Incident Response Report

Ransomware Outbreak — Weekend of 14 July 2025
Prepared by: IT Manager on Call

1. Immediate Plan of Action (Hour 0 – 6)

1.1 Activate Incident Response Team (IRT)
• Call tree: Security Operations Lead, CIO, General Counsel, Communications Director, Facilities Security.
• Switch to out-of-band voice/text (personal mobiles or Signal) to avoid actor monitoring.

1.2 Contain & Stabilise

1. **Disconnect affected segments at the core switch; if spread unknown, pull the external uplink and fall back on cellular hot-spots for business-critical traffic.**
2. **Power-down endpoints that cannot be isolated logically (last resort).**
3. **Capture ransom-note screenshots and volatile memory from two representative machines for forensics.**
4. **Block all VPN/RDP ingress, disable SSO temporarily, rotate privileged credentials.**

1.3 Preserve Evidence & Assess
• Snapshot key virtual machines and cloud volumes before any rebuilds.
• Collect firewall, EDR, AD and VPN logs for the previous 72 h.
• Determine footprint: servers (HR, Finance), 31 Windows laptops, 4 Linux file servers.
• Identify variant via NoMoreRansom ID-Ransomware utility; note → "OblivionX" (example).1.4 External Engagement
• Open case with cyber-insurance breach coach.
• Contact FBI field office and CISA via stopransomware@cisa.dhs.gov.
• Retain IR consultancy (SANS-certified) under NDA.
• Activate legal privilege via outside counsel before sharing artefacts.1.5 Business Continuity
• Fail over e-commerce to static "maintenance" landing page; record telephone order line in IVR.
• Have payroll and ERP teams remain offline until clean network stands up.
• Convene exec crisis call every two hours.1.6 Media / On-Site Reporter
• Security escort informs reporter that an official statement will follow; no speculative

comments.

- **Draft holding statement (see § 2).**

2. Sequenced Communications Plan

T + hrs	Audience	Channel	Key Message	Sender
0–1	CIO, CEO	Signal call	“Ransomware detected; network isolated; no evidence of exfil yet.”	IT Manager
1–2	IRT & Board	Email via O365 crisis tenant	Situation overview, next steps, legal obligations.	CIO
2–3	All employees	SMS / WhatsApp broadcast	Do not power on corporate devices; await further instruction.	HR Director
4	Media (holding)	Press release	“Company investigating IT disruption; following established protocols; no comment on specifics.”	Comms Dir.

T + hrs	Audience	Channel	Key Message	Sender
6	Key customers & suppliers	Signed PDF via dedicated portal	Possible service delays; point-of-contact info; reassurance of data-privacy focus.	VP Ops
24	Regulators (HIPAA, GDPR DPA)	Secure web form filings	Preliminary breach notification.	Legal
48	Public update	Website & social	Progress, expected restoration window, credit-monitoring offer if PII compromised.	CEO
72	Employees	Company Town-Hall (Zoom)	Root cause, recovery plan, training refresh dates.	CIO & CISO
Closure	All stakeholders	Final report & lessons learned.	CISO	

Draft Correspondence Snippets

1. **Employee SMS (T + 2 h)**
   "URGENT: A network security incident was detected. Please keep work devices OFF and disconnected. Updates soon. –IT"
2. **Press Holding Statement (T + 4 h)**
   "We are currently investigating a cybersecurity incident that has interrupted some internal systems. Our top priority is the protection of our customers, employees, and partners. We have engaged leading security experts and relevant authorities. We will provide further information as it becomes available."
3. **Customer Letter (T + 6 h)**
   "Dear [Name],
   Early this morning we detected unauthorized encryption activity on parts of our network. Out of caution we have temporarily paused certain services while we restore operations from secured backups. At this stage we have no evidence that your data has been accessed, but we will update you within 24 hours. For questions contact 1-800-555-HELP.
   Sincerely,
   [VP Operations]"
4. **Final Transparency Blog (Day 7)**
   "…Forensic analysis confirms the attacker leveraged a compromised contractor VPN account without MFA, deployed 'OblivionX' ransomware, and attempted—but failed—to exfiltrate file-shares. No customer payment data was accessed. We rebuilt 97 % of production from immutable backups and have accelerated our zero-trust roadmap…"

---

3. Post-Incident Prevention & Response Plan (90-Day Programme)

3.1 Governance & Policy
• Update Cyber-Incident Response Plan (CIRP): integrate lessons learned, on-call matrix, evidence-handling SOP.
• Board-level risk appetite statement and budget approval cycle.**3.2 Technical Controls**

1. Identity
   – Mandatory hardware-token MFA for all privileged and VPN accounts (within 30 days).
   – Quarterly privileged-access review.

2. Endpoint & Network
   – Roll out next-gen EDR with automatic host isolation (Pilot by Day 40).
   – Segment OT/IoT, finance, and guest networks via micro-segmentation.
3. Backup & Recovery
   – Enforce 3-2-1-1 rule (offline and immutable copy) and quarterly restore drills.
   – Deploy write-once S3 object-lock for snapshots.
4. Patch & Vulnerability Management
   – 14-day SLA for high CVEs; real-time SBOM tracking.
   – Add automated configuration hardening scans.
5. Email & Web Security
   – Implement sandboxed click-through for URLs; DMARC "reject."
   – Mandatory security awareness phishing simulations bi-monthly.

3.3 People & Processes

• Annual tabletop exercises with execs and PR.
• New-hire cyber-hygiene training and signed acceptable-use policy.
• Create "security champions" in each department.**3.4 External Collaboration**
• Join ISAC for sector intelligence.
• Subscribe to CISA KEV alerts and automate block-lists.
• Pre-contract an IR retainer with 24 × 7 SLA.

3.5 Metrics & Timeline

Milestone	Owner	Due	KPI
Immutable backups complete	Infrastructure Lead	Day 30	RPO ≤ 15 min
MFA for all remote access	IAM Lead	Day 30	100 % coverage
EDR auto-contain in prod	SecOps	Day 45	Mean time to isolate < 5 min

Milestone	Owner	Due	KPI
First full restore test	DR Manager	Day 60	Success ≥ 95 %
Board tabletop	CISO	Day 75	Action items closed ≥ 90 %
External audit	3rd-party	Day 90	Pass with ≤ 3 minors

4. Reflection on AI Reasoning Model

Using the OpenAI o3 Pro model to draft this report showed:• **Strength – Breadth & Synthesis:** The model rapidly merged authoritative guidance from CISA, NCSC, IBM, and recent (2025) industry articles into a coherent, actionable plan, saving hours of manual research.

• **Weakness – Contextual Specificity:** It cannot see our exact network topology or contractual obligations, so recommendations (e.g., 3-2-1-1 backup, MFA vendor choice) still need tailoring by our engineers and legal team.