Title: Developing Disaster Recovery Plans

Slide 1: Title Slide

Title: Developing Disaster Recovery Plans
Subtitle: Ensuring Network Resilience and Business Continuity
Your Name/Team Name
Date

Slide 2: Importance of Disaster Recovery in Network Infrastructure

- Disasters can be **natural** (floods, earthquakes) or **man-made** (cyberattacks, hardware failures).
- Network infrastructure is **critical** for business operations.
- Downtime leads to **financial losses** and **reputational damage**.
- Disaster Recovery (DR) ensures **minimal disruption** and **quick recovery**.
- DR is a **subset of Business Continuity Planning (BCP)**.

Slide 3: Key Principles of Disaster Recovery and Business Continuity

- **RTO (Recovery Time Objective):** Maximum acceptable downtime.
- **RPO (Recovery Point Objective):** Maximum data loss acceptable (measured in time).
- **Redundancy:** Duplication of critical components to ensure availability.
- **Scalability:** Ability to adapt to growing business needs.
- **Testing and Maintenance:** Regular testing of DR plans to ensure effectiveness.

Slide 4: Backup Strategies

- **Full Backup:** Complete copy of all data.
- **Incremental Backup:** Only changes since the last backup.
- **Differential Backup:** Changes since the last full backup.
- **3-2-1 Rule:**
  - 3 copies of data (1 primary + 2 backups).
  - 2 different storage types (e.g., cloud + physical).
  - 1 offsite backup.

Slide 5: Redundancy Mechanisms

- **RAID (Redundant Array of Independent Disks):**
  - RAID 0: Striping (performance).
  - RAID 1: Mirroring (redundancy).
  - RAID 5: Striping with parity (balance).
- **Load Balancers:** Distribute traffic across multiple servers to prevent overload.
- **Failover Systems:** Automatic switching to a standby system during failure.
- **Geographical Redundancy:** Data centers in multiple locations.

Slide 6: Network Recovery Procedures After a Breach or Failure

- **Step 1:** Identify the Cause (analyze logs, monitor traffic, detect anomalies).
- **Step 2:** Contain the Damage (isolate affected systems to prevent spread).
- **Step 3:** Restore Systems (use backups to restore data and services).
- **Step 4:** Test and Validate (ensure systems are fully functional and secure).
- **Step 5:** Review and Improve (update DR plans based on lessons learned).

Slide 7: Hands-on Lab: Designing and Implementing a Disaster Recovery Plan

- **Objective:** Create a DR plan for a sample network infrastructure.
- **Steps:**
  1. Identify critical assets and prioritize them.
  2. Define RTO and RPO for each asset.
  3. Choose backup and redundancy strategies.
  4. Simulate a disaster scenario (e.g., server failure, ransomware attack).
  5. Execute the DR plan and measure recovery time.
  6. Document results and refine the plan.
- **Tools:** Backup software (e.g., Veeam, Acronis), virtualization tools (e.g., VMware, Hyper-V), monitoring tools (e.g., Nagios, PRTG).

Slide 8: Best Practices for Disaster Recovery Planning

- Regularly update DR plans to reflect changes in infrastructure.
- Train staff on DR procedures and roles.
- Conduct periodic disaster recovery drills.
- Use automated tools for backups and monitoring.
- Collaborate with stakeholders to align DR plans with business goals.

Slide 9: Case Study: Real-World Disaster Recovery Example

- **Scenario:** A company faced a ransomware attack that encrypted critical data.
- **Response:**
    - Isolated infected systems.
    - Restored data from offsite backups.
    - Implemented stronger cybersecurity measures.
- **Outcome:** Minimal downtime and no data loss.

Slide 10: Conclusion and Q&A

- Disaster recovery is essential for maintaining business continuity.
- A well-designed DR plan minimizes downtime and data loss.
- Regular testing and updates are crucial for DR plan effectiveness.
- **Q&A:** Open the floor for questions.

Slide 11: References

- NIST SP 800-34: Contingency Planning Guide.
- ISO 22301: Business Continuity Management.
- Books: "Disaster Recovery Planning" by Jon William Toigo.
- Tools: Veeam, Acronis, VMware, etc.
