MSP Internal IR One-Pager

Primary scenarios: Ransomware • BEC/M365 account takeover • Third-party/SaaS compromise

HOT TAKES: Speed beats perfection, but don't nuke evidence. Contain first. Clean later. Call insurance/legal before fixing.

1) Declare an incident if…

- EDR flags ransomware or widespread malware
- Global Admin sign-in from weird location/time/device
- Mailbox rules forwarding externally or mass phishing
- Vendor breach notice touching data/tokens
- Impossible travel / token theft indicators

When in doubt: declare it and downgrade later.

2) Quick severity triage

SEV1: Active encryption, widespread malware, live ATO, confirmed data access. **Contain in minutes.**

SEV2: Sketchy admin activity, isolated endpoint, weird OAuth. **Contain quickly, investigate same day.**

3) Escalation Chain: Service Desk → On-call Security / Incident Commander (IC) → Cyber Insurance + Breach Counsel (Early!)

4) First 5 Minutes (IC Playbook)

- **Declare SEV1/SEV2.** Start a timeline doc.
- **Secure Comms.** Move core team to safe channel (Signal/phone).
- **Containment NOW.** Isolate identities/endpoints first.
- **Call Insurance/Legal.** Early notice = coverage.
- **Assign Roles.** IC, Containment, Identity, Comms, Scribe.

5) First Call Script (Staff Instructions)

- Do NOT power off. (RAM evidence matters)
- Disconnect from network (Wi-Fi/Ethernet).
- Don't run cleanup tools/reset passwords yet.
- If asked 'are we breached?': Don't speculate. Wait for official language

6) First 60 Minutes Checklist

- **Containment:** Isolate EDR, quarantine hosts, block IoCs.
- **Evidence:** Snapshot logs. Don't rely on tickets.
- **Identity:** Disable accounts, nuke inbox rules, revoke tokens.
- **OAuth:** Remove sketchy consents/grants.
- **Backups:** Confirm immutability. Lock down admin access.
- **Insurance/Legal:** Document notification time & guidance.
- **Decide:** Confirm SEV, scope, next 2-hour plan.

7) Containment Options Menu

Endpoint / EDR

- ☐ Isolate host(s) (EDR/RMM)
- ☐ Block hashes/domains/IPs
- ☐ Don't reimage yet

Network

- ☐ Segment/isolate VLANs
- ☐ Block egress
- ☐ Grab firewall logs

Third-party / SaaS

- ☐ Revoke OAuth integrations
- ☐ Rotate API keys
- ☐ Check vendor status

Identity / M365

- ☐ Disable accounts
- ☐ Revoke tokens/sessions

Backups

- ☐ Confirm immutability
- ☐ Lock backup admin

Cleanup (Wait for IC)

- ☐ Remove rules/delegates
- ☐ Rollback admin changes

8) Evidence / Logs (Where to look)

- Identity: Audit logs, role changes, MFA, consents
- EDR: Process trees, isolation times
- Net: VPN logs, geo anomalies, egress
- Email: Message trace, fwd rules
- Backups: Job history, deletion events

9) Communications Do's & Don'ts

DO: Brief, factual, time-stamped updates via safe channels (Signal). Share actions, not theories.

DON'T: No speculating. No 'breach' word yet. No promises on time. No cleaning until evidence saved.

10) 10-Min Tabletop (Run Today)

Prompt: Finance sees weird wire. Users see MFA prompts. You find fwd rules + OAuth app.

Discuss: SEV level? Contain what first? Evidence to grab? Who calls legal?

11) This Week: Quick Wins

- ☐ Run the 10-minute tabletop
- ☐ Confirm Insurance contact info
- ☐ Verify Break-Glass admin access
- ☐ Test EDR isolation