Disaster Recovery Plan
Qi Bank.

By
Timi Ogunjobi
Information Security Analyst & Project Manager
timiasservice@gmail.com
470-727-0678

1. Introduction

Purpose: To establish a comprehensive plan for the recovery of IT systems and data in the aftermath of a cybersecurity disaster, ensuring the bank can quickly resume critical operations.

Scope: Applies to all digital assets, IT infrastructure, applications, and data essential to the bank's operations, including systems managed by third-party vendors.

Objectives:
- Rapidly restore critical systems and data to operational status.
- Minimize financial and reputational damage.
- Ensure continuity of service to customers.

2. Disaster Recovery Team (DRT)

Composition:
- **DRT Lead**: Coordinates disaster recovery efforts across departments.
- **IT Operations**: Responsible for restoring systems and network services.
- **Data Management**: Manages data restoration and integrity checks.
- **Communications Officer**: Handles internal and external communications.
- **Facilities Management**: Ensures physical infrastructure is available for recovery operations.

Responsibilities:
- Pre-defined roles activate upon declaration of a disaster, with clear lines of authority and communication.

3. Risk Assessment and Critical Systems Identification

Risk Assessment:
- Conduct a comprehensive risk assessment to identify potential cybersecurity threats and their impact on the bank’s IT infrastructure.

Critical Systems Identification:
- Identify and prioritize critical systems and applications essential to the bank's core operations, based on their importance to business continuity.

4. Recovery Strategy

Data Backup and Replication:
- Implement a robust data backup and replication strategy, ensuring critical data is regularly backed up and stored in secure, geographically diverse locations.

System Redundancy:
- Establish redundant systems and networks that can be quickly activated in the event primary systems are compromised.

Recovery Sites:
- Maintain hot, warm, and cold recovery sites equipped to rapidly resume operations with varying degrees of readiness and data recency.

5. Recovery Procedures

Activation Protocol:
- Outline clear criteria for activating the disaster recovery plan, including who has the authority to declare a disaster.

System and Data Restoration:
- Provide step-by-step procedures for restoring systems, applications, and data from backups, including integrity checks and validation processes.

Communication Plan:
- Detail communication protocols for updating internal stakeholders, customers, regulators, and other relevant parties about the status of recovery efforts.

6. Testing and Maintenance

Regular Testing:
- Schedule annual or bi-annual tests of the disaster recovery plan, including simulated disasters and recovery drills, to evaluate the effectiveness of recovery procedures and the readiness of the DRT.

Plan Maintenance:
- Regularly review and update the disaster recovery plan to reflect changes in the IT environment, critical systems, and potential threats.

7. Training

DRT Training:
- Conduct ongoing training for all members of the Disaster Recovery Team to ensure familiarity with the disaster recovery procedures and their roles in the process.

Bank-wide Awareness:
- Promote bank-wide awareness of the disaster recovery plan and the importance of cybersecurity preparedness through regular information sessions and training.

8. Documentation and Compliance

Documentation:
- Maintain comprehensive documentation of the disaster recovery plan, including recovery procedures, contact lists, and logs of recovery efforts.

Regulatory Compliance:
- Ensure the disaster recovery plan and all recovery efforts comply with relevant regulations and standards, such as the Gramm-Leach-Bliley Act (GLBA) and international standards like ISO 22301.

9. Post-Recovery Review

Debriefing and Lessons Learned:
- After a disaster recovery operation, conduct a debriefing session to review the effectiveness of the recovery, document lessons learned, and identify improvements to the plan.