INFORMATION TECHNOLOGY SECURITY INFORMATION BREACH NOTIFICATION PROCEDURE

Document Version: 2018-10-01

This material is based upon work supported by the National Science Foundation under DUE #1501990. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the National Science Foundation.

XYZ College

Information Technology Security Information Breach Notification Procedure

Table of Contents

XYZ College

Information Technology Security Information Breach Notification Procedure

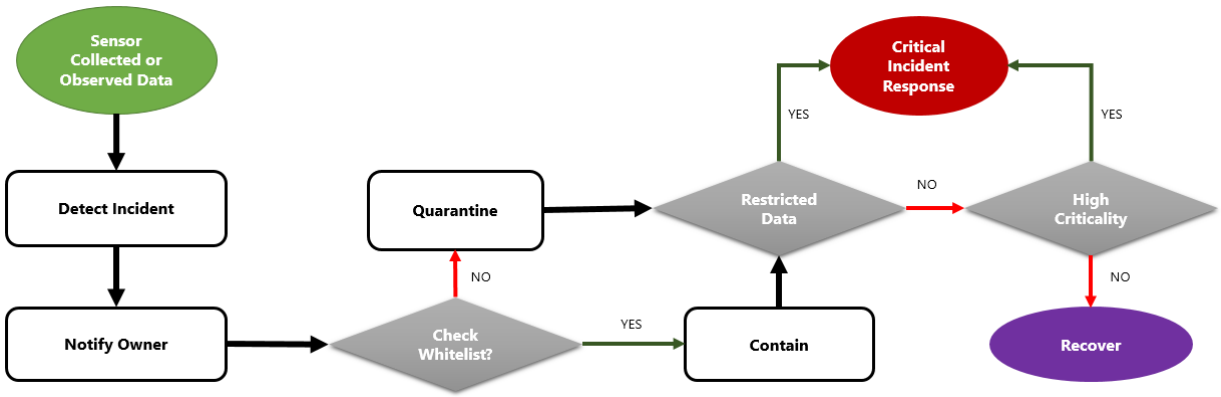
1. Introduction to Incident Response

A cybersecurity incident is an event involving an IT resource at XYZ College that has the potential of having an adverse effect on the confidentiality, integrity, or availability of that resource or service. Resources may include individual computers, mobile devices, servers, storage devices, network devices, and media as well as electronic information, messages, and files that are being stored or in-transit. Swift detection and proper handling of cybersecurity incidents are necessary to protect XYZ College's information technology assets.

The purpose of this procedure is to provide general guidance to XYZ College staff and administrators who manage IT resources in order to effectively recover from an information security incident. The procedure also enables incident response in a methodical manner in order to carry out all necessary steps to handle an incident correctly. The proper implementation of this procedure will avert or minimize disruption of critical computing services while minimizing the loss or theft of sensitive or mission critical information.

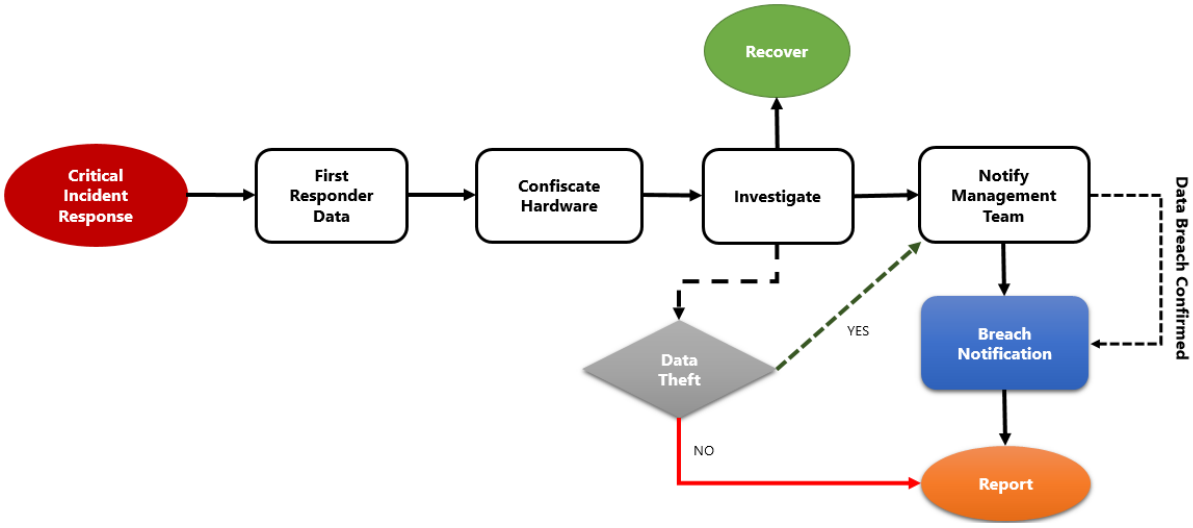
2. Incident Response Workflow Process

The diagram below is a visual depiction of the incident response procedure.



Critical Incident Response Workflow Process

If the data breach affects critical student, institution, or employee data on the compromised system in the diagram above, the critical incident response (CIR) procedure should be followed. The CIR flowchart is depicted below.



3. Incident Response Roles and Responsibilities

a) **Incident Handler**: an IT security staff member from the XYZ College IT department
b) **System Administrator**: a technical staffer 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**: a staff member or management member who has responsibility for the business function performed by the system (Since the college “owns” all of the systems, the system owner is the person who has control over it.)
d) **Network Operations**: a technical staffer responsible for network infrastructure at the site hosting the system at risk
e) **PCI Compliance Manager**: a person responsible for overseeing the XYZ College PCI compliance program (visit PCI ComplianceGuide.org to learn more)

4. Identification

The identification phase of incident response process is outlined below.

a) **Identify a potential incident**. An incident handler identifies potential incidents several different ways. This includes observing security sensors, event logs, system alarms, and outside monitoring services. Detection may also be a result of observing suspicious system behavior. Any member of the college 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 XYZ College community who suspect an IT system has been accessed without authorization must immediately report the situation to CIRT@XYZCollege.edu. Once the incident handler receives the email, he or she is responsible for alerting local system administrators. Once an incident is detected, no one should interact with the system, unless approved by the incident handler at XYZ.
c) **Quarantine.** The incident handler will quarantine compromised hosts at the time of notification unless they are on the quarantine whitelist. The whitelist details the college's mission-critical devices that must be maintained for the college to operate such as safety systems, phone systems, and financial systems. If a system is on the quarantine whitelist, the incident handler will promptly reach out to the system administrator or system owner to create a plan to contain the incident.

5. Verification

One of the most important functions of an incident response process is to verify whether data breaches are malicious or not. This phase precedes critical incident response (CIR) and is performed in order to confirm that the compromise is authentic and presents sufficient risk to engage the CIR process:

a) Classify – The CIR must be initiated if:
    i. The system owner indicates that the system is a high-criticality asset according to the system classification audit.
    ii. OR the system owner asserts that the system contains restricted data as defined by the system classification audit.
    iii. OR someone of appropriate authority (for example, the XYZ College CISO) determines that the system poses a unique risk that warrants investigation.
b) Verify – The critical incident response (CIR) process should be initiated ONLY if:
    i. The incident handler verifies that the triggering incident is not a false positive.
    ii. AND the type of data or system at risk is verified to be of an appropriate classification, as determined above.
    iii. OR the system owner provides a detailed description of the data at risk, including approximate numbers of unique data elements at risk.

The verification steps above can vary, but the CIR response process is only initiated after the verification of the criticality of the asset is confirmed. The process also eliminates the possibility of a false positive event from triggering the CIR response. In cases where the CIR process is not required, the incident handler can resolve the case as follows:

a) Obtain a written statement from the system owner documenting that the system has no restricted data and is not a high-criticality asset.
b) Obtain a written statement from the system owner that the system has been reinstalled or otherwise effectively remediated before lifting the quarantine.

6. Containment

The containment phase represents the beginning of the CIR process. The containment process has the following goals:

a) **Prevent data leakage:** If the affected host cannot be immediately removed from the network, the incident handler should initiate a capture of all data going to and coming from the affected device for later review.
b) **Eliminate attacker access:** Whenever possible, perform a network quarantine at the time of detection OR unplug the network cable OR implement a port-block to eliminate attacker access.
c) **Determine scope of incident:** The incident handler will collect data to 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.
    ii. The incident handler will capture disk images for all media that are suspected of containing evidence, including external hard drives and flash drives.
    iii. System administrators will deliver the system to the incident handler after the first responder captures the data and disk imaging and analysis is performed.
    iv. The incident handler will dump network flow data and other sensor data for the affected system.
    v. The incident handler will create an analysis plan to guide the next phase of the investigation.

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. During this phase, the system owner is 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 in cases where host-based analysis is required.

7. Analysis

The analysis phase is an in-depth investigation of the available network-based and host-based evidence. The primary goal of analysis is to determine whether there is reasonable belief that the attacker(s) successfully accessed restricted data. The analysis process is also used to generate an attack timeline and ascertain the attackers' actions. 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?
c) **Evidence of Access to Critical Data:** Are file access audit logs available that indicate whether the information has been accessed?
d) **Length of Compromise:** How long was the host compromised and online?
e) **Method of Attack:** Any indications of signatures of a human involved versus automated attack? What tools were deployed in the attack?

f) **Attacker Profile:** Is there any indication of the attackers' motives?

If, during analysis, it appears probable that restricted data has been breached, the incident handler should consult with the chief information officer (CIO) and the chief information security officer (CISO) or other appropriate XYZ College IT executives to determine the appropriate officials to inform regarding the situation.

At the conclusion of the analysis, but before the final report is written, a peer review should be performed by the CISO's office. Complete the write-up of the notes. 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 was available to unauthorized persons. The determination of whether the circumstances warrant a breach notification will be made jointly by the CIO and CISO, upon review of the results of the investigation and peer review.

8. Recovery

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

1. The system administrators will remediate the immediate compromise and restore the host to normal function. This is often performed by reinstalling the compromised host. If the investigation confirms that the attacker did not have root/administrator access, other remediation plans may be effective.
2. 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 President's office and general counsel and relevant compliance officers as to whether the incident handler and the responsible officials feel there is a reasonable belief that critical data was disclosed impermissibly without authorization and the degree of probability that security or privacy has been compromised. The report must be made in sufficient time to allow notification, if appropriate, within any legally mandated period.

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 processes that could reduce operating risk in the future.

10. Data Retention

a) The incident handler will archive the final report in case it is needed for reference in the future; reports must be retained for six (6) years.
b) Incident notes should be retained for six (6) months from the date that the report is issued. This includes the investigation page and processed investigation materials such as IDS/IPS-generated reports.
c) Raw incident data should be retained for thirty (30) days from the date that the report is issued. This includes disk-images, IDS/IPS data, and other data that was collected but deemed not relevant to the investigation.