Cyber Incident Response Plan

10-MARCH-2020

Version 1.0

|  |  |
| --- | --- |
| Document Title | Cyber Incident Response Plan |
| Document Owner |  |
| Review Cycle | Annual |

|  |  |  |  |
| --- | --- | --- | --- |
| Document State | **Date** | **Pages Affected** | **Description** |
| Document Creation 1.0 | 10-MARCH-2020 | N/A | Document Creation |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Table of Contents

[1 Overview 4](#_Toc34749977)

[1.1 Introduction 4](#_Toc34749978)

[1.2 Document Purpose 4](#_Toc34749979)

[1.3 General Purpose of the Cyber Incident Response Team 4](#_Toc34749980)

[1.4 Operational Objectives of the Cyber Incident Response Team 4](#_Toc34749981)

[1.5 Audience and Accountability 4](#_Toc34749982)

[1.6 CIRP Implementation 5](#_Toc34749983)

[1.7 Roles, Responsibilities, and Exceptions 5](#_Toc34749984)

[1.8 Non-Information Security Incident 6](#_Toc34749985)

[1.9 Information Security Incident 6](#_Toc34749986)

[2 Incident Types 7](#_Toc34749987)

[3 Information Incident Security Risk Categories 7](#_Toc34749988)

[4 Information Incident Security Sources 8](#_Toc34749989)

[5 Incident Response Process 9](#_Toc34749990)

[5.1 Stages of Response 9](#_Toc34749991)

[5.2 Organization 9](#_Toc34749992)

[5.3 Escalation Levels 10](#_Toc34749993)

[5.4 Assessment 11](#_Toc34749994)

[5.5 Escalation Considerations 11](#_Toc34749995)

[5.6 Response 12](#_Toc34749996)

[5.7 Cyber Incident Response Team Roles and Responsibilities 13](#_Toc34749997)

[5.8 After-Action Review 16](#_Toc34749998)

[6 Communication Plan 16](#_Toc34749999)

[7 Documentation, Metrics, and Reporting 16](#_Toc34750000)

[8 CIRP Maintenance Activities 17](#_Toc34750001)

[8.1 Review of the CIRP 17](#_Toc34750002)

[8.2 Incident Response Training 17](#_Toc34750003)

[9 Escalation 17](#_Toc34750004)

[APPENDIX A: CONTACT LISTS 18](#_Toc34750005)

[APPENDIX B: Incident Response Diagram and Examples 19](#_Toc34750006)

[Threat Example 1: Server Software Vulnerability.........................................................................20](#_Toc34750007)

[Threat Example 2: Ongoing Phishing Attack on Employees.........................................................22](#_Toc34750008)

[Threat Example 3: Stolen Asset, Leaked Confidential Information..............................................25](#_Toc34750009)

[APPENDIX C: Security Incidents Reporting Template 30](#_Toc34750010)

Overview

Introduction

A Cyber Incident Response Plan is required in order to bring needed resources together in an organized manner to deal with an adverse event related to the safety and security of an Entity’s Information System Resources. This adverse event may be malicious code attack, unauthorized access to an Entity’s systems, unauthorized use of an Entity’s services, denial of service attacks, general misuse of systems, accidental loss or hoaxes. This document applies to all information and associated processes used in the conduct of IT operations, concerning Cyber Incident Handling Guide (NIST SP 800-61r2).

Document Purpose

This document describes the overall Cyber Incident Response Plan (“the CIRP”) for responding to information security incidents. It defines the roles and responsibilities of individuals, characterization of incidents, relationships to other procedures and guidelines, and reporting requirements. The goal of the CIRP is to detect and react to security incidents, determine their scope and risk, respond appropriately to the incident, communicate the results and risk to all stakeholders, and reduce the likelihood of the incident from reoccurring. This CIRP provides a roadmap for implementing an incident response environment and protects information assets and helps readers comply with the Incident Management Procedures.

General Purpose of the Cyber Incident Response Team

The purpose of the Cyber Incident Response Team is to:

* Protect an Entity’s Information assets
* Provide a central organization to handle incidents
* Comply with requirements
* Prevent the use of an Entity’s systems in attacks against other systems (which could cause the Entity to incur legal liability)
* Minimize the potential for negative exposure.

Operational Objectives of the Cyber Incident Response Team

The objectives of Entity’s Cyber Incident Response Team is to:

* Limit immediate incident impact to customers and partners
* Recover from the incident
* Determine how the incident occurred
* Find out how to avoid further exploitation of the same vulnerability
* Avoid escalation and further incidents
* Assess the impact and damage in terms of financial impact, loss of image etc.
* Update policies and procedures as needed
* Determine who initiated the incident

Audience and Accountability

This document is written for all of the Entity’s users, administrators, and system owners of Entity information assets, including members of the Entity’s Cyber Incident Response Team (CIRT), each of whom is accountable for complying with this document.

CIRP Implementation

The Chief Information Security Officer is responsible for the overall endorsement and implementation of this CIRP and ensures that all individuals are properly trained.

Copies of the CIRP are distributed to all stakeholders as described in the next section.

Roles, Responsibilities, and Exceptions

The CIRT (Cyber Incident Response Team) is responsible for the daily execution of this CIRP and is comprised of management and experienced individuals who can promptly handle a cyber incident so that cyber incident identification, assessment, and response can quickly occur. The CIRT is also empowered with decision-making authority prior, during, and after a cyber incident to assist in the incident response process. The CIRT maintains, protects access to, and manages the approved CIRP.

If there is a need for an exception to be made to a portion of this document, including grandfathering, a required written

request is addressed to the Chief Information Security Officer (CISO) for the Entity for review. Exception requests are not automatically granted; those within the Entity environment require additional approval from IT Management for HIPAA and PCI Compliance.

The table below shows a list of CIRT members for Entity and their roles.



Event Definitions

An **event** occurs when something different happens outside of the normal operation of the IT infrastructure. In a computing context, events include any identifiable occurrence that has significance for system hardware or software.

A **security event** is a change in the everyday operations of a network or information technology service indicating that a security policy may have been violated or a security safeguard may have failed which may have significance to the security of systems or data.

Not all events become incidents. However, the Entity views each suspected incident as an information security incident until it has been determined not to be**.** The following sections provide definitions for the identification of an event as a non-information security incident or a security incident.

Non-Information Security Incident

There are many types of malicious activity that are not technically information security incidents, although they may still be serious in nature and require immediate action. The following are examples of malicious activities that are not classified as information security incidents and that are not required to be reported for HIPAA and PCI Compliance:

All distributed denial of service (DDoS), malicious code, scans/probes/attempted access incidents that do not contain, transfer, access, modify, or otherwise affect personal identifying information (PII) as it relates to HIPAA and PCI Data.

Simple loss of mobile devices and/or laptop computers that do not contain PII or HIPAA or PCI Data.

If an incident is determined to be reportable for HIPAA, the appropriate contact would be *“First Last”,* HIPAA Security Officer; for PCI, *“First Last”,* PCI Technical Coordinator.

Information Security Incident

The Entity defines **incidents** as events that are assessed by the CIRT and are in violation of the Entity’s computer security procedures, acceptable use procedures, or standard security practices for malicious intent. The types of activity that are widely recognized as being security incidents are violations categorized as, but are not limited to:

Successful attempts to gain unauthorized access to a system or its data.

Unwanted disruption or denial of service (DoS).

The unauthorized use of a system for the processing or storage of data, or changes to system hardware, firmware, or software characteristics without the owner’s knowledge, instructions, and approval.

Unauthorized processing of data belonging to the Entity’s personnel or the Entity’s customers.

Incident Types

The incident types that occur within the Entity’s environment are classified as:

* security incidents with privacy impacts
* security incidents with no privacy impacts
* privacy incidents with no security impacts

While the majority of incidents that are security-related do *not* have privacy impacts, the Entity’s individuals must take into consideration events that fall into this category. These include incidents that contain associated HIPAA and PCI requirements, legal requirements and protections necessary for compliance and general privacy laws and regulations. Also, if applicable, these incidents frequently are affected by country- and industry-specific laws and regulations that relate to Personally Identifiable Information (PII).

Information Incident Security Risk Categories

Information Security Incidents can be classified into different risk categories based on impact (severity) and urgency. The following categories are used to measure the impact (severity) of an incident. The initial impact (severity) rating may be adjusted during CIRP execution.

**Low Impact (Severity):** Intruder attempted access/modified in an unauthorized manner against the Entity assets, but no sensitive data has been accessed and no privileged access was gained.

**Medium Impact (Severity):** Asset(s) have been accessed/modified in an unauthorized manner, but no privileged access has been gained and no confidential data has been accessed; partial disruption of services by a malicious party.

**High Impact (Severity):** Asset(s) have been accessed/modified by an unauthorized manner and privileged access has been gained but no confidential data has been accessed/modified or service is not available; disruption of services by a malicious party.

**Critical Impact (Severity):** Asset or assets have been accessed in an unauthorized manner with privileged access and confidential data has been accessed/modified or can be accessed.



*Table 2*

Information Incident Security Sources

Information Security Incidents can be reported via:

* User Reporting:
  + End Users
  + App Services Team
  + Service Desk/ Incident Response
  + Information Services
* Reporting and Scanning Tools
* IT Audits

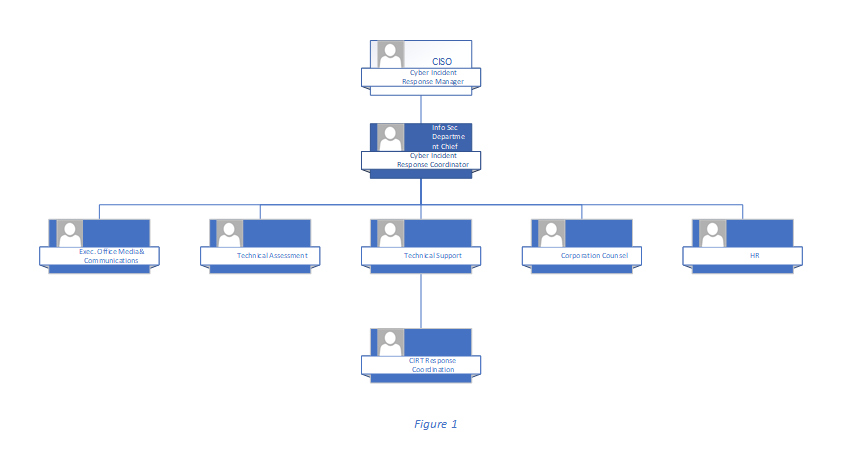
Incident Response Process

Stages of Response

1. **Preparation:** one of the most important facilities to a response plan is to know how to use it once it is in place. Knowing how to respond to an incident BEFORE it occurs can save valuable time and effort in the long run.
2. **Identification:** identify whether or not an incident has occurred. If one has occurred, the cyber incident response team can take the appropriate actions.
3. **Containment:** limiting the scope and magnitude of an incident. Because so many incidents observed currently involve malicious code, incidents can spread rapidly. This can cause massive destruction and loss of information. As soon as an incident is recognized, immediately begin working on containment.
4. **Eradication:** removing the cause of the incident. It can involve virus removal, conviction of perpetrators, or dismissing employees.
5. **Recovery:** restoring a system to its normal business status. Once a restore has been performed, it is also important to verify that the restore operation was successful and that the system is back to its normal condition.
6. **Follow-up:** post-incident activity to determine if changes are needed or activities need to be taken against the attackers. Some incidents require considerable time and effort - often once the incident appears to be terminated there is little interest in devoting any more effort to the incident. Performing follow-up activity is, however, one of the most critical activities in the response procedure. This follow-up can support any efforts to prosecute those who have broken the law. This includes changing any company policies that may need to be narrowed down or be changed altogether.

Organization

To adequately respond to an intrusion or incident, predetermined teams will participate depending on the incident characteristics. As the situation develops and the impact becomes more significant, the various teams will be called to contribute. Figure 1 depicts the Cyber Incident Response organization.

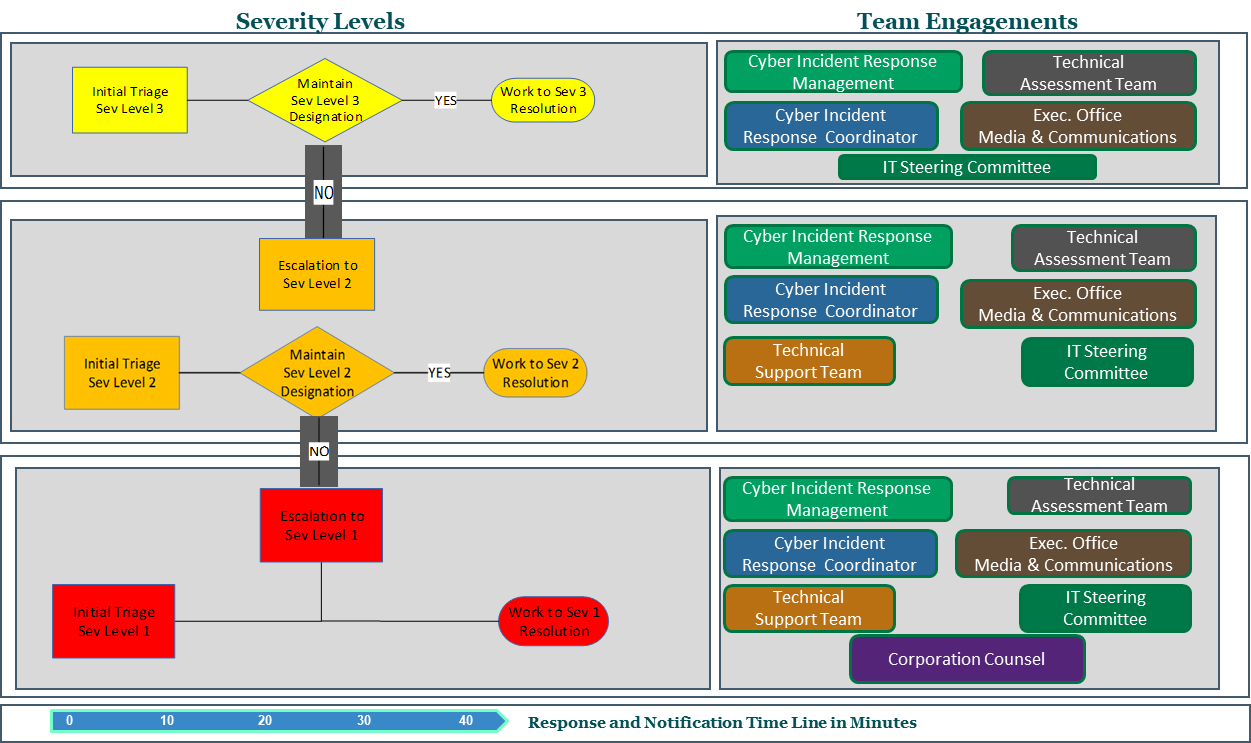


Escalation Levels

The escalation process will be invoked to involve appropriate resources as the incident has more impact (severity level increases). Incidents should be handled at the lowest escalation level that is capable of responding to the incident with as few resources as possible in order to reduce the total impact, and to keep tight control. Table 3 defines the escalation levels with the associated team involvement.

|  |  |  |
| --- | --- | --- |
| Escalation  Level | Affected Team(s) | Description |
| 4 | · Cyber Incident Response Coordinator · Technical Assessment Team | Incident where the impact is minimal. Examples are e-mail SPAM, isolated Virus infections, etc. |
| 3 | · Cyber Incident Response Management  · Cyber Incident Response Coordinator · Technical Assessment Team  · Technical Support Team · Communications Team | Incident where the impact is significant. Examples are a delayed ability to provide services, meet the Entity’s mission, delayed delivery of critical electronic mail or EDI transfers, etc. |
| 2 | · Cyber Incident Response Management  · Cyber Incident Response Coordinator · Technical Assessment Team  · Technical Support Team · Communications Team | Incident where the impact is severe. Examples are a disruption to the services, and/or performance of our mission functions. The Entity’s proprietary or confidential information has been compromised, a virus or worm has become wide spread, and is affecting over 50% of employees, Pubic Safety systems are unavailable or the Entity’s Executive management has reported it. |
| 1 | · Cyber Incident Response Management  · Cyber Incident Response Coordinator · Technical Assessment Team  · Technical Support Team · Communications Team · Corp Counsel | Asset or assets have been accessed in an unauthorized manner with privileged access and secret data has been accessed/modified or can be accessed |

*Table 3*

**

*Table 4*

Assessment

After an incident has been identified, the Cyber Incident Response Coordinator records the event and makes an initial assessment of the scope and impact (severity).

Escalation Considerations

Cyber Incident Response Management will consider several characteristics of the incident before escalating the response to a higher level. They are:

* How widespread is the incident?
* What is the impact to business operations?
* How difficult is it to contain the incident?
* How fast is the incident propagating?
* What is the estimated financial impact to the Entity?
* Will this affect the Entity’s image negatively?



The above table utilizes the framework for the Lockheed Martin Kill-Chain

Response

During the response phase, an identified security incident is mitigated by:

containing the impacted system

eradicating the threat, and/or

recovering the system to a production safe state.

During the Response phase, additional procedures are set forth such as escalating the matter to Cyber Incident Response Manager, documenting/recording evidence, and providing communication as deemed appropriate.

Cyber Incident Response Team Roles and Responsibilities

### Escalation Level 4

Technical Assessment Team

1. Monitors all known sources for alerts or notification of a threat.
2. Notify the Incident Coordinator

Cyber Incident Response Coordinator

1. Receive and track all reported potential threats.

### Escalation Level 3

A Possible threat has been discovered.

Technical Assessment Team

1. Determine initial defensive action required,
2. Notify the Incident Coordinator
3. If employee action required such as updating anti-virus files, notify the Service Center.

Cyber Incident Response Coordinator

1. Receive and track all reported potential threats,
2. Escalate Cyber Incident Response to Level 2 if a report is received indicating that the threat has manifested itself,
3. Determine relevant membership of the Technical Assessment and Technical Support teams,
4. Alert IT organizations and applicable support organizations of the potential threat and any defensive action required,
5. Alert Cyber Incident Response Management of the potential threat,
6. Alert the Executive Office Media & Communications team.

Internal Services Communications

1. If employee action required, message employees of required action.

Cyber Incident Response Management

1. Receive notification of events
2. Monitor for need for additional Governance

### Escalation Level 2

The threat has manifested itself.

Cyber Incident Response Coordinator

1. Notify Cyber Incident Response Management of the manifestation of the threat,
2. Alert the Cyber Incident Response Support Team of the incident,
3. Alert the Extended Team,
4. Receive status from the Technical Assessment Team and report to Cyber Incident Response Management,
5. Start a chronological log of events.

Note: The chronological log will be used to support possible follow on legal action as determined by the Entity’s General Counsel and Executive Directors.

Technical Assessment Team

1. Determine best course of action for containment of the incident,
2. Notify the Technical Support Team of any action that is required,
3. Report actions taken and status to the Cyber Incident Response Coordinator.

Cyber Incident Response Management

1. Assume responsibility for directing activities in regard to the incident,
2. Determine whether Escalation Level 2 is appropriate or escalate to level 1,
3. Determine when the risk has been mitigated to an acceptable level.

Technical Support Team

1. Take whatever action as determined by the Technical Assessment Team
2. Report actions taken; number of personnel involved etc. to Incident Coordinator for the chronological log.

Internal Services Communications

1. Message employee population informing them of the incident if deemed appropriate by Cyber Incident Response Management,
2. Message employee population of any action they need to take as determined by the Technical assessment team and directed by Cyber Incident Response Management.

### Escalation Level 1

The threat has become widespread or has become a high impact (severity) level.

Cyber Incident Response Management

1. Direct the Cyber Incident Response Support team to:

* Set up communications between all Cyber Incident Response Team Managers, and the Technical Support Team in the field,
* Assume occupancy of the command center.
* Initialize an incident voice mail box where status messages can be placed to keep the Entity’s personnel statuses.

1. Alert the Extended Team of the incident notifying them of the Impact (Severity) Level,
2. Determine when the risk has been mitigated to an acceptable level,
3. Status Executive Management (EMT) as appropriate.

Corporation Counsel, HR, Police Department (local)

1. Contact local authorities if deemed appropriate,
2. If local authorities are called in, make arrangements for them to be allowed into the command center
3. Ensure that all needed information is being collected to support legal action or financial restitution.

Cyber Incident Response Coordinator

1. Continue maintaining the Chronological Log of Event
2. Post numbered status messages in the incident voice mail box for status the Entity’s Executive Management.

Executive Office Media & Communications

1. Message general company population as directed by Cyber Incident Response Management

Executive Office Media & Communications

1. Message Public as deemed necessary or obligation due to compliance

Technical Assessment Team

1. Continue to monitor all known sources for alerts looking for further information or actions to take to eliminate the threat,
2. Continue reporting status to the Cyber Incident Response Coordinator for the chronological log of events,
3. Monitor effectiveness of actions taken and modify them as necessary,
4. Status Cyber Incident Response Management on effectiveness of actions taken and progress in eliminating the threat,

Technical Support Team

1. Continue actions to eradicate the threat as directed by Cyber Incident Response Management and the Technical Assessment team,
2. Continue to report actions taken, number of personnel etc. to the Cyber Incident Response Coordinator for the chronological log.

After-Action Review

The after-action review analyzes an incident and conveys metrics and “lessons learned” to help strengthen the Entity’s security defenses and detection capabilities. The review also identifies potential future courses of action for incidents and improves training activities.

Cyber Incident Response Management

1. Prepare a report for the Entity Executive Management to include:

* Estimate of damage/impact,
* Action taken during the incident (not technical detail),
* Follow on efforts needed to eliminate or mitigate the vulnerability,
* Policies or procedures that
* Efforts taken to minimize liabilities or negative exposure.

1. Provide the chronological log and any system audit logs requested by the Extended Team,
2. Document lessons learned and modify the Cyber Incident Response Plan accordingly.

Corporation Counsel, HR, Sheriff Department (local)

1. Legal and Finance work with the local authorities as appropriate in the case that the incident was from an external source,
2. HR and IT work with the Entity management to determine disciplinary action in the case that the incident was from an internal source.
3. EMT (Emergency Management Team) leveraged to take decisions and communicate as necessary.

Communication Plan

Communication of a security incident is an essential part of the CIRP. Because communications about an incident often occurs soon after its confirmation, communication between CIRT members and other groups must also occur both internally (e.g., human resources, legal) and externally (e.g., law enforcement) in a timely manner.

Documentation, Metrics, and Reporting

The Entity should use metrics and reporting tools to measure and monitor incident response capabilities and actual incidents. Using SIEM software, responders have access to an immediate reporting framework to measure analytics and provide conclusions. Defining, tracking, managing, mitigating, measuring, and improving incident response handling are functions the tools facilitate in adherence to the acceptable risk levels defined in Section 5 above.

To ensure CIRP success, audits are conducted on an annual basis that assess performance and identify problems and/or deficiencies that can be corrected.  The tools help the Entity to gain a complete understanding of the adequacy of the Entity security incident response controls and direct the allocation of resources and technology investments for ongoing improvements.

All incident response activities are documented to include information obtained using

methods consistent with chain of custody and confidentiality requirements.

CIRP Maintenance Activities

Review of the CIRP

Periodic review and testing of the Plan and post-incident findings provide for continuous improvement and procedural enhancements. At least once a year, the Entity Information Security Operations must do the following to ensure the CIRP complies with current requirements:

Plan and run one or more incident response tabletop exercises to train the individuals who have a responsibility on the CIRT and to test the CIRP meeting the Entity’s Incident Response Standard.

* Review the contact information for each of the CIRT members and update as appropriate.

Re-distribution of the CIRP

The Cyber Incident Manager must distribute the CIRP annually.

Incident Response Training

Incident response training is an important element to ensuring successful Cyber Incident Response Plan implementation.  At least annually (or more frequently when required due to system changes), training and refresher training, consistent with assigned roles and responsibilities, ensures that new hires, participants, and leads are appropriately trained and knowledgeable of how to fulfill their security responsibilities. It also ensures that individuals are aware of any system updates and changes in a timely manner.

**Escalation**

At any time during the incident response process, a member of the CIRT may escalate any issue the about the process or incident to management.

APPENDIX A: CONTACT LISTS

Cyber Incident Response Teams (see document link)

Insert “On-Call” list here

APPENDIX B: Incident Response Diagram and Examples



Threat Example 1: Server Software Vulnerability

**Escalation Level 4**

***TECHNICAL ASSESSMENT TEAM***

1. A critical *zero-day* (discovered by its use in the wild) software vulnerability affects the operating system on a widely used production server. The vulnerability allows for an unauthorized privilege escalation and therefore unauthorized data access. The threat is escalated to Level 1.

***CYBER INCIDENT RESPONSE COORDINATOR***

1. Monitors IR Queue.

**Escalation Level 3**

***TECHNICAL ASSESSMENT TEAM***

1. Determines that the defensive action required is a patch of the operating system from the vendor.

2. Notifies the Incident Coordinator of the vulnerability.

3. Determines that employee action is not required.

***CYBER INCIDENT RESPONSE COORDINATOR***

1. Receives and tracks the status of the vulnerability.

2. Does not escalate the threat to Level 2, since the vulnerability has not manifested itself.

3. Determines relevant membership of the Technical Assessment and Technical Support team.

4. Alerts IT organizations and applicable support organizations of the vulnerability. The action required to contain the threat is a patch of the operating system from the vendor. This patch must be applied and tested on a development server before being propagated to the production server.

5. Alerts Cyber Incident Response Management of the vulnerability.

6. Alerts the Communications Team.

***EXECUTIVE OFFICE MEDIA & COMMUNICATIONS***

1. Since employee action is not required, no message to employees is necessary.

***CYBER INCIDENT RESPONSE MANAGEMENT***

1. Receive status reports and maintain governance over process

**Post Incident**

***CYBER INCIDENT RESPONSE MANAGEMENT***

1. Prepare a report for the Entity Executive Management to include: a. Estimate of the impact of addressing the vulnerability and the potential cost of not doing so,

a. Action taken during the vulnerability’s assessment,

b. Follow on efforts needed to eliminate or mitigate the vulnerability,

c. Policies or procedures that may require updating (if applicable), and

d. Efforts taken to minimize the liabilities of negative exposure of the vulnerability.

2. Provides the chronological log and any system audit logs requested by the Extended Team.

3. Documents any lessons learned and modifies the Cyber Incident Response Plan accordingly.

***CORPORATION COUNSEL, HR, POLICE (LOCAL)***

1. Not needed, because there was no manifestation of the vulnerability.

Threat Example 2: Ongoing Phishing Attack on Employees

**Escalation Level 4**

***TECHNICAL ASSESSMENT TEAM***

1. Emails have been circulating to employees that link users to a fraudulent website designed specifically to gather user authentication credentials from the Entity’s employees. The threat is escalated to Level 1.

***CYBER INCIDENT RESPONSE COORDINATOR***

1. Monitors IR Queue.

**Escalation Level 3**

***TECHNICAL ASSESSMENT TEAM***

1. Determines that the initial defensive action required is to notify employees of the phishing scam and educate them on avoiding these types of attacks.

2. Notifies Incident Coordinator.

3. Determines that employee action will be required, notifies Service Center.

***CYBER INCIDENT RESPONSE COORDINATOR***

1. Receives and tracks the phishing attack.

2. Escalates the threat to Level 2, since it has manifested itself.

3. Determines relevant membership of the Technical Assessment and Technical Support team.

4. Alerts IT organizations and applicable support organizations of the phishing. The organizations begin modifying internal firewalls to block the offending website as well as initiating a system-wide password reset.

5. Alerts Cyber Incident Response Management of the phishing threat.

6. Alerts the Communications Team.

***EXECUTIVE OFFICE MEDIA & COMMUNICATIONS***

1. A message is composed to all employees and sent system wide. Additionally, all departmental managers are alerted to the phishing scam and asked to notify all employees in person immediately.

***CYBER INCIDENT RESPONSE MANAGEMENT***

1. Receive status reports and maintain governance over process

**Escalation Level 2**

***CYBER INCIDENT RESPONSE COORDINATOR***

1. Notifies Cyber Incident Response Management of the phishing attack.

2. Alerts the Cyber Incident Response Support Team of the phishing attack.

3. Alerts the Extended Team.

4. Receives status from the Technical Assessment Team regarding the status of employee education. Reports the status to the Cyber Incident Response Management.

5. Starts a chronological log of the events, including logs of emails and, if possible, logs of users accessing the offending website.

***TECHNICAL ASSESSMENT TEAM***

1. Determines that the best course of action for containing the attack is educating all employees about the attack and blocking any further emails from arriving on mail servers. Additionally, concludes that blocking the fraudulent website from being accessed internally. Finally, decides that a system-wide user password reset is necessary, since email is accessible from outside of the Entity’s network and merely blocking the offending site will not be sufficient and the emails have been circulating for an unknown amount of time to only select employees.

2. Notifies the Technical Support Team of the above actions that are required.

3. Reports actions taken and status to the Cyber Incident Response Coordinator.

***CYBER INCIDENT RESPONSE MANAGEMENT***

1. Assumes responsibility for directing activities in regard to the phishing attack.

2. Determines that the attack does not need to be escalated to Level 3.

3. Determines when the risk has been mitigated to an acceptable level.

***TECHNICAL SUPPORT TEAM***

1. Takes the actions required by the Technical Assessment Team.

2. Reports the actions taken, the number of personnel involved etc. to Incident Coordinator for the chronological log.

***EXECUTIVE OFFICE MEDIA & COMMUNICATIONS***

1. Carries out the education of the Entity’s employees by informing them of the incident and making sure everyone is aware of the scam as deemed appropriate by Cyber Incident Response Management.

2. Messages the Entity’s employees about the system-wide password reset, and how the employees must go about regaining access to their user accounts as determined by the Technical assessment team and directed by Cyber Incident Response Management.

**Post Incident**

***CYBER INCIDENT RESPONSE MANAGEMENT***

1. Prepare a report for the Entity Executive Management to include: a. Estimate of the impact of addressing the phishing attack and the potential cost of not doing so,

a. Action taken during the attack’s assessment,

b. Follow on efforts needed to eliminate or mitigate the vulnerability presented by the phishing attack,

c. Policies or procedures that may require updating, such as password change rules and procedures, and

d. Efforts taken to minimize the liabilities of negative exposure of the attack.

2. Provides the chronological log and any system audit logs requested by the Extended Team.

3. Documents any lessons learned and modifies the Cyber Incident Response Plan accordingly.

***CORPORATION COUNSEL, HR, POLICE (LOCAL)***

1. Legal works with the authorities to present any information relating to the phishing party.

2. No disciplinary action will need to be taken.

3. Emergency Management Team (EMT) leveraged to communicate to employees about the threat of phishing attacks and to be vigilant.

Threat Example 3: Stolen Asset, Leaked Confidential Information

**Escalation Level 4**

***TECHNICAL ASSESSMENT TEAM***

1. An employee has his or her laptop stolen, which contains unencrypted confidential personal information of the Entity’s customers, including names, addresses, Social Security numbers, etc. The information has been found and posted on the public Internet. The threat is escalated to Level 1.

***CYBER INCIDENT RESPONSE COORDINATOR***

1. Monitors IR Queue.

**Escalation Level 3**

***TECHNICAL ASSESSMENT TEAM***

1. Determines that the attack has already taken place and that there is no initial technical defense possible in this circumstance. However, an internal data security practices audit is necessary to keep a data leak from happening again.

2. Notifies the Incident Coordinator.

3. Determines that employee action required to secure confidential data in the future through education. Contacts Service Center to arrange for instructions.

***CYBER INCIDENT RESPONSE COORDINATOR***

1. Receives and tracks the stolen data event.

2. Escalates to Level 2, because the threat has manifested itself.

3. Determines relevant membership of the Technical Assessment and Technical Support teams.

4. Alerts IT organizations and applicable support organizations of the situation. Defensive action that must be taken involves an audit of information security practices internally to ensure further data breaches do not occur.

5. Alert Cyber Incident Response Management of the data leak.

6. Alert the Communications team.

***EXECUTIVE OFFICE MEDIA & COMMUNICATIONS***

1. Employee action is going to be required for the internal information security practices audit. The Communications Team notifies employees of the data breach and the actions that are going to be taken to prevent such a leak in the future.

***CYBER INCIDENT RESPONSE MANAGEMENT***

1. Receive status reports and maintain governance over process

**Escalation Level 2**

***CYBER INCIDENT RESPONSE COORDINATOR***

1. Notifies Cyber Incident Response Management of the data leak.

2. Alerts the Cyber Incident Response Support Team of the data leak.

3. Alerts the Extended Team.

4. Receives status of the information security audit from the Technical Assessment Team and reports to Cyber Incident Response Management.

5. Starts a chronological log of events from the origin of the data to determine how the data ended up in a situation where it could be leaked. The chronological log will be used to support possible follow on legal action as determined by the Entity’s General Counsel and Executive Directors.

***TECHNICAL ASSESSMENT TEAM***

1. Determines that containment of the incident is going to be legal in nature, but that information security practices will need to be overhauled.

2. Notifies Technical Support of the CIRP to audit and augment data security practices internally, including any technical measures that will need to be put into place to that end.

3. Reports actions taken and status to the Cyber Incident Response Coordinator.

***CYBER INCIDENT RESPONSE MANAGEMENT***

1. Assumes responsibility for directing activities in regard to the incident.

2. Determines that escalation Level 2 is not sufficient and escalates the incident to Level 3.

3. Determines when the risk has been mitigated to an acceptable level.

***TECHNICAL SUPPORT TEAM***

1. Takes action to begin comprehensive information security practices audit internally, as determined by the Technical Assessment Team.

2. Reports actions taken; number of personnel involved etc. to Incident Coordinator for the chronological log.

***EXECUTIVE OFFICE MEDIA & COMMUNICATIONS***

1. Messages employee population informing them of the information leak and the ensuing legal action, as deemed appropriate by Cyber Incident Response Management.

2. Messages employee population of the forthcoming comprehensive information security practices audit and the organization-wide practices that will be augmented as determined by the Technical assessment team and directed by Cyber Incident Response Management.

***CYBER INCIDENT RESPONSE MANAGEMENT***

1. Receive status reports and maintain governance over process

**Escalation Level 1**

***CYBER INCIDENT RESPONSE MANAGEMENT***

1. Directs the Cyber Incident Response Support team to: a. Set up communications between all Cyber Incident Response Team Managers, and the Technical Support Team in the field,

a. Assume occupancy of the command center, and

b. Initialize an incident voice mail box where status messages can be placed to keep personnel up to status.

2. Alerts the Extended Team of the incident notifying them of the Impact (Severity) Level.

3. Determines when the risk has been mitigated to an acceptable level after the comprehensive information security data protection audit and overhaul.

4. Statuses Executive Management as appropriate.

***CORPORATION COUNSEL, HR, SHERRIFF OFFICE (LOCAL)***

1. Contacts local, state, and federal authorities.

2. Makes arrangements for authorities to be allowed into the command center.

3. Ensures that all needed information is being collected to support legal action against the leaker and financial restitution for those affected by the breach of their personal information by the Entity’s personnel.

***CYBER INCIDENT RESPONSE COORDINATOR***

1. Continues maintaining the Chronological Log of the event.

2. Posts numbered status messages in the incident voice mail box for status the Entity EMT (Emergency Management Team).

***EXECUTIVE OFFICE MEDIA & COMMUNICATIONS***

1. Messages population as directed by Cyber Incident Response Management regarding the status of the information security data practices audit and any forthcoming changes to be made to policy.

***TECHNICAL ASSESSMENT TEAM***

1. Continues to monitor all known sources for alerts looking for further information or actions to take to eliminate the threat of further data being lost in any way, both internally and externally.

2. Continues reporting status to the Cyber Incident Response Coordinator for the chronological log of events.

3. Monitors effectiveness of the information security practices audit and subsequent changes and modifies them as necessary.

4. Statuses Cyber Incident Response Management on effectiveness of actions taken and progress in eliminating the threat of further information leakage.

***TECHNICAL SUPPORT TEAM***

1. Continues the information security practices audit and changes to eradicate the further threat of data leaks as directed by Cyber Incident Response Management and the Technical Assessment team.

2. Continues to report actions taken, number of personnel etc. to the Cyber Incident Response Coordinator for the chronological log.

**Post Incident**

***CYBER INCIDENT RESPONSE MANAGEMENT***

1. Prepare a report for Executive Management to include: a. Estimate of the impact of addressing the data leak and the potential cost of not doing so,

a. Action taken during the comprehensive information security practices audit and assessment,

b. Follow on efforts needed to eliminate or mitigate any and all vulnerabilities that exist in terms of confidential data security,

c. Policies or procedures that may require updating to ensure strict oversight of sensitive data within the Entity,

d. Efforts taken to minimize the liabilities of negative exposure of the attack.

2. Provides the chronological log and any system audit logs requested by the Extended Team.

3. Documents any lessons learned and modifies the Cyber Incident Response Plan accordingly.

***CORPORATION COUNSEL, HR, SHERRIFF OFFICE (LOCAL)***

1. Legal works with the authorities to present any information relating to the leaking party that may lead to prosecution.

2. Human Resources and Information Technology work with management to determine disciplinary action for the negligent employee.

3. Emergency Management Team (EMT) leveraged to communicate to employees about the seriousness of keeping data safe and the costs of not doing so, as exemplified in this case.

APPENDIX C: Security Incidents Reporting Template

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| IT Security Incident Report | | | | |
| Incident Detector’s Information | | | | |
| Date/Time of Report |  | | | |
| First Name |  | | | |
| Last Name |  | | | |
| Department/Division |  | | | |
| Title/Position |  | | | |
| Work Email Address |  | | | |
| Contact Phone Numbers | *Work* | *Mobile* | *Pager* | *Other* |
| Reported Incident Information | | | | |
| Initial Report Filed  With (Name, Organization) |  | | | |
| Start Date/Time |  | | | |
| Incident Location |  | | | |
| Incident Point of  Contact (if different than above) |  | | | |
| Priority | *Level 3 / Level 2 / Level 1* | | | |
| Data Breach? | *YES / NO* | | | |
| Breach Category |  | | | |
| Incident Type |  | | | |
| US-CERT Category | *DoS / Malicious Code / Probes and Scans / Unauthorized Access / Other* | | | |
| US-CERT Number |  | | | |
| Description |  | | | |
| Additional Support Action Requested |  | | | |
| Method Detected | *IDS/Log Review/ A/V Systems/ User Notification/ Other* | | | |
| Configuration Item(s) Affected |  | | | |
| Department/ Division Impact |  | | | |
| Information Sharing | *Entities with which IT can share incident data.* | | | |
| System | *Name of reported system (if known)* | | | |
| Status | *Ongoing/ Resolved/ Etc.* | | | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Attacking Computer(s) Information | | | | |
| IP Address / Range | Host Name | Operating System | Ports Targeted | System Purpose |
|  |  |  |  |  |
|  |  |  |  |  |
| Victims Computer(s) Information | | | | |
| IP Address / Range | Host Name | Operating System | Ports Targeted | System Purpose |
|  |  |  |  |  |
|  |  |  |  |  |
| Action Plan | | | | |
| Action Description |  | | | |
| Requestor |  | | | |
| Assignee |  | | | |
| Time Frame |  | | | |
| Status |  | | | |
| Conclusion / Summary | | | | |
| Entities Notified |  | | | |
| Resolution | *Include whether lost materials recovered as part of the solution* | | | |