State of New Hampshire

Physical Security 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	Revised draft based on comments matrix	Nov 2023
Doug Schelb	DCISO	Reviewed/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 physical security incidents with a cyber component or impact.

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

Identification of a physical security incident may not be obvious to responders. Physical security incidents may at first appear to be something unrelated, such as an unexplained network outage or degradation with no obvious virtual cause. Other times, a physical security incident may have unforeseen cyber implications, such as a loss of access control to a building resulting in malicious access to critical network equipment. In any case involving physical security, the potential for cyber impacts must be considered, and vice-versa.

The State of New Hampshire (SoNH) Teams may be alerted to a physical security incident in one of the following ways:

- Alert of anomalous activity on card reader or camera system.
- Staff complaints and visual signs of tampering.
- Another incident type develops into a physical security incident.

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?

Key Considerations:

- At the location of the incident, who is responsible for physical security?
    - Date Center, building, room, etc.
- What was the scope of the incident?
    - Is it just one part of the building or was the entire space impacted?
- Is the event an infrastructure issue or is it a physical security incident?
    - Was there scheduled building maintenance?
    - Are there environmental causes?
    - Can uncontrolled access to critical cyber infrastructure be ruled out?
- Are there active life or safety risks associated with the incident?
    - Criminal activity, unauthorized personnel in controlled spaces, etc.
- What badge access and camera systems are used and who can be contacted about them?
- Can a physical inspection of the space be completed?
    - Are there visible signs of tampering?
    - Does anything appear to be stolen, missing, or out of place?
    - Was there possible access to digital systems?
- Does the physical security breach have a potential cybersecurity impact?
- What evidence (digital and physical) can be collected?
    - Camera logs.
    - Badge access logs.
    - Destroyed or damaged infrastructure or hardware.
    - System logs
    - Name, title, and phone number of individuals involved in evidence collection.
    - Time(s) and date(s) of evidence handling.

Investigating a physical security incident may call for collaboration across multiple organizations, including the police or other non-state security officials. If the incident involves potential criminal activity or physical access to State government buildings by unauthorized personnel, law enforcement should be engaged by contacting the Emergency Operations Center (EOC) and Department of Safety/Homeland Security and Emergency Management (HSEM). If the incident involves threats to life or safety, a 911 call should be placed followed by notification to the EOC.

Key Communications:

- Notify Department of Safety/Homeland Security and Emergency Management (HSEM) of incidents requiring law enforcement assistance or support.
- 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.
- ***Call 911 if there is ongoing threat to life or safety of State personnel***.

Containment, Eradication, & Recovery

After the scope of the incident is identified, the IRT will need to determine if the event is contained or escalating. For a physical security incident, this could mean the building is not secured or in the event of a disaster, the environmental event is still ongoing. If an incident is not contained, the following NIST SP 800-61 criteria should be considered while developing an appropriate strategy:

- Potential damage to and theft of resources.
- 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).

Key Considerations:

- Is there an ongoing life/safety or emergency issue? Are unauthorized personnel in the building?
    - Coordination of incident response with law enforcement may be necessary.
- Consider the implications of the incident to both physical *and* cyber security during containment.

For example: if the server room door was propped open, and a cable appears to be unplugged. The containment would include both securing the physical room and replacing badges as needed, but also involve scanning the network to ensure that no unauthorized connections have been made.

Due to the wide array of physical security scenarios that are possible, eradication and recovery will look different in each case. Incident eradication may involve both physical and virtual steps, thus it is crucial to understand the full scope of impact. Also, eradication may take place in conjunction with recovery, so these two phases may occur simultaneously.

Key Considerations:

- With the types of devices or assets accessed, can these systems be recovered?
- Were any physical items stolen?
- Are there any damaged cameras, card readers, or entry points that need to be replaced or fixed?
- Did the intruder get onto the network?
- Any access gained to digital systems should be removed, and a final scan should take place to ensure the adversary did not gain any other access.
- If back-up systems and facilities needed to be used to aid in business continuity, rollback to primary systems should take place.

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:

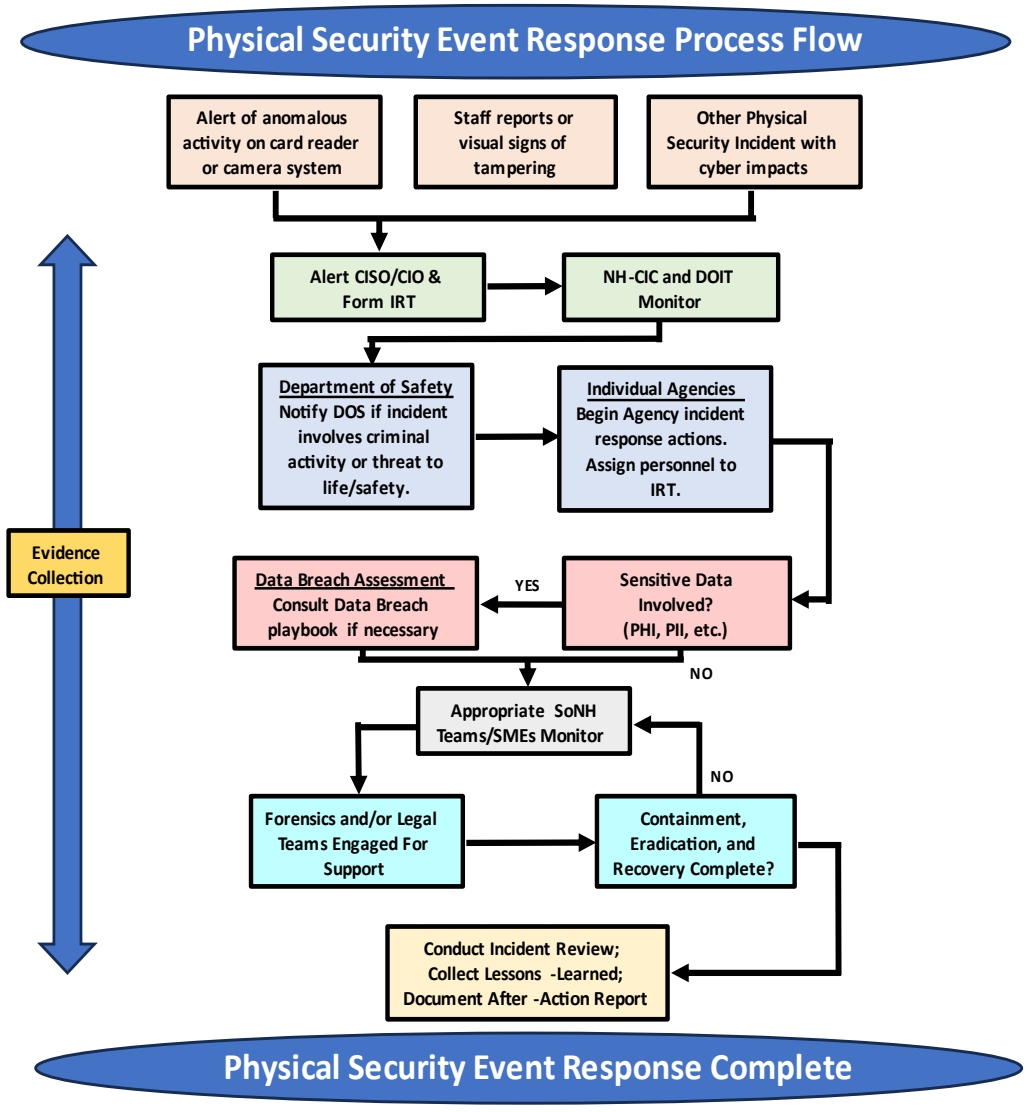
- Exactly what happened, and at what times?
- How well did staff and management perform in handling the incident? Were the documented procedures followed? Were they adequate?
- What information was needed sooner?
- Were any steps or actions taken that might have inhibited the recovery?
- What would the 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 physical security incident 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.

Flow Chart


Physical Security Event Response Process Flow
Alert of anomalous activity on card reader or camera system
Staff reports or visual signs of tampering
Other Physical Security Incident with cyber impacts
Alert CISO/CIO & Form IRT
NH-CIC and DOIT Monitor
Department of Safety
Notify DOS if incident involves criminal activity or threat to life/safety.
Individual Agencies
Begin Agency incident response actions. Assign personnel to IRT.
Evidence Collection
Data Breach Assessment
Consult Data Breach playbook if necessary
YES
Sensitive Data Involved? (PHI, PII, etc.)
NO
Appropriate SoNH Teams/SMEs Monitor
NO
Forensics and/or Legal Teams Engaged For Support
Containment, Eradication, and Recovery Complete?
Conduct Incident Review; Collect Lessons -Learned; Document After -Action Report
Physical Security Event Response Complete