Incident Response Decision Log

FinanceFirst Credit Union Ransomware Simulation

Course: GRC105 - Incident Management and Business Continuity

Group: 2

Week 20 Practical Simulation Lab

Date: December 11, 2025

Chronological Decision Log

Timestamp	Decision Point	Decision Made	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	Rapid mobilization is critical to coordinate actions and maintain chain of custody; establishes governance from minute one	Wait for more data before activation; informal coordination via 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	Stops active encryption and lateral movement while preserving volatile evidence (memory) where feasible	Full enterprise shutdown; keep systems online to observe attacker	No further encryption observed on isolated hosts; business

		interfaces and blocking at switches			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	Early evidence ensures defensible investigation and supports regulatory/legal needs	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 Communications Officer with a concise situational summary and initial actions; paged all CSIRT members	Ensures leadership awareness, legal oversight, and comms readiness while technical team executes containment	Notify only CISO and proceed; broad notification later	Executives aligned; comms lead prepared holding lines; CSIRT fully engaged
Mon 7:10 AM	Network-wide risk assessment	Assessed need for full network shutdown; decided against full shutdown due	Balance containment vs. continuity; maintain critical services on isolated segments;	Immediate full shutdown of corporate network	Branches continue limited operations; risk managed via

		to core banking isolation and member-facing services still operational	avoid cascading business disruption		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	Reduces attacker privilege, limits persistence, and aligns to least privilege principles	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	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	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

		negotiator (no payment authorization)			
Mon 8:15 AM	Communications posture	Directed preparation of member/press holding statements (no confirmation of breach yet); centralized media inquiries via CCO	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	Payment lacks guarantees and increases risk of future targeting; focus on resilience and backups	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-core systems	Establish recovery feasibility without ransom; identify data reconciliation requirements	Assume backups unusable; wait for decryptor	Feasible recovery paths identified; reconciliation effort scoped

		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	Evidence meets definition of unauthorized acquisition of sensitive info; legal clocks start	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)	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	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	Reduce attacker movement/persistence	Maintain current	Observed drop in suspicious

		filtering, blocked risky protocols (SMB, RDP) across segments, enforced MFA for privileged accounts	during investigation and recovery	posture until rebuild	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	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 decryptor: sandbox validation, hash comparison, staged restore with integrity checks; no keys applied to production until criteria met	Prevents corrupt restores and embeds quality control	Apply decryptor 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	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 member support, rebuild, and security upgrades	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
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	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)	Codifies improvements and aligns investment to executive expectations	Defer lessons until after full recovery	Actionable roadmap approved; owners assigned
Wed 1:00 PM	Security architecture commitments	Approved investments: network segmentation, PAM, EDR+SIEM tuning, email security hardening, backup immutability and air gap	Addresses identified gaps and reduces 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 references; ensured legal review; compiled executive	Creates defensible record for regulators, board, and insurer	Produce informal summary only	Report near-final; review cycle scheduled

		summary and appendices			

Editors comments:

ALL IS WRITTEN WELL CONGRATS BUT;

2. Clear Identification of IR Phases

- **Improvement:** Add a column or label indicating the phase for each decision:
    - Preparation
    - Detection & Analysis
    - Containment & Eradication
    - Recovery & Lessons Learned

3. Explicit Link to Injects or Simulation Events

Improvement: all relevant Injects are well identified; but some actions like “Initial incident triage” or “Backup strategy check” might have been prompted by Injects but aren’t labeled. This shows you are responding to simulation cues.

4. Metrics / Impact Assessment

- You mention outcomes qualitatively (e.g., “branches functional for basics”).

Improvement: how about you might consider adding **quantitative or measurable outcomes** where possible:

- Number of systems isolated
- Number of users affected
- Size of data recovered or impacted
- Time to partial restore
  This will give strength to the justification and inturn demonstrate awareness of business impact.

5. Decision Justification Depth

Most rationales are clear and concise well done .

Improvement: For a few decisions, you could please **tie the rationale to standards, frameworks, or policies** (e.g., GLBA, NCUA rules, ISO 27035 principles, least privilege policy). This will show alignment with governance and compliance.

6. Alternatives Consideration

Alternatives are mostly listed, which is great.

Improvement: For a couple of critical decisions (e.g., ransom payment, network rebuild), briefly **note the risks and benefits of each alternative** so as to demonstrates strategic thinking.

7. Post-Incident Learning

You included “Lessons learned session” and “Security architecture commitments” niceeee.

Improvement: Could you also **link each remediation decision back to the original incident causes** explicitly (e.g., “Segment HQ network to prevent future lateral movement like seen on Mon 6:50 AM”).