SAMPLE INCIDENT BRIEF

RANSOMWARE RECOVERY BRIEF

Redacted sample format - not a client case

This downloadable brief shows the kind of leadership record 3PS leaves behind: what failed, what evidence was reviewed, what actions were taken, what recovered, what remains risky, and what should be funded before the next emergency.

PACKET ID

3PS-SAMPLE-PROOF-001

CLIENT	Redacted organization
INCIDENT TYPE	Identity-assisted ransomware recovery
AUDIENCE	Leadership, counsel, insurance, operations
PREPARED BY	3PS senior escalation owner

EXECUTIVE SUMMARY

WHAT LEADERSHIP NEEDS TO KNOW

This sample uses representative details only. In a real incident brief, every finding below is tied to evidence, timestamps, owner names, and decision records.

PRIMARY FAILURE POINT

Identity. A phishing path became session abuse before endpoint tools could make the business safe.

SECONDARY FAILURE POINT

Backup validation. Restore points existed, but dependency and clean-point evidence lagged behind the recovery need.

STABILIZATION

Suspicious sessions were revoked, affected hosts were isolated, high-risk indicators were blocked, and restore order was confirmed.

LEADERSHIP ANSWER

The outage was not a single tool failure. Coverage existed, but response ownership and cross-signal correlation were missing.

3PS FIRST-HOUR OBJECTIVE

Stop spread, preserve evidence, establish one owner, force vendor facts into one timeline, and make recovery decisions visible.

TIMELINE

WHAT CHANGED, WHEN

T+00 3PS engaged. Clean bridge opened. One escalation owner assigned. Change freeze requested.

T+15 Access paths inventoried: identity, endpoint, firewall/VPN, M365, backup, hypervisor, core apps.

T+35 Risky sessions identified. Suspect user tokens revoked. MFA and admin role exceptions reviewed.

T+55 Affected hosts isolated. Endpoint evidence preserved. Known indicators blocked at mail and network layers.

T+90 Backup job history reviewed. Candidate restore points marked clean, suspect, or unknown.

T+140 Vendor tickets consolidated. Conflicting claims mapped against logs and business workflow tests.

T+180 Recovery order approved. Leadership brief delivered with open risks and next authorization points.

EVIDENCE RULE

Every real timeline entry includes source, timestamp, owner, and whether it is confirmed, likely, or still unknown.

EVIDENCE AND CONTAINMENT

WHAT 3PS REVIEWED AND CHANGED

	Reviewed	Action
IDENTITY	M365 sign-ins, risky users, admin roles, MFA exceptions, session tokens	Revoked suspect sessions, tightened admin access, marked users for password/MFA reset
ENDPOINT	EDR alerts, process tree, isolation state, hash/URL/domain indicators	Isolated affected hosts, preserved evidence, blocked known indicators
EMAIL	Message trace, mailbox rules, forwarding, sender authentication, payload path	Removed suspicious rules, blocked sender indicators, marked related recipients
FIREWALL/VPN	Remote access logs, allowed objects, geolocation, active sessions	Closed suspect sessions, reviewed stale objects, confirmed intended exposure
BACKUP	Job history, restore point age, immutability, dependency notes	Tagged restore points, validated order, separated clean from unknown

CONTAINMENT STANDARD

A control change is not trusted until the business path is tested and the evidence shows the risky path stopped.

RECOVERY AND PREVENTION

WHAT HAPPENS AFTER IT STOPS

RECOVERY STATUS

- Priority systems ranked by business impact.
- Restore points tagged clean, suspect, or unknown.
- Application dependencies checked before broad restore.
- Leadership briefed on open risk before go-live decisions.

RESIDUAL RISK

- Accounts that still require password/MFA reset.
- Logs or evidence sources that expired before collection.
- Vendors still required to confirm support-side changes.
- Systems that need deeper restore testing.

MONTHLY PREVENTION PATH

- Identity and mailbox review.
- Endpoint, server, and firewall policy review.
- Backup restore test and dependency check.
- Vendor cleanup, stale access removal, and readiness note.

DECISION POINTS

- Accept, mitigate, or transfer remaining risk.
- Fund stack management or keep current tools with gaps noted.
- Schedule tabletop or restore drill.
- Update incident runbook and escalation contacts.

WHEN THIS IS REAL

A live 3PS incident brief names the evidence source, owner, timestamp, decision, and remaining risk for every material finding.