IT Incident Response Plan

07/25/2019

System Administrator, Steve Krasinski
HIPAA/HITECH 164.308(a)(6), ISO/IEC 27001 A.13.1.1, A.13.1.2, A.13.2.1, A.13.2.2

This Incident Response Plan is documented to provide a well-defined, organized approach for handling any potential threat to computers and data, as well as taking appropriate action when

the source of the intrusion or incident at a third party is traced back to the **THIEL COLLEGE's** private network. This Incident Response Plan identifies and describes the roles and responsibilities of the Incident Response Team. The Incident Response Team is responsible for putting the plan into action.

Incident Response Team

The Incident Response Team is established to provide a quick, effective and orderly response to computer related incidents such as virus infections, hacker attempts and break-ins, improper disclosure of confidential information to others, system service interruptions, breach of personal information, and other events with serious information security implications.

The Incident Response Team's mission is to prevent a serious loss of profits, client confidence or information assets by providing an immediate, effective and skillful response to any unexpected event involving computer information systems, networks or databases.

The Incident Response Team is authorized to take appropriate steps deemed necessary to contain, mitigate or resolve a computer security incident. The Incident Response Team is responsible for investigating suspected intrusion attempts or other security incidents in a timely, cost-effective manner and reporting findings to management and the appropriate authorities as necessary. The Director of Information Technology will coordinate these investigations.

Incident Response Team Members

Director of Information Technology
Director of Information Security
Help Desk Manager
Network/Systems Manager
Public Safety
Legal Counsel

Incident Response Team Notification

For ease of reporting, and to ensure a timely response 24 hours a day, seven days a week, the IT Department Help Desk will act as the central point of contact for reporting any incidents.

All computer security incidents reported to Help Desk must be reported to the Director of Information Technology. A preliminary analysis of the incident will take place by the Director of Information Technology that will determine whether Incident Response Team activation is appropriate.

Types of Incidents

There are many types of computer incidents that may require Incident Response Team activation. Some examples include:

- Breach of personal information
- Denial of service/Distributed denial of service
- Excessive port scans
- Firewall breach
- Virus outbreak

Breach of Personal Information — Overview

This Incident Response Plan outlines steps our organization will take upon discovery of unauthorized access to personal information on an individual that could result in harm or inconvenience to the individual such as fraud or identity theft. The individual could be either a client or employee of **THIEL COLLEGE.**

Personal information is information that is, or can be, about or related to an identifiable individual.

It includes any information that can be linked to an individual or used to directly or indirectly identify an individual. Most information the firm collects about an individual is likely to be considered personal information if it can be attributed to an individual.

Personal information is defined as an individual's first name or first initial and last name, in combination with any of the following data:

- Social Security number
- Driver's license number or Identification Card number
- Financial account number, credit or debit card number
- Home address or e-mail address
- Medical or health information

Definitions of a Security Breach

A security breach is defined as unauthorized acquisition of data that compromises the security, confidentiality or integrity of personal information maintained by **THIEL COLLEGE**. Good faith acquisition of personal information by an employee or agent of our company for business purposes is not a breach, provided that the personal information is not used or subject to further unauthorized disclosure.

Ransomware Attack

- Isolate the infected computer immediately. Infected systems should be removed from the network as soon as possible to prevent ransomware from attacking network or share drives.
- Isolate or power-off affected devices that have not yet been completely corrupted. This may afford more time to clean and recover data, contain damage, and prevent worsening conditions.
- Immediately secure backup data or systems by taking them offline. Ensure backups are free of malware.
- Contact law enforcement immediately. We strongly encourage you to contact a local

field office of the Federal Bureau of Investigation (FBI) or U.S. Secret Service immediately upon discovery to report a ransomware event and request assistance. Public Safety can assist with this.
• If available, collect and secure partial portions of the ransomed data that might exist.
• If possible, change all online account passwords and network passwords after removing the system from the network. Furthermore, change all system passwords once the malware is removed from the system.
• Delete Registry values and files to stop the program from loading.

Employee Responsibilities

All firm employees must report any suspected or confirmed breach of personal information on individuals to the IT Department immediately upon discovery. This includes notification received from any third-party service providers or other business partners with whom the organization shares personal information on individuals.

The employee reporting the suspected breach will assist in acquiring information, preserving evidence and providing additional assistance as deemed necessary by the Director of Information Technology or other Incident Response Team members throughout the investigation.

Classification / Identification of a Potential Incident

All reports of a potential incident shall be classified as a high/medium/low risk to facilitate the actions to take.

- Criticality: High

Definition: Incidents that have a monumental impact on the firm's business or service to clients.
Example: Unauthorized system access.

- Criticality: Medium

Definition: Incidents that has a significant or has the potential to have a monumental impact on the firm's business or service to its clients.
Example: Password cracking attempt.

- Criticality: Low

Definitions: Incidents that has the potential to have a significant or monumental impact on the firm's

business or service to its clients.
Example: Firewall scanning.

	Urgency: A measure of how long it will be until an Incident has a significant Impact on the organization. For example, a high Impact Incident may have low Urgency, if the Impact will not affect the organization until the end of the financial year.			
Impact: A measure of the effect of an Incident based upon the number of clients affected.	Urgency 1- Incident causes significant disruption affecting critical business processes, academic services or affects life safety,	Urgency 2- Incident causes a significant disruption to critical business processes, but not affecting life safety or academic services, and no workaround is available.	Urgency 3- Incident will cause a disruption in the near term, a workaround is available	Urgency 4- Work not affected or readily available work around
All of campus affected	Critical (P1)	Critical (P1)	High (P2)	Normal (P3)
Learning Spaces or multiple departments or residence halls	Critical (P1)	High (P2)	Normal (P3)	Low (P4)
Several people or a single department or residence hall	High (P2)	High (P2)	Normal (P3)	Low (P4)
One person affected	High (P2)	Normal (P3)	Normal (P3)	Low (P4)

Response

Once a potential incident has been reported, the appropriate member of the IT Department should be notified for response. Members of the IT Department will be responsible for performing the initial investigation to determine if an incident has occurred. The following checklist identifies steps that can be used to facilitate in classifying the incident, if one in fact has occurred:

- Collection and review of log files
- Review of installed or running privileged programs
- Inspection for system file tampering
- Sniffer or Network Monitoring Programs reports
- Detection of unauthorized services installed on systems
- Evidence of password file changes
- Review system and network configurations
- Detection for unusual files
- Examination other hosts

Note: In responding to a reported incident, it may be good prudence to shut down any or all systems for the stopping of an attack in real time and/or the preservation of any potential forensic evidence.

Recovery

The main purpose of this Incident Response Program is to ensure an efficient recovery through the eradication of security vulnerabilities and the restoration of repaired systems. Recovery includes the

ensuring the attacker's point of penetration and any associated vulnerabilities have been eliminated and all system operations have been restored.

Periodic Testing & Remediation

It is the responsibility of the IT Department to test and review the Incident Response Plan quarterly. When testing is done, each system should be scanned for the open vulnerability before remediation and then scanned again after the remediation to verify that the vulnerability has been eliminated.

This document discusses the steps taken during an incident response plan**.**

1) Anyone who discovers the incident will contact the IT Help Desk. The Help Desk will log:
    a. Name of caller or source of incident alert (software notifications).
    b. Time of first report.
    c. Nature of the incident.
    d. What system(s) or persons were involved?
    e. Location of equipment or persons involved.
    f. How incident was detected.
2) The IT staff member who received the call will refer to their contact list for Incident Response Team to be contacted. The IT Help Desk will contact those designated on the list. The IT Help Desk will contact the IT Director using both email and phone messages. The IT Help Desk will log the information received. The IT Help Desk could possibly add the following information to the report:
    a. Is the equipment affected business critical?
    b. What is the severity of the potential impact?
    c. Name of systems being targeted, along with operating system, IP address, and location.
    d. IP address or any other information about the origins of the incident.
3) Contacted members of the response team will meet or discuss the situation over the telephone and determine a response strategy.
    a. Is the incident real or perceived?
    b. Is the incident still in progress?
    c. What data or property is threatened and how critical is it?

d. What is the impact on the business should the attack succeed? Minimal, serious, or critical?

e. What system or systems are targeted, where are they located physically and on the network?

f. Is the incident inside the trusted network?

g. Is the response urgent?

h. Can the incident be quickly contained?

i. Will the response alert the attacker and do we care?

j. What type of incident is this? Example: virus, worm, intrusion, abuse, damage.

4) An incident ticket will be created. The incident will be categorized into the highest applicable level of one of the following categories:

   a. High - Incidents that have a monumental impact on the firm's business or service to clients.

   b. Medium - Incidents that has a significant or has the potential to have a monumental impact on the firm's business or service to its clients.

   c. Low - Incidents that has the potential to have a significant or monumental impact on the firm's business or service to its clients.

5) Member of the IT Department will use investigative techniques, including reviewing of system logs, looking for gaps in logs, reviewing intrusion detection or firewall logs and interviewing witnesses to determine how the incident was caused. Only authorized personnel should be performing interview or examining IT systems. A chain of custody must be established and all potential evidence preserved and secured for turnover to proper authorities.

6) Incident Response Team will recommend changes to prevent the occurrence from happening again or spreading to other systems.

7) The IT Department will restore the affected system(s) to the pre-incident state and assess potential damages.

8) Post-mortem review of response and update policies – take preventive steps so the incident doesn't happen again.

   a. Would an additional policy have prevented the incident?

   b. Was a procedure or policy was not followed which allowed the incident? What could be changed to ensure that the procedure or policy is followed in the future?

c. Was the incident response appropriate? How could it be improved?

d. Was every appropriate party informed in a timely manner?

e. Were the incident-response procedures detailed and did they cover the entire situation? How can they be improved?

f. Have changes been made to prevent another incident? Have all systems been patched, systems locked down, passwords changed, anti-virus updated, email policies set, etc.?

g. Should any security policies be updated?

h. What lessons have been learned from this experience.