Carnegie Mellon
INFORMATION SECURITY OFFICE

Computer Security Incident Response Plan

Name of Approver: Mary Ann Blair	Effective Date: 23-FEB-2014
Date of Approval: 23-FEB-2014	
Date of Review: 18-MAR-2024	Name of Reviewer: Laura Raderman/John Lerchey

Carnegie Mellon
INFORMATION SECURITY OFFICE

Table of Contents

Introduction

Purpose

This document describes the overall plan for responding to information security incidents at Carnegie Mellon University. It defines the roles and responsibilities of participants, characterization of incidents, relationships to other policies and procedures, and reporting requirements. The goal of the Computer Security Incident Response Plan is to provide a framework to ensure that potential computer security incidents are managed in an effective and consistent manner. This includes evaluation to determine scope and potential risk, appropriate response, clear communication to stakeholders, containment, remediation and restoration of service, and plans for reducing the chance of recurrence.

Scope

This plan applies to the Information Systems, Institutional Data, and networks of Carnegie Mellon University and any person or device who gains access to these systems or data.

Maintenance

The University's Information Security Office (ISO) is responsible for the maintenance and revision of this document.

Authority

The ISO is charged with executing this plan by virtue of its original charter and various policies such as the Computing Policy, Information Security Policy, and HIPAA Policy.

Relationship to other Policies

This plan incorporates the risk profiles for Institutional Data as outlined in the Guidelines for Data Classification.

Relationship to Other Groups at CMU

The ISO acts on behalf of the University community and will ask for cooperation and assistance from community members as required. The ISO also works closely with University administrative groups such as the Student Life Office, Human Resources, and the Office of General Counsel in investigations and e-discovery matters, and at their behest may assist Law Enforcement.

Definitions

Event

An event is an exception to the normal operation of IT infrastructure, systems, or services. Not all events become incidents.

Incident

An incident is an event that, as assessed by ISO staff, violates the Computing Policy; Information Security Policy; other University policy, standard, or code of conduct; or threatens the confidentiality, integrity, or availability of Information Systems or Institutional Data.

Incidents may be established by review of a variety of sources including, but not limited to ISO monitoring systems, reports from CMU staff or outside organizations and service degradations or outages. Discovered incidents will be declared and documented in ISO's incident documentation system.

Complete IT service outages may also be caused by security-related incidents, but service outage procedures will be detailed in Business Continuity and/or Disaster Recovery procedures.

Incidents will be categorized according to the potential for restricted data exposure, the criticality of a resource, scope, and the potential for persistence using a High-Medium-Low designation. The initial severity may be adjusted during plan execution.

Detected vulnerabilities will not be classified as incidents. The ISO employs tools to scan the CMU environment and depending on severity of found vulnerabilities may warn affected users, disconnect affected machines, or apply other mitigations. In the absence of indications of compromise or sensitive data exposure, vulnerabilities will be communicated and the ISO will pursue available technology remedies to reduce risk.

Data Classification

Incident response processes take into account data classification when determining the categorization of an incident and relevant communications. Data classifications are found at: https://www.cmu.edu/iso/governance/guidelines/data-classification.html

Roles and Responsibilities

The Incident Response Process incorporates the Information Security Roles and Responsibilities definitions and extends or adds the following Roles.

Incident Response Coordinator

The Incident Response Coordinator is the ISO employee who is responsible for assembling all the data pertinent to an incident, communicating with appropriate parties, ensuring that the information is complete, and reporting on incident status both during and after the investigation.

Incident Response Handlers
Incident Response Handlers are employees of the ISO, other CMU staff, or outside contractors who gather, preserve and analyze evidence so that an incident can be brought to a conclusion.

Insider Threats
Insiders are, according to CERT[1], current or former employees, contractors, or business partners who have access to an organization's restricted data and may use their access to threaten the confidentiality, integrity or availability of an organization's information or systems. This particular threat is defined because it requires special organizational and technical amendments to the Incident Response Plan as detailed below.

Law Enforcement
Law Enforcement includes the CMU Police, federal, state and local law enforcement agencies, and U.S. government agencies that present warrants or subpoenas for the disclosure of information. Interactions with these groups will be coordinated with the Office of General Counsel (see below).

Office of General Counsel (OGC)
The University's Office of General Counsel (OGC) acts as the liaison between the ISO and external Law Enforcement, and provides guidance on the extent and form of all responses and disclosures to law enforcement and the public.

Officers
Officers are the staff designates for various regulatory frameworks to which the University is required to comply.

Key Stakeholders
Key Stakeholders are those individuals that have decision-making authority for their areas of responsibility.

Users
Users are members of the CMU community or anyone accessing an Information System, Institutional Data or CMU networks who may be affected by an incident.

Methodology
This plan outlines the most general tasks for Incident Response and will be supplemented by specific internal guidelines and procedures that describe the use of security tools and/or channels of communication. These internal guidelines and procedures are subject to amendment as technology changes. These guidelines will be documented in detail and kept up-to-date.

[1] This is a paraphrase of the definition presented in the Software Engineering Institute's 2009 publication entitled "Common Sense Guide to Prevention and Detection of Insider Threats" (Capelli et al, third edition, v3.1)

Constituencies

The ISO represents the entire University's Information System(s) and Institutional Data, supporting the Users. Some departments and schools maintain their own IT staffs and some branches of the university are located in other cities or countries. To the extent possible, the ISO will attempt to coordinate its efforts with these other groups and to represent the University's security posture and activities. Specific actions to be taken will be determined by the type, scope, and risk of the threat. For example, more resources may be applied to a potential disclosure of PII or ePHI than would be applied to a single ad-ware infection.

Evidence Preservation

The goal of Incident Response is to reduce and contain the scope of an incident and ensure that IT assets are returned to service as quickly as possible. Rapid response is balanced by the requirement to collect and preserve evidence in a manner consistent with the requirements of rules 26-34 of the Federal Rules of Civil Discovery, and to abide by legal and Administrative requirements for documentation and chain of custody. ISO will maintain and disseminate procedures to clarify specific activities in the ISO and in CMU departments with regard to evidence preservation, and will adjust those procedures as technologies change.

Operational-Level Agreements, Governance

Computing groups have operational-level agreements with the customers they serve. Interruption of service is a hardship and the ISO will cooperate with these groups to ensure that downtime is minimized. However, the ISO's management supports the priority of investigation activities where there is significant risk, and this may result in temporary outages or interruptions.

Staffing for an Incident Response Capability, Resiliency

The ISO will endeavor to maintain sufficient staffing and third-party augmentation to investigate each incident to completion and communicate its status to other parties while it monitors the tools that detect new events. Insufficient staffing will impact rapid response capability and resiliency, as will degradation of the tools used for detection, monitoring, and response.

Training

The continuous improvement of incident handling processes implies that those processes are periodically reviewed, tested and translated into recommendations for enhancements. CMU staff inside and outside of the ISO will be periodically trained on procedures for reporting and handling incidents to ensure that there is a consistent and appropriate response to incidents, and that post-incident findings are incorporated into procedural enhancements.

Tooling

The ISO makes available to enterprise resources Endpoint Detection and Response (EDR) tools in addition to central monitoring and detection services.

Incident Response Phases

The basic incident process encompasses six phases: preparation, detection, containment, investigation, remediation and recovery. The dynamic relationship between those phases is highlighted in Figure 1. These phases are defined in NIST SP 800-61 (Computer Security Incident Handling Guide). The ISO's overall incident response process includes detection, containment, investigation, remediation and recovery, documented in specific procedures it maintains. This plan is the primary guide to the preparation phase from a governance perspective; local guidelines and procedures will allow the ISO to be ready to respond to any incident. Recovery includes re-evaluating whether the preparation or specific procedures used in each phase are appropriate and modifying them if inappropriate.

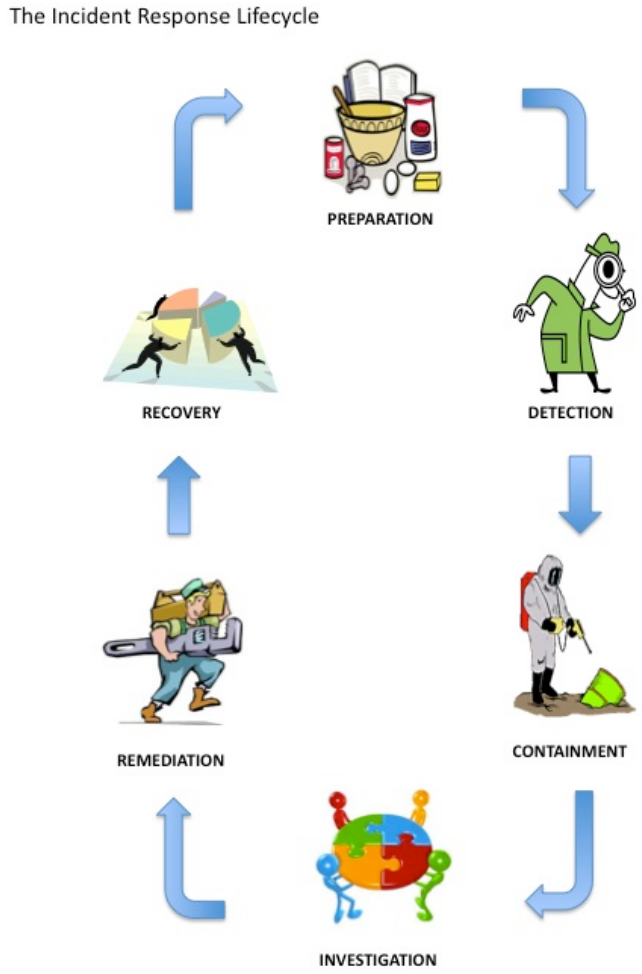

Figure 1

Preparation

Preparation includes those activities that enable the ISO to respond to an incident: policies, tools, procedures, effective governance and communication plans. Preparation also implies

that the affected groups have instituted the controls necessary to recover and continue operations after an incident is discovered. Post-mortem analyses from prior incidents should form the basis for continuous improvement of this stage.

Detection

Detection is the discovery of the event with security tools or notification by an inside or outside party about a suspected incident. This phase includes the declaration and initial classification of the incident, as well as any initial notifications required by law or contract.

Containment

Containment is the triage phase where the affected host or system is identified, isolated or otherwise mitigated, and when affected parties are notified and investigative status established. This phase includes sub-procedures for seizure and evidence handling, escalation, and communication.

Investigation

Investigation is the phase where ISO personnel determine the priority, scope, risk, and root cause of the incident.

Remediation

Remediation is the post-incident repair of affected systems, communication and instruction to affected parties, and analysis that confirms the threat has been remediated. Any determination of regulatory requirements and all internal and external communications are determined by Key Stakeholders. Apart from any formal reports, the post-mortem will be completed at this stage as it may impact the remediation and interpretation of the incident.

Recovery

Recovery is the analysis of the incident for its procedural and policy implications, the gathering of metrics, and the incorporation of "lessons learned" into future response activities and training.

Specific procedures related to this Incident response plan are documented at the ISO's Policies and Procedures internal site.

Guidelines for the Incident Response Process

In the process of responding to an incident, many questions arise and problems are encountered, any of which may be different for each incident. This section provides guidelines for addressing common issues. The Incident Response Coordinator, Director of Information Security, Chief Information Security Officer and Office of General Counsel should be consulted for questions and incident types not covered by these guidelines.

Insider Threats

In the case that a particular Incident Response Handler is a person of interest in an incident, the Incident Response Coordinator will assign other Incident Response Handlers to the incident.

In the case that the Incident Response Coordinator is a person of interest in an incident, the Chief Information Security Officer will act in their stead or appoint a designee to act on their behalf.

In the case that the Chief Information Security Officer is a person of interest in an incident, the Chief Information Officer (CIO) will act in their stead or appoint a designee to act on their behalf.

In the case that another CMU administrative authority is a person of interest in an incident, the ISO will work with the remaining administrative authorities in the ISO's reporting line to designate a particular point of contact or protocol for communications.

Interactions with Law Enforcement

All communications with external law enforcement authorities are made after consulting with the Office of General Counsel. The ISO works with CMU Police, where authorized by OGC, to determine their information requirements and shares the minimum necessary information as required for incident response.

Communications Plan

All public communications about an incident or incident response to external parties outside of CMU are made in consultation with OGC and Media Relations. Private or internal communications with other affected or interested parties contain the minimum information necessary. The minimum information necessary to share for a particular incident is determined by the Incident Response Coordinator and the Chief Information Security Officer in consultation with OGC or other campus administrative authorities.

Privacy

The Computing Policy provides specific requirements for maintaining the privacy of University affiliates. All incident response procedures will follow the current privacy requirements as set out in the Computing Policy. Exceptions must be approved by OGC.

Documentation, Tracking and Reporting

All incident response activities will be documented to include artifacts obtained using methods consistent with chain of custody and confidentiality requirements. Documentation is sufficient to support the declaration, remediation, and recovery from the incident. Incidents will be prioritized and ranked according to their potential risk. As an investigation progresses, that ranking may change, resulting in a greater or lesser prioritization of ISO resources.

Incidents will be reviewed post-mortem to assess whether the investigational process was successful and effective. Subsequent adjustments may be made to methods and procedures used by the ISO and by other participants to improve the incident response process.

Artifacts obtained during the course of an investigation may be deleted after the conclusion of the investigation and post-mortem analysis unless otherwise directed by OGC.

Escalation

At any time during the incident response process, the Incident Response Coordinator, Director of Information Security and the Chief Information Security Officer may be called upon to escalate any issue regarding the process or incident.

The Incident Response Coordinator and Chief Information Security Officer in consultation with OGC will determine if and when an incident should be escalated to external authorities.

Further Information

Further information on the Computer Security Incident Response Plan and associated procedures can be obtained from the Incident Response Coordinator of the ISO via iso-ir@andrew.cmu.edu or 412-268-2044.

Revision History

Version	Date	Author	Description
1.0	13-FEB-2014	Laura Raderman <lbowser>	Initial Document
1.1	31-MAY-2016	Laura Raderman <lbowser>	Added “local” to the definition of law enforcement, and changed link to NIST SP 800-61
1.2	24-MAR-2017	John Lerchey <lerchey>	Minor edits.
1.3	31-MAY-2017	Laura Raderman <lbowser>	Updated links.
1.4	06-JUN-2019	John Lerchey <lerchey>	Reviews and minor detail updates. Added GDPR PII definitions.
1.5	08-SEP-2020	Laura Raderman <lbowser>	Minor edits

1.6	10-FEB-2022	Laura Raderman <lbowser>	Removed section of data types and reference Guidelines for Data Classification, minor updates for 2021 GLBA Safeguards Rule
1.7	13-MAR-2024	Laura Raderman <lbowser> John Lerchey <lerchey>	Added tooling section to mention EDR and SIEM tools available.