Cybersecurity Incident
Response & Communications Toolkit

Luminate
LOUISIANA CREDIT UNIONS

Toolkit Contents

1. Immediate Response Checklist

☐ Designate an incident lead and backup contact.
☐ Inventory every affected product, platform, system and service used by the credit union.
☐ Identify data categories stored, processed, shared or accessible through each affected system or third-party relationship.
☐ Document unavailable or impaired services and approved workarounds.
☐ Preserve incident notices, emails, portal messages, call notes, alerts and other material updates.
☐ Review incident-response, business-continuity and vendor-management plans.
☐ Review contracts for incident notification, cooperation, data security, business continuity and indemnification provisions.
☐ Engage legal counsel, compliance, information security and the cyber insurer as appropriate.
☐ Assess NCUA and applicable state reporting obligations based on the credit union's facts; document the decision, rationale and timing.
☐ Brief executive leadership and the board.
☐ Give member-facing employees approved talking points and an escalation contact.
☐ Track member complaints, delayed claims, service failures and suspected phishing/fraud related to the incident.
☐ Prepare member and media communications in advance, but hold compromise-specific language until facts support it.
☐ Monitor authoritative incident sources and retain material updates.

2. If Member Information Is Determined to Be Compromised

First 24 Hours

☐ Activate the incident-response team and executive sponsor.
☐ Engage legal/privacy counsel and notify the cyber insurer as appropriate.
☐ Obtain written, credit-union-specific details from the affected provider or internal incident team: affected systems, data elements, dates, affected population and known remediation.
☐ Determine whether NCUA or other regulator reporting is required and meet applicable deadlines.
☐ Determine which entity is responsible for consumer and regulator notifications.
☐ Preserve evidence and maintain a decision log.
☐ Prepare a board update and approved frontline holding language.

24-72 Hours

☐ Validate the affected member population and exact data elements.
☐ Coordinate required consumer, regulator and Attorney General notices with counsel.
☐ Prepare member notice, FAQ, call-center script, website language and media holding statement.
☐ Confirm whether identity protection, credit monitoring or other remediation will be offered and by whom.
☐ Increase monitoring for phishing, impersonation and fraud patterns tied to the incident.
☐ Establish a process for escalating member complaints and suspected losses.

Ongoing

☐ Update communications as confirmed facts change.
☐ Track service restoration and member-impact metrics.
☐ Retain notices, approvals, board updates, filings and vendor communications.
☐ Complete a post-incident vendor-risk, contract and business-continuity review.
☐ Document lessons learned and update response procedures.

3. Incident Information Request

Request credit-union-specific answers in writing whenever possible.

☐ Was information belonging to our credit union, members or employees accessed, acquired, viewed, altered or exfiltrated?
☐ Which systems, applications or environments associated with our credit union were affected?
☐ What specific categories of information were involved?
☐ What date range of records was potentially affected?
☐ How many individuals associated with our credit union are potentially affected?
☐ Has unauthorized data access or exfiltration been confirmed? If so, when?
☐ Will the affected provider or incident team provide an affected-person list and data-element file specific to our credit union?
☐ What forensic findings can be shared with our credit union, counsel, insurer and regulators?
☐ Who is responsible for consumer, regulator and Attorney General notifications?

☐ Who will provide or fund notices, call-center support, identity protection or credit monitoring, if applicable?
☐ Which services remain unavailable or impaired, and what approved workarounds exist?
☐ What is the current restoration sequence or expected recovery window?
☐ What actions are recommended for our credit union now?
☐ Who is our designated incident contact and escalation contact?
☐ What documentation will be provided for our vendor-management and board records?

4. Executive Leadership Talking Points

- A cybersecurity incident has been identified or reported, and investigation, containment, recovery and restoration efforts are underway.
- Our priorities are continuity of member service, protection of information, regulatory compliance and accurate communication.
- We have inventoried affected dependencies and are documenting operational impacts, data flows and workarounds.
- We are separating confirmed facts from unknowns and will not speculate about member-data compromise.
- We are independently evaluating our regulatory, contractual and insurance obligations based on our credit union's facts.
- We have requested incident-specific information, including affected systems, data elements, populations and restoration status.
- We have prepared communications that can be activated quickly if member information is determined to be affected.
- We are providing frontline staff with approved language and an escalation process.

5. Sample Board Briefing Template

Incident: [CYBERSECURITY INCIDENT / AFFECTED SYSTEM OR PROVIDER]

Date/Time: [DATE/TIME]

Prepared by: [NAME/TITLE]

What is confirmed: [Verified incident information and credit-union-specific facts.]

What remains unknown: [Data impact, population, restoration timing, other open questions.]

Our exposure: [Affected products/services, systems, data flows and operational dependencies.]

Member/operational impact: [Service disruption, complaints, workarounds; clearly state data-impact status.]

Regulatory/legal assessment: [NCUA and applicable state-law reporting decisions, counsel/insurer status.]

Actions completed: [Incident team, vendor requests, monitoring, staff briefing, workarounds.]

Top risks: [Operational, member, regulatory, financial, reputational.]

Decisions/oversight requested: [Any board action or acknowledgement needed.]

Next update: [DATE/TIME OR TRIGGER].

Board Discussion Questions

- What affected products, systems and data flows create exposure for our credit union?
- What facts remain unknown, and who owns obtaining them?
- How significant is the disruption for members and operations?
- Have NCUA, applicable state, contractual and insurance requirements been assessed?
- What will trigger member notification or a change in our public posture?
- How are complaints, fraud concerns and service failures being tracked?
- How sustainable are current workarounds?

6. Member Communications

A. Current Member Note - Service Disruption / Data Impact Unknown

Use when: members need an update now, but the credit union has not confirmed that member information was affected

We are sharing an update regarding a cybersecurity incident affecting [SYSTEM / SERVICE / THIRD-PARTY PROVIDER].

Response and recovery efforts are underway. Some services may remain unavailable or delayed while the incident is investigated and systems are restored.

[Credit Union Name] is monitoring the situation and evaluating the impact on services used by our members. We are not going to speculate about whether member information was affected. If we receive information that requires action by our members, we will communicate directly.

For assistance with [SERVICE/CLAIM], please use [APPROVED WORKAROUND/LINK/CONTACT].

Please remain alert for suspicious emails, text messages or calls referencing this incident. Never provide passwords, PINs or one-time verification codes in response to an unsolicited request.

B. Member Notice - If Member Information Is Determined to Be Compromised

Sample notice can be obtained by reaching out to legal counsel.

7. Employee & Frontline Communications

Internal Employee Update

Team,

A cybersecurity incident affecting [SYSTEM / SERVICE / THIRD-PARTY PROVIDER] has been reported. We are monitoring updates and assessing operational and information-security implications for our credit union.

Please do not speculate with members, partners or on social media about the cause of the incident, the threat actor, or whether information was compromised. Use only approved talking points and escalate questions you cannot answer to [DESIGNATED CONTACT].

Be especially alert for phishing emails, calls or text messages referencing the incident, service disruption, claims or cybersecurity concerns. Verify unusual requests through known channels and report suspicious activity through [INTERNAL PROCESS].

We will provide updates as confirmed information becomes available.

Thank you,
[NAME/TITLE]

Employees Should Not

- Call the event a confirmed member data breach unless that has been established for the credit union.
- Promise that a member's information is safe or unaffected unless verified.
- Guess what data an affected system or provider holds or what information may have been accessed.
- Identify a threat actor or cause based on rumor or unofficial reporting.
- Forward screenshots, social posts or unverified articles as authoritative incident information.
- Promise reimbursement, identity protection, credit monitoring or restoration dates unless authorized.

8. Business Partner Communication

Partner/Vendor Operational Notice

Use when: another partner is affected by an incident-related dependency or workaround

[Credit Union Name] is responding to a cybersecurity incident that has affected availability of certain systems or services.

Our current operational impact involving your organization is [DESCRIBE IMPACT/WORKAROUND]. Please use [TEMPORARY PROCESS/CONTACT] for [FUNCTION].

We are not asking partners to draw conclusions about data compromise beyond confirmed information. If we identify an issue requiring action by your organization, we will contact you directly.

Please direct questions to [CONTACT].

9. Media Inquiry Materials

Media Holding Statement

Use when: a reporter asks about the incident

[Credit Union Name] is aware of a cybersecurity incident affecting [SYSTEM / SERVICE / THIRD-PARTY PROVIDER].

We are monitoring developments and evaluating information regarding any potential impact to our credit union, our members and affected services.

The security and privacy of member information are priorities for our credit union. We will communicate directly with members if confirmed information indicates that additional action is necessary.

Questions regarding technical investigation details should be directed to [DESIGNATED INCIDENT CONTACT / AFFECTED PROVIDER], as appropriate.

Media Guardrails

- Use one designated spokesperson.
- State what is known and what remains under review.
- Do not confirm affected-member counts until validated.
- Do not discuss forensic details, vulnerabilities, security controls or legal strategy.
- Do not repeat unverified claims about ransomware, attackers or stolen data.
- Do not say member information is safe unless verified.

10. Website & Social Copy

Website Alert

Use when: service disruption / awareness

[Credit Union Name] is responding to a cybersecurity incident that has affected availability of certain services. We are monitoring the situation and working to assist members who use affected services.

For help with [SERVICE], contact [PHONE/EMAIL]. Please remain alert for phishing attempts and never share passwords, PINs or verification codes in response to an unsolicited message.

Social Media Holding Post

Use when: a short public update is appropriate

We are aware of a cybersecurity incident affecting services used by our members and are monitoring its impact. For assistance with [SERVICE], contact us at [CONTACT]. Please be cautious of unsolicited messages referencing the incident and never share account credentials or verification codes.

11. Member FAQ

- **What is happening?**

    - A cybersecurity incident has affected [SYSTEM / SERVICE / THIRD-PARTY PROVIDER]. Investigation, containment, recovery and service-restoration efforts are underway.
- **Does this mean my credit union was hacked?**
    - The credit union should explain whether the incident affects its own systems, a third-party provider or both, based on verified monitoring and investigation results.
- **Was my personal information compromised?**
    - Do not answer yes or no unless verified. State the current confirmed status and explain that affected members will be contacted if action is required.
- Why can't I access a service?
    - Explain the known service disruption and provide the current approved workaround or contact process.
- **Should I change my online banking password?**
    - Do not imply credit-union credentials were exposed without evidence. Encourage strong, unique passwords and phishing awareness; provide additional steps if facts warrant them.
- **Who will notify me if my data was involved?**
    - Explain the notification process once responsibility among the credit union, affected provider and other parties is confirmed.
- **Where can I get updates?**
    - Direct members to the credit union's designated resource page/contact and, when appropriate, the affected provider's official incident resource page.