Cyber Response Plan

Introduction

Note to organizations – The purpose of an cyber response program is to ensure the effective response and handling of cyber security incidents that affect the availability, integrity, or confidentiality of organization information assets. In addition, a cyber response program will ensure cyber events, incidents and vulnerabilities associated with information assets and information systems are communicated in a manner enabling timely corrective action.

This template is intended to be a guide to assist in the development of an cyber response plan, one component of an cyber response program. Organizations may have various capacities and business needs affecting the implementation of these guidelines.

<organization> has developed this Cyber Response Plan to implement its cyber response processes and procedures effectively, and to ensure that [organization] employees understand them. The intent of this document is to:

- describe the process of responding to a cyber incident,
- educate employees, and
- build awareness of security requirements.

An cyber response plan brings together and organizes the resources for dealing with any event that harms or threatens the security of information assets. Such an event may be a malicious code attack, an unauthorized access to information or systems, the unauthorized use of services, a denial of service attack, or a hoax. The goal is to facilitate quick and efficient response to incidents, and to limit their impact while protecting information assets. The plan defines roles and responsibilities, documents the steps necessary for effectively and efficiently managing an cyber incident, and defines channels of communication. The plan also prescribes the education needed to achieve these objectives.

1) **Authority**: Provide the organizational authority such as policy, rules, or laws.
2) **Terms and Definitions**: Organizations should adjust definitions as necessary to best meet their business environment.
3) **Asset**: Anything that has value to the organization.
4) **Control**: Means of managing risk, including policies, procedures, guidelines, practices or organizational structures, which can be of administrative, technical, management, or legal nature.
5) **Cyber Response Plan**: Written document that states the approach to addressing and managing incidents.
6) **Cyber Response Procedures**: Written document(s) of the series of steps taken when responding to incidents.
7) **Cyber Security Event**: An observable, measurable occurrence in respect to an information asset that is a deviation from normal operations.
8) **Incident**: A single or a series of unwanted or unexpected information security events (see definition of "information security event") that result in harm, or pose a significant threat of harm to information assets and require non-routine preventative or corrective action.
9) **Incident Response Policy**: Written document that defines organizational structure for incident response, defines roles and responsibilities, and lists the requirements for responding to and reporting incidents.
10) **Incident Response Program**: Combination of incident response policy, plan, and procedures.

11) **Information**: Any knowledge that can be communicated or documentary material, regardless of its physical form or characteristics, including electronic, paper and verbal communication.

12) **Information Security**: Preservation of confidentiality, integrity and availability of information; in addition, other properties, such as authenticity, accountability, non-repudiation, and reliability can also be involved.

13) **Threat**: A potential cause of an unwanted incident, which may result in harm to a system or the organization.

Roles and Responsibilities

Note to organizations – These role descriptions here are an example. Organizations should adjust these descriptions as necessary to best meet their business environment and include any additional roles that have been identified in the organization that apply such as Security Officer, Privacy Officer, etc. Organizations need to identify roles, responsibilities and identify who is responsible for incident response preparation and planning, discovery, reporting, response, investigation, recovery, follow-up and lessons learned.

Staffing will be dependent on organization's capabilities. The same person may fulfill one or more of these roles provided there is sufficient backup coverage. The following are suggested roles and responsibilities organizations should consider: incident response team members, incident commander, and point of contact to interface with external organizations.

1) **Organizations Head Executive:** Responsible for information security in the organization, for reducing risk exposure, and for ensuring the organization's activities do not introduce undue risk to the enterprise. The <Organizations Head Executive> also is responsible for ensuring compliance with security policies, standards, and security initiatives, and with local, state and federal regulations.

2) **Incident Response Point of Contact**: Responsible for communicating with external organizations and coordinating organizations actions with external organizations in response to an information security incident.

3) **Information Owner**: Responsible for creating initial information classification, approving decisions regarding controls and access privileges, performing periodic reclassification, and ensuring regular reviews for value and updates to manage changes to risk.

   User Responsible for complying with the provisions of policies, procedures and practices.

Program

Detail on organizations governance structure – identify who is responsible for managing cyber response for the organization, who is responsible for developing policy, who is responsible for developing procedures, who is responsible for awareness, identification of any governing bodies such as management committees and work groups, etc.

Include what cyber response capabilities the organization has or identify outside resource and their capabilities. Include how the organization will test plan and frequency. Include other related program areas such as business continuity planning, risk management, and privacy as they relate to incident response.

Note to organizations –Procedures may in include Incident Reporting Procedures for staff, management, information technology, and Point of Contact.

The Incident Response Program is composed of this plan in conjunction with policy and procedures. The following documents should be reviewed for a complete understanding of the program:

1) <Organization> Incident Response, Policy <XXX-XX>, located in Appendix <insert appendix number> at the end of this document.

2) <Organization> Procedure: Cyber Response, located in Appendix <insert appendix number> at the end of this document. The related flowchart for this procedure is found in Appendix <insert appendix number> at the end of this document.

Cyber incidents will be communicated in a manner allowing timely corrective action to be taken. This plan shows how the <organization> will handle response to an incident, incident communication, incident response plan testing, training for response resources and awareness training.

The Incident Response Policy, Plan, and procedures will be reviewed <insert interval here, i.e. annually> or if significant changes occur to ensure their continuing adequacy and effectiveness. Each will have an owner who has approved management responsibility for its development, review, and evaluation. Reviews will include assessing opportunities for improvement and approach to managing cyber response in regards to integrating lessons learned, to changes to <organization's> environment, new threats and risks, business circumstances, legal and policy implications, and technical environment.

Identification

Identification of an incident is the process of analyzing an event and determining if that event is normal or if it is an incident. An incident is an adverse event and it usually implies either harm, or the attempt to harm the <organization>. Events occur routinely and will be examined for impact. Those showing either harm or intent to harm may be escalated to an incident.

<Detail who is responsible for this step and the process that will be used>

The term "incident" refers to an adverse event impacting one or more <organization's> information assets or to the threat of such an event. Examples include but are not limited to the following:

- Unauthorized use
- Denial of Service
- Malicious code
- Network system failures (widespread)
- Application system failures (widespread)
- Unauthorized disclosure or loss of information
- Information Security Breach
- Other

Incidents can result from any of the following:

- Intentional and unintentional acts
- Actions of employees
- Actions of vendors or constituents
- Actions of third parties
- External or internal acts
- Credit card fraud
- Potential violations of <organization's> Policies
- Natural disasters and power failures
- Acts related to violence, warfare or terrorism
- Serious wrongdoing

- Other

Incident Classification

Once an event is determined to be an incident, several methods exist for classifying incidents.

<Detail who is responsible for this step and the process that will be used>

The following factors are considered when evaluating incidents:

- Criticality of systems that are (or could be) made unavailable
- Value of the information compromised (if any)
- Number of people or functions impacted
- Business considerations
- Public relations
- Enterprise impact
- Multi-agency scope

Triage

The objective of the triage process is to gather information, assess the nature of an incident and begin making decisions about how to respond to it. It is critical to ensure when an incident is discovered and assessed the situation does not become more severe.

<Detail who is responsible for this step and the process that will be used>

- What type of incident has occurred
- Who is involved
- What is the scope
- What is the urgency
- What is the impact thus far
- What is the projected impact
- What can be done to contain the incident
- Are there other vulnerable or affected systems
- What are the effects of the incident
- What actions have been taken
- Recommendations for proceeding
- May perform analysis to identify the root cause of the incident

Evidence Preservation

Carefully balancing the need to restore operations against the need to preserve evidence is a critical part of incident response. Gathering evidence and preserving it are essential for proper identification of an incident, and for business recovery. Follow-up activities, such as personnel actions or criminal prosecution, also rely on gathering and preserving evidence.

<Detail who is responsible for this step and the process that will be used>

Forensics

Note to organizations – in cases involving potential exposure of personally identifiable information it is recommended that technical analysis be performed.

In incidents involving computers, when necessary <organization> will technically analyze computing devices to identify the cause of an incident or to analyze and preserve evidence.

<Organization> will practice the following general forensic guidelines:

- Keep good records of observations and actions taken.
- Make forensically-sound images of systems and retain them in a secure place.
- Establish chain of custody for evidence.
- Provide basic forensic training to incident response staff, especially in preservation of evidence

<Detail who is responsible for this step and the process that will be used>

Threat/Vulnerability Eradication

After an incident, efforts will focus on identifying, removing and repairing the vulnerability that led to the incident and thoroughly clean the system. To do this, the vulnerability(s) needs to be clearly identified so the incident isn't repeated. The goal is to prepare for the resumption of normal operations with confidence that the initial problem has been fixed.

<detail who is responsible for this step and the process that will be used>

Confirm that Threat/Vulnerability has been Eliminated

After the cause of an incident has been removed or eradicated and data or related information is restored, it is critical to confirm all threats and vulnerabilities have been successfully mitigated and that new threats or vulnerabilities have not been introduced.

<Detail who is responsible for this step and the process that will be used>

Resumption of Operations

Resuming operations is a business decision, but it is important to conduct the preceding steps to ensure it is safe to do so.

<Detail who is responsible for this step and the process that will be used>

Post-incident Activities

An after-action analysis will be performed for all incidents. The analysis may consist of one or more meetings and/or reports. The purpose of the analysis is to give participants an opportunity to share and document details about the incident and to facilitate lessons learned. The meetings should be held within one week of closing the incident.

<Detail who is responsible for this step and the process that will be used>

Education and Awareness

<Organization> shall ensure that cyber response is addressed in education and awareness programs. The programs shall address:

- <Discuss training programs, cycle/schedule, etc. Identify incident response awareness and training elements – topics to be covered, who will be trained, how much training is required.>
- <Detail training for designated response resources>

Communications

Note to organizations - Communication is vital to incident response. Therefore, it is important to control communication surrounding an incident so communications is appropriate and effective. The following aspects of incident communication should be considered:

- *Define circumstances when employees, customers and partners may or may not be informed of the issue*
- *Disclosure of incident information should be limited to a need to know basis*
- *Establish procedures for controlling communication with the media*
- *Establish procedure for communicating securely during an incident*
- *Have contact information for the external organizations and vendors contracted to help during a security emergency, as well as relevant technology providers*
- *Have contact information for customers and clients in the event they are affected by an incident*

Because of the sensitive and confidential nature of information and communication surrounding an incident, all communication must be through secure channels.

<Detail procedures for internal and external communications>

<Detail how to securely communication, what is an acceptable method>

<Detail who is responsible for communications and who is not authorized to discuss incidents>

Compliance

<Organization> is responsible for implementing and ensuring compliance with all applicable laws, rules, policies, and regulations.

<detail compliance objectives and initiatives>

<list policies (see authority section of plan, federal and state regulations), statutes, administrative rules that apply, etc.>

<All organization in Oregon are subject to the Oregon Consumer Information Protection Act ORS 646A.600. Breaches as defined in the Oregon Consumer Information Protection Act are only one type of an incident. If your organization is subject to the regulations list below for example, you should consider the following:

- The Payment Card Industry-Data Security Standards requires entities to develop an Incident Response Plan, require organizations to be prepared to respond immediately to a breach by following a previously developed incident response plan that addresses business recovery and continuity procedures, data backup processes, and communication and contact strategies
- HIPAA requires entities to implement policies and procedures to address security incidents, requires the creation of a security incident response team or another reasonable and appropriate response and reporting mechanism. Organizations subject to HIPAA should have both an incident response plan and an Incident response team, as well as a method to classify security incidents>

Specific to the Oregon Consumer Information Protection Act, plans should cover the following:

Consider potential communication channels for different circumstances, e.g., your plan may be different for an employee as opposed to a customer data breach.

- Your human resources office
- Public Information Officer (PIO)
- Legal Counsel
- State Of Oregon, Cyber Security Services, eso_soc@oregon.gov or 503-378-5930
- Oregon State Police – 503-378-3720 (ask for the Criminal Lieutenant)
- Other organizations that may be affected
- If security breach affects more than 1,000 consumers, contact all major consumer-reporting agencies that compile and maintain reports on consumers on a nationwide basis; inform them of the timing, distribution and content of the notification given to the consumers.
- Contact the credit monitoring bureaus in advance if directing potential victims to call them
    - Equifax – 1-800-525-6285
    - Experian – 1-888-397-3742
    - TransUnion – 1-800-680-7289

<Organization> maintains personal information of consumers and will notify customers if personal information has been subject to a security breach in accordance with the Oregon Revised Statute 646A.600 – Oregon Consumer Information Protection Act. The notification will be done as soon as possible, in one of the following manners:

- Written notification
- Electronic, if this is the customary means of communication between you and your customer, or
- Telephone notice provided that you can directly contact your customer.

Notification may be delayed if a law enforcement agency determines that it will impede a criminal investigation.

If an investigation into the breach or consultation with a federal, state or local law enforcement agency determines there is no reasonable likelihood of harm to consumers, or if the personal information was encrypted or made unreadable, notification is not required.

Substitute notice If the cost of notifying customers would exceed $250,000, that the number of those who need to be contacted is more than 350,000, or if there isn't means to sufficiently contact consumers, substitute notice will be given. Substitute notice consists of:

- Conspicuous posting of the notice or a link to the notice on your Web site if one is maintained, and
- Notification to major statewide Oregon television and newspaper media.
- *Notifying credit-reporting agencie*s If the security breach affects more than 1,000 consumers <organization> will report to all nationwide credit-reporting agencies, without reasonable delay, the timing, distribution, and the content of the notice given to the affected consumers.

<The regulations listed above are provided as examples of compliance requirements and are not intended to be a complete listing.>

Implementation

<Summary of initiatives, plans to develop tactical projects initiatives to meet plan components, including timelines, performance measures, auditing/monitoring requirements for compliance, etc.>

Approval

<Approval sign off by organizations decision makers, i.e. administrator, security officer, CIO, etc.>

By Name: _____

Title: _____

Dated: _____

By Name: _____

Title: _____

Dated: _____