Security Incident Response Guide

Contents

1.0 Overview

Information Security Incident response is a vital component of adequate information and cyber risk management. Effective incident response is a complex and multi-dimensional undertaking whose success depends on planning and resources. The primary objective of Incident Response is to mitigate and contain the risk associated with computer security incidents.

This document provides guidance for managing incident response such as phishing attacks, malware and viruses, denial of resources or services, unauthorized access or attempts to gain unauthorized access, inappropriate use of network resources, data breaches, changes to system hardware, firmware or software without owner’s knowledge, an unlawful activity involving computer networks and processing equipment.

All IT professionals at the University should be review the document to become familiar with the Incident Response process.

The Incident Response Working group under the Information Security Council is tasked with reviewing this document on an annual basis.

The purpose of this document is to:

- Outline a process for responding to information security incidents.
- Provide a resource toolkit on Incident Management Training (proactive) and Handling (during a live incident).

2.0 Initial steps after discovering a potential significant information security incident

- Stay calm – this may become an emotional experience for you and your colleagues, but we will get through this together.
- If it involves computing assets that you control, immediately remove the device(s) from the network.
    - Do not power off or attempt to "clean" with an anti-virus scanner! Doing this may damage critical forensics information that could lead to increased exposure, cost, and liability
    - For virtual machines, also take a snapshot to preserve the state of the machine
- Contact your manager, who will escalate to your unit risk management function as appropriate to the incident's severity. If the incident involves sensitive personal data, also escalate to your FOIL if it is not the same person.
- To contact the Institutional Incident Response Team, email security.response@utoronto.ca, including the following information:
    - Your name and contact information
    - Date of the incident (if available)
    - Your preliminary classification
    - What you have observed - provide IP addresses or domains (if known)
    - Whether the situation may involve more than one computer or device
    - Whether potentially sensitive or confidential information is involved.

3.0 What happens after I inform Information Security?

- The Information Security team will work with you to triage the incident and collect information from security systems and logs.
- If the severity is high enough, the incident will be escalated to the CISO (if not already notified).
- If warranted and not already in motion, the CISO will form a Computer Security Incident Response Team (CSIRT) from the affected unit(s) and key legal, privacy, risk, and communications staff as necessary. The CISO will also assign an Incident Manager and technical security lead as required.
- This designation will unlock support and resources to help you manage the incident.

4.0 Incident Response Model & Checklist

Preparation — Includes documentation, testing, training and other preparatory activities.

- Review and adopt the University Incident response plan, or use it to create your own.
- Create a prioritized list of critical information assets to the functioning of your unit.
- Ensure a communication plan is in place for each severity of incident.
- Identify who will be on your CSIRT team; this can be specific people or identified positions.
- Identify any tools needed for communication, artifact collection, or other activities.
- Document as much as possible ahead of time and ensure that the files are somewhere it will be available when needed.
- Training staff or faculty on how to identify an incident and how to report it. For members of the CSIRT team run tabletop an exercise, so they understand their role and responsibilities in the process.
- Review the plan and documentation annually to ensure it stays up to date.

Identification —This identifies what data, devices, or systems were damaged, accessed, or exposed as part of the breach. Additionally includes the collection of logs, system images, and other artifacts. Activation of the CSIRT happens at this time.

- Understand what has happened, what assets are affected, and the overall impact
- Begin documenting the incident timeline, any actions taken, and artifacts collected. This may be the best estimate for the timeline, as details may not be available at this point.
- Classify the data and criticality of impacted assets
- Determine the severity of the incident
- Assemble a Security Incident Response Team (CSIRT) and assign an Incident Manager
- Activate the communication channels needed for the CSIRT team and others that must be notified.
- Determine if breach coach or external forensics is needed
- Collect Logs related to the event. These include but are not limited to those from:
    - Network devices
    - Centralized logging (SIEM, Syslog Servers)
    - Authentication sources (LDAP, Active Directory, RADIUS, etc.)

Containment — Initial short-term containment of the incident, primarily this will be disconnecting devices or networks to limit any spread of malware or malicious activity.

- Start Short-term containment to stop the attack/issue. This includes:
    - Isolate affected assets – disconnect from the network but do not power off!
    - Assess risk to other systems
    - Apply additional interim mitigations, additions to monitoring, etc.
- Collect evidence for additional review, and any possible legal proceedings
    - Create forensics images of the hard drives and memory

  - Take a snapshot of Virtual machines to preserve the current state.
  - Retrieve hard copies of any disclosed personal information.
- Continue to document findings
- Report results to CSIRT

Eradication— Identify the root cause of the incident. Remove malware, malicious code and vulnerabilities from all affected systems using the identification step's collected information.

- Identify the root cause — It's critical to understand what caused the incident to prevent future compromises for the same reason.
- Scan for malware — use anti-malware software or Next-Generation Antivirus (NGAV) if available to help determine the root cause.
- Restore, Rebuild, or Replace — A compromised system should never be cleaned and restored to production unless there is no other option.
  - Restoring a system from backup can be an effective method to get a system back into production quickly; however, any backups used must be from before the compromise occurred.
  - Rebuilding a system from scratch is more time consuming but ensures a clean system.
  - Replacing an old system with newer versions of the OS and applications is more time-consuming but is an effective way to ensure a system is up to date and secure.

Recovery — Return systems carefully back to production status, ensuring mitigation of the root cause occurs first.

- Fully patch all systems before connecting to the network.
- Change all local system and user passwords on affected systems before redeployment. This should extend to any centralized accounts that used the system as well.
- All passwords and private keys stored on the system used to access other systems must be changed.
- Harden a system to a well-documented standard. (i.e. CIS Benchmarks)
- Scan for and remediate discovered vulnerabilities before redeployment.
- Document any exceptions for vulnerabilities that cannot be remediated, including the compensating controls used instead.
- Improve monitoring to help stop any recurrence of the incident.

Lessons learned — Review the root cause of the incident and identify opportunities to improve detection and defenses to lessen a reoccurrence chance. Also, review the process of dealing with the incident and determine any improvements there as well.

- Hold a lessons learned session with stakeholders and CSIRT members to identify opportunities to improve detection of malicious activity, defenses, and the incident response process.

- Create a report based on that session's results with the issues identified and recommendations for improvement. Ensure management views the report if they were not involved with the lessons learned session.
- Create a plan to implement any recommended changes and improvements with target dates for completion.

5.0 References

Data classification & FAQ

https://isea.utoronto.ca/policies-procedures/standards/data-classification/

NIST 800-61 Incident Handling Guide:
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

UBC Incident Response Plan:
https://it.ubc.ca/sites/it.ubc.ca/files/UBC_Incident_Response_Plan7600.pdf

University of California Incident Response plan:
https://security.ucop.edu/files/documents/policies/incident-response-standard.pdf

Incident response technical tools: https://github.com/meirwah/awesome-incident-response