**Cybersecurity Incident Response Plan**

[Date]

**Overview**

The Cybersecurity Incident Response Plan (CIRP) documents detailed guidance for general enterprise incident management (EIM) and communication about cybersecurity issues, including high impact cyber incidents, vulnerabilities and threats, within the organization, and to impacted stakeholders throughout the enterprise. The organizational structure, operational structure, processes, and procedures outlined in this plan will assist with identifying, managing, investigating, and remediating various types of cybersecurity issues.

The CRP provides the scope, process framework, roles and responsibilities, and communications templates and mechanisms to facilitate information sharing and reporting about technical and cross-enterprise response and remediation activities. The CRP defines the appropriate channels through which information will flow during a cyber incident.

|  |  |
| --- | --- |
| **Scope**: | High and critical severity cybersecurity issues, such as vulnerabilities, threats and incidents, including those impacting the business, assets (e.g., Crown Jewels, etc.), or customers/patients. |
| **Document Managers:** | [Enterprise Name] |

**Version History**

This is a living document, which will be formally reviewed and revised on an annual basis. It may also be periodically updated as an after-action activity resulting from exercises and real-world incidents.

|  |  |  |
| --- | --- | --- |
| **Version** | **Revision Date** | **Notes** |
|  |  |  |

The CRP and its accompanying communications products and templates will be stored within the enterprise SharePoint or secure repository. The cybersecurity team will review this document on an annual basis and test it through tabletop exercises.

Cybersecurity Response Plan

Table of Contents

[1. Introduction 4](#_Toc164108875)

[1.1 Introduction 4](#_Toc164108876)

[1.2 Purpose 4](#_Toc164108877)

[1.3 Goals 4](#_Toc164108878)

[1.4 Scope 5](#_Toc164108879)

[1.5 Escalation Flow 5](#_Toc164108880)

[1.6 Severity Matrix 5](#_Toc164108881)

[2. Cybersecurity Response Process Overview 6](#_Toc164108882)

[2.1 Roles & Responsibilities 6](#_Toc164108883)

[2.1.1 CRP Commander 6](#_Toc164108884)

[2.1.2 Communications Lead 7](#_Toc164108885)

[2.1.3 Technical Response SMEs 7](#_Toc164108886)

[2.1.4 Communications Liaisons 7](#_Toc164108887)

[2.1.5 Corporate Response SMEs 7](#_Toc164108888)

[2.2 Process Framework 7](#_Toc164108889)

[3. Process Manual 9](#_Toc164108890)

[3.1 Preparedness 9](#_Toc164108891)

[3.2 Detection & Assessment 9](#_Toc164108892)

[3.3 Containment, Response & Recovery 13](#_Toc164108893)

[3.4 Post-Incident Activity 14](#_Toc164108894)

[4. Coordination Resources 16](#_Toc164108895)

[4.1 Coordination and Communications Tools 16](#_Toc164108896)

[4.2 Setting Up the War Room 16](#_Toc164108897)

[4.2.1 Establishment of a War Room 16](#_Toc164108898)

[4.2.2 Decommission of a War Room 17](#_Toc164108899)

[4.3 CRP Operational Tempo 17](#_Toc164108900)

[4.4 Communications Templates 17](#_Toc164108901)

[SOC Generated Content 17](#_Toc164108902)

[Escalation Brief and Deck 18](#_Toc164108903)

[Activation Text Messages 19](#_Toc164108904)

[Escalation Emails 19](#_Toc164108905)

[Meeting Agendas for Technical and Managerial Coordination Meetings 20](#_Toc164108906)

[SOC Priority Report 22](#_Toc164108907)

[Post-Mortem Report 22](#_Toc164108908)

[4.5 Privileged Communication and Appropriate Document Markings 22](#_Toc164108909)

[Appendix A Glossary 23](#_Toc164108910)

[Appendix B Associated Plans and Procedures – Internal 25](#_Toc164108911)

[Appendix C Associated Plans and Procedures – External 25](#_Toc164108912)

[C.1. Protected Health Information (or Personal Health Information) 26](#_Toc164108913)

[C.2. Individual Notice 26](#_Toc164108914)

[C.3. Media Notice 26](#_Toc164108915)

[C.4. Administrative Requirements and Burden of Proof 27](#_Toc164108916)

[C.5. Credit Card (Payment Card Industry) 27](#_Toc164108917)

[C.6. Personally Identifiable Information 28](#_Toc164108918)

[C.7. Cyber Liability Insurance 28](#_Toc164108919)

[Appendix D Additional Resources 29](#_Toc164108920)

[D.1. Revisable Communications Products and Templates 29](#_Toc164108921)

[D.2. Crown Jewels and Critical Assets 29](#_Toc164108922)

# Introduction

## Introduction

Company Information Technology (IT) systems are fundamental to business operations, and any problem affecting IT resources can quickly impact the business. Responding efficiently and effectively to cybersecurity issues is crucial for minimizing risks to the business, customers, and the partners. This Cybersecurity Response Plan (CRP), along with the greater Cybersecurity Team defined herein will enable the Company to effectively respond to cybersecurity issues.

## Purpose

The purpose of this plan is to provide organizational structure, operational structure, processes, and procedures to Company personnel, so that they can properly respond to High and/or Critical vulnerabilities, threats, and incidents that may affect the function and security of IT assets, information resources, and business operations.

The CRP will assist Client in identifying, managing, investigating, and remediating various types of cybersecurity issues. It describes the processes for initiating a response and establishing the structure needed to ensure response execution. This CRP will also reference procedural documentation that provides operational-level details specific to handling the various incident types (see Appendices).

This CRP documents guidelines and resources for internal procedures during a cybersecurity incident to help effectively communicate about the technical, corporate, and executive activities during a cybersecurity incident. Associated plans and procedures, such as Corporate Crisis Management Plans and Privacy and Compliance Procedures, and scenario-specific playbooks that address tailored play-by-play for the most common cybersecurity issues are available in Appendix B.

## Goals

The CRP will help accomplish the following objectives:

* Ensure the safety of our products and patients.
* Compliance with all applicable laws and regulations.
* Minimize interruptions in service for customers and clients.
* Retain customer/client/consumer confidence.
* Document the occurrence of the incident and the actions taken in response.
* Determine and report what occurred and how it occurred.
* Obtain and preserve information regarding the incident.
* Determine the known facts of the incident.
* Determine the timeline of events that transpired during the incident.
* Establish a basis for making operational business decisions that cause a positive outcome from the incident response.
* Notify all appropriate parties.
* Assess the impact of the incident on Client personnel or business operations.
* Contain the incident, avoiding further escalation.
* Remediate and recover from the incident.
* Determine how to avoid recurrence of similar incidents and vulnerabilities.
* Update existing (or develop new) policies and procedures as needed.
* Determine the need for legal recourse as necessary.

## Scope

The criteria for what constitute a High or Critical severity cybersecurity issue is outlined in Section 2.3. For more information on what constitutes a cybersecurity issue, see Figure 1.1.



Figure 1.1 Table of In-Scope and Out-of-Scope Events with Sample Scenarios

## Escalation Flow

The core cybersecurity response team is comprised of CTI, IR, TDO, Forensics, VM, CYBER STRATEGY & OPS , and the CRP Commander. Extended business units - Communications Liaisons and Corporate Response SMEs, are included in the full cybersecurity response team, but sit outside of the CFC.

When the core cybersecurity response team detect a High or Critical severity security issue, the following sequential next steps will ensue:

## Severity Matrix

The Severity Matrix identifies the circumstances for activating the CRP. It categorizes security issues as Low, Medium, High and Critical. The CRP should only be triggered for cybersecurity issues that meet the High and Critical thresholds.

The Severity Matrix may be used as a guide to help discern whether a situation would warrant the activation of the CRP. The Severity Matrix also helps CYBER STRATEGY & OPS work together with adjacent technical and functional teams to determine the audience and appropriate communications tools necessary to communicate.

All checkboxes listed under the High or Critical category **DO NOT** need to be checked off in order to activate the CRP.

When teams are having difficulty determining the severity, CYBER STRATEGY & OPS will facilitate dialogue across teams to help determine the severity. Additionally, if any of the following top priorities are impacted, the CRP should be initiated.

1. **Priority One:** Protect human life and safety.
2. **Priority Two:** Protect critical business operations, systems, and networks.
3. **Priority Three:** Protect sensitive data, such as, PII/PCI.

The criteria for determining what qualifies as a critical asset is available in Appendix B. The list of Crown Jewels will be provided by the IT Resource Management Services team.

The accompanying communications products and templates paired with each severity category are available in Section 4.



Figure 1.3 Screenshot of Severity Matrix checklist

# Cybersecurity Response Process Overview

This section provides framework for coordinating cybersecurity response communications activities. This section defines roles and responsibilities, highlights functional relationships along with management hierarchy, and includes a flowchart denoting process and information flow at each phase of the cybersecurity response lifecycle.

## Roles & Responsibilities

This section outlines key roles and responsibilities related to communications during a cybersecurity incident.

There are five key roles. The Incident Response Commander, Communications Lead and Technical Response SMEs are roles within the CFC. The Communications Liaisons and Corporate Response SMEs are corporate and communications roles beyond the SOC that are primarily responsible for extending communications throughout the business and if necessary, externally to the public and media. See Figure 2.1 to see a summary of roles and responsibilities.

Swim lanes will engage the RSA Archer Incident Management (“Archer”), xMatters, and Remedy tools to accomplish their roles and responsiblities. Section 3 details how the tools will help expedite the overall process framework in each phase of the IR lifecycle.

## CRP Commander

The CRP Commander at Client has the ultimate ownership for ensuring that a cybersecurity response effort is conducted in an efficient and effective manner and holds the overarching responsibility to the Executive Leadership and the Board of Directors to ensure that Client is able to appropriately respond to cybersecurity incidents.

## Communications Lead

The CYBER STRATEGY & OPS team serves as a cornerstone in information sharing and reporting processes by facilitating communications throughout the SOC, as well as up and out of the SOC to adjacent Corporate Response SMEs and Communications Liaisons.

## Technical Response SMEs

Technical Response SMEs are primarily comprised of teams and personnel within the SOC as well as specific technical teams within ITRMS, such as, the Data Loss Prevention team, that are highly likely to be at the forefront of any incident response effort. They provide technical expertise at the initial discovery of a cybersecurity issue, and provide insight and assistance throughout the cybersecurity lifecycle, containing and remediating the situation. Technical Response SMEs work closely with the CYBER STRATEGY & OPS team to provide regular situational updates and data for reporting.

## Communications Liaisons

Communications Liaisons are comprised of teams and personnel that are responsible for contextualizing messages for their respective audiences and disseminating messaging from CYBER STRATEGY & OPS to the larger enterprise, and at times, to the media and public. They are also responsible for capturing questions from the extended business and funneling them back to the SOC via CYBER STRATEGY & OPS for clarification. It is critical for communications liaisons to keep open lines of communications with the CYBER STRATEGY & OPS team to maintain awareness of the cybersecurity situation and provide clear updates and next steps to the extended business, as necessary.

## Corporate Response SMEs

Corporate Response SMEs are comprised of departments and personnel that may be called upon to engage their specific expertise during cybersecurity response effort. The frequency, complexity, and diversity of incidents that may occur necessitate that these organizations remain in an “as-needed” status. Once engaged and participating in the CRP, the team will take direction from the CRP Commander for the purposes of responding to the cybersecurity issue until they are no longer required for the effort. The severity of the incident will dictate the depth of their engagement, whether engaged full time or for some portion of their workday.

Figure 2.2 Functional relationships during an incident, denoting process and information flow along with management hierarchy.

## Process Framework

The CRP process framework is triggered in the event of a High or Critical cybersecurity issue. The framework shows the specific coordination steps across all roles and responsibilities during a High or Critical cybersecurity issue.



*\*Templates and samples of communications products are available in Section 5.4.*

Figure 2.3 Activities that take place throughout a full Cybersecurity response lifecycle

Detailed instructions for each phase of the process are further described in Section 3, and additional resources and templates to execute these activities are provided in Section 4. Section 3 details how the tools will help expedite the overall process framework in each phase of the cybersecurity response lifecycle.

# Process Manual

This section describes the detailed steps for each phase of the full cybersecurity response lifecycle.

## Preparedness

During the Preparedness phase, the key players consist of Technical Response SMEs and the Communications Lead.

SOC teams will regularly update CYBER STRATEGY & OPS and the CRP Commander by sharing updates during the ITRMS – SOC Daily Briefing. The ITRMS – SOC Daily Briefing can be supported by other SOC generated communications products, such as the CYBER THREAT INTEL Flash Report or relevant case tickets.

|  |
| --- |
| Preparedness |
|  |
| Role | Process Steps | Outputs |
| SOC Technical Response SMEs | * Provide the CYBER STRATEGY & OPS team and CRP Commander with daily updates on the status of Client’s cyber environment as well as cybersecurity issues at large outside of Client’s environment
 | * Daily Standup Meeting
 |
| CYBER STRATEGY & OPS  | * Maintain and update the CRP, as needed
 | * CRP
 |
| Success Criteria:* The SOC technical teams and CYBER STRATEGY & OPS team expediently share clear, usable information about Client’s internal cyber environment and the cyber landscape at large.
* All high and critical incidents are quickly accompanied by the appropriate communications product.
 |

## Detection & Assessment

During the Detection & Assessment phase, the key players include the Technical Response SMEs, the Communications Lead and the CRP Commander. Corporate Response SMEs and Communications Liaisons will be notified and called in to analyze the situation towards the tail end of this phase.

In the event the Technical Response SMEs within the Cyber Fusion Center (CFC) were to detect a vulnerability, threat or incident that meets the criteria for a High or Critical cybersecurity issue, they would escalate a Threat Ticket via Archer with initial context to the IR Manager. Upon discovery, SOC teams are empowered to determine the severity of the situation and make a strong recommendation on the severity of the cybersecurity issue. CYBER STRATEGY & OPS is available to facilitate conversation among SOC teams to help SOC teams come to a unanimous decision on incident severity.

**Order of Succession**

*In the absence of a clear successor, CYBER STRATEGY & OPS will facilitate conversations across SOC teams to appoint a CRP Commander.*

**Determining Severity**

*Depending on where the cyber event originates, the SOC team that first discovers the incident is empowered to determine initial incident severity. CYBER STRATEGY & OPS will also facilitate conversation among SOC teams via the SOC Initiation Meeting to help SOC teams come to a unanimous decision on incident severity.*

When a unanimous decision is reached and the cybersecurity issue is deemed as a High or Critical severity issue, CYBER STRATEGY & OPS will open the technical bridge.

CYBER STRATEGY & OPS will notify the SOC Director, who then assumes the role of CRP Commander. In the absence of the SOC Director and Deputy Director, CYBER STRATEGY & OPS will notify the IR Manager who will then assume the role of CRP Commander. In the absence of a clear successor, CYBER STRATEGY & OPS will facilitate conversations across SOC teams to appoint a CRP Commander.

The CRP Commander will then call the Global Operations Center (GOC) at **(XXX) XXX-XXXX** and click “Option 1”, to report the High or Critical severity cybersecurity issue, request that an Activation Text be sent via xMatters, and that the Escalation Email (pre-populated by the CYBER STRATEGY & OPS team) be forwarded to notify Corporate Response SMEs and Communications Liaisons. The CRP Commander can also notify the GOC of the High or Critical severity cybersecurity issue via the GOC Edge mobile application.

**Contact the GOC**

*It is critical to notify the Global Operations Center (GOC) at the initial discovery of a High or Critical cybersecurity issue. When notified, the GOC will alert respective stakeholders of the discovery, as well as other major events and executive decisions – especially decisions that may have “business impact”, such as taking a server and/or application offline.*

*Contact the GOC via* XXXX at XXXX@client.com *or by calling the GOC Hotline at* **(XXX) XXX-XXXX***. Click Option 1.*

*The CRP Commander can also notify the GOC via the GOC Edge mobile application.*

*In the case that the GOC lead is unavailable, reach out to the* ***Global Operations Center Tier 3 Team*** *at* globaloperationscentertier3@Client.com.

The GOC will open the managerial bridge for senior management and extended business units.

The CYBER STRATEGY & OPS team will play a critical role in facilitating knowledge sharing, providing updates that are congruent within the SOC as it is across the business, and facilitating communication and coordination throughout the IR lifecycle.

In the case that a Crown Jewel were to be impacted, contact XXXX at XXXX@client.com. To verify whether a Crown Jewel has been impacted, refer to the list of Crown Jewels, provided by the IT Resource Management Services team.

In the case that a priority site was to be impacted, contact XXXX at XXXX@client.com. To verify whether a priority site has been impacted, refer to the list of priority sites in Appendix C.

|  |
| --- |
| **Detection & Assessment** |
|   |
| Role | Process Steps | Outputs |
| Technical Response SMEs | * Inform CYBER STRATEGY & OPS team of vulnerabilities, threats and incidents via the SOC Daily Briefing and other SOC generated communications products (e.g., CYBER THREAT INTEL Flash Report)
* What system does the incident impact?
* Who does it impact?
* What is the business impact?
* What initial actions have been taken to contain the incident?
* What actions should stakeholders take?
* Conduct initial analysis and communicate the root cause, if known
* Consult the Severity Matrix to determine the severity
* Report updates via the Technical Coordination Meeting\*
* Global Operations Center will open the Managerial Coordination Meeting\*, including the CRP Commander, Corporate Response SMEs and Communications Liaisons
 | * SOC Daily Briefing
* SOC Generated Communications Products (e.g., CYBER THREAT INTEL Flash Report)
* Managerial Coordination Meeting\*
* SOC Initiation

Meeting |
| CRP Commander | * Call the Global Operations Center at **(XXX) XXX-XXXX** and click “Option 1”. Request to send the Activation Text\* and forward the Escalation Email\* to alert Corporate Response SMEs and Communications Liaisons.
* Provide initial information to Corporate Response SMEs and Communications Liaisons by forwarding the Escalation Brief\*
 | * Activation Text\*
* Escalation Email\*
 |
| Comms Lead | * Interface between the functional response teams to collect necessary information about the nature of the incident such as:
	+ What system does the incident impact?
	+ Who does it impact?
	+ What is the business impact?
	+ What initial actions have been taken to contain the incident?
	+ What actions should stakeholders take?
* Facilitate conversations across SOC teams to help determine severity via the SOC Initiation Meeting
* Document all findings within the initial Escalation Brief\*
* Maintain an activity log and record key decisions along a timeline
* Send Escalation Brief\* to CRP Commander
* Set up the Technical Coordination Meeting\*, including Technical Response SMEs, the CRP Commander and CYBER STRATEGY & OPS team
* Equip CRP Commander with sufficient information to report to Corporate Response SMEs and Communications Liaisons
 | * Escalation Brief\*
* SOC Initiation

Meeting |
| Corporate Response SMEs & Comms Liaisons | * Maintain full awareness of the situation
* Regularly attend the Managerial Coordination Meetings\*
* Activate associated plans to communicate updates to appropriate stakeholders
 | * Associated Plans
 |
| Success Criteria:* The Technical Response SMEs and CYBER STRATEGY & OPS team expediently share clear, usable information about High and Critical severity cybersecurity issues with the CRP Commander within 4 hours for a High and 2 hours for a Critical severity cybersecurity issue, paired with the appropriate Threat Ticket and other SOC collateral used to provide technical updates (e.g., CYBER THREAT INTEL Flash Report, case tickets).
* Information shared within and beyond SOC are congruent.
* All Corporate Response SMEs and Communications Liaisons join the appropriate call for updates and next steps within 4 hours for a High severity cybersecurity issue, and 2 hours for a Critical severity cybersecurity issue.
 |

## Containment, Response & Recovery

During the Containment, Response & Recovery phase, all swim lanes are fully engaged – Technical Response SMEs, Communications Lead, CRP Commander, Corporate Response SMEs and Communications Liaisons.

**External Inquiries**

*Do* **NOT** *speculate about the incident or provide information about the incident. If a member of the Cyber Fusion Center or any other internal stakeholder is contacted by an external source, the proper procedure is to redirect them to the appropriate department.*

*A detailed script is available in section C.3. Media Relations for reference.*

* *For media inquiries, refer them to the Media Relations team at* *mediarelations@Client.com* *and the Corporate Crisis Management team at* kevin.cruise@Client.com*. Detailed instructions for how one should respond to media inquiries is available in* ***Appendix C.3 Media Relations****.*
* *For third parties and quasi-external parties, refer them to* XXXX at XXXX@client.com

After the CRP Commander alerts the Corporate Response SMEs and Communications Liaisons of the cybersecurity issue and the full IR team is debriefed via their respective Technical Coordination Meeting and Managerial Coordination Meeting, the CYBER STRATEGY & OPS team collects updates from the SOC teams to draft succinct and clean updates in the form of an updated Escalation Brief, to send to the CRP Commander for quick sharing with Corporate Response SMEs and Communications Liaisons. This will allow technical teams within the SOC to focus on addressing the cybersecurity issue at hand, while CYBER STRATEGY & OPS and the CRP Commander focus on communicating with adjacent Corporate Response SMEs and Communications Liaisons to extend communications to the rest of the enterprise, and enable them to activate associated plans appropriately and make informed enterprise-wide decisions to maintain business operations. See Appendix B to see a list of associated plans.

After the cybersecurity issue has matured, CYBER STRATEGY & OPS will consolidate data collected from all SOC technical teams, Escalation Briefs and other SOC generated content, and draft a SOC Priority Report for circulation.

|  |
| --- |
| **Containment, Response & Recovery** |
|   |
| Role | Process Steps | Outputs |
| Technical Response SMEs | * Conduct containment, response and recovery activities
* Provide real-time updates to the CYBER STRATEGY & OPS team regarding the cybersecurity issue
* Review content created by the CYBER STRATEGY & OPS team to ensure accuracy
 | * SOC Generated Communications Products (e.g., CYBER THREAT INTEL Flash Report)
 |
| CRP Commander | * Share Progress Report\* with Corporate Response SMEs and Communications Liaisons
* Review content created by the CYBER STRATEGY & OPS team to ensure accuracy
* Facilitate regular Managerial Coordination Meetings\*
* Funnel questions from across the business via the Corporate Response SMEs and Communications Liaisons to GMC
 | * Managerial Coordination Meetings\*
 |
| Comms Lead | * Interface between the technical response teams and CRP Commander to continue to provide updates via the Progress Report\* and SOC Priority Report\*
* Equip CRP Commander with sufficient information to report up and out of the SOC
* Facilitate regular Technical Coordination Meetings\*
* Collaborates regularly with Technical Response SMEs to provide answers to questions from across the business
 | * Updated Escalation Brief\*
* SOC Priority Report\*
* Technical Coordination Meetings\*
 |
| Corporate Response SMEs and Communications Liaisons | * Continue actions from Detection & Analysis phase
* Submits questions to IT Help Desk, which then generates a Remedy ticket for CFC
 | * Associated Plans
 |
| Success Criteria:* Information shared within and beyond SOC are accurate.
* Next steps are implemented swiftly, due to clear and well-communicated instructions.
* Materials succinctly and clearly communicate relevant, useable, and need-to-know information.
* Corporate Response SMEs and Communications Liaisons are quickly and comprehensively communicated to about the situation, and are provided with sufficient information to be able to activate associated plans.
* Extended communications are responsive, transparent, and controlled.
* Questions are addressed in a timely manner.
 |

## Post-Incident Activity

During the Post-Incident Activity phase, only the SOC teams and CYBER STRATEGY & OPS team continue to engage in the CRP.

Following the Containment, Response & Recovery phase, the CYBER STRATEGY & OPS team collects data from the SOC teams to create an in-depth post-mortem report summarizing the performance throughout the full cybersecurity response lifecycle. The report will include lessons learned and guide improved EIM in the future.

|  |
| --- |
| **Post-Incident Activity** |
|  |
| Role | Process Steps | Outputs |
| Technical Response SMEs | * Collaborate with CYBER STRATEGY & OPS Team on After Action review
 | * Timeline of events
* Data for Post-Mortem Report
 |
| Comms Lead | * Collect metrics on the reach and response of all communications messaging including:
* Audiences reached
* Audience sentiment
* No. and type of communications issued
* Long-term follow-ups needed
* Document and archive communications materials and high-level insights based on audience response to inform lessons learned and improve future response efforts
* Collect feedback from all swim lanes
* Produce final Post-mortem Report\*
 | * Archived copies of communications materials with reach and response insights
* Post-Mortem Report\*
 |
| Success Criteria:* Report details failures and success, lessons learned and recommendations for improved IR in the future.
* Comprehensive understandings of the audience reach to determine whether incident details were communicated broadly and effectively.
 |

Communications Liaisons should be invited. Refer to the RACI Matrix in Appendix C for additional details regarding the degree of engagement expected of each stakeholder.

|  |
| --- |
| **Email Distribution List for Managerial Coordination Meeting** |
| **Stakeholders** | **Email Recipients** |
| Corporate Response SMEs |  |
| Communications Liaisons | Risk Liaisons, Security Awareness Team |

In the event that Customer/Patient data is impacted, it is essential to be compliant with various data privacy laws and regulations. It is essential to loop in the following key stakeholders, in the table below. Refer to the **ITRMS/Global Privacy Office (GPO) Data Breach Process** for further guidance, which is available in Appendix B.

|  |
| --- |
| **Email Distribution List for GDPR Compliance** |
| **Stakeholders** | **Email Recipients** |
| Global Privacy Office |  |
| Legal Department |  |
| Treasury |  |
| Privacy & Compliance |  |
| Data Loss Prevention |  |
| Third-Party and Supply Risk Management Team |  |

Notice: The IR Commander is responsible for identifying any other stakeholders that are not already captured in the email distribution lists, on a case by case basis. Upon identifying the stakeholders that need to be aware and informed, the IR Commander should communicate this with the CYBER STRATEGY & OPS team to ensure that all necessary stakeholders are accounted for in communications moving forward.

# Coordination Resources

This section includes resources for the teams within the SOC to quickly and appropriately work with the Communications Liaisons to disseminate information via the right methods to the right audiences.

Refer to the RACI Matrix in Appendix E for more information on the level of expected engagement across stakeholders.

## Coordination and Communications Tools

This section details the various tools that swim lanes will utilize throughout the cybersecurity response lifecycle to organize and expedite communications and coordination.

Figure 5.1 Tools Matrix

## Setting Up the War Room

During a high-visibility, critical, and/or extremely pervasive incident, establishing a specific physical or virtual “War Room” may help to centralize communications and operations. A war room is typically isolated from standard business operations to assure the privacy of the discussions, to control the access to information made during discovery, or to provide a location that allows for better focus. This section provides detailed instructions on the establishment, operation, and decommission of a War Room.

## Establishment of a War Room

The CYBER STRATEGY & OPS team is responsible for identifying, reserving and establishing a war room. Key characteristics to look for when deciding on a war room include:

* Centrally located office/boardroom location;
* Facility can be locked; and
* Facility provides a reasonably high level of privacy.

The war room should include the following supplies and resources:

* Conference phone/bridge
* Push-to-talk handheld devices/mobile phones
* Printer/Copier/Scanner/Fax capability
* Power, power strips, and extension cords
* Office supplies, pen, paper, blank media, etc.
* TV/DVD player, for news, ability to play back closed-circuit cameras, etc.

## Decommission of a War Room

At the end of a war room should include the following supplies and resources:

* Return any resources loaned or displaced during incident.
* As appropriate, shred any documents not requiring retention.
* Clean all white boards.

## CRP Operational Tempo

A defined operational tempo provides structure to situations that can be chaotic at times. This section documents two different operational tempos.

One operational tempo is more technical and involves the incident responders that are analyzing various artifacts and evidence. The other operational tempo is more operational and involves discussions that focus on the approach of the incident response and critical decisions that need to be made. The CRP Commander usually leads both these meetings.

The format of the meetings should follow the general precept of the Observe, Orient, Decide, and Act (OODA) Loop[[1]](#footnote-2). Leveraging this idea provides structure and efficiency to the discussions, decisions, and actions that must be tasked out to the CIRT.

* **Observe**: What do we know and how do we know it?
* **Orient**: What do we need to know and how will we get it, or do we have the capability to know it?
* **Decide**: Develop a variety of Courses of Action (COAs) and evaluate the merits and issues with them and whether they contribute to the solution.
* **Act**: Execute selected COAs, monitor, and supervise. Repeat all of this at the next meeting.

## Communications Templates

The following sections includes templates for coordination, information sharing, and reporting throughout the incident. The table below indicates how quickly and frequently information will be disseminated. Links to all communications products and the accompanying template are listed in Appendix B.

### SOC Generated Content

**SOC Daily Status Update:** The SOC Daily Status Update presents notable cybersecurity issues discovered within the Client environment and/or in the news. The update will provide an overview of most recent activities, including detection, analysis and remediation, around current, as well as emerging cybersecurity issues. The update is shared daily and includes all cybersecurity issues detected within the last 24 hours.

**CYBER THREAT INTEL Flash Report:** The CYBER THREAT INTEL Flash Report provides initial context and information surrounding the cybersecurity issue. It also provides real-time updates throughout the lifecycle of the incident.

### Escalation Brief and Deck

The following template should be used for leadership escalation during the initial stages of a **High** or **Critical** severity cybersecurity issue. Fill it after the initial alert from the SOC teams.

|  |
| --- |
| **Escalation Brief:** From CYBER STRATEGY & OPS Team to CRP Commander |
| **Incident #**  |  |
| **Date and Time** |  |
| **Initial Severity** | * **3 – Medium (Incident)**
 | * **2 – High (Incident)**
 | * **1 – Critical (Crisis)**
 |
| **Incident Snapshot** | **Scale** * >25 users affected
* Department-wide
* One region affected
* Multiple regions affected
* Global
 | **Asset Type*** Make, Move, Sell systems
* Business-critical systems
* Intellectual property
* Sensitive financial info
* Operational systems
* Confidential data
* PII
* GXP
* Crown Jewels
 | **Impact Type*** Make, Move, Sell
* Safety
* Legal/liability
* Customer/patient
* Operational disruption
* Brand/public disclosure
* B2-level or above impact
 |
| **Incident Summary** | *[List incident type, potential entry vector, initial remediation actions]* |
| **Recommended Action** | * *No EIM Required*
* Monitor severity with the IR Team
* *EIM Required*
* Convene the full IR team
* Escalate to:
* CISO
* CIO
* C-Suite
 | * Activate Cross-Enterprise Resources**:**
* Business Continuity Management
* Global Communications
* IT Communications
* Corporate Crisis Management Team
* PR
* Legal
* Network Operations
* Network Engineering
* Security Engineering
* Software Engineering
* Compliance
* Forensics
* Plant Floor Networks
* Other: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
 |
| **Initial Response Actions**  |
| **Root Cause** **(If Known)**  | [Insert Text] |
| **Initial Response Actions** | * Intrusion Detection
* Endpoints
* Virtual Server Platforms
* Servers
* Security Tools

Other: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | [Insert Text] |
| **Next Steps** | [Insert Text]ContainmentMitigate the threat |
| **Organizations Currently Engaged** | [Insert Text] | [Insert Contact] |

The Escalation Deck will be supplemental to the Escalation Brief and present the information contained in the Escalation Brief with additional details and visuals. The deck includes an executive summary with background information and the status of the incident. It also includes an overview of the remediation plan and status of remediation across various platforms.

The Escalation Deck will provide updates throughout the lifecycle of the incident. Old and new updates will be included in the deck to track progress of the cybersecurity issue through each phase of the IR lifecycle.

The Escalation Deck can be used during the Technical and Managerial Coordination Meetings.

### Activation Text Messages

For High or Critical severity cybersecurity issues, the following activation texts will be sent by the CRP Commander to notify Corporate Response SMEs and Communications Liaisons of a High or Critical severity cybersecurity issue. The text messages will include the severity of the situation, current remediation status, and next steps for recipients.

|  |  |  |
| --- | --- | --- |
| **Severity**  | **Status** | **Message** |
| High Severity | Under Control | ALERT: A [vulnerability, threat or incident] of [high severity] has been identified. The situation is under control. Stay tuned for additional details. |
| High Severity | Being Analyzed | ALERT: A [vulnerability, threat or incident] of [high severity] has been identified. The situation is being analyzed. Stay tuned for an email with additional details. |
| Critical Severity | Needs Immediate Attention | ALERT: A [vulnerability, threat or incident] of [critical severity] has been identified. The situation needs immediate attention. Prepare to join a call. |

### Escalation Emails

For High or Critical severity cybersecurity issues, the following draft initial alert emails will be used by the CYBER STRATEGY & OPS team to notify the CRP Commander, and for the CRP Commander to notify Corporate Response SMEs and Communications Liaisons. The CYBER STRATEGY & OPS team will attach the Escalation Brief and Deck in the initial Escalation Email to the CRP Commander for further sharing to Corporate Response SMEs and Communications Liaisons.

|  |
| --- |
| **FROM: CYBER STRATEGY & OPS** **TO: CRP Commander** |
| **Subject: URGENT: Cybersecurity Issue; Action Required – [INSERT TLP]**Salutation, The Cyber Fusion Center identified a [High or Critical severity] cybersecurity incident that could have significant business impact to Client. Details follow. **Description of the incident:** An [vulnerability, threat or incident] that causes [effect] is present on [operational system]. We discovered it on [date] at [time]. Upon initial analysis, we validated the issue and predict it could cause [scope of incident] if not handled immediately. **Initial containment:** The [team within the CFC] has [action taken] to mitigate the impact. **Stakeholders impacted:** We recommend alerting executive leadership and the following business units [impacted stakeholders]. **Next steps:** In the case that this [vulnerability, threat, or incident] is confirmed as a High or Critical severity security issue, we recommend activating the CRP per protocol. You’ll see a meeting notice for [time] to provide additional background and coordinate all necessary stakeholders. In the meantime, contact me directly at [cell phone] for more information. **Resources:** List of references and citations.Regards, CYBER STRATEGY & OPS Team Lead  |

### Meeting Agendas for Technical and Managerial Coordination Meetings

Technical response and managerial response will be coordinated via two separate conference bridges.

**Technical Coordination Meeting:** For High or Critical severity security issues, the CYBER STRATEGY & OPS team will convene the SOC for a daily briefing. This may be less frequent for medium severity cybersecurity issues. During the first technical stand-up meeting, CRP Commander should set a cadence for coordination and status update meetings. The CYBER STRATEGY & OPS team will share information and facilitate the call, and track and record participation, key decisions, remediation activity and business impacts.

**Managerial Coordination Meeting:** The CRP Commander will convene Corporate Response SMEs and Communications Liaisons for a daily briefing. The CRP Commander will share information and updates. The CYBER STRATEGY & OPS team will track and record participation, key decisions, remediation activity and business impacts. The CRP Commander will field questions as the CYBER STRATEGY & OPS team records them.

*Note: For rapid coordination and effective recordkeeping between the CRP Commander and the technical response teams, information sharing within the case management system is preferred to email or formal meetings.*

Meeting types may include the following:

| **Technical Coordination Meetings:** Information sharing across Technical Response SMEs and SOC Lead |
| --- |
| **Purpose** | To coordinate activities across SOC workstreams. To update CRP Commander on progress and provide detailed understanding of current efforts to carry forward concise, informed messages to leadership |
| **Attendees** | CRP Commander, SOC Teams, CYBER STRATEGY & OPS Team |
| **Logistics** | Technical Bridge Line:  |
| **Timing** | Depending on Severity—twice daily to as needed |
| **Agenda** | *CYBER STRATEGY & OPS*  | **Opening.** Convene meeting and set agenda.  |
| **Severity.** Determines severity of the incident. |
| *SOC Teams* | **Key Details and Response Updates.** Information about initial triage and containment activity.  |
| *CRP Commander* | **Next Steps.** Determines whether the cybersecurity issue needs to be escalated higher, provides direction to the SOC team for continued activity, and shares information from across the business. |
| *CYBER STRATEGY & OPS*  | **Closing.** Questions, concerns, and schedule next update. |

The updated Escalation Brief is the same checklist as the Escalation Brief, updated on an ongoing basis. It will be circulated every couple hours and will be the primary tool that provides the extended business with real-time updates on the status of the cybersecurity issue. It will later be paired with the SOC Priority Report, which will provide fuller context as the cybersecurity issue matures.

The following template should be used for executive-level status updates to track activities on **High or Critical** severity cybersecurity issues.

|  |
| --- |
| **Updated Escalation Brief:** Status Update |
| **Incident #**  |  |
| **Date and Time** |  |
| **Incident Severity** | * **3 – Medium (Incident)**
 | * **2 – High (Incident)**
 | * **1 – Critical (Crisis)**
 | * *No Change*
 |
| **Incident Snapshot** | **Scale** * >25 users affected
* One region affected
* Multiple regions affected
* Global
 | **Asset Type*** Make, Move, Sell systems
* Business-critical systems
* Intellectual property
* Sensitive financial info
* Operational systems
* Confidential data
* PII
* GXP
* Crown Jewels
 | **Impact Type*** Make, Move, Sell
* Safety
* Legal/liability
* Customer/consumer
* Operational disruption
* Brand/public disclosure
* B2-level or above
 |
| **Incident Summary** |  |
| **Initial Remediation**  |
| **Root Cause (If Known)**  | [Insert Text] | * *No Change*
 |
| **Recommended Mitigation Actions** | [Insert Text] | * *No Change*
 |
| **Organizations and Individuals Currently Involved**  | [Insert Text] | * *No Change*
 |
| **Challenges and Outstanding Action Items**  | [Insert Text] |
| **Estimated Time to Response Completion**  | [Insert Text}  |

### SOC Priority Report

CYBER STRATEGY & OPS will combine information collected across SOC teams to create a quick and digestible updated SOC Priority Report to share during Managerial Coordination Calls. The SOC Priority Report will include details, such as, the business impact, a risk scorecard and next steps.

Technical response teams will be tasked with completing different portions of the SOC Priority Report and submit the data to the CYBER STRATEGY & OPS team. The CYBER STRATEGY & OPS team will compile the data into a single SOC Priority Report. SOC teams will provide the following data:

* CTI: Critical information about the threat actor.
* VM: Difficulty to exploit the vulnerability and additional insight into the situation.
* IR: Recommended remediation activities, root cause analyses, and containment actions.
* TDO/Hunt: Reports associated activities within the network related to the threat, vulnerability or incident.
* Forensics: Deep-dive information related to hardware.

### Post-Mortem Report

The Post-mortem Report will assess and summarize performance across all roles, channels and phases of the IR lifecycle, to provide recommendations for improvement.

The report will provide an overview of the response to the threat, vulnerability or incident, including:

* **Scope:** An overview of events, and additional context of the High or Critical severity cybersecurity issue.
* **Analysis:** A deep-dive analysis of adherence to the CRP, and overall performance throughout the IR lifecycle will provide insight into strengths and weaknesses.
* **Recommendations:** The analysis portion of the report will review the four phases of the IR lifecycle, including the preparation, detection, response and recovery phases, engendering greater speed and transparency in future IR efforts.

The CYBER STRATEGY & OPS team will work with the SOC technical teams to gather data in the form of interviews, artifacts and benchmarks. The Archer tool will aide in tracking performance metrics along a timeline to examine response time and efficiency.

## Privileged Communication and Appropriate Document Markings

Given the potential sensitive nature of cybersecurity incidents, proper message discipline and confidentiality are required. The Traffic Light Protocol (TLP) is the model for sharing of information about cybersecurity incidents and crisis. The TLP was designed so that sensitive information is shared with the correct audience. It employs four colors to indicate different degrees of sensitivity and the corresponding sharing considerations to be applied by the recipient(s).

In certain cases, a cybersecurity incident will create the potential for legal fallout in the form of lawsuits and regulatory scrutiny. Global Privacy Office / Legal will need to consider early in the cybersecurity incident response process, whether privilege may or may not need to be invoked and communications will be required to be marked as “Privileged and Confidential.” Communication flows regardless of privilege status will be on a “need to know” basis. If a decision to invoke privilege is made, refer to the Legal Department’s Privilege protocol for instructions on this process and its requirements as provided by the Legal Department.

1. Glossary

| Term | Explanation |
| --- | --- |
| **Access** | The ability or opportunity to gain knowledge of computing resources. |
| **Affected Person** | The individual to whom personally identifiable information that has been breached belongs. |
| **AH** | Animal Health |
| **Alert** | A mechanism which brings attention to an Event. (e.g., a flashing icon, “ding”, a written warning displayed in a monitoring console). |
| **Awareness (Privacy)** | A learning process that sets the stage for training by changing individual and organizational attitudes to realize the importance of privacy and data protection practices and the adverse consequences of its failure. |
| **Business Continuity Management** |  Holistic management process that identifies potential threats to an organization and the impacts to business operations those threats, if realized, might cause, and which provides a framework for building organizational resilience with the capability of an effective response that safeguards the interests of its key stakeholders, reputation, brand and value-creating activities. Provides a framework to ensure that business processes can continue during a time of emergency or disaster, such as in the face of a cybersecurity issue. |
| **Breach** | Breach – An Incident that results in the exfiltration of data.A breach may result in a disclosure of information that compromises the security or privacy of personal or sensitive corporate data. Affected parties may include its employees, or its customers. Types of data breaches which may require disclosure to affected persons would include those of personal health information, personally identifiable information, or credit / debit card information. Sensitive corporate data is also a frequent target of an intentionally orchestrated data breach. |
| **Breach Notification** | Refers generally to those laws that apply to an entity which require such entity to notify individuals and, where applicable, government authorities and/or consumer protection groups when unauthorized access to personal data has occurred or is reasonably believed to have occurred or as otherwise provided pursuant to such laws. |
| **SOC** | SOC – refers to a center of information security, incident management and response in an organization where all the technical response units reside, including:* Incident Response (IR) Manager
* Incident Response (IR) Team
* Threat Detection Operations (TDO)/Hunt Team
* Cyber Threat Intelligence (CTI) Team
* Forensics Team
* Vulnerability Management (VM) Team
 |
| **Confluence** | Confluence is a software written on Java used to help teams to collaborate and share knowledge efficiently. With Confluence, users can create pages and blogs which can be commented on and edited by all members of the team. Additionally, it enables users to create a roadmap easily, create notes containing checklists, create a knowledge base and centralize all documents in one place. |
| **Crown Jewels** | Deemed a “high value asset” to the company. Approximately, less than 300 assets are considered a Crown Jewel. |
| **Full Incident Response Team** | The cybersecurity incident response team is made up of a group of stakeholders and groups that are assigned roles and responsibilities for the investigation, management and remediation of security and privacy related incidents related to electronic data. |
| **Cybersecurity Incident (CSI)** | An occurrence in the computing environment, whether physical or electronic, that has potential to damage the image and integrity. Incidents sometimes provide indication that a breach is occurring, however not all events are incidents. |
| **Cybersecurity Incident Response** | Actions taken to resolve or mitigate a cybersecurity incident, coordinate and disseminate information, and implement follow-up strategies to stop the cybersecurity incident from happening again. |
| **Device (Electronic)** | Laptops, desktops, servers, handhelds or other devices that can store or process electronic information. |
| **Encryption** | Method of converting an original message of regular text into encoded text. The text is encrypted by means of an algorithm (a type of formula). If information is encrypted, there is a low probability that anyone other than the receiving party who has the key to the code oraccess to another confidential process could be able to decrypt (translate) the text and convert it into plain, comprehensible text. |
| **Eradicate** | Remediation that gives assurance that the cybersecurity incident has stopped and the damage has been minimized or mitigated.* Determine how the attack occurred;
* Remove root cause;
* Discuss recovery with management; determine how the Remediate sub-phase will affect other areas of the business.
 |
| **Event** | An observable occurrence in a network or system. See Event Conditions for more details. |
| **Forensics Team** | Vendor or internal resource with the skills, experience, training and technology to perform Digital Forensics and Incident Response. |
| **GDPR Data Breach Notification** **Process** | General Data Protection Regulation Data Breach Notification Process - A regulation in EU law on data protection and privacy for all individuals within the European Union. It addresses the export of personal data outside the EU. The GDPR aims primarily to give control back to citizens and residents over their personal data and to simplify the regulatory environment for international business by unifying the regulation within the EU. Refer to Appendix B for more information regarding the GDPR Data Breach Notification Process. |
| **GHH** | Global Human Health |
| **GSF** | Global Support Functions |
| **GTO** | Global Technology Operations |
| **GXP** | Any department can replace the ‘X’ variable for the “GXP” to be tailored to represent a variety of departments. |
| **Impact** | The predicted or actual results of an Incident(e.g., a Windows based attack against a Unix system is an example of an Incident that will likely have no Impact. As a real, confirmed attack did take place, it is important to track the Event as an Incident for proper tracking and to fully understand the organization risk posture.) |

1. Associated Plans and Procedures – Internal

The CRP cannot anticipate and provide guidance for all potential cybersecurity issues. Management and incident responders should consider the current situation, business impact, and security needs of Client and balance those against the guidance and recommendations provided by the CIRP.

Associated plans and procedures that may need to be triggered and tailored to the scope, severity and nature of the cybersecurity issue include the following:

| Associated Plan and/or Procedure | Summary |
| --- | --- |
| **ITRMS/GPO Data Breach Process** | In the event of a data breach leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal information transmitted, stored or otherwise processed either in electronic or paper records, the company is legally required to assess the risks to data subjects and may be required to notify data protection authorities and affected data subjects. This is the process by which the Company conducts required notifications in the event of a data breach. |
| **Corporate Crisis Plan** | Reach to XXX at XXXX@client.com to initiate the Corporate Crisis Management Plan. |
| **PR/Global Communications – Public Announcement Domains** | The PR/Communications team will share Client’s external communications response during an incident on one of the following domains: * Clientresponds.com
* Clientresponse.com

The domains will only go live during an actual incident. |
| **Third-Party Incident Management Runbook** | Adjacent to the CRP, a third-party incident management process was created to provide guidance for when third-party vendors and/or suppliers are impacted by a cyber incident. See the runbook for additional details. Reach to XXXX at XXXX@client.com to contact third parties and/or vendors. |

1. Associated Plans and Procedures – External

Various regulations require mandatory reporting of data breaches involving protected data, such as Personally Identifiable Information (PII), Protected Health Information (PHI), or Payment Card Industry (PCI) cardholder data (CHD). The definitions of protected data vary between states, industries, and the Federal government. All incidents involving the potential loss of protected data are classified as Critical or High. Incidents of these severities require the engagement of General Counsel to assist in guiding the organization’s required actions in all fifty states, Federal government, foreign governments, and with regard to regulatory obligations.

Depending on the type of protected data involved, the organization is required to notify affected parties within a predetermined timeframe. Currently, manages or utilizes the following types of information and is thus subject to the associated regulations:

C.1. Protected Health Information (or Personal Health Information)

Following a breach of unsecured protected health information (PHI), covered entities[[2]](#footnote-3) must provide notification of the breach to affected individuals, the Secretary of Health and Human Services (HHS), and, in certain circumstances, to the media. In addition, business associates[[3]](#footnote-4) must notify covered entities if a breach occurs at or by the business associate.

C.2. Individual Notice

Covered entities must notify affected individuals following the discovery of a breach of unsecured PHI. Covered entities must provide this individual notice in written form by first-class mail, or, alternatively, by e-mail if the affected individual has agreed to receive such notices electronically. 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. If the covered entity has insufficient or out-of-date contact information for fewer than 10 individuals, the covered entity may provide substitute notice by an alternative form of written notice, by telephone, or other means.

C.3. Media Notice

Covered entities that experience a breach affecting more than 500 residents of a State or jurisdiction are, in addition to notifying the affected individuals, required to provide notice to prominent media outlets serving the State or jurisdiction. Covered entities will likely provide this notification in the form of a press release to appropriate media outlets serving the affected area. Similar to individual notice, this media notification must be provided without unreasonable delay and in no case later than 60 days following the discovery of a breach and must include the same information required for the individual notice.

When an employee is approached by a media representative, he/she should respond by using the following message:

*“Thank you for your interest. Unfortunately, I am not a contact person for media inquiries. However, I can let our PR department know about your interest and they will get back to you. Could you please let me know the topic you are interested, and the questions you would like to ask? When do you need the answers? Please also give me your mobile phone number and email.”*

* **Never** say “No Comment.” This gives the public the impression you’re hiding something.
* If you don’t know, don’t speculate. Instead, refer to the External Communication SOP for Corporate Policy 4: Global Media Relations.
* Unless a Client employee is specifically authorized to speak on behalf of our company to media, all requests or questions from print, broadcast or digital media for information should be forwarded to the Global Media Relations Team or an appropriate communications representative via mediarelations@Client.com.

C.4. 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 PHI has been compromised by the impermissible use or disclosure; or (2) the application of any other exceptions to the definition of “breach.”

Covered entities are also required to comply with certain administrative requirements with respect to breach notification.

C.5. Credit Card (Payment Card Industry)

Entities that have experienced a suspected or confirmed security breach must take prompt action to help prevent additional exposure of cardholder data and ensure compliance with the Payment Card Industry Data Security Standard (PCI DSS), PCI Payment Application Data Security Standard (PA-DSS), and PCI PIN Security Requirements.

Visa recommends the following guidelines for addressing and reporting cardholder data compromises:

Immediately contain and limit the exposure. Minimize data loss. Prevent the further loss of data by conducting a thorough investigation of the suspected or confirmed compromise of information. Compromised entities should consult with their Incident Management Team and legal counsel. To preserve evidence and facilitate the investigation, adhere to the following:

* Do not access or alter compromised systems (i.e., don’t log on at all to the compromised systems and change passwords; do not log in as ROOT. Visa highly recommends that the compromised system not be used to avoid losing critical volatile data.
* Do not turn the compromised systems off. Instead, isolate compromised systems from the network (i.e., unplug network cable).
* Preserve evidence and logs (i.e., original evidence, security events, web, database, firewall, etc.)
* Document all actions taken.
* 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).
* Be on high alert and monitor traffic on all systems with cardholder data.

Alert all necessary parties immediately:

* The internal Incident Management Team.
* If you are a merchant, contact your merchant bank.
* If you do not know the name and/or contact information for your merchant bank, notify the card brand’s Incident Response Manager immediately.
* If you are a financial institution, contact the appropriate card brand region at the number or e-mail provided.

Notify the appropriate law enforcement agency. If necessary, contact the card brand Incident Response Manager above for assistance in contacting local law enforcement agency.

Visa has developed a communication guideline in responding to a data breach for compromised entities. There are some good basic communications principles that can be applied to most data breach situations. This guideline is intended to provide some best-practice guidance for compromised entities on how to think about, prepare for, and respond to data breaches. You can download a copy of the guideline here:

* **PCI – PFI (Forensic Investigator) Program**
	+ <https://www.pcisecuritystandards.org/approved_companies_providers/pci_forensic_investigator.php>

C.6. Personally Identifiable Information

The National Conference of State Legislatures maintains a status of current [Security Breach Notification Laws](http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx) (current as of January 2016), by state.

The CIRT and General Counsel shall use this resource as a starting point for identifying regulatory requirements associated with data breaches and engage outside counsel when necessary to assist.

C.7. Cyber Liability Insurance

Cyber breaches can result in devastating financial consequences for any business. The Treasury should be notified immediately, and is responsible for overseeing the cybersecurity insurance, a policy designed specifically to trigger when a cybersecurity issue results in a financial loss

1. Additional Resources

D.1. Revisable Communications Products and Templates

Figure E.1 provides an overview of all the communications products that are engaged, their respective owners and the cadence in which they are circulated, throughout the full cybersecurity response lifecycle

Editable versions of the communications products and templates are available on Confluence.

D.2. Crown Jewels and Critical Assets

Crown Jewels constitute the high value assets within the Client network. A link to the Crown Jewels List is managed by the IT Resource Management Services team.

1. Boyd, John R. (September 3, 1976). [*Destruction and Creation*](http://www.goalsys.com/books/documents/DESTRUCTION_AND_CREATION.pdf) (PDF). U.S. Army Command and General Staff College. [↑](#footnote-ref-2)
2. 45 CFR 160.103: A HIPAA covered entity is any organization or corporation that directly handles Personal Health Information (PHI) or Personal Health Records (PHR). [↑](#footnote-ref-3)
3. 45 CFR 164.502(e), 164.504(e), 164.532(d) and (e): A “business associate” is a person or entity that performs certain functions or activities that involve the use or disclosure of protected health information on behalf of, or provides services to, a covered entity.   [↑](#footnote-ref-4)