Cyber Security Incident Response Plan

CONTENTS

PURPOSE
GENERAL RESPONSE STEPS
THREAT SEVERITY LEVELS
RESPONSE TEAM
EXTERNAL PROVIDERS
LOCATIONS AND NETWORKS
CRITICAL BUSINESS FUNCTIONS

Purpose

Appropriate Cyber Security Incident Response (CSIR) is dependent on the perceived initial severity of the incident coupled with communication, persistent monitoring, and a willingness to escalate to higher level actions should circumstances warrant. This document contains general guidance on Mount Rushmore Society Corp's planned response to cyber security incidents, contact information for key people and entities, and other pertinent information that would prove useful should an event occur.

General Response Steps

Respected response methodologies have been developed by the NIST and SANS organizations. While there are subtle differences, they can be boiled down to the following 6 steps.
Note that Step 1 occurs prior to an incident.

1. **Governance/Preparation**
    a. Create IT and Incident Response policies.
    b. Implement end user security training.
    c. Establish threat levels based on organizational impact and risk.
    d. Establish a CSIR specific communication plan.
    e. Identify a well-balanced response team.
        i. Outline roles, responsibilities, and communication channels.
    f. Regularly train on procedures and responses with tabletop exercises.
    g. Familiarize the team with available tools and procedures.
    h. Maintain an up-to-date inventory of critical assets, systems, and data.
    i. Anticipate that incidents will be reported from a wide variety of sources.
    j. Conduct regular penetration testing.
2. **Identification**
    a. Detect and analyze the nature and source of the incident.
    b. Determine the scope of the incident.
    c. Determine the root cause.
    d. Document Who, What, When, Where, Why, and How.
    e. Implement communication strategies based on an evaluation of severity and impact.
    f. Engage appropriate team members as severity dictates.
        i. Error on the side of over engagement.
        ii. Understand any time sensitive legalities.
3. **Containment**
    a. Limit the damage as soon as possible.
        i. Isolate compromised systems and network segments if appropriate.

        ii. Shut down production servers and re-route to failover servers if necessary/possible.
        iii. Disconnect affected systems.
    b. Reset passwords and revoke access for affected accounts.
    c. Prevent the destruction of potential evidence.
        i. Deploy a Forensic Tool Kit if possible.
        ii. Back up affected systems prior to wiping and re-imaging when practical.
4. **Eradication**
    a. Rebuild or reimage affected system to ensure malicious content was removed.
    b. Harden defensive tooling.
    c. Install patches and fix vulnerabilities that led to the exploitation.
    d. Continuously monitor for any signs of re-infection.
5. **Recovery**
    a. Test, monitor, and validate systems as restoration occurs.
    b. Re-visit communication strategies and act appropriately.
    c. Ensure that all legalities and social obligations have been addressed.
6. **Post Incident Reflection**
    a. Consider this a critical phase and do not skip.
    b. Finish any documentation not yet completed.
    c. Learn from what occurred and identify areas for improvement.
    d. Write report as a play-by-play review of the entire incident.
    e. Review and update incident response plans to enhance future readiness.

<u>Threat Severity Levels</u>

Mount Rushmore Society has identified the following threat severity levels based on organizational impact and has established general guidelines as to what constitutes appropriate responses.

The nature of any cyber incident is such that a given event will not clearly fall into one of the threat level categories and cookie-cutter responses are not practical.

LOW:

Example incidents

- Unauthorized / Unsuccessful Access Attempts
- Brute-force password attacks
- Probing of network services with no successful penetration

Potential Responses

- Investigate attempts to understand the nature and intent.

MINOR:

Example incidents

- Social Engineering Attacks
- Phishing emails
- Social media manipulation

Potential Responses

- Implement appropriate lower-level responses.
- Communicate with stakeholders transparently on steps being taken, and the expected impact.
- Implement appropriate lower-level responses.

MEDIUM:

Example incidents

- Malware Infections.
- Limited scope ransomware attacks.
- successful network intrusions.
- Data Breaches involving benign information.

Potential Responses

- Implement appropriate lower-level responses.
- Engage with law enforcement if necessary.

MAJOR:

Example incidents

- Advanced Persistent Threats (APTs)
- data breaches that compromise sensitive information

Potential Responses

- Implement appropriate lower-level responses.
- Notify affected parties in compliance with relevant regulations.
- Activate the incident response team.
- conduct a forensic investigation.

CRITCAL:

Example incidents

- Catastrophic Events
- System Compromises
- Widespread ransomware attacks
- Large-scale infrastructure compromises
- systemic failures

Potential Responses

- Implement appropriate lower-level responses.
- Declare a state of emergency and mobilize a cross-functional crisis management team.
- Initiate disaster recovery plans.

CONTACTS AND ENTITIES

Cyber Incident Response Team

A well-balanced response team will include members that understand the consequences to both operations and corporate strategy that each threat level response represents. The team, individually and collectively, must be willing to concede authority when situations call for it.

EXECUTIVE RESPONSE LEADER

Name:
Job Title:
Office Phone:
Cell Phone:

TECHNICAL LEAD
Name:
Job Title:
Office Phone:
Cell Phone:

FINANCIAL LEAD
Name:
Job Title:
Office Phone:
Cell Phone:

PRIMARY LEGAL LEAD
Name:
Job Title:
Office Phone:
Cell Phone:

ADDITIONAL RESPONSE LEADER
Name:
Job Title:
Office Phone:
Cell Phone:

EXTERNAL PROVIDERS
PRIMARY IT PROVIDER
Company Name:
Primary Contact:
Secondary Contact:
Office Phone:
Cell Phone:

CYBER SECURITY SOLUTION PROVIDER
Company Name:
Primary Contact:
Secondary Contact:
Office Phone:

ADDITIONAL SOFTWARE PROVIDERS
Company Name:
Primary Contact:
Secondary Contact:
Office Phone:
Cell Phone:

CYBER INSURANCE INFORMATION
Company Name:
Primary Contact:

Secondary Contact:
Office Phone:
Cell Phone:

LOCATIONS AND NETWORKS

PRIMARY BUSINESS LOCATION

(provide full address & phone)

RETAIL OFFICES

(provide full address & phone)

OTHER LOCATIONS

(provide full address & phone)

ADDITIONAL IT LOCATIONS & PROVIDERS

DATA CENTER LOCATION

(provide full address & phone)

CLOUD PRESENCE INFORMATION

Microsoft 365

Email hosting

SharePoint/Teams data storage

Office Software Programs

Software – (provide a list of critical software providers)

REMOTE WORK & ACCESS

(how do staff remotely access the network/servers)

WEBSITE INFORMATION

(provide hosting company & contacts)

CRITICAL BUSINESS FUNCTIONS

(list critical business functions)
