State of New Hampshire

Ransomware Playbook

February 2024

Revision List

Table 1: Plan Revisions

Name	Title	Content Revised	Date of Revisions
NuHarbor Security	Information Assurance Team	Initial Draft	06 Oct 2023
NuHarbor Security	Information Assurance Team	Revisions based on comments matrix.	13 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 ransomware.

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 Team will be alerted to ransomware in one of the following ways:

1. An endpoint with a Managed Detection and Response (MDR) agent installed sends an alert.
2. An endpoint without an MDR agent installed alerts that there is ransomware.
3. Another State agency is impacted with ransomware and reports the incident.
4. A third-party vendor is impacted with ransomware and reports the incident.
5. An employee reports that they are experiencing ransomware on their device.
6. Direct communication to someone within the SoNH team(s) from a threat actor.

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

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

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?
- Does the breach involve State government data?
    - Is there more than one Agency involved?
    - Are there interagency data sharing agreements in place?
- What is the business impact of the malware?
    - Has the Ransomware encrypted any data?
- Is there evidence of lateral movement of the malware?
- Have the Ransomware actors directly contacted anyone involved in the breach?
- 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.

It is important to determine whether the incident involves ***data encryption*** (i.e., state data remains in place but is not accessible) ***and/or data exfiltration*** (theft of data). For the former, mitigating business interruption will a primary concern. For the latter case, data owners must be prepared to shift to a data breach response if sensitive data is involved in the compromise.

Key Consideration:

- Is data exfiltration of sensitive data suspected or confirmed?
    - If so, consult the Data Breach Playbook for guidance on Agency regulatory Federal, State, and consumer reporting requirements for sensitive data breach.

Ransomware is considered criminal activity, particularly in the event of an associated ransom demand. State and potentially Federal law enforcement agencies should be notified as soon as Ransomware is confirmed during this phase. Law enforcement guidance on evidence collection should be followed throughout all response phases.

Key Consideration:

- Is there evidence of criminal activity? Is law enforcement involvement necessary?
- 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?
- Is ransom payment a consideration?

In addition to law enforcement, Agency leaders should consult with the Office of the Attorney General if ransom payment is a consideration. If ransom payment is considered, the details the transaction and any associated communication with malware actors must in careful coordination with law enforcement.

DoIT has an Incident Response firm on retainer that is comprised of personnel who are experienced with both forensic investigations and (ransom) negotiation support. The CISO can arrange for activation of this support as soon as the need is identified.

Key Communications:

- Agencies and CIO coordinate with DOS/HSEM to notify State Law Enforcement of criminal Ransomware activity.
- Agencies and CIO coordinate with DOS/HSEM to notify NH Office of the Attorney General assigned counsel of suspected malware incident.
- Agencies and CIO coordinate with DOS/HSEM to notify Federal response partners (e.g., FBI, Secret Service).
- 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:

- Deleting all malware and removing all ransomware from systems.
- Disabling breached user accounts.
- Identifying and mitigating vulnerabilities that were exploited.
- Identifying all affected hosts for proper remediation.
- Test to ensure that the ransomware is completely eradicated.

Please note that eradication may take place in conjunction with recovery, so these two steps may happen simultaneously.

Strategies for system recovery should consider the following:

- Restoring systems from clean backups.
- Rebuilding systems from scratch.
- Replacing compromised files with clean versions.
- 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:

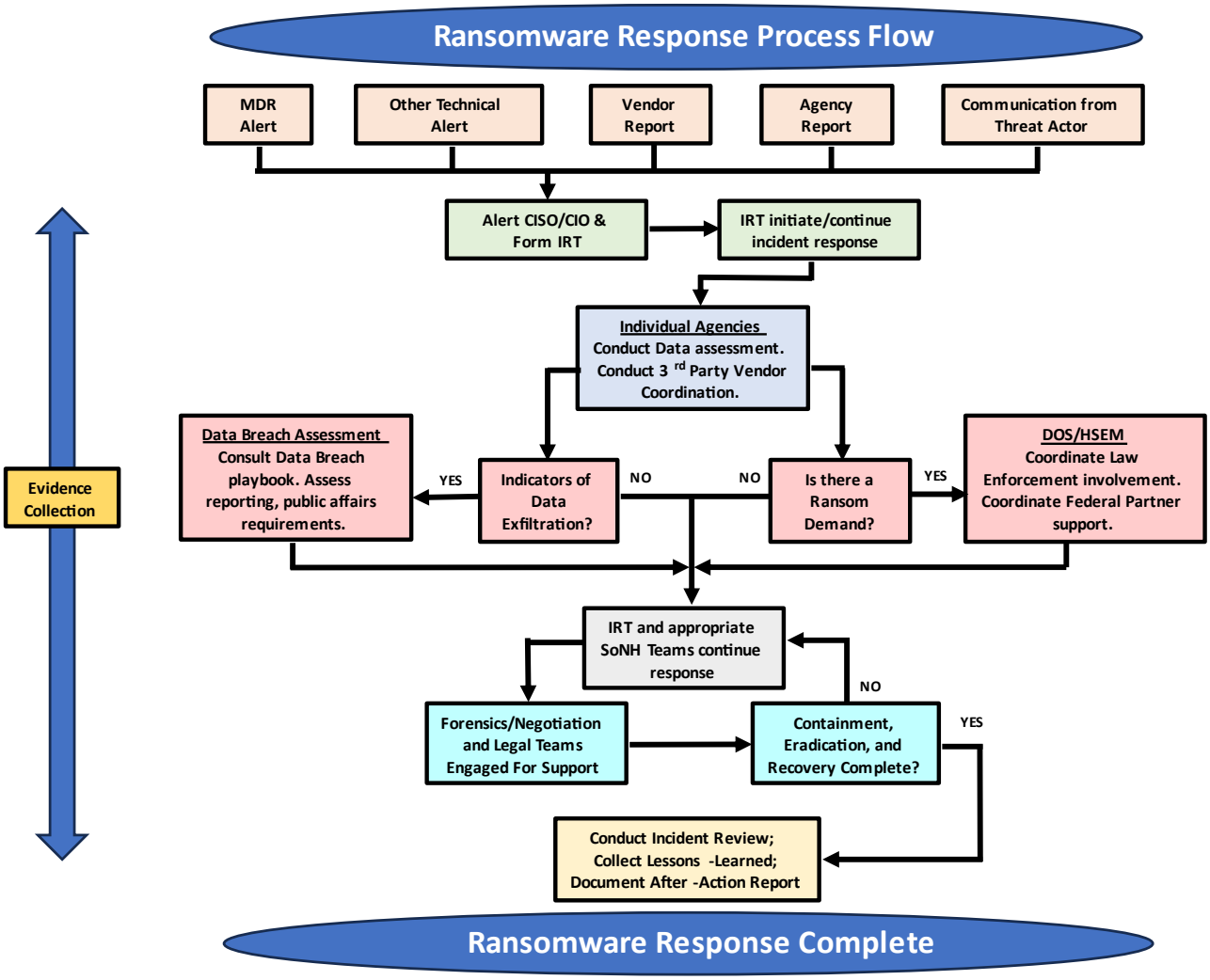
- Exactly what happened, and at what times?
- How well did staff and management perform in handling the incident? Were the documented procedures followed? Were they adequate?
- What information was needed sooner?
- Were any steps or actions taken that might have inhibited the recovery?
- What would the 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 ransomware attack to effectively respond to and recover from the 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.
SoNH Department of Justice	• Advise Agencies on Federal Law Enforcement coordination. • Advise Agencies on ransomware negotiation, as necessary. • 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 incidents. • Serve as advocate for New Hampshire citizens' rights (Consumer Protection & Antitrust Bureau) associated with a data breach.

Flow Chart


Ransomware Response Process Flow
MDR Alert
Other Technical Alert
Vendor Report
Agency Report
Communication from Threat Actor
Alert CISO/CIO & Form IRT
IRT initiate/continue incident response
Individual Agencies
Conduct Data assessment.
Conduct 3 rd Party Vendor Coordination.
Data Breach Assessment
Consult Data Breach playbook. Assess reporting, public affairs requirements.
YES
Indicators of Data Exfiltration?
NO
NO
Is there a Ransom Demand?
YES
DOS/HSEM
Coordinate Law Enforcement involvement. Coordinate Federal Partner support.
Evidence Collection
IRT and appropriate SoNH Teams continue response
NO
Forensics/Negotiation and Legal Teams Engaged For Support
Containment, Eradication, and Recovery Complete?
YES
Conduct Incident Review; Collect Lessons -Learned; Document After -Action Report
Ransomware Response Complete