Taken

Ransomware Infection Response Plan

The Facts Were These: Liam downloads a malicious attachment that encrypts his critical files and displays a ransom note.

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 (0-15 minutes)

Detection

Ransomware note displayed or encryption detected.
Unusual file system activity alerts.
Network traffic anomalies.

Immediate Response

[1]Don't pay ransom or interact with the ransom note.
Immediately isolate infected systems from network.
Preserve evidence by taking screenshots of ransom notes.
Activate incident response team.

Containment (15 minutes - 1 hour)

Network Isolation

Disconnect affected systems from network immediately.
Block suspicious IP addresses at firewall.
Disable affected user accounts.
Isolate network segments if lateral movement detected.

Asset Protection

Power down infected systems (if safe to do so).
Identify and protect backup systems.
Verify backup integrity and isolation.
Secure clean system images for investigation.

[1] Or threaten them with your particular set of skills.

Investigation (1-8 hours)

Malware Analysis

Identify ransomware variant and capabilities.
Determine attack vector and timeline.
Assess scope of encryption and data loss.
Check for data exfiltration capabilities.

Forensic Analysis

Preserve infected systems for forensic examination.
Analyze network logs for lateral movement.
Review email logs for initial infection vector.
Document all compromised systems and data.

Recovery (8 hours - several days)

System Restoration

Restore systems from clean backups.
Rebuild compromised systems from scratch.
Install latest security patches.
Restore data from verified clean backups.

Validation

Perform malware scans on restored systems.
Verify system functionality and data integrity.
Test security controls and monitoring.
Gradually restore network connectivity.

Communication	
Internal	**External**
Notify executive leadership immediately	Report to law enforcement (FBI/local authorities)
Inform legal and compliance teams	Notify regulatory bodies if required
Coordinate with insurance providers	Coordinate with cyber insurance providers
Update employees on system availability	Consider engaging external forensics team

Post-Incident

Review and test backup procedures.
Implement additional endpoint protection.
Conduct security awareness training.
Review incident response procedures.
Consider cyber insurance coverage adequacy.