operational support.

High Availability (HA)

- Uptime of 99.999 percent or higher - few minutes per year of downtime.
- Duplicate hardware.
- Building redundancy and resiliency into the architecture.

Safe alarm systems in modern cars.

Client/Server Systems

Server Contingency Considerations

- **Store backups offsite** or at an alternate site.
- **Standardize hardware and software** - System recovery is faster if hardware and software are standardized throughout.
- **Coordinate** contingency solutions with **cyber incident response procedures**.

Client Contingency Considerations

- **Minimize** the amount of data **stored on a client computer** - Critical user data should be stored on central servers.
- Provide **guidance on saving data** on client computers.
- **Automate** backup.

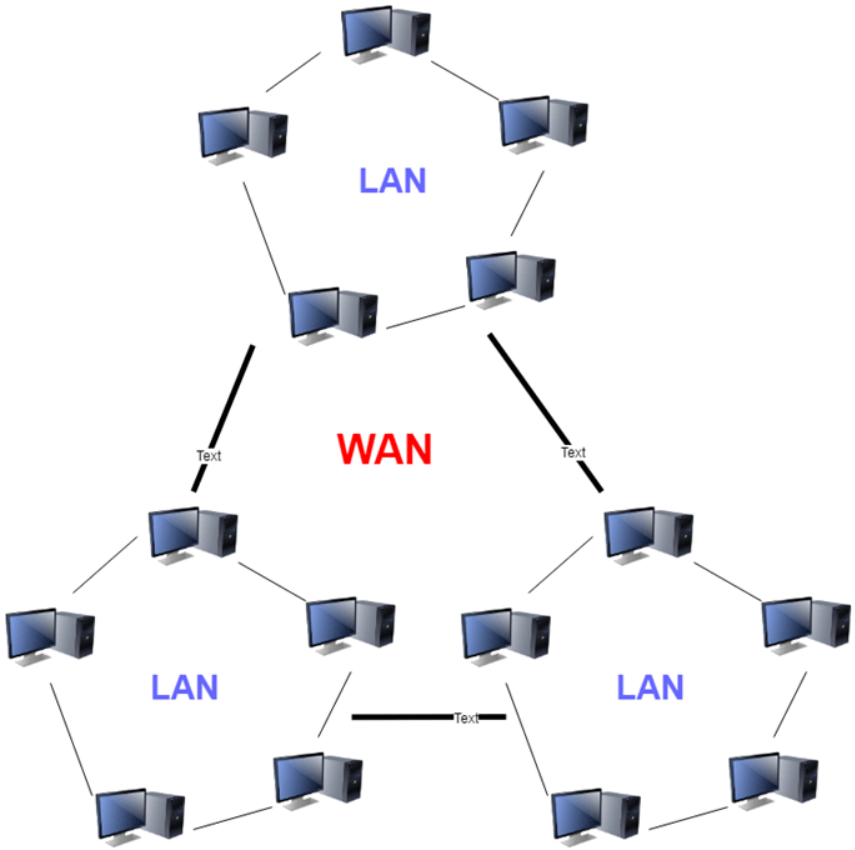
Solutions

- First of all: **Encryption**
- Second of all: **Backups**
  - DVD
  - Network Storage
  - External Hard Drives
  - Internet Backup

Example: all data resides in one location and is replicated to the local sites. This means that if the headquarters server were to fail, data could still be accessed at the local sites over the WAN.

Telecommunications Systems

LAN - group of computer and peripheral devices that are connected in a limited area such as school, laboratory, home, or office building.
WAN - computer network that is spread across a large geographical area.



Considerations

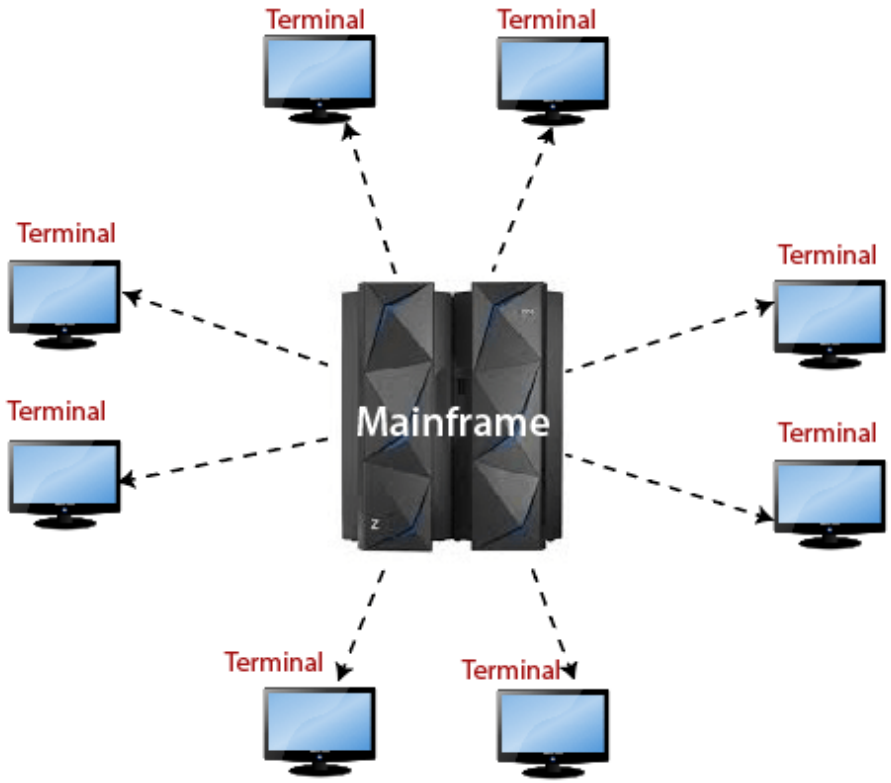
- Store **backup media offsite**, **far from each other** to reduce likelihood that both sites will be affected by the same event, e.g. earthquake.
- Document system configurations and vendors.

Solutions

- for LAN:
  - Remote access: VPNs, RDPs, VNCs.
  - Redundant cables, **cable between floors** so that local hosts could be reconnected.
  - **Backup Wi-Fi LANs**, no need for cabling.
- for WAN:
  - Redundant: **communications links**, **NSP** (Network Service Provider), **network-connecting devices**, **ISP** (Internet Service Provider).
  - Monitoring software for **disruption detection**, quick response.

Mainframe Systems

Mainframe - multi user computer system. Mainframe systems store all data in a central location rather than dispersing data among multiple machines.



Considerations

- Physical diagrams should be up to date and **displayed** in the office.
- System configuration and vendor information documentation also NSP. **contact details** should be **displayed** in the office.
- **Threats to the cabling system**: cable cuts, electromagnetic and radio frequency interference, fire, water, and other hazards damage.

Solutions

- A **gas** or **diesel** generator to survive power outage.
- **Commercial systems** for keeping backups.
- Because of centralization, good contingency strategy is to have alternate **warm** or **hot site**.

Thank you for attention

References

https://www.spotern.com/en/spot/tv/mr-robot/3115/the-case-in-a-cd-rack-of-elliot-in-mr-robot.
[Online; accessed 9-April-2022].

https://www.techtarget.com/searchdatabackup/tip/.
[Online; accessed 8-April-2022].

https://www.acronis.com/en-us/articles/incremental-differential-backups/.
[Online; accessed 9-April-2022].

M. S. et al.
Contingency planning guide for federal information systems.
NIST Special Publication 800-34 Rev. 1, 2010.