State of New Hampshire

Data Breach Playbook

February 2024

Revision List

Table 1: Plan Revisions

Name	Title	Content Revised	Date of Revisions
NuHarbor Security	Information Assurance Team	Initial Draft	Oct 2023
NuHarbor Security	Information Assurance Team	Revisions based on comments matrix.	Oct 2023
Doug Schelb	DCISO	Edited/approved final draft	Jan 2024
Doug Schelb	DCISO	Added requirement to request log retention in “Key Communications” section	Nov 2024

Contents

Introduction

This playbook is a Cyber Incident Response Plan (CIRP) supplemental procedure and should be used in conjunction with the CIRP to assist in responding to cyber incidents involving data breach or data loss.

This document is aligned with the National Institute of Standards and Technology (NIST) Cybersecurity Framework and follows the four step NIST Incident Response Framework. Specifically, this document addresses response steps two through four. Preparatory actions (Step one) are addressed in the CIRP.

1. Preparation (addressed in CIRP)
2. Detection & Analysis
3. Containment, Eradication, & Recovery
4. Post Incident Activities

This playbook is not intended to be a checklist for response actions. The variance in cyber incidents and associated response requirements is too great to develop prescriptive guidance. Instead, this playbook is designed to serve as a decision support tool to guide incident response by focusing on key questions, considerations, and communications for the incident response team (IRT).

Detection & Analysis

The SoNH Teams will be alerted to a data breach in one of the following ways:

- Alert from various Data Loss Prevention tools that are in place throughout the State.
- Inadvertent posting/publishing of information on a State-operated websites (by a State employee or vendor).
- Malicious/intentional posting of information by a State employee on a State or other website.
- Misconfiguration of a State system which results in information being posted/released/etc.
- Notification by a member of the public or a contracted 3rd Party vendor.

Questions to ask during this phase, regardless of method of identification include:

- What is the scope of this incident?
- Which systems are impacted?
    - Evaluate system backups.
- Has sensitive data been impacted (PII, PHI, FTI, PCI, etc.)?
- How is this incident impacting the public?

As data owners, individual Agencies have specific responsibilities when a suspected data breach occurs. Agencies will have a significant role in the Analysis portion of this phase and will determine the initial extent of the breach and quantifying and qualifying the impact of the data loss or compromise.

The IRT will assist Agencies in conducting an in-depth analysis of all data sources to determine all systems that may have been involved with a breach and will begin Containment action in parallel if possible. If necessary, forensics teams should be engaged for evidence collection and preservation prior to the commencement of Eradication actions.

***Key Considerations*:**

- Where is the location of the compromise?
    - State Enterprise network?
    - Agency-specific application?
- Is there any indication the breach is the result of an insider threat?
- Does the breach involve State government data?
    - Is there more than one Agency involved?
    - Are there interagency data sharing agreements in place?
- How many users are impacted by the compromise?
    - Is the scope large enough to activate ESF-17?

If the breach involves a contracted 3rd Party vendor, the Agency holding the contract will assume the primary responsibility of liaising with service providers/vendors to assist in the Analysis phase.

If sensitive data is involved in the compromise, Agencies must be prepared to immediately identify and address any specific federal or other regulatory reporting requirements.

***Key Considerations*:**

- Is a State-contracted 3rd Party vendor involved?
    - Which Agency has lead for vendor contact/coordination (contract owner)
- Is sensitive data involved (e.g., PII, PHI, PCI, etc.)?
    - Are there specific regulatory reporting requirements for the data type?
- What specific regulatory reporting requirements are associated with the data class/type?
    - What are the timelines?

If citizen data is suspected to have been publicly exposed, there must be a focus on notifying citizens in a timely manner, even while the Containment effort is ongoing. Agencies have requirements to notify citizens and state employees within a specific time (Agency dependent).

***Key Considerations*:**

- What are the public reporting requirements?
- Is a public affairs strategy necessary? Who has lead?
    - Is the Joint Information Center activated in the EOC? If not, should it be activated?

The Dept. of Justice Consumer Protection & Antitrust Bureau plays a central role in response activities when a data breach is suspected, and they should be contacted early in this phase. The department will advise Agencies and response teams on legal considerations to include evidence collection, as well as any coordination necessary with Federal, State, or local law enforcement agencies as part of the response.

***Key Considerations*:**

- What evidence (digital and physical) can be collected?
    - Identifying information (e.g., the location, serial number, model number, hostname, media access control (MAC) addresses, and IP addresses of a device).
    - System logs
    - Name, title, and phone number of individuals involved in evidence collection.
    - Time(s) and date(s) of evidence handling.
- Is there a requirement for technical forensics?
    - DOIT has a cybersecurity forensics firm on retainer to support incident response.
- Is there evidence of criminal activity? Is law enforcement involvement necessary?

Key Communications:

- Agencies and CIO coordinate with DOS/HSEM to notify NH Office of the Attorney General assigned counsel of suspected breach.
- Agencies contact NH Department of Justice Consumer Protection & Antitrust Bureau ***within 5 days*** if citizen data is involved in the breach.
- NH CIC contact CrowdStrike Falcon Complete team to request retention and export of all CrowdStrike system logs for the duration of the event and through all phases of incident response.
- CISO contact cybersecurity services retainer for Forensics support if necessary.

Containment, Eradication & Recovery

After the scope of the incident is determined, the incident response team will need to determine if the event is contained or escalating. If an incident is not contained, the following NIST SP 800-61 criteria should be considered while developing an appropriate strategy:

- Need for evidence preservation.
- Service availability (e.g., network connectivity, services provided to external parties).
- Time and resources needed to implement the strategy.
- Effectiveness of the strategy (e.g., partial containment, full containment).
    - Testing should occur to verify if containment efforts have been successful.
- Duration of the solution (e.g., emergency workaround to be removed in four hours, temporary workaround to be removed in two weeks, permanent solution).

Steps for eradication may include the following:

- Disabling breached user accounts.
- Identifying and mitigating vulnerabilities that were exploited.
- Identifying all affected hosts for proper remediation.

Strategies for recovering systems that have been affected by a breach may include the following:

- Enhancing base configurations of all DLP systems in use.
- Restoring systems from clean backups.
- Rebuilding systems from scratch.
- Installing patches.
- Changing passwords.
- Tightening network perimeter security.

Key Considerations:

- Ensure all required forensic actions have been completed and all required data saved prior to beginning eradication.
- Ensure all required evidence collection and preservation have been completed prior to beginning eradication.
- Ensure all associated system logs are preserved, archived, and handled appropriately for the given classification.

Post Incident Activities

Per the CIRP, NH-CIC is responsible for producing after-action reports for all cyber incidents with the assistance of the IRT members and their parent organizations. NH-CIC will also develop recommendations for updates to this playbook based on lessons-learned developed during post incident activities.

Key Considerations:

The after-action phase of incident response should include addressing the following questions:

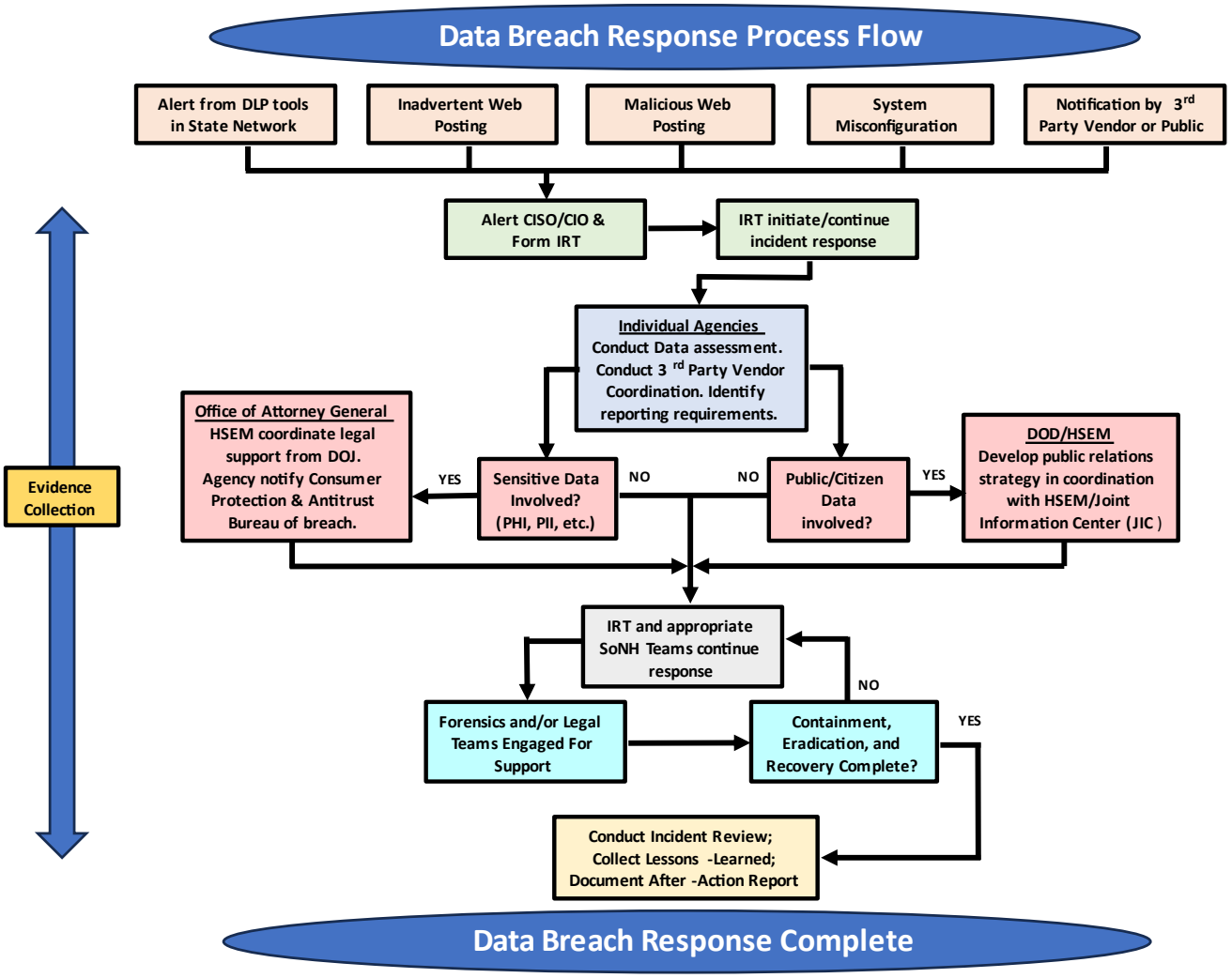
- Exactly what happened, and at what times?
- How well did staff and management perform in handling the incident? Were the documented procedures followed? Were they adequate?
- What information was needed sooner?
- Were any steps or actions taken that might have inhibited the recovery?
- What would the staff and management do differently the next time a similar incident occurs?
- How could information sharing with other organizations have been improved?
- What corrective actions can prevent similar incidents in the future?
- What precursors or indicators should be watched for in the future to detect similar incidents?
- What additional tools or resources are needed to detect, analyze, and mitigate future incidents?

Roles and Responsibilities

The following roles and responsibilities may be performed during a data breach to effectively respond to and recover from an incident. The incident response team (IRT) membership will be scenario specific but will generally include members from these parties and organizations.

Party	Response Roles and Responsibilities
NH State Agencies	• Provide Agency subject matter experts to participate in IRT. • Provide guidance on incident impact to Agency operations and delivery of critical government services. • Activate continuity of operations and/or data classification protocols as required.
NH-CIC	• Serve as core members of the IRT. • Provide technical oversight and direction of all IRT response actions throughout all incident response phases. • Facilitate information sharing between State partners. • Direct Post Incident Activities to include after action reporting.
User Services Division (USD)	• Provide technical experts to serve as core members of the IRT. • Manage response tasks associated with messaging, email, data, and endpoint security and identity management (IAM).
Infrastructure and Operations Division (IOD)	• Provide technical experts to serve as core members of the IRT. • Manage response tasks associated with network, database, web services, and telecommunications security. • Direct Continuity of Operations (COOP) and Disaster Recovery (DR) actions for Enterprise IT capabilities. • Advise State Agencies on COOP/DR actions for non-Enterprise capabilities.
Business Relationship Management Division (BRMD)	• Assist with identifying incident impact to Agency operations and delivery of critical government services. • Manage coordination between State agency(s) and DOIT Divisions as required.
NH Department of Justice	• Advise Agencies (data owner) on legal reporting, compliance, and evidence collection requirements associated with data loss or compromise. • Advise Agencies on contract protections for 3rd Party vendor data incidents. • Advise Agencies on Federal Law Enforcement coordination. • Serve as advocate for New Hampshire citizens' rights (Consumer Protection & Antitrust Bureau) associated with a data breach.

Flow Chart


Data Breach Response Process Flow
Alert from DLP tools in State Network
Inadvertent Web Posting
Malicious Web Posting
System Misconfiguration
Notification by 3rd Party Vendor or Public
Alert CISO/CIO & Form IRT
IRT initiate/continue incident response
Individual Agencies
Conduct Data assessment. Conduct 3 rd Party Vendor Coordination. Identify reporting requirements.
Office of Attorney General
HSEM coordinate legal support from DOJ. Agency notify Consumer Protection & Antitrust Bureau of breach.
YES
Sensitive Data Involved? (PHI, PII, etc.)
NO
NO
Public/Citizen Data involved?
YES
DOD/HSEM
Develop public relations strategy in coordination with HSEM/Joint Information Center (JIC)
Evidence Collection
IRT and appropriate SoNH Teams continue response
NO
Forensics and/or Legal Teams Engaged For Support
Containment, Eradication, and Recovery Complete?
YES
Conduct Incident Review; Collect Lessons -Learned; Document After -Action Report
Data Breach Response Complete