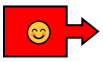
Rogue's Gallery



Unauthorized Wireless Access Point Response Plan

The Facts Were These: A rogue access point was discovered on the internal network, possibly allowing external access.

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

Rogue access point discovered during network scan.
Unusual wireless network activity.
New wireless networks detected in area.
Network monitoring alerts.

Initial Response

Locate and physically disconnect the rogue access point.
Document access point details and location.
Isolate affected network segments.
Begin investigation of potential security breach.

Containment (30 minutes - 2 hours)

Network Security

Scan for additional unauthorized access points.
Implement wireless network monitoring.
Block unauthorized wireless traffic.
Segment network to prevent lateral movement.

Physical Security

Secure physical access to network infrastructure.
Review and update physical security controls.
Implement access point detection systems.
Coordinate with facilities management.

Investigation (2-8 hours)

Security Analysis

Analyze access point configuration and capabilities.
Review network logs for unauthorized access.
Assess potential data compromise.
Investigate source and purpose of access point.

Forensic Analysis

Preserve access point for forensic examination.
Analyze network traffic and access patterns.
Review physical security logs and access records.
Document timeline and scope of exposure.

Recovery (8-24 hours)

Network Restoration

Verify network integrity and security.
Implement additional wireless security controls.
Update network monitoring and detection systems.
Validate network segmentation and access controls.

Security Enhancement

Implement wireless intrusion detection systems.
Update wireless security policies and procedures.
Enhance physical security controls.
Improve network access control systems.

Communication:

- **Internal**
    - Notify executive leadership and stakeholders
    - Inform legal and compliance teams
    - Update IT operations and security teams
    - Coordinate with facilities and physical security
- **External**
    - Consider law enforcement notification
    - Report to regulatory authorities if required
    - Coordinate with security vendors
    - Update customers if services are affected

Post-Incident

Implement continuous wireless monitoring.
Conduct regular wireless security assessments.
Update physical security procedures.
Review and update incident response procedures.