Incident Response Plan
Qi Bank.

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

1. Introduction

Purpose: To outline the procedures and processes to be followed in response to a cybersecurity incident, ensuring a swift, effective, and coordinated recovery.

Scope: Applies to all IT systems, networks, and data managed by the bank, including third-party services and vendors.

Objectives:
- Minimize the impact of incidents on bank operations, customers, and stakeholders.
- Rapidly restore normal operations and services.
- Ensure accurate documentation and compliance with legal and regulatory requirements.

2. Incident Response Team (IRT)

Composition:
- **IRT Lead**: Oversees incident response efforts and decision-making.
- **Security Analysts**: Perform technical analysis and forensics.
- **Communications Officer**: Manages internal and external communications.
- **Legal Advisor**: Provides advice on legal and regulatory implications.
- **IT Operations**: Assists in containment, eradication, and recovery efforts.

Responsibilities:
- Each member has predefined roles and responsibilities activated upon incident detection.

3. Incident Detection and Reporting

Detection:
- Utilize SIEM tools, intrusion detection systems, and network monitoring solutions to detect anomalies indicative of a cybersecurity incident.

Reporting:
- Establish clear reporting channels for employees, customers, and vendors to report suspected incidents.
- Define procedures for initial incident assessment and classification based on severity and potential impact.

4. Incident Analysis

Initial Analysis:
- Gather all relevant information about the incident, including logs, affected systems, and potential entry points.
- Use forensic tools and techniques to analyze the incident's scope and impact.

Classification:
- Classify the incident based on its nature (e.g., malware, phishing, data breach) and severity to prioritize response efforts.

5. Containment, Eradication, and Recovery

Containment:
- Implement immediate measures to contain the incident, such as isolating affected systems or blocking malicious traffic.

Eradication:
- Identify and remove the cause of the incident, such as malware or unauthorized access points.

Recovery:
- Restore affected systems and services using backups.
- Gradually return operations to normal, monitoring for any signs of residual impact.

6. Communication

Internal Communication:
- Inform relevant internal stakeholders, including senior management and affected departments, about the incident and ongoing response efforts.

External Communication:
- Coordinate with the Communications Officer to release information to customers, regulators, and the public as required by law and in line with the bank's communication policy.

7. Post-Incident Review

Debriefing:
- Conduct a post-incident review involving all IRT members and relevant stakeholders to discuss what occurred, the effectiveness of the response, and lessons learned.

Improvements:
- Update the IRP and other security policies based on insights gained from the review.
- Implement recommended improvements to prevent future incidents.

8. Documentation and Compliance

Documentation:
- Maintain detailed records of the incident, response actions, decisions made, and lessons learned for regulatory compliance and future reference.

Regulatory Compliance:
- Ensure all response actions comply with applicable laws and regulations, such as GDPR or GLBA, and report incidents to regulatory bodies as required.

9. Training and Exercises

Regular Training:
- Conduct regular training sessions for the IRT and relevant employees on incident response procedures and updates to the plan.

Simulated Exercises:

- Perform simulated incident response exercises annually to test the effectiveness of the IRP and team readiness.