Incident Management Plan

Incident Response Plan Template Developed By: Olumuyiwa Olufunmilola Agunbiade

Table of Contents

Version History.....

Introduction..... 5

Contact Information..... 6

Roles and Responsibilities..... 7

Cyber Security Incident Handling Team (IHT)..... 7

Chief Information Officer (CIO/CTO)..... 7

Cyber Security Incident Response Team (CSIRT)..... 7

IR Commander..... 8

Incident Response Team Members..... 8

Recorder..... 9

Incident Response Framework..... 10

Phase I – Preparation..... 10

Phase II – Identification and Assessment..... 10

Phase III – Containment and Intelligence..... 10

Phase IV – Eradication..... 10

Phase V – Recovery..... 10

Phase VI – Lessons Learned..... 11

Phase I – Preparation Details..... 12

Reporting Incidents..... 12

Phase II - Identification and Assessment..... 13

Identification..... 13

Assessment..... 14

Key Decisions for Exiting Identification and Assessment Phase:..... 17

Phase III – Containment and Intelligence..... 17

Containment Strategies..... 18

Common Containment Steps..... 18

Key Decisions for Exiting Containment Phase..... 21

Investigation..... 21

Initial Cause (“Root Cause”) Investigation..... 21

Phase IV – Eradication Details..... 22

Eradication..... 22

Key Decisions for Exiting Eradication Phase..... 23
Phase V – Recovery Details..... 23
Key Decisions for Exiting Recovery Phase..... 24
Phase VI - Lessons Learned..... 24
Documentation..... 24
Lessons Learned and Remediation..... 24
Forensic Analysis & Data Retention..... 25
Key Decisions for Exiting Lessons Learned Phase..... 25
Notification and Communication..... 26
Interaction with Law Enforcement..... 26
Regulatory Authorities..... 26
Customers..... 27
Public Media Handling..... 27
Plan Testing and Review..... 27
Appendices..... 28
Appendix I. Logging, Alerting, and Monitoring Activities List..... 29
Appendix II. Two Minute Incident Assessment Reference..... 30
Step 1: Understand impact/potential impact (and likelihood if not an active incident)..... 30
Step 2: Identify suspected/potential cause(s) of the issue..... 30
Step 3: Describe recommended remediation activities..... 30
Step 4: Communicate to Management..... 30
Appendix III. Incident Response Checklist..... 32
Appendix IV. Notification Requirements..... 33
PCI DSS..... 33
HIPAA..... 35
FDIC / OCC..... 37
State of Minnesota..... 38
CCPA..... 40
GDPR..... 40
Appendix V. Media Statements..... 41
Pre-scripted Immediate Responses to Media Inquiries..... 41
Pre-scripted Responses..... 41

Statement Writing Tips.....42
Appendix VI. Customer Letter Template.....45
Formal Email and/or Letter Template.....45
Appendix VII. Incident Response Organizations.....47
Appendix VIII. Containment Strategies.....48
Stolen credentials.....48
Ransomware.....48
Virus Outbreak.....49
Appendix IX. Cyber Insurance and Third-Party Service Agreements.....51
Appendix X. Supporting Document List.....52

Introduction

The (Company Name)Incident Management Plan has been developed to provide direction and focus to the handling of information security incidents that adversely affect (Company Name)**Information Resources**. The (Company Name)Incident Management Plan applies to any person or entity charged by the (Company Name)Incident Response Commander with a response to information security related incidents at the organization, and specifically those incidents that affect (Company Name)**Information Resources**.

The purpose of the Incident Management Plan is to allow (Company Name)to respond quickly and appropriately to information security incidents.

Event Definition

Any observable occurrence in a system, network, environment, process, workflow, or personnel. Events may or may not be negative in nature.

Adverse Events Definition

Events with a negative consequence. This plan only applies to adverse events that are computer security related, not those caused by natural disasters, power failures, etc.

Incident Definition

A violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practicesthatjeopardizes the confidentiality, integrity, or availability of information resources or operations. A security incident may have one or more of the following characteristics:

A. Violation of an explicit or implied (Company Name) security policy
B. Attempts to gain unauthorized access to a (Company Name) Information Resource
C. Denial of service to a (Company Name) Information Resource
D. Unauthorized use of (Company Name) Information Resources
E. Unauthorized modification of (Company Name) information

F. Loss of (Company Name) Confidential or Protected information

Reference

- Blue Team Handbook: Incident Response Edition, Don Murdoch
- NIST SP800-61r2: Computer Security Incident Handling Guide

Contact Information

Updated November 2023

Name	Title	Role	Contact Information	Escalation (1-3)*
	Information Security Manager	IR Commander, CSIRT manager		**1**
	Infrastructure Manager	IR Manager		**1**
	CIO	CIO		**2**
	Communications Manager	IHT member		3
	Legal	IHT member		3
	Risk Manager	IHT member		3
	HR Representative	IHT member		3
	Physical Security Representative	IHT member		3
	3rd Party Support			3
	Cyber Insurance Provider			3
	Regulatory/Government Reporting Body			3

*Escalation level determines order in which notification should occur:

1. Notify first, required on all incidents
2. Required on all moderate or high-severity incidents
3. Involve as needed

Roles and Responsibilities

Cyber Security Incident Handling Team (IHT)

- Consists of legal experts, risk managers, and other department managers that may be consulted or notified during incident response.
- Advise on incident response activities relevant to their area of expertise.
- Maintain a general understanding of the Plan and policies of the organization.
- Ensure incident response activities are in accordance with legal, contractual, and regulatory requirements.
- Participate in tests of the incident response plan and procedures.

Responsible for internal and external communications pertaining to cyber security incidents.

Chief Information Officer (CIO/CTO)

- Seek approval from Executive Management for the administration of the Incident Response Program.
- Coordinate response activities with auxiliary departments and external resources as needed to minimize damages to information resources.
- Provide updates on response activities to Incident Handling Team (IHT) and other stakeholders during an incident.
- Ensure service level agreements with service providers clearly define expectations of the organization and the service provider in relation to incident response.
- Ensure policies related to incident management accurately represent the goals of the organization.
- Review the Cyber Security Incident Response Plan ("the Plan") to ensure that it meets policy objectives and accurately reflects the goals of the organization. Seek Plan approval from IHT.
- Work with the IR Commander to periodically evaluate the effectiveness of the Plan and CSIRT.
- Ensure CSIRT managers are given the necessary authority to seize assets and stop services quickly to contain a moderate or critical-severity incident.
- Approve close of moderate or critical-severity incidents.
- Ensure Cyber Insurance is maintained as necessary and appropriate stakeholders are informed. (See Appendix IX)
- Ensure lessons learned are applied/weighed based on risk for Severity 1 incidents.

Cyber Security Incident Response Team (CSIRT)

The CSIRT is comprised of IT management and experienced personnel. The role of the CSIRT is to promptly handle an incident so that containment, investigation and recovery can occur quickly. Where third-party services are leveraged, ensure they are engaged as necessary.

Roles within the CSIRT include:

IR Commander

The incident response manager oversees and prioritizes actions during the detection, analysis, and containment of an incident. They are also responsible for conveying the special requirements of high severity incidents to the rest of the organization as well as communicating potential impact to the CIO. Additionally, they are responsible for understanding the SLAs in place with third parties, and the role third parties may play in specific response scenarios.

Further responsibilities:

- Act as a liaison for all communications to and from the CIO.
- Assemble a Cyber Security Incident Response Team (CSIRT).
- Ensure personnel tasked with incident response responsibilities are trained and knowledgeable on how to respond to incidents.
- Update Plan and procedures as needed based on results from testing, incident response lessons learned, industry developments and best practices.
- Review the Plan and procedures at least annually.
- Initiate tests of the Plan and procedures at least annually.
- Ensure team activities comply with legal and industry requirements for incident response procedures.
- Act as the primary Incident Response Manager, responsible for declaring a cyber security incident, managing team response activities, and approving close of Severity 2 & 3 incidents.
- Be aware of Cyber Insurance Policies, contact mechanisms, and when to include providers. (See Appendix IX)

Incident Response Team Members

The Incident Response Manager is supported by a team of technical staff that work directly with the affected information systemsto research the time, location, and details of an incident. Team members are typically comprised of subject matter experts (SMEs), senior level IT staff, third parties, outsourced security or forensic partners.

Further responsibilities:

- Assist in incident response as requested. CSIRT responsibilities should take priority over normal duties.
- Understand (Company Name) incident response plan and procedures to appropriately respond to an incident.
- Continue to develop skills for incident response management.
- Ensure tools are properly configured and managed to alert on security incidents/events.
- Analyze network traffic for signs of denial of service, distributed denial of service, or other external attacks.
- Review log files of critical systems for unusual activity.
- Monitor business applications and services for signs of attack.
- Collect pertinent information regarding incidents at the request of the IR Commander.
- Consult with qualified information security staff for advice when needed.
- Ensure evidence gathering, chain of custody and preservation is appropriate.
- Participate in tests of the incident response plan and procedures.
- Be knowledgeable of service level agreements with service providers in relation to incident response.

Recorder

The Incident Response Manager may assign a team member to begin formal documentation of the incident.

Table 1: (Company) CSIRT Team Members

No.	CSIRT Member	Role

Incident Response Framework

(Company Name) recognizes that, despite reasonable and competent efforts to protect **Information Resources**, a breach or other loss of information is possible. The organization must make reasonable efforts and act competently to respond to a potential incident in a way that reduces the loss of information and potential harm to customers, partners, and the organization itself.

Developing a well-defined incident response framework is critical to an effective incident response plan. The (Company Name) incident response framework is comprised of sixphases that ensure a consistent and systematic approach.

Phase I – Preparation

It is essential to establish a Cyber Security Incident Response Team (CSIRT), define appropriate lines of communication, articulate servicesnecessary to support response activities, and procure the necessary tools. (SeePhase I – Preparation Details)

Phase II – Identification and Assessment

Identifying an eventand conducting an assessment should be performed to confirm the existence of an incident. The assessment should include determining the scope, impact, and extent of the damage caused by the incident. In the event of possible legal action, digital evidence will be preserved, and forensic analysis may be conducted consistent with legislative and legal requirements. (See Phase II - Identification and Assessment)

Phase III – Containment and Intelligence

Containment of the incident is necessary to minimize and isolate the damage caused. Steps must be taken to ensure that the scope of the incident does not spread to include other systems and Information Resources. Root cause analysis is required prior to moving beyond the Containment phase and may require expertise from outside parties. (SeePhase III – Containment and Intelligence)

Phase IV – Eradication

Eradication requires removal or addressing of all components and symptoms of the incident.Further, validation must be performed to ensure the incident does not reoccur. (SeePhase IV – Eradication Details)

Phase V – Recovery

Recovery involves the steps required to restore data and systems to a healthy working state allowing business operations to be returned.

Phase VI – Lessons Learned

The Lessons Learned phase includes post-incident analysis on the system(s) that were impacted by the incident and other potentially vulnerable systems. Lessons learned from the incident are communicated to executive management and action plans developed to improve future incident management practices and reduce risk exposure.

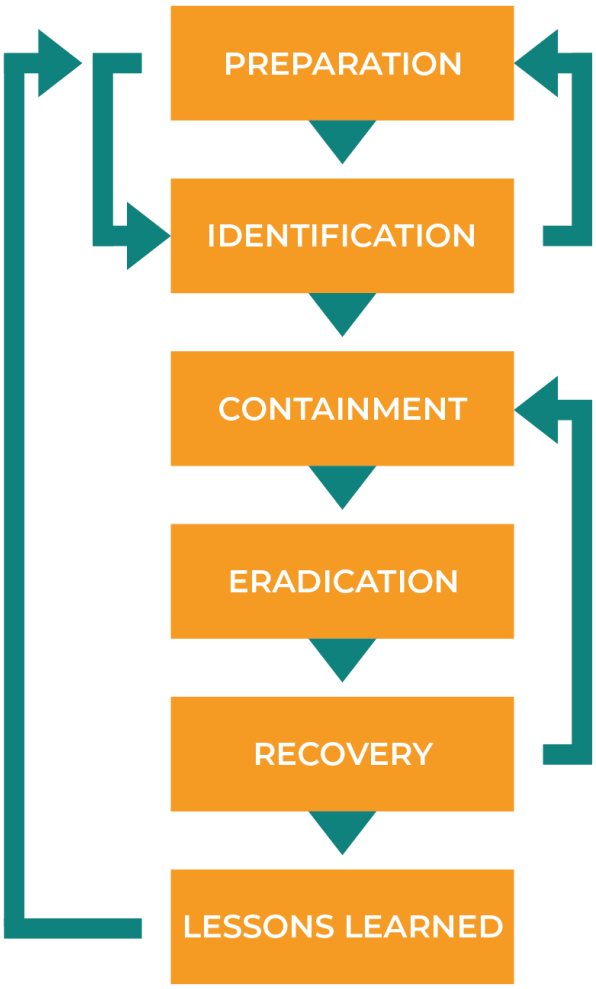


FIGURE 1:PICERL FRAMEWORK MODEL

Reference

- SANS PICERL Incident Response Model

Phase I –Preparation Details

The Preparation phase is easily the most important and often overlooked phase. Without proper preparation incident response activities may be disorganized, expensive, and could cause irreparable harm to (Company Name). Tasks included in the Preparation phase include but are not limited to the following.

- Establish Cyber Security Incident Handling Team (IHT) and Cyber Security Incident Response Team (CSIRT).
- Ensure appropriate parties are aware of incident reporting processes. (See Reporting Incidents)
- Document and share cyber insurance details with appropriate parties. (See Appendix IX)
- Validate Logging, Alerting, and Monitoring policy compliance.
- Ensure CSIRT receives appropriate training based on skill gap analysis, career development efforts, and skill retention needs.
- Ensure CSIRT has access to the tools and equipment needed based on estimated ROI and the organization's risk appetite.
- Define and document standard operating procedures and workflows for both IHT and CSIRT.
- Improve documentation, checklists, references, etc.
- Maintain and validate Network Diagrams and Asset Inventories.
- Review Penetration Test reports and validate remediations to findings.
- Review Vulnerability Management reports and validate remediation efforts.
- Establish disposable and disabled Administrative credentials to be enabled and used for investigations.

Finally, it should be noted that the Phase I is continuous or at least cyclical as incidents are brought to conclusion.

Reporting Incidents

Effective ways for both internal and outside parties to report incidents is equally critical as sometimes users of (Company Name) systems and information may be the first to observe a problem. Review the different types of incidents addressed in Phase II under *Incident Categorization* and list or establish reporting methods for a variety of incident types.

Table 2: Incident Reporting Guide

Incident Type	Reporting Method	Available To	Anonymous	Response Time
Website defacement, data modification or exposure	Website support contact	Customers	Yes	1 business day
Many	800 Support line	Customers & Employees	Yes	Immediate during office hours. Otherwise within 1 hour of open.
Many	IT Help Desk	Employees	No	Up to 4 hours during office hours. Otherwise within 2 hours of open.
Physical access	Alert Office Manager	Employees	No	Immediate

Many	IT emergency support line	Employees	No	Immediate

Phase II - Identification and Assessment

Identification

When a (Company Name) employee or external party notices a suspicious anomaly in data, a system, or the network, or a system alert generates an event, Security Operations, Help Desk, or CSIRT must perform an initial investigation and verification of the event.

Events versus Incidents

As defined above, Events are observed changes in normal behavior of the system, environment, process, workflow or personnel. Incidents are events that indicate a possible compromise of security or non-compliance with (Company Name) policy that negatively impacts (or maynegatively impact) the organization.

To facilitate the task of identification of an incident, the following is a list of typical symptoms of security incidents, which may include any or all of the following:

A. Email or phone notification from an intrusion detection tool.
B. Suspicious entries in system or network accounting, or logs.
C. Discrepancies between logs.
D. Repetitive unsuccessful logon attempts within a short time interval.
E. Unexplained new user accounts.
F. Unexplained new files or unfamiliar file names.
G. Unexplained modifications to file lengths and/or dates, especially in system files.
H. Unexplained attempts to write to system files or changes in system files.
I. Unexplained modification or deletion of data.
J. Denial/disruption of service or inability of one or more users to login to an account.
K. System crashes.
L. Poor system performance of dedicated servers.
M. Operation of a program or sniffer device used to capture network traffic.
N. Unusual time of usage (e.g. users login during unusual times)
O. Unusual system resource consumption. (High CPU usage)
P. Last logon (or usage) for a user account does not correspond to the actual last time the user used the account.
Q. Unusual usage patterns (e.g. a user account associated with a user in Finance is being used to login to anHR database).
R. Unauthorized changes to user permission or access.

Although there is no single symptom to conclusively prove that a security incident has taken place, observing one or more of these symptoms should prompt an observer to investigate more closely. Do not spend too much time with the initial identification of an incident as this will be further qualified in the containment phase.

NOTE: Compromised systems should be disconnected from the network rather than powered off. Powering off a compromised system could lead to loss of data, information or evidence required for a forensic

investigation later. ONLY power off the system if it cannot be disconnected from the wired and wireless networks completely.

Assessment

Once a potential incident has been identified, part or all of the CSIRT will be activated by the IR Commanderto investigate the situation. The assessment will determine the category, scope, and potential impact of the incident. TheCSIRT should work quickly to analyze and validate each incident, following the process outlined below, and documenting each step taken.

The 2 Minute Incident Assessment, found at Appendix II, should be leveraged to rapidly determine if further investigation is necessary. Further, it can be modified and used to report the incident to appropriate leadership as required.

The Incident Response Manager will assign a team member to be “Recorder” to begin formal documentation of the incident. The below determined categorization, scope, and impact must be included with documentation of the incident.

Incident Categorization

The MITRE ATT&CK Framework is a globally-accessible knowledge base of adversary tactics and techniques and should be leveraged when categorizing security incidents.While many techniques may be used in a single incident, select the method that was primarily leveraged by the adversary. Some examples of this may be:

- Phishing
- Unsecured Credentials
- Network Sniffing
- Man-in-the-Middle
- Data Destruction
- OS Credential Dumping
- Event Triggered Execution
- Account Creation
- Disk Wipe
- Network Denial of Service
- Resource Hijacking
- Defacement
- File and Directory Permissions Modification

It should be noted that the MITRE ATT&CK Framework may not address some situations, specifically those without malicious intent, that trigger the Incident Response Management Plan. The following exceptions may require categories of their own as dictated by the organization's Risk Management entities or policies:

- Data Loss
- Administrative Errors
- Unsecured Credentials
- Data Destruction
- Lax File and Directory Permissions
- Account Creation
- Disk Wipe
- Network Denial of Service
- Resource Misuse (non-malicious)
- ADD OTHERS AS APPLICABLE TO THE ORGANIZATION/INDUSTRY

Incident Scope

Determining the scope will help the CSIRT understand the potential business impact of the incident. The following are some of the factors to consider when determining the scope:

- How many systems are affected by this incident?
- Is Confidential or Protected information involved?
- What is/was the entry point for the incident (e.g. Internet, network, physical)?
- What is the potential damage caused by the incident?
- What is the estimated time to recover from the incident?
- What resources are required to manage the situation?
- How could the assessment be performed most effectively?

Incident Impact

Once the categorization and scope of an incident has been determined, the potential impact of the incident must be agreed upon. The severity of the incident will dictate the course of action to be taken in order to provide a resolution; however, in all instances an incident report must be completed and reviewed by the Incident Response Commander. Functional and informational impacts are defined with initial response activity below:

Functional Impact	Definition	CSIRT Response
None	No effect to the organization's ability to provide all services to all users.	Create ticket and assign for remediation.
Limited	Minimal effect; the organization can still provide all critical services to all users but has lost efficiency.	Create ticket and assign for remediation, notify the CIO and IHT.
Moderate	The organization has lost the ability to provide a critical service to a subset of system users.	Initiate full CSIRT, involve the CIO and IHT
Critical	The organization is no longer able to provide some critical services to any user.	Initiate full CSIRT, CIO, and IHT. Consider activation of the Disaster Recovery Plan

Informational Impact	Definition	CSIRT Response
None	No information was accessed, exfiltrated, changed, deleted, or otherwise compromised.	No action required
Limited	Public or non-sensitive data was accessed, exfiltrated, changed, deleted, or otherwise compromised.	Notify the data owners to determine the appropriate course of action.
Moderate	Internal Information was accessed, exfiltrated, changed, deleted, or otherwise compromised.	Notify the CIO and IHT. CIO will work with management, legal, and data owners to determine appropriate course of action.
Critical	Protected Data was accessed, exfiltrated, changed, deleted, or otherwise compromised.	Notify the CIO and IHT. CIO will work with legal to determine whether reportable, and the appropriate notification requirements.

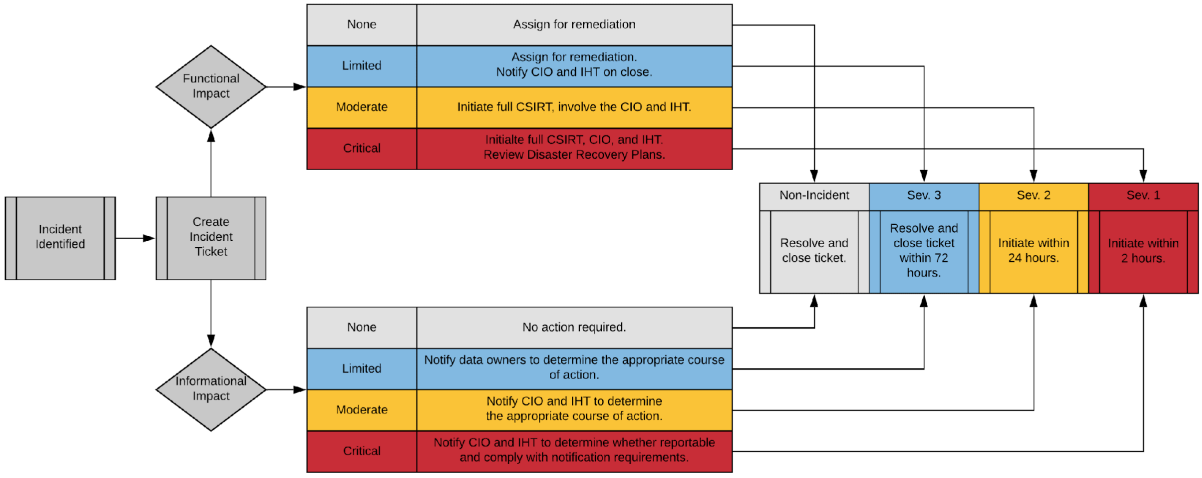
All incidents must be logged in the **Incident Handling Log & Assessment Tool** (location). A record of all action taken to remediate the incident, including chain of custody records, and deviations from SOP must be included in the documentation.

The **Incident Handling Log & Assessment Tool** and Response Level table below will help determine the severity of the incident and urgency of response activities.

Response Level Classification		Informational Impact			
		None	**Limited**	**Moderate**	**Critical**
Functional Impact	**None**	N/A	Sev. 3	Sev. 2	Sev. 1
	Limited	Sev. 3	Sev. 3	Sev. 2	Sev. 1
	Moderate	Sev. 2	Sev. 2	Sev. 2	Sev. 1
	Critical	Sev. 1	Sev. 1	Sev. 1	Sev. 1

The severity level should be used to determine how rapidlyinitial response activities should occur.

Severity Level	SLA
Sev. 3	Within three days
Sev. 2	Within 24 hours
Sev. 1	Within 2 hours



Key Decisions for Exiting Identification and Assessment Phase:

- If the Identification and Assessment process has determined the event constitutes a real incident, the IR process must be continued.
- All details in the Identification phase must be documented in the Incident Reporting Form if the event is determined to be an incident.

Phase III –Containment and Intelligence

The objective of the containment phase of the incident response is to regain control of the situation and limit the extent of the damage. To achieve this objective, (Company Name) has defined a number of containment strategies relevant to a variety of incident types. Reference the procedures related to one or more of the Containment Strategies listed below.

Containment Strategies

Use the list of strategies below to choose the procedure(s) most appropriate for the situation. Full procedures for each of the strategies listed below can be found in Appendix VIII. If none of these strategies match the current situation, refer to ***Common Containment Steps*** listed below.

- Stolen credentials – disable account credentials, reset all active connections, review user activity, reverse changes, increase alerting, harden from future attacks.
- Ransomware – isolate the impacted system, validate the ransomware claim, contact insurance carrier, identify whether additional systems have been impacted and isolate as needed.
- If DOS/DDOS - control WAN/ISP.
- Virus outbreak – contain LAN/system.
- Data loss – review user activity, implement data breach response procedures.
- Website defacement – repair site, harden from future attacks.
- Compromised API – review changes made, repair API, harden from future attacks.

Common Containment Steps

Containment requires critical decision making related to the nature of the incident. The Incident Response Manager, in coordination with the Incident Response Commander and other members of Executive Management, should review all the containment steps listed below to formulate a strategy to contain and limit damages resulting from the incident.

All attempts to contain the threat must consider every effort to minimize the impact to the business operations. Third party resources or interested parties may need to be notified. Where law enforcement may become involved, efforts must be made to preserve the integrity of relevant forensic or log data and maintain a clear chain-of-custody. Where evidence cannot be properly maintained due to containment efforts, the introduced discrepancy must be documented.

When evaluating containment steps, consider the following:

- Enable disposable Administrative accounts for use during the investigation and reset associated passwords if believed to have been at risk of compromise while in being used. (See Phase I – Preparation Details)
- Will the ability to provide critical services be impacted? How? For how long?
- When should the Cyber insurance carrier be notified? (See Contact Information)
- Is a legal investigation or other action likely? Does evidence need to be preserved? (See Preserve Evidence)
- How likely is the containment step to succeed? What is the end result,full containment or partial?
- What resources are required to support the containment activity?
- What is the potential damage to equipment and other resources?
- What is the expected duration of the solution? (temporary, short-term, long-term, or permanent)
- Should IR team members act discretely to attempt to hide their activities from the attacker?
- Is the assistance of a third party required? What is the expected response time?
- Do interested parties (customers, partners, investors) need to be notified? If so, when? (seeAppendix IV)
- Does the impact to (Company Name) equipment, network, or facilities necessitate the activation of the Disaster Recovery Plan?
- Does the data impacted include protected data such as cardholder data? If yes, refer to Notification Requirements.

Engage Resources

The CSIRT should select the option based on the severity of the incident, the damage incurred by (Company Name) and legal considerations.

	In-house investigation	Law enforcement	Private forensic specialist
Time Response	Quick response	Varies by area and agency	Quick response
Competency	Skills vary	Depends on local law enforcement	Highly skilled, often with law enforcement background
Preservation of evidence	Does not ensure evidence integrity	Preserve evidence integrity and present evidence in court	Preserve evidence integrity and present evidence in court

Reputation impact	Minimal effect	Potential loss of reputation if certain incidents reach public	Potential loss of reputation if certain incidents reach public

Preserve Evidence

NOTE: If there is strong reason to believe that a criminal or civil proceeding is likely, the (Company Name) Chain of Custody form (location) must be used any time evidence has been taken into custody, or custody is transferred for the purpose of investigation. *For incidents involving cardholder data, Visa has defined specific requirements to be followed to preserve evidence and facilitate the investigation. Refer to Notification Requirements for more information.*

Consult legal counsel regarding applicable laws and regulations related to evidence collection and preservation. Create a detailed log for all evidence collected, including:

- Identification information (e.g.serial number, model, hostname, MAC address, IP address, or other identifier).
- Name and contact information for all individuals who have handled the evidence during the investigation.
- Date and time of each transfer or handling of the evidence.
- List of all locations where the evidence was stored.
- Deviations from SOP and associated justifications.

Follow guidance from NIST SP 800-86, *Guide to Integrating Forensic Techniques into Incident Response*, when preserving evidence.

Reduce Impact

Depending on the type of incident, the team must act quickly to reduce the impact to affected systems and/or reduce the reach of the attacker. Actions may include, but are not limited to the following:

- Stop the attacker using access controls (disabling accounts, resetting active connections, changing passwords, implementing router ACLs or firewall rules, etc.).
- Isolate compromised systems from the network.
- Avoid changing volatile state data or system state data early on.
- Identify critical external systems that must remain operational (e.g. email, client application, DNS) and deny all other activity.
- Maintain a low profile, if possible, to avoid alerting an attacker that you are aware of their presence or giving them an opportunity to learn the CSIRT's tactics, techniques, or procedures.
- To the extent possible, consider preservation of system state for further investigation or use as evidence.

Collect Data and Increase Activity Logging

Increase monitoring and packet capture on affected systems while the CSIRT investigates the scope and impact of the incident. Continue increased logging and monitoring as you move onto the Eradication and Recovery phases.

- Enable full packet capture.
- Collect and review system, network, and other relevant logs.
- Create a memory image of impacted systems.

- Take a forensic image of affected systems.
- Monitor possible attacker communication channels.

Conduct Research

Performing an Internet search, consulting third party resources, and/or consulting IT Insurance carrierusing the apparent symptoms and other information related to the incident you are experiencing may lead to more information on the attack. For example, if the insurance carrier has received multiple reports of similar incidents, or if a mailing list message contains the same IP or text of the message you received.

Notify Interested Parties

Once an incident has been identified, determine if there are others who need to be notified, both internal (e.g. human resources, legal, finance, communications, business owners, etc.) and external (e.g. service providers, government, public affairs, media relations, customers, general public, etc.). Always follow the "need to know" principle in all communications. Most importantly, remain factual and avoid speculation. See Notify Interested Parties for more detail.

Depending on the degree of sensitivity of the incident, it may be necessary for Legal/Management to require employees to sign NDAs or issue gag orders to employees who need to be involved.

Key Decisions for Exiting Containment Phase

- The attacker's ability to affect the network has been effectively controlled/stopped.
- The affected system(s) are identified.
- Compromised systems volatile data collected, memory image collected, and disks are imaged for analysis.

Investigation

As the CSIRT works to contain, eradicate, and recover from the incident, the investigation will be ongoing. As the investigation proceeds, you may find that the incident is not fully contained, eradicated, or recovered. If that is the situation, additional it may be necessary to revisit earlier phases (seeFigure 1:PICERL Framework Model). The Containment, Eradication, and Recovery phases are frequently cyclical.

The investigation attempts to fully identify all systems, services, and data impacted by the incident, including root cause analysis, which helps to determine the entry point of an attacker or weakness in the system that allowed the event to escalate into an incident.

A third-party may need to be contracted if investigation is beyond the skills of the CSIRT, impacted systems are owned by a Cloud Service Provider, or forensic analysis is required.

Initial Cause ("Root Cause") Investigation

Investigation should be conducted with consideration given to the ongoing impact to critical business operations. Ideally, the Initial Cause Investigation should be concluded before leaving the Eradication phase. At times, however, it may be necessary or appropriate to continue investigation during or after eradication andrecovery. Delaying the Investigation should only be considered when the CSIRT is confident that the incident has been fully contained and the full scope of the impact is known. Delays or modifications to the scope of investigation activities must be approved by the Incident Response Commander.

The investigation techniques utilized will vary by the type of incident. The investigation may rely on some (or all) of the following:

- Interviews with witnesses and/or affected persons.
- Capturing images, snapshots, or memory dumps of affected systems.
- Obtaining relevant documents.
- Conducting observations.
- Taking photographs of physical locations.
- Reviewing security camera footage.
- Analyzing the logs of the various devices, technologies and hosts involved (e.g. firewall, router, anti-virus, intrusion detection, host).
- Reviewing email rules (compromised email account).
- Compare the compromised system to a known good copy.
- Anomaly detection/behavior monitoring (compare to preestablished baseline).

Phase IV –EradicationDetails

The Eradication consists of full elimination of all components of the incident.

Eradication

NOTE: The specific administrative tools on a compromised host could be altered versions of the originals. Use a separate set of administrative tools (e.g. boot disk) than those on a compromised host for investigation whenever possible.

Steps to eradicate components of the incident may include:

- Disable breached user accounts.
- Reset any active sessions for breached accounts.
- Identify and mitigate vulnerabilities leveraged by the attacker.
- Close unnecessary open ports.
- Increase authentication security measures (implement MFA, add geolocation restrictions).
- Increase security logging, alerting, and monitoring.
- Clean installation of affected operating systems and applications.

All re-installed operating systems and applications must be installed according to (Company Name) system build standards, including but not limited to:

A. Applying all the latest security patches.
B. Disabling all unnecessary services.
C. Installing anti-virus software.
D. Applying (Company Name) hardened system configuration baselines.
E. Changing all account passwords (including domain, user and service accounts).

NOTE: It may be possible to restore the system without the need to perform a full clean installation. IT personnel, at the direction of the CSIRT, will make this determination.

Key Decisions for Exiting Eradication Phase

- Has the root cause been identified and identified vulnerabilities been remediated?
- Have all impacted accounts, including CSIRT burner credentials been reset?

- CSIRT is confident that the network and systems are configured to eliminate a repeat occurrence.
- There is no evidence of repeat events or incidents.
- Sign-off from IR Manager for limited-severity incidents or CIO for moderate and critical-severity incidents

Phase V – Recovery Details

Prior to restoring systems to normal operation,it is critical that the CSIRT validate the system(s) to determine that eradication was successful, and the network is secure. Once the organization has been attacked successfully, the same attackers will often attack again using the same tools and techniques leveraged in the initial attack. Having gained access to the compromised system(s) or network once, the attacker has more information at their disposal to leverage in future attacks.

If feasible, the system should be installed in a test environment to determine functionality prior to re-introduction into a production environment.

Furthermore, network monitoring should be implemented for as long as necessary to detect any unauthorized access attempts.

Recovery steps may include:

- Restoring systems from a clean backup.
- Replacing corrupted data from a clean backup.
- Restoring network connections and access rules.
- Communicating with interested parties about changes related to increased security.
- Increasing network and system monitoring activities (short or long-term).
- Increasing internal communication/reporting related to monitoring.
- Engaging a third party for support in detecting or preventing future attacks.

Key Decisions for Exiting Recovery Phase

- Have business operations been restored?

Phase VI - Lessons Learned

The follow-up phase includes reporting and post-incident analysis on the system(s) that were the target of the incident and other potentially vulnerable systems. The objective of this phase is continued improvement to applicable security operations, response capabilities, and procedures.

Documentation

All details related to the incident response process must be formally documented and filed for easy reference. The following items must be maintained, whenever possible:

A. All system events (audit records, logs).
B. All actions taken (including the date and time that an action is performed).
C. All external conversations.
D. Investigator Notes compiled.
E. Any deviations from SOP and justifications.

An incident report, documenting the following will be written by the CSIRT at the end of the response exercise:

A. A description of the exact sequence of events.
B. The method of discovery.
C. Preventative measures put in place.
D. Assessment to determine whether recovery was sufficient and what other recommendations should be considered.

The objective of the report is to identify potential areas of improvement in the incident handling and reporting procedures. Hence, the review of the report by management should be documented, together with the lessons learned, to improve on the identified areas and used as reference for future incidents.

Lessons Learned and Remediation

The CSIRT will meet with relevant parties (technical staff, management, vendors, security team, etc.) to discuss and incorporate lessons learned from the incident to mitigate the risk of future incidents. Based on understanding of the root cause, steps will be taken to strengthen and improve (Company Name)information systems, policies, procedures, safeguards, and/or training as necessary. Where mitigations or proposed changes are rejected, a Risk Acceptance Process must be followed. Incidents should be analyzed to look for trends and corrective action should be considered where appropriate.

Lessons Learned discussion should cover:

- Review of discovery and handling of incident(s).
- How well staff and management performed and whether documented procedures were followed.
- Review of actions that slowed or hindered recovery efforts.
- Proposed improvements to future response and communication efforts.
- Recommendations to increase the speed of future detection and response efforts.
- Recommendations for long and short-term remediation efforts.

At the end of Lessons Learned meetings, some sort of remediation needs to occur,either resolving the issues, installing compensating controls, or at a minimum formally assessing and accepting the risk. Recommendations for long and short-term remediation efforts must be added into the overall treatment plan.

Updates to the incident response procedures should also be considered and incorporated where areas of improvement are found.

Voluntary information sharing should occur whenever possible with external stakeholders to achieve broader cybersecurity situational awareness(InfraGard, ISAC, etc.). Legal and Management must be consulted before doing so if a formal Information Sharing policy and process do not exist.

Forensic Analysis & Data Retention

In the event of possible legal action, forensic analysis will ensue in such manner as to preserve digital evidence consistent with legislative and legal requirements. Outside legal counsel and forensic experts may be required.

Consider the following when deciding whether and for how long to retain evidence related to the incident:

- Prosecution – is it likely that the attacker will be prosecuted? If so, evidence may need to be retained for multiple years.

- Reoccurrence – consider whether the evidence collected may be useful in case the attacker or a similar attack should occur in the future.
- Data Retention Policies – Consider the contents of evidence held (such as a system image capture) and retention policies related to this data (e.g. email retention policy).
- General Records Schedule (GRS) 24 specifies that incident handling records should be kept for three years.
- Cost – Depending on the type and amount of data or equipment preserved as evidence, cost may be a limiting factor.

Key Decisions for Exiting Lessons Learned Phase

- Management is satisfied that the incident is closed.
    - IR Manager makes the decision for limited-severity incidents. CIO makes the decision for moderate and critical-severity incidents.
- There is an action plan to respond to operational issues which arose from this incident. At this point, it is time to return to the Preparation Phase(See Figure 1:PICERL Framework Model).

Notification and Communication

Required notification and communication both internally and with third parties (customers, vendors, law enforcement, etc.) based on legal, regulatory, and contractual requirements must take place in a timely manner.

- The Incident Response Commander must report the incident to the senior leadership.
- The senior leadershipmust report any potential breaches and/or incidents involving customer data to the Incident Handling Team (IHT) promptly.
- The IHT is responsible for appropriate notification to:
    - Personnel.
    - Affected customers and/or partners (within 48 hours, based on SLA, based on legal or regularity compliance, whichever is shorter).
    - Local, state or federal law officials as required by applicable statutes and/or regulations.

Depending on the type and scope of breach, consider using the **Customer Data Breach Report** (location) to inform impacted business entities.

Interaction with Law Enforcement

Interaction between law enforcement and emergency services personnel should be coordinated by the Incident Response Commander.The Incident Response Commander will manage ongoing communication with authorities. It must be noted however that Law Enforcement's priorities are eventual prosecution of offenders and not necessarily returning the Company to a functional state. Ensure Legal is consulted and provides direction before and while communicating with Law Enforcement.

Regulatory Authorities

- (Company Name) is subject to various regulatory oversight, depending on the data impacted. If there is the potential that regulated data were breached, it may be necessary to notify the Secretary of the U.S. Department of Health & Human Services or Payment Card Industry Security Standards Council (PCI SSC). (See Appendix IV) Depending upon the nature of the breach it may be required to contact other governmental regulators.(Company Name)
- Only members of the IHT are permitted to discuss the nature and/or details of an incident with any regulatory agencies.
- The IHT should contact regulators as soon as practical. (See Appendix IV)

Customers

- All customers who are affected by the incident must be notified according to applicable contract language, service level agreements (SLAs), applicable statutes and/or regulations.
- Communications with customers must be consistent, with the same or similar message delivered to each. The message sent to customers will be created by members of the Communications Team.
- Customer service and/or customer account managers will communicate with customers according to the message developed by the Communications Team.

Public Media Handling

All Information concerning an incident is to be considered **confidential**, and at no time should any information be discussed with anyone outside of (Company Name) without approval of executive management and our legal counsel.

Public or media statements must be carefully managed to ensure that any investigation/legal proceedings are not jeopardized, and reputational damage is minimized. Decisions concerning the disclosure and method of disclosure of (Company Name) incident information will only be made by a designated spokesperson assigned by the IHT, likely someone from the Communications Team or a representative coached by the Communications Team.

Inquiries from media agencies must be directed to the designated IHT representative. Employeesfound to be discussing incidents without approval from executive management/legal counsel will be subject to disciplinary action, up to and including termination.

Refer to Appendix V for guidance in communicating with the Media.

Plan Testing and Review

The (Company Name) Incident Response Plan and procedures must be tested at least annually. The IR Commander will conduct training using a scheduled simulated incident to guide and test procedures. (Refer to *NIST SP 800-61r2, Appendix A—Incident Handling Scenarios* for test scenarios) The plan and procedures will be updated to reflect lessons learned and to incorporate any new industry developments.

CSIRT members, the CIO, and members of the IHT must participate in test exercises at least annually.

The Incident Response Plan and procedures are reviewed no less than annually and updates are tracked in the version history on page 1.

Plan review should include:

- Review supporting documents and forms listed in Supporting Document List (Appendix X) to ensure they are accurate and effective.
- Review Appendices to ensure they are accurate and effective.
- Review completed Incident Reporting Forms and corrective action plans for recommended plan and procedure updates.
- Compare recent changes to the organization's infrastructure and management structure to documented plan and procedures.

Appendices

Index of Appendices

- Logging, Alerting, and Monitoring Activities List
- Two Minute Incident Assessment Reference
- Incident Response Checklist
- Notification Requirements
- Media Statements
- Customer Letter Template
- Incident Response Organizations
- Containment Strategies
- Cyber Insurance and Third-Party Service Agreements
- Supporting Document List

Appendix I. Logging, Alerting, and Monitoring Activities List

Logging, alerting, and monitoring activities may target individual systems or a range of activities across multiple systems and applications. Keep a list of logging, alerting, and monitoring activities and review the list regularly to ensure that technicians can respond to abnormal events quickly. If you have a managed asset inventory these activities may be added to the existing list.

Prepared by:				**Date updated:**	
System/Application Name	**Logging System**	**Events Logged**	**System Owner**	**Monitoring frequency**	**Alerting**
Exchange Server	AlienVault	Authentication, configuration changes, service startup/shutdown/restart	Name	Daily or when alerts are received	Automated email
Webserver	Local	Content changes, administrator authentication	Web administrator	Weekly	Customer email

Appendix II. Two Minute Incident Assessment Reference

Step 1: Understand impact/potential impact (and likelihood if not an active incident)

- What is the value of the asset? If not significant, why react?
- Roughly quantify the potential worst-case impact.
- Include rough estimate of likelihood of experiencing this impact.

Step 2: Identify suspected/potential cause(s) of the issue

- Any and all possible scenarios should be considered.
- Quickly eliminate those that can be proven incorrect.
- Share most likely scenarios when communicating.

Step 3: Describe recommended remediation activities

- How do you close the hole/stop the bleeding?
- Include any steps that could reduce the experienced impact.
- Don't forget about reputation damage and legal expectations.

Step 4: Communicate to Management

- Describe the issue at a high level. (what and how it happened)
- Explain what it means to the business. (financial, reputation, etc.)
- Share short-term actions needed to move the risk from critical/high to something more acceptable.

Value of the Asset (H/M/L)	Example of high might be access to the full client database vs. low might be a proprietary internal process document with limited IP.
Potential Impact	What would the loss or felt impact be if the incident were real and fully realized? Try to quantify into both $ and impact like reputation or legal liability.
Likelihood of Impact	Immediate risk (internet accessible cataloged trivial vulnerability to exploit) of not likely known and complex (requires sophisticated expertise and specific circumstances to exploit)
Suspected causes (list all potential causes that should be investigated)	Configuration error, remote vulnerability exploited, lost device, targeted denial of service by political or financially motivated party (DDOS to cover up a fraud), etc.
Most likely cause(s)	These sources should be quickly pursued to prove correct or incorrect.
Recommended Remediation Short-term	Turn off internet, remove server from external access, implement a patch or configuration change, communicate issue to employees or customers, etc.
Long-term Actions	Change in process or architecture, acquisition of tools or systems to reduce the risk to an acceptable level over the long term.
Communication	
Describe Issue in simple terms	Describe the problem within a business context if possible. Examples are useful to illustrate the issue in operational terms.

Explain the "So What" factor	Why is this important to our business? What could it cost us if we fail to act?
Suggested Immediate Actions	Propose specific responses and why we should take them. What will taking that action provide the business with regards to reduced impact or liability? There may be more than one potential path. If there are viable options, they should be presented for decisioning.
Other Proposed Remediation	Are there follow-on risks that require additional action? Examples are communication strategy, user awareness activities, process changes, systems/tools enhancements or implementations (long-term actions)

Appendix III. Incident Response Checklist

Refer to the Incident Response Form in (Location).

No.	Description	Remarks
	Preparation Phase (IR Commander)	
1	Prepare contact list and disseminate to relevant parties	
	Identification (IT Support)	
2	Complete sections 1 and 2 of the Incident Response Form	
	Assessment (CSIRT)	
3	Complete sections 3 – 5 of the Incident Response Form	
4	Notify relevant parties.	
	Containment (CSIRT/Support)	
5	Perform system backup to maintain current state of the system	
6	Change local passwords for the affected system(s)	
	Eradication (CSIRT/Support)	
7	Do not use the system administrative tools. Use separate administrative tool sets for investigation.	
8	Re-install a clean operating system	
9	Harden the operating system (e.g. apply patches, disable unnecessary services, install anti-virus software, etc.)	
	Recovery (CSIRT/Support)	
10	Validate that the system has been hardened	
11	Restore system data with clean backup	
12	Put the affected system(s) under network surveillance for future unauthorized attempts	
	Follow-up (IR Commander)	
13	Perform post-mortem analysis on affected system(s) to identify (potential) vulnerable areas	
14	Submit an Incident Response Report for management review	
15	File all documentation on the incident response process for future reference	

Appendix IV. Notification Requirements

List all requirements that apply to the organization

Requirement	Clients Impacted	Notification Timing	Notes
PCI DSS		Immediately, no later than 24 hours after discovery	
HIPAA		No later than 60 days following a breach	
FDIC / OCC		No later than 7 days after the date on which there is a reasonable basis to conclude that a major incident has occurred	
CCPA		"…the most expedient time possible and without unreasonable delay…"	
GDPR		72 hours after becoming aware of a breach	
Add others as applicable			

PCI DSS

Any security incident involving a breach of cardholder data must adhere to all notification and response requirements of the Payment Card Industry (PCI) Security Standards Council.

Visa

Taking immediate action

Merchants and service providers that have experienced a suspected or confirmed security breach must take immediate action to help prevent additional damage and adhere to Visa CISP requirements.

Alert all necessary parties immediately:

- Your internal incident response team and information security group.
- Your merchant bank.
- If you do not know the name and/or contact information for your merchant bank, notify Visa Incident Response Manager immediately at U.S. – (650) 432-2978 or usfraudcontrol@visa.com

Loss or theft of account information

Members, service providers or merchants must immediately report the suspected or confirmed loss or theft of any material or records that contain Visa cardholder data.

Forensic Investigation Guidelines

A Visa client/member or compromised entity must engage a Payment Card Industry Forensic Investigator (PFI) to perform a forensic investigation. Visa will NOT accept forensic reports from non-approved forensic companies. It is the Visa client or member's responsibility to ensure their merchant or agent engage a PFI to perform a PFI forensic investigation. Visa has the right to engage a PFI to perform a further forensic investigation as it deems appropriate and will assess all investigative costs to the appropriate Visa client, in addition to any assessment that may be applicable. PFIs are required to release forensic reports and findings to Visa. All PFIs must utilize Payment Card Industry reporting templates.

Note: For a list of PFIs, please go to: https://www.pcisecuritystandards.org/approved_companies_providers/pci_forensic_in vestigator.php.

Note: Visa has the right to reject the report if it does not meet the PFI requirements. PFIs are required to address with Visa, the acquirer, and the compromised entity, any discrepancies before finalizing the report.

To preserve evidence and facilitate the investigation:

- Do not access or alter compromised system(s) (e.g., don't log on at all to the compromised system(s) and change passwords; do not log in as ROOT). Visa highly recommends the compromised system not be used to avoid losing critical volatile data.
- Do not turn the compromised system(s) off. Instead, isolate compromised systems(s) from the network (e.g., unplug network cable, shut down switchport, etc.).
- Preserve all evidence and logs (e.g., original evidence, security events, web, database, and firewall logs, etc.)
- Document all actions taken, including dates and individuals involved.
- If using a wireless network, change the Service Set Identifier (SSID) on the wireless access point (WAP) and other systems that may be using this connection (with the exception of any systems believed to be compromised).
- Block suspicious IPs from inbound and outbound traffic.
- Be on high alert and monitor traffic on all systems with cardholder data.

For more information on the forensic investigation guideline, please refer to the document labeled PCI Forensic Investigator (PFI) Program Guide.

MasterCard

The MasterCard Account Data Compromise User Guide sets forth instructions for MasterCard members, merchants, and agents, including but not limited to member service providers and data storage entities regarding processes and procedures relating to the administration of the MasterCard Account Data Compromise (ADC) program.

Discover

To contact Discover regarding Data Security or PCI Compliance:

Data Security: 1-800-347-3083 Call Mon–Fri 8:30am to 12:30pm and 1:30pm to 4:00pm Eastern Time, excluding holidays

Questions on Security or PCI Compliance: AskDataSecurity@discover.com

Report data compromise or cardholder data breach: 1-800-347-3083 Call Mon–Fri 8:30am to 4:00pm Eastern Time, excluding holidays

American Express

Data Incident Management Obligations: Merchants must notify American Express immediately and in no case later than twenty-four (24) hours after discovery of a Data Incident.

To notify American Express, please contact the American Express Enterprise Incident Response Program (EIRP) toll free at (888) 732-3750 (US only), or at 1-(602) 537-3021 (International), or email at EIRP@aexp.com. Merchants must designate an individual as their contact regarding such Data Incident.

Please see the American Express Data Security Operating Policy for all details pertaining to Data Incident Management Obligations.

HIPAA

Reference: http://www.hhs.gov/hipaa/for-professionals/breach-notification/

The HIPAA Breach Notification Rule, 45 CFR §§ 164.400-414, requires HIPAA covered entities and their business associates to provide notification following a breach of unsecured protected health information.

HIPAA Breach Definition

A breach is, generally, an impermissible use or disclosure under the Privacy Rule that compromises the security or privacy of the protected health information. An impermissible use or disclosure of protected health information is presumed to be a breach unless the covered entity or business associate, as applicable, demonstrates that there is a low probability that the protected health information has been compromised based on a risk assessment of at least the following factors:

1. The nature and extent of the protected health information involved, including the types of identifiers and the likelihood of re-identification;
2. The unauthorized person who used the protected health information or to whom the disclosure was made;
3. Whether the protected health information was actually acquired or viewed; and
4. The extent to which the risk to the protected health information has been mitigated.

There are three exceptions to the definition of “breach.”

- The first exception applies to the unintentional acquisition, access, or use of protected health information by a workforce member or person acting under the authority of a covered entity or business associate, if such acquisition, access, or use was made in good faith and within the scope of authority.
- The second exception applies to the inadvertent disclosure of protected health information by a person authorized to access protected health information at a covered entity or business associate to another person authorized to access protected health information at the covered entity or business associate, or organized health care arrangement in which the covered entity participates. In both cases, the information cannot be further used or disclosed in a manner not permitted by the Privacy Rule.

- The final exception applies if the covered entity or business associate has a good faith belief that the unauthorized person to whom the impermissible disclosure was made, would not have been able to retain the information.

If a covered entity determines that a breach has occurred, the following breach notification obligations apply:

1. **Notice to Individuals:** Affected individuals must be notified without unreasonable delay, but in no case later than 60 calendar days after discovery.
    a. If the covered entity has insufficient or out-of-date contact information for 10 or more individuals, the covered entity must provide substitute individual notice by either posting the notice on the home page of its web site for at least 90 days or by providing the notice in major print or broadcast media where the affected individuals likely reside. The covered entity must include a toll-free phone number that remains active for at least 90 days where individuals can learn if their information was involved in the breach.
2. **Notice to Media:** If a breach affects more than 500 residents of a state or smaller jurisdiction, the covered entity must also notify a prominent media outlet that is appropriate for the size of the location with affected individuals.
3. **Notice to HHS:** Information regarding breaches involving 500 or more individuals (regardless of location) must be submitted to HHS without reasonable delay and no later than 60 days following a breach.
    a. If a particular breach involves 500 or fewer individuals, the covered entity is required to report the breach to HHS within 60 days after the end of the calendar year in which the breach occurred via the HHS web portal.
4. **Notice by Business Associates to Covered Entities:** A business associate of a covered entity must notify the covered entity if the business associate discovers a breach of unsecured PHI. Notice must be provided without unreasonable delay and in no case later than 60 days after discovery of the breach. See the **Customer Data Breach Report** (location).
5. **Administrative Requirements and Burden of Proof:** Covered entities and business associates, as applicable, have the burden of demonstrating that all required notifications have been provided or that a use or disclosure of unsecured protected health information did not constitute a breach. Thus, with respect to an impermissible use or disclosure, a covered entity (or business associate) should maintain documentation that all required notifications were made, or, alternatively, documentation to demonstrate that notification was not required: (1) its risk assessment demonstrating a low probability that the protected health information has been compromised by the impermissible use or disclosure; or (2) the application of any other exceptions to the definition of "breach."

FDIC / OCC

When a financial institution becomes aware of an incident of unauthorized access to sensitive customer information, the institution should conduct a reasonable investigation to promptly determine the likelihood that the information has been or will be misused.

If the institution determines that misuse of its information about a customer has occurred or is reasonably possible, it should notify the affected customer as soon as possible. However, notice may be delayed if an appropriate law enforcement agency determines that notification will interfere with a criminal investigation.

Under the guidance, a financial institution should notify its primary federal regulator of a security breach involving sensitive customer information, whether or not the institution notifies its customers.

Customer Notification Content

The contents of a breach notification should contain the following elements:

- a general description of the incident and the information that was the subject of unauthorized access;
- a telephone number for further information and assistance;
- a reminder "to remain vigilant" over the next 12 to 24 months;
- a recommendation that incidents of suspected identity theft be reported promptly, and;
- a general description of the steps taken by the financial institution to protect the information from further unauthorized access or use.

Filing a SAR

https://www.ffiec.gov/bsa_aml_infobase/pages_manual/OLM_015.htm

Banks, bank holding companies, and their subsidiaries are required by federal regulationsto file a SAR with respect to:

- Criminal violations involving insider abuse in any amount.
- Criminal violations aggregating $5,000 or more when a suspect can be identified.
- Criminal violations aggregating $25,000 or more regardless of a potential suspect.
- Transactions conducted or attempted by, at, or through the bank (or an affiliate) and aggregating $5,000 or more, if the bank or affiliate knows, suspects, or has reason to suspect that the transaction:
    - May involve potential money laundering or other illegal activity (e.g., terrorism financing).
    - Is designed to evade the BSA or its implementing regulations.
    - Has no business or apparent lawful purpose or is not the type of transaction that the particular customer would normally be expected to engage in, and the bank knows of no reasonable explanation for the transaction after examining the available facts, including the background and possible purpose of the transaction.

A transaction includes a deposit; a withdrawal; a transfer between accounts; an exchange of currency; an extension of credit; a purchase or sale of any stock, bond, certificate of deposit, or other monetary instrument or investment security; or any other payment, transfer, or delivery by, through, or to a bank.

The SAR rules require that a SAR be electronically filed through the BSA E-Filing System no later than 30 calendar days from the date of the initial detection of facts that may constitute a basis for filing a SAR. If no suspect can be identified, the time period for filing a SAR is extended to 60 days.

Use this link to file a SAR: http://bsaefiling.fincen.treas.gov/main.html

State of Minnesota

For a listing of all states, see this link:
http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx

Any person or business that conducts business in this state, and that owns or licenses data that includes personal information, shall disclose any breach of the security of the system following discovery or notification of the breach in the security of the data to any resident of this state whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The disclosure must be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in paragraph (c), or with any measures necessary to

determine the scope of the breach, identify the individuals affected, and restore the reasonable integrity of the data system.

(b) Any person or business that maintains data that includes personal information that the person or business does not own shall notify the owner or licensee of the information of any breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person.

(c) The notification required by this section and section 13.055, subdivision 6, may be delayed to a date certain if a law enforcement agency affirmatively determines that the notification will impede a criminal investigation.

For purposes of this section and section 13.055, subdivision 6, "personal information" means an individual's first name or first initial and last name in combination with any one or more of the following data elements, when the data element is not secured by encryption or another method of technology that makes electronic data unreadable or unusable, or was secured and the encryption key, password, or other means necessary for reading or using the data was also acquired:

(1) Social Security number;

(2) driver's license number or Minnesota identification card number; or

(3) account number or credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account.

(f) For purposes of this section and section 13.055, subdivision 6, "personal information" does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.

(g) For purposes of this section and section 13.055, subdivision 6, "notice" may be provided by one of the following methods:

(1) written notice to the most recent available address the person or business has in its records;

(2) electronic notice, if the person's primary method of communication with the individual is by electronic means, or if the notice provided is consistent with the provisions regarding electronic records and signatures in United States Code, title 15, section 7001; or

(3) substitute notice, if the person or business demonstrates that the cost of providing notice would exceed $250,000, or that the affected class of subject persons to be notified exceeds 500,000, or the person or business does not have sufficient contact information. Substitute notice must consist of all of the following:

(i) e-mail notice when the person or business has an e-mail address for the subject persons;

(ii) conspicuous posting of the notice on the Web site page of the person or business, if the person or business maintains one; and

(iii) notification to major statewide media.

CCPA

The California Consumer Privacy Act (CCPA)was passed in 2018 and was California's attempt to bring some of the same protections (and more) offered by GDPR to the state. The law applies to for profit companies that do business in California and meet any of the following:

- Have a gross annual revenue of over $25 Million
- Buy, receive, or sell the personal information of 50,000 or more California residents, households, or devices
- Derive 50% or more of their annual revenue from selling California residents' personal information.

While California's Medical Information Specific Breach Notification Statute does specify a 15 day deadline for PHI, CCPA's timeframe is less well defined stating "…the most expedient time possible and without unreasonable delay…" Further, CCPA's definition of personal information is broader than those in GDPR. If it is believed that CCPA applies to the company, consult professional legal services when developing breach notification procedures.

GDPR

The General Data Protection Regulation (GDPR) is the toughest privacy and security legislation in the world. It was passed by the European Union (EU) on May 25th, 2018 but imposes obligations on organizations everywhere, if they collect data on people in the EU. Violation of GDPR can result in harsh fines for those who violate its privacy or security standards. Maximum violations can be either €20 Million or 4% of a company's global revenue, whichever is higher. Further, it allows individuals whose data has been mishandled to seek compensation for damages.

Per GDPR, any data breach involving the personal data of EU residents must be reported to an EU DPA within 72 hours although there are provisions that allow for the company to report reasons for delay. Due to the severe penalties involved and far reaching security requirements imposed on organizations, if the Company has business in the EU or with EU residents, they are advised to seek professional legal advice regarding their obligations.

Appendix V. Media Statements

Below are sample statements to use if members of the media call before a press release is issued. ***All communications with the media should be directed to the Incident Response Commander or other representative designated by executive management.*** Getting the facts correct is a priority. Do not give information to the media before confirming facts with internal personnel and management. Changing information after it is released can lead to media confusion and loss of focus on the key messages.

Pre-scripted Immediate Responses to Media Inquiries

Use this template if the media is "at your door" and you need time to assemble the facts for the initial press release statement.

Getting the facts is a priority. It is important that (Company Name) not give in to pressure to confirm or release information before you have confirmation.

The following responses give you the necessary time to collect the facts.

Pre-scripted Responses

If on the phone to the media:

- "We've just learned about the [situation, incident, event] and are trying to get more complete information now. How can I reach you when I have more information?"
- "All our efforts are directed at [bringing the situation under control]. I'm not going to speculate about [the situation]. How can I reach you when I have more information?"
- "I'm not the authority on this subject. Let me have [name] call you right back."
- "We're preparing a statement now. Can I get back to you in about [number of minutes or hours]?"
- "You may check our website for background information, and I will fax/e-mail you with the time of our next update."

If in person at the incident site or in front of a press meeting:

- This is an evolving [situation, incident, event], and I know you want as much information as possible right now. While we work to get your questions answered, I want to tell you what we can confirm right now:
- At approximately [time], a [brief description of what happened].
- At this point, we do not know [how long the advisory will last, how many customers are affected, etc.].
- We have a [system, plan, procedure, operation] in place. We are being assisted by [local officials, experts, our legal team] as part of that plan.
- The situation is [under, not yet under] control. We are working with [local, state, federal] authorities to [correct this situation, determine how this happened].
- We will continue to gather information and release it to you as soon as possible. I will be back to you within [amount of time in minutes or hours] to give you an update. As soon as we have confirmed information, it will be provided.
- We ask for your patience as we respond to this [situation, incident, event].

Statement Writing Tips

The following information/tips can be used to create a good media statement. Not all of them need to be included, but typically two or three will ensure an effective statement.

Honesty

If (Company Name) is at fault, admit it. By attempting to deflect responsibility, journalists and the public will be far less forgiving when the details around the incident are exposed and the Company is found wanting. Even in a real crisis, you can gain respect for holding your hands up.

If it is not your fault, you need to make it very clear without overtly blaming any other individual or organization.

- Words to use: take or share responsibility, committed to openness, transparent.
- Words not to use: blame, fault.

Context

Presenting negatives in a broad context can go a long way to minimizing the impact of the bad news.

If the story is about a service user who has had a bad experience, you can refer to the many other service users who have had good experiences. This is where external advocates are useful – particularly other service users.

Broadening context also means isolating the incident – simply a case of stating that the negative incident is 'very rare'/'isolated' and placing it within a wider, more positive framework.

- Words to use: very rare, isolated.
- Words not to use: frequent mistakes, another error.

Framing Effect

The Framing Effect is a form of cognitive bias, which causes people to prefer positive sounding statements over negative ones, despite otherwise being logically identical. For example when discussing a risky surgery, patients will be a lot more likely to go through with a surgery when it is explained that "the odds of survival one month after surgery is 90%" as opposed to "mortality within one month of surgery is 10%" despite both statements equating to the same amount of risk. Be aware of this form of cognitive bias when developing and delivering messages to the public.

Partnership

There are occasions when it is useful to subtly remind a critical audience that you are not solely responsible for the conduct of a particular individual. This can be achieved without it appearing as if you are 'buck-passing' or absolving yourselves of responsibility and without upsetting relations with other key partners.

For example, you may simply state that 'as one of a number of organizations involved in supporting the individual concerned, you are 'committed to providing the best possible service for service users in the area'.

- Word to use: working together, joint responsibility, as one of a number of organizations.
- Words not to use: X is to blame, we don't know what others think of this but.

Action

Media statements should not merely talk about the problem; they should stress action on the part of the organization.

You will not improve any media situation if you are seen to be passive in the case of a negative situation or media crisis.

A word of caution: avoid saying you will be holding an 'investigation'/'inquiry' in the case. These words are headline fodder for the media and can imply guilt.

- Words to use: taking immediate action, taking appropriate measures, working closely with.
- Words not to use: we are holding an investigation, we will look into it.

Positives

Don't be afraid to point out how successful your organization is in any media statement. Mistakes happen and emphasizing the positive things you've done can help people see past minor blips.

- Words to use: we have seen positive results, we have been successful in, we will continue to provide the best service
- Words not to use: there are a number of areas we need to work on (unless you accompany that with a positive statement e.g. that you will be taking measures to change this).

Empathy

Negative media situations obviously create a gap between you and the public involved. Expressions of empathy can help bridge the gap.

- Words to use: we understand, we appreciate, we know, we recognize.
- Words not to use: these things happen, everyone faces these issues.

Be Concise

Journalists are typically not interested in lengthy statements – they would prefer to spend the effort on details of the event/incident. Further, if the person speaking with the media is not accustomed to doing so, lengthy statements may result in the speaker making an error.

As a rule, statements for printed media should be no more than two paragraphs long – one tight sentence per paragraph.

Broadcast media may give you more space, but you should still bear length in mind as the producer/editor may be looking to produce a shortened version of your statement to drop into a later news bulletin.

Statements Should Avoid

- **Confrontation** - the objective of media statements in a crisis is to diffuse the situation – not make it worse. Avoid blaming/buck-passing because it will simply result in a media-based argument between opposing parties – remember journalists love confrontational stories. e.g. 'They were wrong', 'it is not our fault'…
- **Ambiguity** - weak, ambiguous statements have no place in handling negative media situations and can leave room for the journalist to re-interpret your response. Be robust and clear at all times. Use strong positive words e.g. 'we are committed to X and will not tolerate Y'. Make sure your statement is completely unambiguous.
- **Personal pronouns** - try and avoid referring to your organization by name in your media statement as doing this could reinforce the link between your organization and the negative issue concerned. You may simply use the first-person plural ('we'/'us'). This also has the advantage of adding a slightly personal and less bureaucratic feel to the statement.

Appendix VI. Customer Letter Template

Formal Email and/or Letter Template

Dear Valued Customer,

As you may be aware, (Company Name) has announced that it experienced a criminal intrusion into a portion of its computer network in some of its retail stores. This criminal intrusion may have resulted in the theft of account numbers, expiration dates, and other numerical information and/or the cardholder's name. The company has not determined that any such cardholder data was in fact stolen by the intruder, and it has no evidence of any misuse of such data.

(Company Name) is providing this notice out of an abundance of caution to all of its customers who have provided their contact information to the company, including you. **YOUR INFORMATION IS NOT NECESSARILY AFFECTED**.

(Company Name) believes that the potentially impacted systems were breached during the period of <insert date> through <insert date>.

Upon recognition of the intrusion, (Company Name) took immediate steps to secure the affected part of its network. An investigation supported by third-party data forensics experts is going on to understand the nature and scope of the incident. (Company Name) believes the intrusion has been contained and is confident that its customers can safely use their credit and debit cards in its stores. (Company Name) currently has no reason to believe that additional information beyond that described above was stolen by the intruder. However, given the continuing nature of this investigation, it is possible that time frames, location, and/or at-risk data in addition to those described above will be identified in the future.

The Company has notified federal law enforcement authorities and is cooperating in their efforts to investigate this intrusion and identify those responsible for the intrusion. The press release and this letter have not been delayed as a result of this law enforcement investigation. (Company Name) has also notified the major payment card brands and is cooperating in their investigation of the intrusion.

(Company Name) has established a call center to answer customer questions about the intrusion and the identity protection services being offered. The call center will be staffed Monday through Friday 8am-8pm CST.

You are a valued customer and we regret any inconvenience that this may cause you.

Sincerely,

<insert name and title>

Possible other considerations to include depending on the nature of the incident

- Provide free credit reports (www.annualcreditreport.com or 1-877-322-8228)
- Fraud Alerts – Equifax (www.equifax.com or 1-877-478-7625), Experian (www.experian.com or 1-888-397-3742), TransUnion Fraud Victim Assistance Division (www.transunion.com or 1-800-680-7289)

Appendix VII. Incident Response Organizations

Below is a list of incident response organizations that may be useful in planning for or responding to an incident:

Organization	URL
Anti-Phishing Working Group (APWG)	https://www.antiphishing.org/
Computer Crime and Intellectual Property Section (CCIPS), US Department of Justice	https://www.justice.gov/criminal-ccips
CERT Coordination Center	https://www.sei.cmu.edu/about/divisions/cert/index.cfm
European Network and Information Security Agency (ENISA)	https://www.enisa.europa.eu/
Government Forum of Incident Response and Security Teams (GFIRST)	https://www.us-cert.gov/government-users/collaboration/gfirst
High Technology Crime Investigation Association (HTCIA)	https://htcia.org/
InfraGard	https://www.infragard.org/
Internet Store Center (ISC)	https://isc.sans.edu/
National Council of ISACs	https://www.nationalisacs.org/
United States Computer Emergency Response Team (US-CERT)	https://www.us-cert.gov/

Appendix VIII. Containment Strategies

(Delete if these exist in SOPs or other documentation, samples are provided below -edit as applicable for your environment. Review Common Containment Steps on page for ideas of what to include in these procedures.)

The following containment strategies have been defined to assist in incident response. If none of the containment strategies outlined below fit the current situation refer to Phase III – Containment*:* Common Containment Steps *on page of this plan.*

Stolen credentials

Containment

Reduce Impact:

- Change the password or disable affected accounts
- If the compromised account had administrator access review activity logs for additional accounts that may have been created. Disable any accounts created by the attacker.

Notify Interested Parties:

- Notify the users responsible for the impacted accounts

Investigation

- Attempt to determine the date and time that the account was compromised
- Review all activities completed by the compromised account during the period of compromise. If logs do not exist, check all configurations the account had access to modify. (e.g. for a compromised email account, check for added or changed forwarding rules)

Eradication and Recovery

- Reverse changes made by the compromised account during the time of compromise

Ransomware

Containment

1) *Block access to command and control (C2) servers*
2) *Set file shares into read-only mode*
3) *Check ownership of encrypted files to determine infected users*
4) *Recall known phishing emails from user mailboxes*
5) *Take infected systems offline*

Eradication & Recovery

1) *Patch third-party applications as soon as possible*
2) *Test and validate back-up processes*
3) *Deploy GPO to block executables and disable macros*
4) *Block email attachments based on file signature and/or extension*
5) *Remove local administrative rights*

Virus Outbreak

Containment

1) *Update antivirus software*
    a. *Obtain detection signature and technical description for virus from AV vendor*
    b. *Test detection signature update provide in test environment*
    c. *Distribute fix to environment*
2) *Submit sample file to AV vendor if latest virus signature does not detect the infection*

Eradication & Recovery

3) *Eradicate the virus, if necessary*
    a. *Contain virus/attack (depending on virus this could include partitioning the network, disabling SMPT email, changing content filtering to block attachments or specific strings of text, removing workstations from the network, etc.)*
    b. *Identify infected systems*
4) *Environment cleanup:*
    a. Obtain the detection signature and any required fix tools for the virus from your antivirus vendor.
    b. Test the fix provided by your vendor for the virus in your virus signatures staging lab. This may include separate repair tools that you need to run before using the updated virus signatures.
    c. Develop a deployment methodology for the fix process.
    d. Create a cleanup plan and validate with all affected teams and your antivirus vendor.
    e. Clean all infected perimeter and email servers and update the virus signatures of the antivirus software providing protection of these avenues of infection.
    f. Distribute the fix to all the workstations and servers in your environment using whatever method you have in place for rapid deployment.
    g. Isolate systems that are infected and require repair.
    h. Run all required fix tools on all infected systems in order to remove the virus from memory or disable it.
    i. Scan all systems with the updated virus signatures to remove all infected files.
    j. Eliminate all temporary and suspicious files, including hidden directories and files.
    k. Remove or alter configuration information used for the functionality of the virus or that might allow the virus to reappear.
    l. Remove configuration information that may cause system failures.
    m. Search for newly mounted partitions created by the virus and eliminate them.
    n. Search for missing log partitions and restore.
    o. Search for added or altered user accounts and remove or restore.
    p. Restore changed or deleted files.
    q. Distribute patch updates to all systems and update patch levels

Appendix IX. Cyber Insurance and Third-Party Service Agreements

Where Cyber Insurance or Third-Party Services are involved, having a clear understanding of their incident response and detection services is essential. For example, many cyber insurance carriers require the organizations they cover to follow a pre-defined process. Examples of third-party service providers that may be involved in IR activities include insurance providers, internet service provider (ISP), cloud service provider (CSP), software vendors, or a multiservice provider (MSP).

The CIO is responsible for reviewing all SLAs with service providers to ensure that responsibilities and expectations are defined in relation to incident response.

IR Commanders are responsible for understanding SLAs with service providers and knowing when the team should engage the service provider.

Table 3: Third Party Support and Response

Service Provider	Applications/Services	When to contact	Service Level/Response Time

Table 4: Insurance Coverage and Contact Information

Insurance Provider	Limits	Term Dates	When to contact	Contact Information
XX *(Primary)*		January 1, 2023-24	Immediately, any financial or data loss	
XX *(Excess)*		January 1, 2022-24	Immediately, any financial or data loss	

**Additional coverage sub-limits may apply per claim.*

Find a copy of the Insurance Declaration page [here]. Direct questions about insurance coverage limits to the Risk Manager. Notify the Risk Manager to activate the insurance plan.

Appendix X. Supporting Document List

- Incident Management Policy – Owner & Location
- Incident Assessment Form/Categorization Sheet - Owner & Location
- Incident Reporting Form - Owner & Location
- Chain of Custody Form - Owner & Location
- Executive Incident Assessment Checklist – Owner & Location
- Logging Standard – Owner & Location
- Customer Data Breach Report – Owner & Location
- Logging, Alerting, and Monitoring Activities List – Owner & Location
- Notification Requirements - Owner & Location
- Relevant documented procedures– see Containment Strategies
- Vulnerability Management Policy/Standard – Owner & Location
- Risk Acceptance Policy/Process – Owner Location
- Data Classification Policy – Owner & Location