Disaster Recovery Planning

Marcus Bendtsen

Institutionen för Datavetenskap (IDA)

Avdelningen för Databas- och Informationsteknik (ADIT)

LiU EXPANDING REALITY

Disaster Recovery Planning

- When a disaster strikes and the business continuity plan fails to prevent interruption of business activities, the ***disaster recovery plan*** (DRP) kicks in.

- There are clear distinctions between BCP and DRP, however they are also similar in some regards.
  - Most likely the team doing BCP will also be doing DRP.
  - This is sometimes known as ***business continuity management***, and includes both BCP and DRP.

Disaster Recovery Planning

- What is a disaster?
  - Technically anything that stops, prevents or interrupts an organisation's ability to perform its work.
  - The moment that IT becomes unable to support mission-critical processes is the moment when DRP kicks in.

- DRP should ideally kick in and run on autopilot, it is important to reduce decision making in a state of emergency.

- Personnel should be well trained in their duties and responsibilities.

Disaster Recovery Planning

Natural disasters

- Earthquakes
  - Damage to buildings and infrastructure.
  - Reduces accessibility, transport can be shut down.
  - Issues with power and telecommunications as power stations and towers are damaged.
  - For some regions maps are available that show the likelihood of earthquakes.
- Floods
  - Can happen in most places, due to excessive rain, tsunamis, etc.
  - Can lead to same issues as earthquakes.
  - Meteorologists usually have maps or models that show likelihoods.

Disaster Recovery Planning

Natural disasters

- Storms
  - Can hit almost anywhere, however can be more predictable than other natural disasters.
  - Rain can **flood** and **hailstorms** can cause damage, **wind speeds** can be devastating.
  - Risk of **lightning**
    - Can cause major damage to electrical components.
    - Can cause fire, can cause power-outages.

Disaster Recovery Planning

Natural disasters

- Fire
  - Can be caused by many things (not only natural disasters).
  - Always mitigate the risks of fire (should also be part of BCP).
  - Don't forget wildfires, regions like southeast Australia suffer from massive wildfires that can impact your business.

Disaster Recovery Planning

Natural disasters

- Geographically diverse businesses need to have different BCP/DRP plans for different sites.
- The likelihood of earthquakes will differ around the world.
- You cannot create one BCP/DRP plan for an entire business, need a new plan for each site.

Disaster Recovery Planning

Man-Made Disasters

- Fires
  - Carelessness, faulty electrical wiring, improper fire protection etc.
- Acts of terrorism
  - Since the beginning of the 21st century businesses are taking into account the impact terrorist attacks may have on their business.
- Bombings/explosions
  - Explosive gas may fill rooms/buildings and later ignite.
  - In some areas bombings should also be of concern.
- Power outages
  - Can be caused by many things, and should always be a concern.

Disaster Recovery Planning

Man-Made Disasters

- Strikes
  - If a large number of people walk out of your business at the same time, what happens to the mission-critical processes?
- Theft/vandalism
  - The likelihood of theft is far greater than that of terrorist attacks.
  - Insurance can mitigate some of the impact.
  - Keep spare parts available to quickly get the business back again (e.g. extra computer screens, RAM sticks, laptops, phones, etc.).

Disaster Recovery Planning

Other utility and infrastructure failures

- It’s natural to think about electrical power to be of high importance, but also consider:
  - Water
  - Gas
  - Sewers

- It is also natural to think about ones own infrastructure (servers, buildings, etc.), but also consider:
  - Airports
  - Highways
  - Railroads

Disaster Recovery Planning

Recovery strategy

- In order to come up with a DRP the process is very much like BIA from BCP.
  - In fact the actual priority list from BCP can be used, as well as the values assigned to assets and processes.

- A few things to remember that may differ:
  - During a disaster it may be acceptable to not bring a process up to 100%, but rather 50% and them move on to the next prioritised item.
  - It may have been prioritised to get the phones working in an office building, but during a disaster maybe the building is completely wiped out, so there is no point in prioritising this.

Disaster Recovery Planning

Alternate Processing Sites

- One of the most important parts of a DRP, and one with many available options.

- When a disaster hits you business you must be able to quickly get going somewhere else.

- What and where is this “somewhere else”?

Disaster Recovery Planning

Alternate Processing Sites

- **Cold Sites – Cheap and slow**
  - Standby facilities that are large enough to handle the business needs and have electrical and environmental support systems.
  - Large warehouses, empty office buildings, etc.
  - A *cold* site has no computing facilities (hardware or software) preinstalled and has no active broadband link.

Disaster Recovery Planning

Alternate Processing Sites

- **Cold Sites – Cheap and slow**
    - A cold site carries low cost – no maintenance on computing facilities, no monthly bills from telecommunications.
    - However, there is a great lag between a disaster and the business getting going again.
        - Hardware needs to be put in, software needs to be installed, backups needs to be restored, communications established.
        - This is usually measured in weeks.

Disaster Recovery Planning

Alternate Processing Sites

- **Hot Sites – Expensive and fast**
  - The backup facility is maintained in constant working order.
    - Servers and workstations are updated and have communication links to assume primary operations instantly.
  - Data on primary servers are regularly replicated to corresponding servers at the hot site.
  - If data replication can be done continuously then moving operations to the hot site can be done instantly.

Disaster Recovery Planning

Alternate Processing Sites

- **Hot Sites – Expensive and fast**
  - If data replication is not continuous there are three options:
    - If there is time then the primary site can be forced to replicate before it goes down.
    - Carry backups from primary site to hot site and manually apply the updates.
    - Accept loss of some data (the data that has not been replicated).

Disaster Recovery Planning

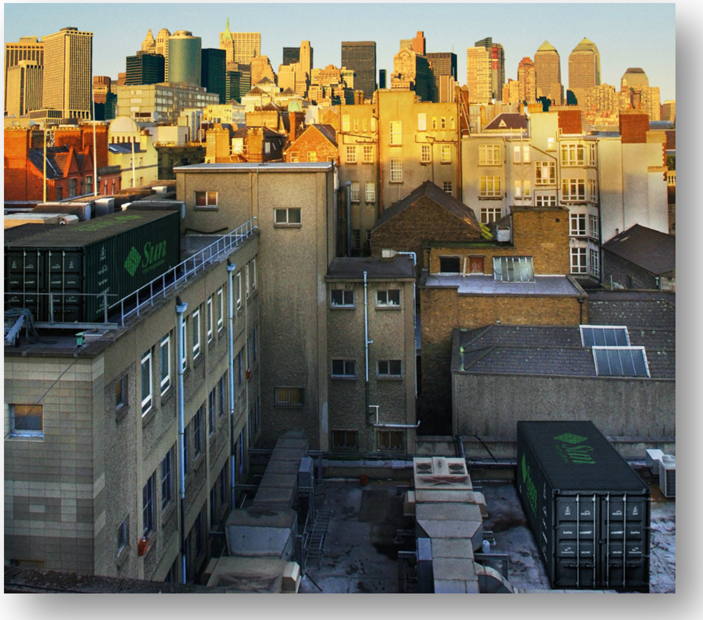
Alternate Processing Sites

- **Warm site – Middle ground**
  - As with hot sites the equipment is usually preconfigured and ready to go, and communication links are ready to go.
  - However there is no data at the site, and so backup copies needs to be delivered to the site and the systems updated with data.
  - Warm sites cut costs by not having to keep maintenance costs and broadband costs of transferring data.
  - Warm sites usually take about 12 hours to start, compared to hot sites which usually take a few seconds up to a minute.

Disaster Recovery Planning

Alternate Processing Sites

- **Mobile sites**
  - Not common, but can be very useful
  - Comes in many shapes, but can be self-contained trailers or containers that are warm or hot.
  - Can relocate and run operations from anywhere.



Disaster Recovery Planning

Alternate Processing Sites

- **Service Bureaus**
  - Service bureaus usually own large server farms and fields of workstations.
  - An organisation can purchase a contract to consume some portion of the processing capabilities.
  - Potential for overloading capacity if many organisations hit by a disaster at the same time.
  - Need to select a service bureau that is far away geographically so that they are not impacted by the same disaster you are.

Disaster Recovery Planning

Alternate Processing Sites

- **Multiple sites**
  - Spreading the organisation geographically can be important from other perspectives (sales, marketing, etc.).
  - This also allows for some redundancy if disaster strikes.
  - The local office in London may be able to take over some of the mission-critical processes from the Seattle office in case of a disaster.

Disaster Recovery Planning

Database recovery

- Databases are at the core of many organisations: transactions, sales, logistics, customers, contractors, etc.

- Ensuring that there are backups of databases, and that they can be accessed, is a critical part of DRP.

Main
Backup

Disaster Recovery Planning

Database recovery

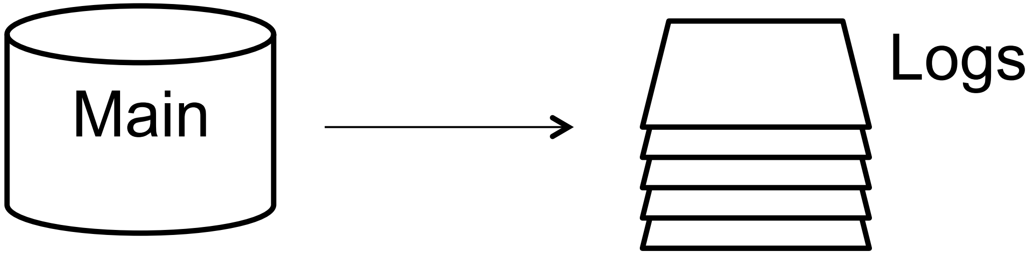
- Electronic Vaulting
  - Database backups are moved to a remote site, the entire database is copied and stored.
  - The remote location may be an alternative hot site, an offsite location, or a service purchased from a contractor.
  - Restoring usually takes longer time, as entire backups need to be read into the new system

  - Amazon Glacier is an example of a vault where storing your data is cheap, but it takes longer to get it back.
    - Cost in the region of $0.01/GB per month.

Disaster Recovery Planning

Database recovery

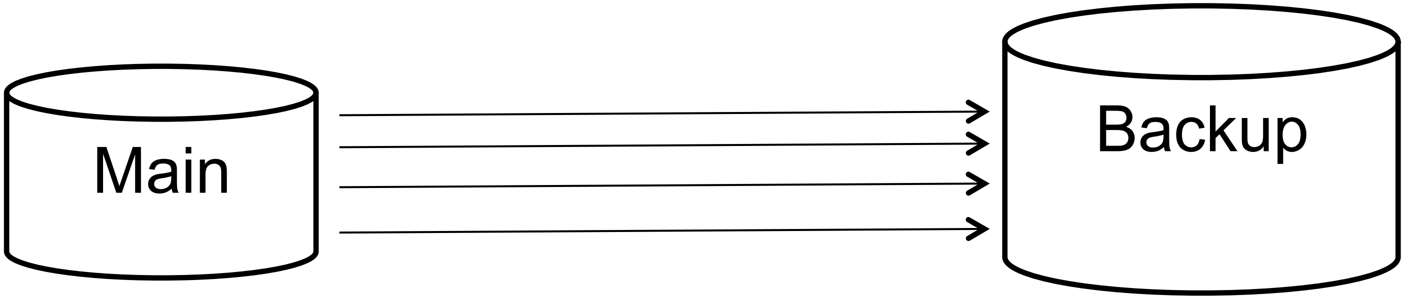
- Remote Journaling
  - Data transfers still occur in bulk, but more frequently, maybe once an hour or so.
  - Remote journaling only copies the transaction logs that have occurred since the last backup.
  - The logs are **not** applied to a live database, so when disaster strikes it is necessary to apply all the transactions on the production database.



Disaster Recovery Planning

Database recovery

- Remote Mirroring
  - A live database server is maintained at the backup site.
  - The remote server receives copies of the database modifications at the same time they are applied to the production server at the primary site.
  - The backup server is ready to go at an instance.
  - Requires more resources and is usually more expensive.



LiU EXPANDING REALITY

Disaster Recovery Planning

Backups and Offsite Storage

- It is important to remember data not stored in databases, these can be employees **workstations**, **image repositories**, etc.

- Backups can usually not be continuous, as they often incur slowdown and lags in file access.
  - Schedule backups during low work peaks – e.g. Sundays

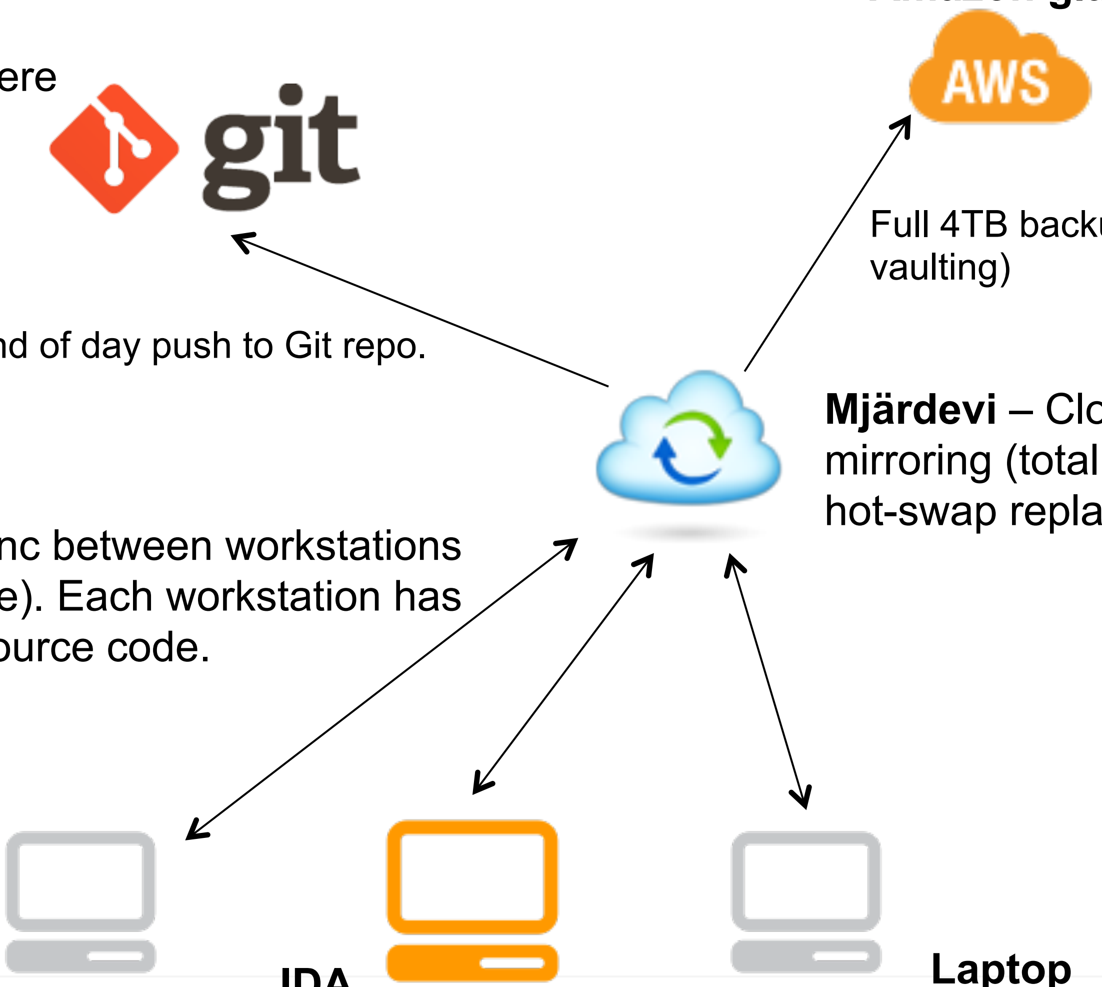
Disaster Recovery Planning

Backups and Offsite Storage

- It is important to remember to **verify** that the backups are not corrupt, and that backup media is healthy.
  - Using techniques such as **RAID** can be done to ensure redundancy even if you have hardware failure.
- The drives that the backup are stored on should be **replaced** as they wear down.

Disaster Recovery Planning

Cheap backup of source code



Amazon glacier - Spread across US

US somewhere

Full 4TB backup every Sunday (Electronic vaulting)

End of day push to Git repo.

Mjärdevi – Cloud Station 2 HDD mirroring (total 4TB), if disk failure hot-swap replace.

Automatic sync between workstations (dropbox style). Each workstation has full copy of source code.

Mjärdevi

IDA

Laptop

Disaster Recovery Planning

Software Escrow Arrangements

- When purchasing software from small companies there is a very real risk that the company will go bankrupt, or otherwise stop to exist.

- If you rely on the software then you need to be able to get updates and apply patches.

- There are third party escrow agents that can hold onto source code and release it only if certain conditions are met (such as bankruptcy).

- This is a way for a small company to protect their propriety property, and for you to cope if they stop existing.

Disaster Recovery Planning

Software Escrow Arrangements

- Developing a new IT platform with a software development company.
- Considerations:
  - What if the development company bankrupts or if they do not have a BCP/DRP plan that mitigates risks?
  - One solution is to use escrow arrangements to ensure that the code can be obtained and another company can take over.
  - Another way is to ensure continuous delivery of the product, so that if something happens at least some of the features exists.

Disaster Recovery Planning

Recovery vs Restoration

- Part of the DRP process is also to restore the original site.
- Here the least priority processes should be taken back to the primary site.
  - If the primary site can handle these low-priority processes then more processes can be moved back.

- The organisation is not out of disaster mode until all services are back at the primary site and running as normal.
- The DRP should specify criteria for when the primary site can be considered normal.

Disaster Recovery Planning

Documentation

- The DRP needs to be documented, some of the important parts include:
  - Executive summary providing high-level overview of the plan.
  - Department-specific plans.
  - Technical guides for IT personnel responsible for implementing and maintaining critical backup systems.
  - Checklists for individuals on the disaster recovery team
    - Simple checklists that can be followed during a time of distress, should include things like calling emergency authorities and activating the DRP.

Disaster Recovery Planning

Training and Testing

- It is dangerous to become falsely assured that the BCP and DRP will take care of disasters without having ever put them in action.
- **Structured walk-through**
  - Key personnel and members of the BCP/DRP team go through step by step what should be done in a scenario given by a moderator. Participants act like they have been trained.
- **Simulation test**
  - Similar to structured walk-through but some of the actions are actually carried out.

Disaster Recovery Planning

Training and Testing

- **Parallel test**
  - Relocating some of the employees to the alternative site and allow them to implement some activation procedures. The primary site is however still active and running.
- **Full-Interruption test**
  - Actually shutting down the primary site and shifting them to the recovery site.
  - Obviously very difficult to get permission to run these, and management will resist.
  - However, the only way to truly test the DRP.

DRP - Real world cases

- Hurricane Sandy (Eastern US 2012)
- IT manager with a NYC firm:
  - “The building’s 31-foot, block-long basement was filled with water (it actually made it up about four feet into the lobby above)” … “The damage to the building was enough that we didn’t have any power at all until five days later” … “The server rack had both UPSes die and they were just replaced”
  - Used several cloud-based services to keep the operations running:
    - Licence manager deployed on AWS.
    - As Sandy approached they copied recently used data to Panzura and they were given access to the firm’s files and systems to continue working.
    - They had partial migration to Gmail already, so employees could continue using their email accounts.

DRP - Real world cases

- CEO of Quest:
  - “We were hit with sever winds and a week of heavy rain that ultimately caused eight utility poles to fall outside of our building.”
  - “The power went out, the road was blocked by hot wires and transformers, and everyone who made it into work that morning were trapped in the building”.
  - “Initially, battery and generator backup provided phone and Internet capability. And by utilizing resources at several other locations, the company was able to continue to function until we got the all-clear to evacuate”
  - “We executed our own DR plan – and by 3pm were operating completely remotely with some of our employees at our Business Resumption Center and others working from home”

DRP - Real world cases

- CEO of Quest:

  Lessons learned

  - “Conducting DR drill and testing our DR plan quarterly was and is fundamental, but even so we had to deal with keeping our 100 person staff up-to-date on what’s happening, no power for 36 hours and the refrigerated food spoiled and no one fed the fish.”

Helping clients **manage their technology** *for over* **30 years**

How can we help?™

With a reputation for maturity, reliability, and distinctive depth of talent, we have earned our place among **the nation's leading Technology Integrators.**

Cloud Services

Flexibility to develop and deliver applications, information, and critical resources to your locations in a safe, secure manner.

Disaster Recovery

We can help you consider the possibilities and plan for the unexpected. We can guide you in implementing an ongoing, sensible and cost-effective continuity plan.

Security Services

We can design, implement, and manage a comprehensive security plan that covers your networks, servers, databases, and applications.

Network & Server Management

Less than optimum network performance may be the biggest threat to your company's productivity. Secure your business with Quest's Network & Server management.

DRP – Real world cases

- IT manager at Louisiana based law firm:
  - “With a location in the Gulf Coast and office in New Orleans, our business is in an area prone to natural disasters and hurricanes.”
  - “When hurricane Katrina struck in 2005, we had to evacuate and our servers had to be shut down, risking critical client information.”
  - “We had to go into New Orleans under armed guard to regain access to documents and emails that had not yet been captured by the tape backup system prior to Katarina’s landfall.”
  - “After this devastating experience we started working with cloud providers”.

DRP – Real world cases

- IT manager for recruitment firm:
  - The National Weather Service is the home page on my internet browser between the months of June 1st and November 1st. On Wednesday September 3rd 2008 it was apparent that the Gulf Coast was going to take a direct hit by hurricane Ike.
  - Employees that could were relocated to Austin – the hotels were packed. People had brought their dogs and cats and people who had not made a reservation were waiting in line to get a room.
  - We were able to connect to backup databases and get files at the alternative site, but we had no email. The email replication solution had failed. Communication instead had to be done by temporary Hotmail accounts and fax machines.
  - Whenever we make significant change to our IT applications or infrastructure we test that modification on the alternative sites.

Linköpings universitet

expanding reality

www.liu.se