Irony Man

Lost or Stolen Device Response Plan

The Facts Were These: Someone stole former thief Anthony Stark's company-issued laptop, which contains sensitive data.

Below is a breakdown of each phase of the plan and a rough estimate of the timeline starting from the detection of the threat to the recovery stage.

Immediate Actions (0-30 minutes)

Detection

Employee reports lost or stolen device.
Device fails to check in with management systems.
Unusual device activity detected.
Device tracking alerts.

Initial Response

Attempt to locate device using tracking features.
Initiate remote wipe if device cannot be recovered.
Disable device access to corporate systems.
Change any stored passwords or credentials.

Containment (30 minutes - 2 hours)

Access Control

Disable VPN and remote access for the device.
Revoke device certificates and authentication tokens.
Remove device from email and application access.
Monitor for unauthorized access attempts.

Data Protection

Assess sensitive data stored on the device.
Implement additional monitoring for data misuse.
Review and update data encryption policies.
Verify backup and recovery procedures.

Investigation (2-8 hours)

Risk Assessment

Determine sensitivity of data on the device.
Assess potential impact of data exposure.
Review device security configurations.
Analyze device usage patterns before loss.

Incident Analysis

Investigate circumstances of device loss.
Review device management and security logs.
Assess effectiveness of security controls.
Document lessons learned and improvements.

Recovery (8-24 hours)

Device Replacement

Provision new device with enhanced security.
Restore data from backups.
Implement additional security controls.
Update device management policies.

Security Enhancement

Review and update mobile device management (MDM).
Implement stronger encryption and authentication.
Update device loss prevention procedures.
Enhance user training on device security.

Communication:

- **Internal**
  - Notify executive leadership if high-risk data involved
  - Inform legal and compliance teams
  - Update IT operations and security teams
  - Coordinate with human resources and employee
- **External**
  - Report to law enforcement if required
  - Notify regulatory authorities if personal data involved
  - Coordinate with insurance providers
  - Update customers if their data was on the device

Post-Incident

Review mobile device management policies.
Implement improved device tracking and security.
Conduct device security awareness training.
Update incident response procedures.