1_ Decision _ Log

Table of Contents

1. Chronological Decision Log

Timestamp	Decision Point	Decision Made	IR Phase	Rationale	Alternatives Considered	Outcome
Mon 6:45 AM	Initial incident triage.	Activated CSIRT and initiated IR plan; opened an incident ticket with unique ID and started a decision log.	Detection & Analysis	Rapid mobilization is critical to coordinate actions and maintain the chain of custody; it establishes governance from minute one. This rationale aligns with ISO 27035.	Wait for more data before activation; informal coordination through chat	CSIRT assembled within 10 minutes; documentation started; preserved early context.
Mon 6:50 AM	Immediate containment affected servers.	Isolated visibly affected servers (file servers, DB, Exchange, Veeam) by disabling network interfaces and blocking at switches.	Containment	Stops active encryption and lateral movement while preserving volatile. NIST SP 800-61 evidence (memory) where feasible.	Full enterprise shutdown; keep systems online to observe attacker.	No further encryption observed on isolated hosts; business impact localized.
Mon 6:55 AM	Evidence preservation kickoff.	Began forensic imaging plan: capture volatile memory on two representative encrypted servers; collect ransom note, hash values, and logs; start chain-of-custody forms.	Detection & Analysis	Early evidence ensures a defensible investigation and supports regulatory/legal needs such as GLBA.	Delay collection until later; rely solely on system logs.	Memory and log artifacts retained; chain-of-custody established.
Mon 7:00 AM	Stakeholder initial notifications	Notified CISO, CEO, General Counsel, and Chief	Preparation	Ensures leadership awareness, legal oversight, and comms	Notify only CISO and proceed;	Executives aligned; comms lead prepared

		Communications Officer with a concise situational summary and initial actions; paged all CSIRT members.		readiness while the technical team executes containment aligning with NCUA guidance.	broad notification later.	holding lines; CSIRT fully engaged.
Mon 7:10 AM	Network-wide risk assessment	Assessed need for full network shutdown; decided against full shutdown due to core banking isolation and member-facing services still operational.		Balance containment vs. continuity; maintain critical services on isolated segments; avoid cascading business disruption.	Immediate full shutdown of corporate network.	Branches continue limited operations; risk managed via segmentation and monitoring.
Mon 7:20 AM	Credential risk response	Forced password reset and account disablement for suspected compromised domain admin accounts; initiated privileged access review.	Containment	Reduces attacker privilege, limits persistence, and aligns to least privilege principles (ISO 27001 A.9).	Delay resets to avoid tipping attacker; reset only after forensics complete.	Admin credentials rotated; reduced lateral movement risk.
Mon 7:30 AM	Containment strategy approval (Inject 1.2)	Approved short-term containment: isolate infected hosts; block C2 indicators; segment HQ from branches; increase firewall egress restrictions.	Containment	Targeted isolation minimizes spread while keeping essential member services online.	Close branch operations entirely; or proceed with business-as-usual.	Containment effective; no new encryption; branches functional for basics.

Mon 7:45 AM	External support engagement	Engaged external forensics firm for 48-hour surge; notified cyber insurance carrier; retained breach counsel; lined up negotiator (no payment authorization).	Preparation	Brings specialized capability, preserves insurance coverage, and ensures legal privilege; negotiator optional for intel.	Handle internally only; engage later if needed.	Contracts executed; on-boarding by 2:00 PM; insurer acknowledged claim.
Mon 8:15 AM	Communications posture	Directed preparation of member/press holding statements (no confirmation of breach yet); centralized media inquiries via CCO.	Preparation	Consistent messaging avoids speculation; aligns with legal guidance.	Silence until full facts; ad-hoc responses by branch staff.	Holding lines ready; staff instructed to escalate inquiries.
Mon 9:00 AM	Ransom payment position (Inject 1.3)	Recommended against immediate payment; prioritize investigation, eradication, and recovery paths; consider payment only after technical, legal, ethical review.	Containment & Eradication	Payment lacks guarantee and increases risk of future targeting; focus on resilience and backups FBI/NCUA	Pay within 24 hours to secure discount and rapid restore.	Executives accepted conditional stance; decision deferred pending forensics.
Mon 11:00 AM	Backup strategy check	Verified offsite tapes (45 days old) and cloud email retention; planned restore path for email and non-	Recovery	Establish recovery feasibility without ransom; identify data reconciliation requirements.	Assume backups unusable; wait for decryption.	Feasible recovery paths identified; reconciliation effort scoped.

		core systems from clean sources.				
Mon 2:00 PM	Data exfiltration determination (Inject 2.1)	Accepted forensic finding of ~340 GB exfiltration; escalated to breach status under GLBA/state laws; initiated regulator/member notification planning.	Detection & Analysis	Evidence meets definition of unauthorized acquisition of sensitive info; legal clocks start (GLBA).	Treat as encryption-only incident; delay notifications.	Compliance track initiated; counsel drafting notices.
Mon 3:00 PM	Eradication approach	Endorsed complete network rebuild for high assurance; parallel targeted remediation for quick wins (email via cloud, core banking untouched).	Eradication	Multiple backdoors and compromised creds make partial clean-up risky; rebuild reduces reinfection risk.	Only targeted remediation on affected hosts.	Rebuild plan funded; project team mobilized.
Mon 4:30 PM	Regulatory engagement (Inject 2.2)	Notified NCUA within the 72-hour window; prepared FinCEN SAR; coordinated with FBI under counsel guidance.	Detection & Analysis	Proactive regulator communication reduces penalties and improves support; law enforcement provides intel.	Avoid regulator contact until later; minimal disclosure.	NCUA briefed; SAR plan set; FBI liaison established.
Mon 6:00 PM	Access controls hardening	Implemented emergency egress filtering, blocked risky protocols (SMB, RDP) across segments, enforced MFA for privileged accounts.	Containment & Eradication	Reduce attacker movement/persistence during investigation and recovery.	Maintain current posture until rebuild.	Observed drop in suspicious activity; admins using break-glass MFA.

Tue 6:00 AM	Recovery strategy decision (Inject 3.1)	Adopted Hybrid Approach (Option D): decrypt only if technically validated while building new infrastructure; migration to clean environment within 21 days.	Recovery	Balances rapid partial restoration with long-term assurance; mitigates business loss and reinfection.	Pay only; Rebuild only; Restore from 45-day tapes only.	Operations partially restored in 48 hours target; rebuild underway.
Tue 9:00 AM	Decryption validation gate	Set acceptance criteria for any decryptions: sandbox validation, hash comparison, staged restore with integrity checks; no keys applied to production until criteria met.	Containment & Eradication	Prevents corrupt restores and embeds quality control.	Apply decryption directly to production to save time.	Validation process established; no corruption observed in tests.
Tue 2:00 PM	Crisis communications (Inject 3.2)	Escalated to full breach disclosure; released public statement, member letters, internal FAQs; launched call center runbook and credit monitoring offer.	Post-Incident Activity	Public leak requires immediate transparency and support; retain trust via clear actions.	Maintain holding statement; wait 24–48 hours.	Member outreach live within hours; initial sentiment stabilized.
Tue 3:00 PM	Ransom reconsideration post-leak	Affirmed recommendation not to pay increased demand ($3.5M); focus funds on	Post-Incident Activity	Partial publication eliminates guarantee value; payment signals weakness and may not stop further leaks.	Pay to stop remaining publication.	Budget redirected to remediation and member protections.

		member support, rebuild, and security upgrades.				
Tue 5:00 PM	Data reconciliation program	Launched cross-functional team to reconstruct 45 days of records using core banking, audit trails, and member confirmations.	Post-Incident Activity	Ensures data integrity and reduces downstream financial errors.	Skip reconciliation; accept data gaps.	Reconciliation underway; error rate tracking established.
Wed 10:00 AM	Lessons learned session (Inject 4.1)	Conducted structured Five Whys analysis; documented root/systemic causes; prioritized remediation roadmap (segmentation, PAM, SIEM rules, immutable backups).	Post-Incident Activity and ISO 27035 lessons learned phase	Codifies improvements and aligns investment to executive expectations.	Defer lessons until after full recovery (risk repeat incident).	Actionable roadmap approved; owners assigned and PAM and SIEM gaps identified.
Wed 1:00 PM	Security architecture commitments	Approved investments: network segmentation, PAM, EDR+SIEM tuning, email security hardening, backup immutability and air gap.	Post-Incident Activity	Addresses identified gaps and reduced future risk materially.	Minimal changes; patch only affected systems.	Budget allocated; procurement initiated.
Wed 4:00 PM	Final Incident Report preparation (Inject 4.2)	Locked structure and evidence reference; ensured legal review; compiled executive	Post-Incident Activity	Creates defensible record for regulators, board, and insurer.	Produce informal summary only.	Report near final; review cycle scheduled.

		summary and appendices.				