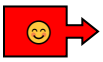
Invasion of the Data Snatchers



Insider Threat Attack Response Plan

The Facts Were These: Karen and Ken, two often disgruntled employees, transfer sensitive data to their personal email and cloud storage.

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 (0-1 hour)

Detection

Unusual data access patterns detected.
Large file transfers to external systems.
After-hours access to sensitive systems.
Data loss prevention (DLP) alerts.

Initial Response

Discreetly gather initial evidence.
Coordinate with HR and Legal teams.
Avoid alerting the suspected insider.
Document initial observations.

Investigation (1-24 hours)

Covert Analysis

Review user activity logs and data access patterns.
Analyze email and file transfer logs.
Check for removable media usage.
Review VPN and remote access logs.

Evidence Collection

Preserve digital evidence following forensic procedures.
Collect relevant system logs and audit trails.
Document user behavior patterns.
Coordinate with legal team on evidence handling.

Containment (24-48 hours)

Access Control

Disable or limit user access privileges.
Revoke VPN and remote access.
Monitor remaining user activities.
Implement additional monitoring controls.

Asset Protection

Identify and protect sensitive data.
Review and restrict data access permissions.
Monitor for continued suspicious activities.
Implement data loss prevention measures.

Recovery (2-7 days)

System Security

Review and update access controls.
Implement additional monitoring.
Secure sensitive data repositories.
Update user access management procedures.

Process Improvement

Review hiring and background check procedures.
Implement user activity monitoring.
Update data classification and handling procedures.
Enhance security awareness training.

Legal and HR Coordination	
Legal Actions	**HR Actions**
Coordinate with legal team on evidence preservation.	Coordinate disciplinary actions with HR.
Consider law enforcement involvement.	Review employee termination procedures.
Review contractual obligations and NDAs.	Implement exit interview processes.
Prepare for potential civil litigation.	Update employee monitoring policies.

Post-Incident

Conduct thorough security review.
Implement improved access controls.
Update insider threat detection capabilities.
Review and update incident response procedures.