OFFICE OF Information Technology

Information Security Incident & Breach Handling Procedure

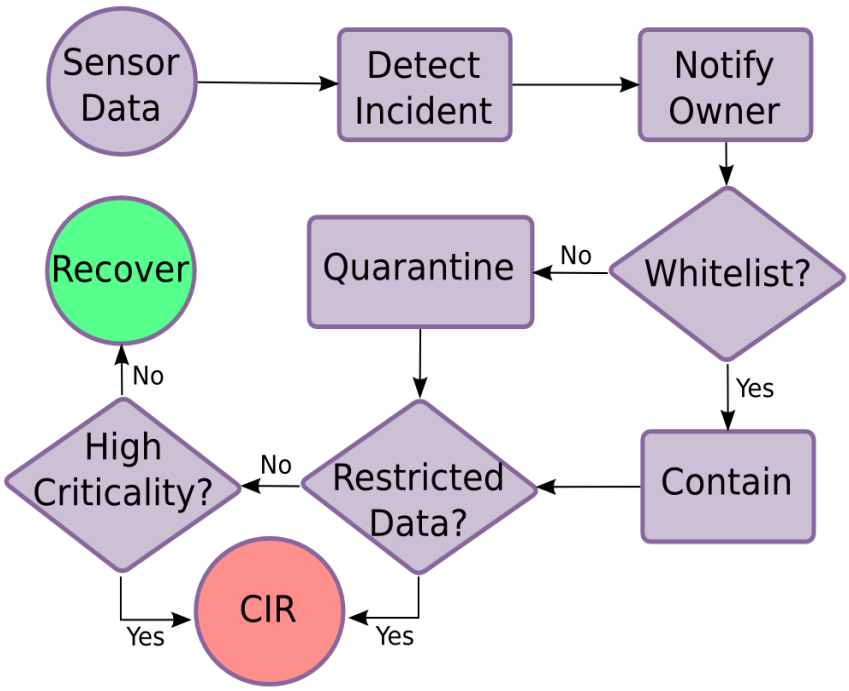
1. Introduction

An information technology (IT) security incident is an event involving an IT resource at University of Alaska (UA) that has an adverse effect on the confidentiality, integrity, or availability of that resource or connected resources. Prompt detection and appropriate handling of these security incidents is necessary to protect UA's information technology assets.

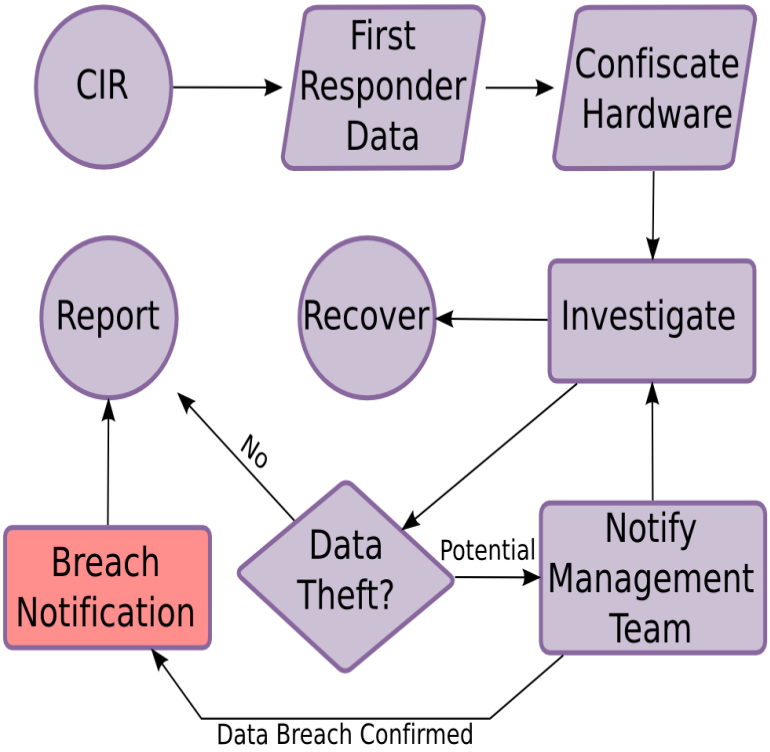
The purpose of this *Information Security Incident & Breach Handling Procedure* is to provide general guidance to UA staff and supervisors who manage IT resources to enable quick and efficient recovery from security incidents; respond in a systematic manner to incidents and carry out all necessary steps to correctly handle an incident; prevent or minimize disruption of critical computing services; and minimize loss or theft of sensitive or mission critical information. The sections below describe: **1) how to notify the appropriate persons upon discovery of an incident; 2) how to handle and recover from an incident in a manner appropriate to the type of incident; 3) establish reporting format and evidence retention procedures.** This document provides an overview of the process; detailed technical procedures can be found in OIT internal documentation. Any questions about this procedure should be directed to OIT Security Administration, security@alaska.edu.

2. Overview of Workflow

The flow-charts below are a visual depiction of the procedure described below. This first chart covers the general incident response procedure followed by the incident handler:



If Restricted Data (including Protected Health Information) is present on the compromised system, the Critical Incident Response (CIR) is followed. The CIR is summarized below.



3. Overview of Roles

a. Incident Handler: This role is filled by IT security staff from OIT Security Administration.
b. System Administrator: This role is filled by the technical staff responsible for deploying and maintaining the system at risk. Also referred to as a "first responder" in the context of this process.
c. System Owner: This role is filled by the staff member or management member who has responsibility for the business function performed by the system.
d. Network Operations: This role is filled the technical staff responsible for network infrastructure at the site housing the system at risk. OIT Network Operations and Engineering.
e. Security Oversight Officer: This role is filled by the Chief Information Security Officer (CISO).
f. HIPAA Privacy Officer and HIPAA EPHI Security Officer: These roles are filled at each HIPAA Covered Component (campus, program, health plan, etc) by designated individuals. At the University level, the Chief Human Resource Officer is the HIPAA Privacy Officer, and the Chief Information Technology Officer and Chief IT Officer for each respective university.
g. PCI Compliance Manager: This role is filled by the person responsible for overseeing UA's PCI compliance program.

4. Identification

The identification phase of incident response has as its goal the discovery of potential security incidents and the assembly of an incident response team that can effectively contain and mitigate the incident:

a. **Identify** a potential incident. The incident handler may do so through monitoring of security sensors. System owners or system administrators may do so by observing suspicious system behavior. Any member of the University community may identify a potential security incident though external complaint/notification, or other knowledge of impermissible use or

disclosure of Restricted Data.

b. **Notify**: Members of the University community that suspect an IT system has been accessed without authorization must immediately report the situation to security@alaska.edu. Once the incident handler is aware of a potential incident, s/he will alert local system administrators.

c. **Quarantine**: The incident handler will quarantine compromised hosts at the time of notification unless they are on the Quarantine Whitelist. If they are on the Quarantine Whitelist, the incident handler will promptly reach out to the system administrator or system owner to create plan to contain the incident. Note that the incident handler may notify on suspicious behavior when s/he is not confident of a compromise; in these cases they do not quarantine the host immediately, but wait 24-48 hours and quarantine only if the registered contact is unresponsive.

5. Verification

This phase also precedes CIR, and has the primary goal of confirming that the compromise is genuine and presents sufficient risk to engage the CIR process:

a. **Classify**: The CIR must be initiated if...
   i. The system owner or system administrator indicates that the system is a high-criticality asset according to the *Reference for Data and System Classification*.
   ii. OR the system owner or system administrator asserts that the system contains Restricted Data as defined by the *Data Classification Table* (https://www.alaska.edu/records/dataclass/).
   iii. OR someone of appropriate authority (OIT Chief Information Technology Officer or higher) determines that the system poses a unique risk that warrants investigation.

b. **Verify**: The CIR process should be initiated ONLY if...
   i. The incident handler verifies that the triggering alert is not a false positive. The incident handler will double-check the triggering alert, and correlate it against other alerting systems when possible.
   ii. AND the type of data or system at risk is verified to be of an appropriate classification, as determined above. The system owner or system administrator should provide a detailed description of the data at risk, including approximate numbers of unique data elements at risk, and the number, location, and type of files it is stored in.

The order of the steps above can vary from incident to incident, but for the CIR process to be initiated the criticality of the asset must be confirmed, and it must be confirmed that the triggering event is not a false positive. In cases where the CIR process is not required, the incident handler can resolve the case as follows:

c. Obtain a written (e-mail is acceptable and preferred) statement from the system owner or system administrator documenting that the system has no Restricted Data and is not a high-criticality asset.

d. Obtain a written statement from the system owner or system administrator that the system has been reinstalled or otherwise effectively remediated before quarantine is lifted.

e. For incidents involving an unauthorized wireless access point, obtain a written statement that the access point has been disabled.

6. Containment

The containment phase represents the beginning of the CIR workflow and has the following goals:

a. If the host cannot immediately be removed from the network, the incident handler will **initiate a full-content network dump** to monitor the attacker's activities and to determine whether relevant data is leaking during the investigation.

b. **Eliminate attacker access:** Whenever possible, this is done via the incident handler performing network quarantine at the time of detection AND by the system administrator unplugging the network cable. In rare cases, the incident handler may request that network operations staff implement a port-block to eliminate attacker access. In cases where the impact of system downtime is very high, the incident handler will work with system

administrators to determine the level of attacker privilege and eliminate their access safely.

c. The incident handler will collect data from system administrators in order to quickly **assess the scope of the incident**, including:
    i. Preliminary list of compromised systems
    ii. Preliminary list of storage media that may contain evidence
    iii. Preliminary attack timeline based on initially available evidence
d. **Preserve forensic evidence**:
    i. System administrators will capture **first responder data** if the system is turned on. The incident handler will provide instructions for capturing this data to the individual performing that task.
    ii. The incident handler will capture disk images for all media that are suspected of containing evidence, including external hard drives and flash drives. System administrators will deliver the system to OIT Security Administration after the first responder data is captured; disk imaging and analysis will occur at OIT Security Administration. The system owner should expect to have it returned within 5 business days.
    iii. The incident handler will dump network flow data and other sensor data for the system.
    iv. The incident handler will create an **analysis plan to guide** the next phase of the investigation.

This is the most time-sensitive and also the most contextually dependent phase of the investigation. The actions that need to be taken will depend on the uptime requirements of the compromised system, the suspected level of attacker privilege, the nature and quantity of data at risk, and the suspected profile of the attacker. The most important goals of this phase are to eliminate attacker access to the system(s) as quickly as possible and to preserve evidence for later analysis.

Additionally, this is the phase where the incident handler works most closely with system administrators and system owners. During this phase they are expected to take instruction from the incident handler and perform on-site activities such as attacker containment, gathering first response data, and delivering the system to OIT Security Administration in cases where host-based analysis is required.

7. Analysis

The analysis phase is where in-depth investigation of the available network-based and host-based evidence occurs. The primary goal of analysis is to establish whether there is reasonable belief that the attacker(s) successfully accessed Restricted Data on the compromised system. Secondary goals are to generate an attack timeline and ascertain the attackers' actions. All analysis steps are primarily driven by the incident handler, who coordinates communications between other stakeholders, including system owners, system administrators, and relevant compliance officers. Questions which are relevant to making a determination about whether data was accessed without authorization include:

a. **Suspicious Network Traffic**: Is there any suspicious or unaccounted for network traffic that may indicate data exfiltration occurred?
b. **Attacker Access to Data**: Did attackers have privileges to access the data or was the data encrypted in a way that would have prevented reading?
c. **Evidence that Data was Accessed**: Are file access audit logs available or are file system mactimes intact that show whether the files have been accessed post-compromise?
d. **Length of Compromise**: How long was the host compromised and online?
e. **Method of Attack**: Was a human involved in executing the attack or was an automated "drive-by" attack suite employed? Did the tools found have capabilities useful in finding or exfiltrating data?
f. **Attacker Profile**: Is there any indication that the attackers were data-thieves or motivated by different goals?

If, during the analysis, it appears likely that Restricted Data has been exposed, the incident handler should consult with the CITO or other appropriate OIT executives to determine the appropriate

University Officials to inform regarding the situation. Those individuals may include, but are not limited to: the Vice President for Academic Affairs, the Vice President for Finance and Administration, the Chief Human Resource Officer, the Chief Risk Officer and the Office of General Counsel. In the case of PHI/EPHI, this will include the HIPAA EPHI Security Officer and Privacy Officer at the relevant Covered Component. In the case of payment card data, this will include the PCI Compliance Manager.

At the conclusion of the analysis, but before the final report is written, a peer review should be requested of the other OIT Security Administration technical staff. Complete the write-up of the notes, including conclusions, and archive processed source materials (e.g., grep-results, file-timelines, and filtered flow-records). The peer review may result in some issues that must be addressed and some issues that may optionally be addressed. All recommendations should be resolved or acknowledged and deferred. The incident handler's role is to determine, from a technical perspective, whether there is a reasonable belief that Restricted Data, including PHI/EPHI, was available to unauthorized persons. The determination of whether the circumstances warrant a breach notification will be made jointly by the University Officials convened upon review of the results of the investigation, the technical opinion of OIT Security Administration , and the advice of the Office of General Counsel.

In addition, in the event of a breach of PHI/EPHI, the HIPAA Privacy Officer and, as necessary, the EPHI Security Officer at the affected Covered Component in conjunction with OIT Security Administration will conduct a risk assessment of the impermissible use or disclosure of PHI/EPHI at the Covered Component to determine if the impermissible use or disclosure compromises the security or privacy of the Protected Health Information and Electronic Protected Health Information (PHI/EPHI) and poses a significant risk of financial, reputational or other harm to the individual. The risk assessment will take into account the following factors to determine whether there is a significant risk of harm to the individual:

i. nature of the data elements breached,
ii. likelihood the information is accessible and usable,
iii. likelihood the breach may lead to harm, and
iv. ability to mitigate the risk of harm.

The burden of determining whether there is a risk of harm resulting from an impermissible use or disclosure belongs to the affected HIPAA Covered Component. In order to make this determination, the Privacy Officer at the affected HIPAA Covered Component will document each impermissible use and disclosure and the risk assessment conducted for each. The HIPAA Privacy Officer will be responsible for conducting the risk assessment, documenting the results of the assessment and whether the impermissible use or disclosure poses a significant risk of financial, reputational or other harm to the individual whose PHI/EPHI was compromised.

8. Recovery

The primary goal of the recovery phase is to restore the compromised host to its normal business function in a safe manner.

a. The system administrators will remediate the immediate compromise and restore the host to normal function. This is most often performed by reinstalling the compromised host; although if the investigation confirms that the attacker did not have root/administrator access other remediation plans may be effective.
b. The system administrators will make short-term system, application, and business process changes to prevent further compromise and reduce operating risk.

9. Reporting

The final report serves two main purposes. First, a recommendation is made to the Office of General Counsel and relevant compliance officers as to whether the incident handler and the responsible

officials feel there is a reasonable belief that PHI/EPHI or other Restricted Data was disclosed without authorization and that there is a significant risk of harm to the individual and notification should be provided. The report must be made in sufficient time to allow notification, if appropriate, within any legally-mandated time period. In the case of HIPAA/HITECH, that will be within 60 days. Second, a series of mid-term and long-term recommendations are made to the owners of the compromised system, including responsible management, suggesting improvements in technology or business process that could reduce operating risk in the future.

a. The incident handler will draft the final report after the investigation is complete. Preliminary reports should be avoided whenever possible since working conclusions can change substantially through the course of an investigation.
b. After the draft report is completed, sign off on the content of the report should be obtained from Technology Oversight Services management. Technical personnel can offer comments now as well, but typically technical issues should be resolved by this stage. Again, a list of issues will be raised which should be resolved or acknowledged/deferred until Technology Oversight Services management accepts the report.
c. For critical incidents involving payment card data, the PCI Compliance Manager will receive a copy of the report and appropriate entities will be notified in the event that cardholder data is accessed without authorization. The PCI Compliance Manager will be responsible for all communication with the payment card brands and will be responsible for coordinating the activities mandated by the payment card brands with respect to the incident.
d. If appropriate, given the analysis, Technology Oversight Services will obtain sign-off from the Chief Information Technology Officer on the report.
e. The incident handler will schedule a meeting to deliver the final report to the system administrator, the system owner, as well as to responsible officials. Although the correct management contact will vary on a case-by-case basis, it should typically be Director-level or above.
f. The incident handler will archive the final report in case it is needed for reference in the future; reports must be retained for six years.
g. The incident handler will ensure that the final report includes the details of the investigation and mid-term and long-term recommendations to improve the security posture of the organization and limit the risk of a similar incident occurring in the future.