Cybersecurity Incident Investigation Report

Organisation: Orion Health Services
Incident Type: Ransomware Attack

1. Summary

Orion Health Services experienced a ransomware attack originating from a phishing email targeting a finance employee. The malicious Excel attachment enabled attackers to gain initial access, harvest credentials, pivot across internal systems and deploy ransomware across key servers. Sensitive payroll data, system credentials and patient schedule data were compromised The incident resulted in operational disruption, partial backup encryption and high potential financial, legal, and reputational impact for the organisation.

2. Nature and Extent of the Breach

Attack Vector

- Phishing email impersonating a trusted supplier.
- Malicious Excel document containing embedded macros.
- User execution enabled remote access.

Timeline Overview

- Morning: Unusual outbound network traffic detected.
- Late morning: User lockouts reported.
- Midday: Ransom note discovered; encryption found across critical servers.

Systems Impacted

- File Server – widespread encryption (.orionlock extension)
- HR & Finance Systems – credential compromise + encrypted files
- Backup Server – partial encryption (suggesting insufficient segmentation)

Compromised Data

- Employee payroll records.
- Patient appointment schedules.
- Internal system credentials (harvested using Mimikatz).

3. Vulnerabilities Exploited

Technical Vulnerabilities

- Lack of MFA on critical internal systems.
- Outdated endpoint protections. Because of this, unable to detect macro-based malware.
- Insufficient network segmentation (ransomware lateral movement to backup server).

- Weak email filtering controls enabling phishing delivery.

Human Vulnerabilities

- User clicked malicious attachment.
- Limited phishing awareness training.
- Lack of verification procedures for external-file-based requests.

Process Gaps

- Ineffective monitoring of anomalous login attempts.
- No Zero-Trust enforcement.
- Backups not fully immutable or offline.

4. Business Impact Assessment

Financial

- Potential ransom payment demand.
- Loss of productivity across affected departments.
- Incident response, digital forensics, and system restoration costs.
- Potential fines for mishandling sensitive healthcare data (Australia's Privacy Act).

Legal

- Mandatory breach notification under OAIC.
- Exposure to regulatory audits.
- Risk of lawsuits from staff or patients if data misuse occurs.

Reputational

- Loss of trust from clinics and healthcare partners.
- Perceived weakness in protecting sensitive patient data.
- Market competitiveness impacted due to service downtime.

Operational

- Disruption of clinic scheduling & appointment systems.
- HR and payroll delays.
- Limited access to historical patient data if backups are unrecoverable.

5. Indicators of Compromise (IOCs)

- Suspicious overseas login attempt just before the breach.
- Execution of **Mimikatz** for credential harvesting.
- Encrypted files renamed with **.orionlock** extension.
- Unusual outbound traffic from internal servers.
- Ransom note deployed on shared drive.

6. Recommendations for Improvement

Immediate Remediation

- Isolate infected servers and endpoints.
- Disable compromised accounts and reset all credentials.
- Restore systems from clean, offline backups.
- Conduct full malware eradication and forensic analysis.

Security Controls Enhancement

- Implement MFA across all internal and privileged accounts.
- Deploy advanced endpoint detection (EDR/XDR).
- Strengthen email filtering (sandboxing, DMARC, anti-phishing controls).
- Block macro-enabled files from external, unverified sources.

Network & Infrastructure Hardening

- Zero-Trust network segmentation.
- Harden backup strategy (immutable, offsite, disconnected backups).
- Log and monitor privileged access aggressively.
- Implement least privilege policies.

Governance & Training

- Mandatory quarterly phishing simulation training.
- Updated incident response plan with ransomware playbook.
- Conduct tabletop exercises with HR, finance and IT teams.
- Clear internal procedures for verifying external attachments.

7. Conclusion

The ransomware attack on Orion Health Services exploited technical, human and procedural weaknesses, resulting in significant compromise of systems and high-risk data. By implementing stronger security controls, enhancing user training, modernising detection systems and adopting Zero Trust practices, Orion Health Services can substantially reduce the risk of future breaches and strengthen its resilience against sophisticated attacks.