**-TLP: AMBER-**

Limited disclosure, restricted to participants’ organization and its clients.

The information in this document may be confidential
pursuant to Texas Government Code § 552.139.

**[Organization Name]**

**Cybersecurity Incident Response
Team Redbook**

Any recommendations are offered solely for your consideration, to the extent applicable to your circumstances. Any third-party views and opinions do not necessarily reflect those of DIR or its employees. By sharing this material, DIR does not endorse any particular person, entity, product or service.

|  |  |  |  |
| --- | --- | --- | --- |
| Role | Name | Phone | Email |
| Sponsor\* | [Sponsor name] | [Sponsor phone] | [Sponsor email] |
| Owner\*\* | [Owner name] | [Owner phone] | [Owner email] |
| \*Sponsor is the executive responsible for compliance\*\*Owner is the owner of this document |
| Last Document Update: [mm/dd/yyyy] |

Incident Response Team Overview

Purpose

This Incident Response Plan establishes membership, roles, responsibilities, and activities of the [organization name] response team in preparation for an actual or suspected cybersecurity incident.

Incident Response Team Mission

The response team’s mission is to support incident response preparedness and build a program that can identify and detect actual or suspected cybersecurity incidents. The response team also responds to and contains, eradicates, and supports the recovery of cybersecurity incidents.

Scope

This plan applies to any computing devices owned or leased by the organization, personal devices used to access the organization’s cloud resources, and cloud-hosted systems as appropriate. Incident response roles and responsibilities are documented in the organization’s response plan.

[Organization name] established a response team to respond to cybersecurity incidents. The response team operates on behalf of the [organization name]’s leadership and engages, informs, and receives support from the Response Team Coordinator. It is comprised of personnel with expertise in responding to a significant actual or suspected cybersecurity incident who are involved in decision making and prioritizing incident response activities. Members of the Leadership Team will designate appropriate personnel for the response team.

There [is/is not] a set protocol to initiate the response team activities in response to an actual or suspected incident. Once activated, the response team is authorized to [require compliance with the organization’s established procedures/request cooperation/establish incident response priorities that may supersede daily operational responsibilities/require attention outside normal business hours].

Incident Response Team Leadership and Responsibilities

The Response Team Coordinator (hereafter referred to as the Coordinator) is designated by and reports to [Leadership Position]. The Coordinator manages all aspects of the response, coordinates direct communication, and ensures necessary notifications are made to the appropriate individual or organization. The Coordinator is the primary internal point of contact during the response.

The incident response team may conduct the following activities, aligned to the incident response life cycle:

* Preparation: Plan for incident response, train on incident response roles, and conduct exercises of incident response plans and procedures.
* Detection and Analysis: Support detection of cyber threats and define the methods used to analyze the potential impact of an incident.
* Containment, Eradication, and Recovery: Quickly respond to limit the impacts of an incident, remove any threat actor persistence in the organization’s systems, and support the recovery of the organization’s systems to pre-incident conditions.
* Post-Incident Recovery: Conduct an after-action review and develop a corrective action plan to continually improve the organization’s response to incidents.

Example incidents that may fall within the response team’s responsibility include, but are not limited to:

* Malware infection, including a computer virus, worm, bot, crypto miner, or trojan.
* Sustained denial of service (DDoS) attack.
* Ransomware infection impacting computers or servers.
* Disclosure of non-public or sensitive data.
* Incidents that are likely to be high-profile or create a significant risk of financial, reputational, or physical harm.

A member of the leadership team may determine whether a scenario that is not described or considered by this Redbook constitutes a significant incident.

Incident Response Team Structure

[The table below provides options for structuring your organization’s incident response team.]

| Team | Function | Members |
| --- | --- | --- |
| Leadership Team | The Leadership Team has decision-making authority to guide incident response priorities and activities, and provides command objectives and institutional knowledge.The Leadership Team prioritizes the work of the Core Team and addresses the organizational or managerial components of incident response. | * Chief Elected Official
* Chief Executive Officer
* Executive Management
* IT/Technology Directors
* Incident Response Team Coordinator
* Legal
* Communications
* Other positions as needed
 |
| Core Team | The Core Team facilitates activities to detect, respond to, contain, eradicate, and recover from a cybersecurity incident.The Core Team works the Extended Response Team to aid with incident resolution and may serve as subject matter experts on privacy, cybersecurity, or technical Information Technology (IT) systems. | * IT Infrastructure
* IT Applications
* Third-Party Security Vendors
* Other positions as needed
 |
| Extended Response Team | The Extended Response Team provides unique subject matter expertise in their respective fields and may support incident response activities.The Extended Response Team may serve as subject matter experts on matters relating to their specific business or operational function. | * Human Resources
* Facilities
* Law Enforcement
* Emergency Management
* Other positions as needed
 |

Incident Response Team Member Roles

[The table below identifies different positions on the incident response team. Customize the positions, their assigned team component, and roles based on your organization’s operational needs, capability, and structure.

The positions and responsibilities described below are based upon best practices in the information privacy and cybersecurity industries. This does not indicate that the example responsibilities are appropriate or necessary for your organization.]

Team Member Roles

| Position | Team | Responsibilities |
| --- | --- | --- |
| Incident Response Team Coordinator | Leadership Team | * Serves as the primary point-of-contact for incident response activities.
* Coordinates incident triage and declaration.
* Establishes, maintains, and updates written response team protocols or incident response plans.
* Identifies roles and responsibilities for response team members.
* [Add additional duties based on organizational requirements]
 |
| Chief Elected Official Executive Officer or Executive Director | Leadership Team | * Holds ultimate accountability for preparedness, response, and recovery activities.
* Monitors the impact to services and recovery efforts.
* Communicates with counsel, court, or commission members.
* [Add additional duties based on organizational requirements]
 |
| City Manager, County Administrator, Superintendent, or Deputy Director | Leadership Team | * Monitors incident response activities and maintains situational awareness of incident response functions.
* Coordinates with external affairs and communication staff on public notices.
* Manages information flow between impacted business units.
* [Add additional duties based on organizational requirements]
 |
| IT/Technology Director or Information Security Officer | Leadership Team | * Monitors incident response activities and maintains situational awareness of incident response functions.
* Updates leadership, and coordinates management-level decisions and actions.
* [Add additional duties based on organizational requirements]
 |
| Legal Counsel | Leadership Team | * Advises on legal compliance matters, such as breach notification laws and privacy compliance.
* [Add additional duties based on organizational requirements]
 |
| Privacy Officer | Leadership Team | * Coordinates and monitors breach notification activities.
* [Add additional duties based on organizational requirements]
 |
| Communications/External Affairs | Leadership Team | * Manages all public communications regarding incidents and may rely on input from technical subject matter experts to craft public messages.
* [Add additional duties based on organizational requirements]
 |
| IT Infrastructureor Applications Manager | Core Team | * Supports incident response activities in alignment with the incident response life cycle and industry best practices.
* Provides situational updates to the response team coordinator.
* [Add additional duties based on organizational requirements]
 |
| System/Network Administrators | Core Team | * Supports incident response activities in alignment with the incident response life cycle and industry best practices.
* Provides situational updates to the response team coordinator.
* [Add additional duties based on organizational requirements]
 |
| Forensic or Cybersecurity Technicians/Consultants | Core Team | * Supports incident response activities in alignment with the incident response life cycle and industry best practices.
* Provides situational updates to the Incident Response Team Coordinator.
* [Add additional duties based on organizational requirements]
 |
| Human Resources | Extended Response Team | * Manages internal communications to employees regarding incident status and may coordinate with technical subject matter experts to craft communications.
* Monitors response team activity and supports staff time tracking.
* [Add additional duties based on organizational requirements]
 |
| Law Enforcement | Extended Response Team | * Supports incident investigation and maintains chain of custody of forensic evidence.
* Provides physical security for response team.
* Coordinates with appropriate law enforcement partners.
* [Add additional duties based on organizational requirements]
 |
| Emergency Management | Extended Response Team | * Provides logistical support for response team activities.
* Coordinates with leadership team to support the organization’s continuity of operations.
* Coordinates with regional and state level emergency management partners for resource support and situational awareness.
* [Add additional duties based on organizational requirements]
 |
| Finance/Purchasing | Extended Response Team | * Provides purchasing and contract support for incident response activities.
* Tracks expenses incurred by the incident response team.
* [Add additional duties based on organizational requirements]
 |
| Facilities | Extended Response Team | * Provides access to facilities and building locations to response team members.
* Supports the activities of the response team as needed.
* [Add additional duties based on organizational requirements]
 |

Incident Response Team Member Contact Information

[The following table contains contact information for the organization’s incident response team members.]

Response Team Contact Information

| Position | Name | Phone | Email | After-Hours Contact |
| --- | --- | --- | --- | --- |
| [Sample Position Name] | [Jane Smith] | [512-555-5555] | [Jane.Smith@email.com] | [512-555-5555] |
| Response Team Coordinator |  |  |  |  |
| Chief Elected Official |  |  |  |  |
| City Manager |  |  |  |  |
| County Administrator |  |  |  |  |
| Superintendent |  |  |  |  |
| IT Director |  |  |  |  |
| Information Security Officer |  |  |  |  |
| Legal Counsel |  |  |  |  |
| Privacy Officer |  |  |  |  |
| Communications/ External Affairs |  |  |  |  |
| IT Infrastructure/ Applications Manager |  |  |  |  |
| System/Network Administrator |  |  |  |  |
| Forensic/ Cybersecurity Technicians/ Consultants |  |  |  |  |
| Human Resources |  |  |  |  |
| Law Enforcement |  |  |  |  |
| Emergency Management |  |  |  |  |
| Finance/Purchasing |  |  |  |  |
| Facilities |  |  |  |  |
| [Additional positions as needed] |  |  |  |  |

Key External Contact Information Sheet

[Based on legislative or regulatory mandates, organizations may be required to report cybersecurity incidents to specific individuals or government entities. This list provides contact information to support those notifications.]

External Contact Information

| Entity or Organization | Title, Dept., or Location | Name | Phone | Email |
| --- | --- | --- | --- | --- |
| Texas State Representative  |  |  |  |  |
| Texas State Senator |  |  |  |  |
| [Chief Elected Official] |  |  |  |  |
| [Manager or Administrator] |  |  |  |  |
| Cyber Insurance Provider |  |  |  |  |
| [Organization] |  |  |  |  |
| [Organization] |  |  |  |  |
| Texas CISO Office | DIR – Incident Response | DIR CIRT | 1-877-347-2476 (24/7 hotline) | CIRT@dir.texas.gov  |
| Texas Division of Emergency Management | Assistant Chief |  |  |  |
| District Chief |  |  |  |
| State Operations Center (SOC) | Daily Ops | 512-424-2208 | soc@tdem.texas.gov  |
| Texas DPS and Criminal Justice Information System (CJIS) | Regional Office |  |  |  |
| CJIS | DPS OIC | 1-800-638-5387 | securitycommittee@dps.texas.gov |
| Texas Fusion Center | Real-Time Watch Center | 512-424-7981 | txfc@dps.texas.gov |

High-Level Incident Response Process Overview

[The high-level process outlined in this document is based on the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-61, Computer Security Incident Handling Guide.]



*Figure .1 NIST Incident Response Life Cycle**[[1]](#footnote-2)*

[The table below outlines key activities and considerations during the incident response life cycle.]

Incident Response Phase and Description/Activities

| Phase | Description/Activities |
| --- | --- |
| Preparation | Preparation activities include activities performed in advance of a cybersecurity incident that help increase the resilience of an organization, reduce the impact of a cybersecurity incident, or improve the organization’s ability to effectively respond to and recover from an incident.Some common preparation activities include:* Establishing an incident response team.
* Developing and testing an incident response plan and procedures.
* Increasing the resilience of systems, networks, and backups.
* Conducting user awareness and training activities.
* Managing vulnerabilities and securing networks and systems.
* [Add additional containment steps based on organizational requirements]

Additional preparation best practices may be found on page 3 of the [MS-ISAC/CISA Joint Ransomware Guide](https://www.cisa.gov/sites/default/files/publications/CISA_MS-ISAC_Ransomware%20Guide_S508C.pdf). |
| Detection and Analysis | Detection and analysis activities determine when an observed anomaly or event is a true information privacy or cybersecurity incident. A true incident should be classified and prioritized to determine the appropriate response.Some common detection and analysis activities include:* Analyzing precursors for signs of a potential attack, which may include targeted threat intelligence, known vulnerabilities being exploited, or network scanning and enumeration.
* Analyzing indicators to determine their potential impact, which may include network intrusion alerts, anti-virus or enhanced detection and response (EDR) warnings, unauthorized system changes, or pre-staged files in sensitive locations.
* Reviewing logs to coordinate potentially malicious events.
* Identifying and triaging an incident to determine its type and scope of impact.
* [Add additional containment steps based on organizational requirements]

Each incident should be prioritized to ensure the appropriate resources are allocated to the response efforts. Additional detection and analysis activities can be found on page 11 of the [MS-ISAC/CISA Joint Ransomware Guide](https://www.cisa.gov/sites/default/files/publications/CISA_MS-ISAC_Ransomware%20Guide_S508C.pdf). |
| Containment, Eradication, and Recovery | Containment of an identified incident limits further damage and reduces the business impact to the organization. Some common containment strategies include:* Isolating the system. (Keep systems powered on to preserve volatile memory unless shutdown is required.)
* Disabling services, protocols, or appliances.
* Disabling account access.
* [Add additional containment steps based on organizational requirements]

Each incident may require unique containment strategies. Preserving evidence and collecting forensic images and logs during the containment phase may better enable threat eradication.Additional containment best practices can be found on page 12 of the [MS-ISAC/CISA Joint Ransomware Guide](https://www.cisa.gov/sites/default/files/publications/CISA_MS-ISAC_Ransomware%20Guide_S508C.pdf).After an incident has been contained, eradication may be necessary to eliminate established threat actor persistence or to remediate an exploited vulnerability. Some common eradication strategies include:* Remediating or mitigating exploited vulnerabilities.
* Removing malware or other malicious files.
* Securing and resetting compromised user accounts.
* [Add additional eradication steps based on organization requirements]

Additional eradication best practices can be found on page 12 of the [MS-ISAC/CISA Joint Ransomware Guide](https://www.cisa.gov/sites/default/files/publications/CISA_MS-ISAC_Ransomware%20Guide_S508C.pdf).In the **recovery** stage, any production systems affected by a threat will be rebuilt or reconstituted and brought back online, including data recovered from backups that has been determined to be safe from tampering. Some common recovery strategies include:* Rebuilding and reimaging impacted workstations and servers.
* Sanitizing user and service accounts.
* Segmenting network and reviewing back up strategy.
* [Add additional recovery steps based on organization requirements]

Additional recovery best practices can be found on page 14 of the [MS-ISAC/CISA Joint Ransomware Guide](https://www.cisa.gov/sites/default/files/publications/CISA_MS-ISAC_Ransomware%20Guide_S508C.pdf). |
| Post-Incident Activity | Post-incident activities include:* Conducting a hot wash and after-action review to gather lessons learned from the incident (involve all parties that participated in incident response and recovery activities).
* Recognizing gaps, reviewing policies and incident response plans, and identifying corrective actions to address gaps.
* Considering opportunities to improve processes, coverage, and refine alerting of security tools.
* Conducting additional training for security and non-security staff.
* Reviewing industry standards to ensure evidence retention requirements are met.
* [Add additional recovery steps based on organization requirements]

Additional post-incident best practices can be found on page 14 of the [MS-ISAC/CISA Joint Ransomware Guide](https://www.cisa.gov/sites/default/files/publications/CISA_MS-ISAC_Ransomware%20Guide_S508C.pdf) and in [Post-Incident After-Action Review and Improvement Plan](#_Post-Incident_After-Action_Review) of this document. |

Incident Analysis and Escalation

Determining the scope and severity of a cybersecurity incident is a critical step in allocating the appropriate resources to quickly contain and eradicate an emerging cyber threat. With the knowledge of the incident’s complexity and scope, response team leadership can communicate business impacts to the appropriate internal and external stakeholders.

Incident Analysis

Once classified, current best practices recommend triaging the incident and assigning a severity level. Classification and triaging inform and direct incident escalation, while communicating the actual or potential impact to the organization. However, cybersecurity incidents are dynamic, and the severity level may change during an investigation or over the course of the response as more information is gathered and the investigation unfolds. Response team leadership is ultimately responsible for incident classification.

Incident Triage

The thresholds below are based on the Cybersecurity and Infrastructure Security Agency (CISA) National Cyber Incident Scoring System (NCISS). Incidents may be categorized based on the threshold of impacts identified in the sample table below.

[The provided template is one example of an incident triage framework for assessing the impact of a cybersecurity incident. Customize the Incident Triage template to fit the needs of your organization.]

| Threshold | Impact Scope | Customer Impact | Continuity of Operations | Cost | Recoverability | Reputation |
| --- | --- | --- | --- | --- | --- | --- |
| 4Emergency | Internal or external organization | Life safety systems impacted | Government services unavailable | >$$ | Data lost and not recoverable | Significant risk for reputational harm |
| 3High | Entire organization | Customer-facing services inoperable | Department services unavailable | $ to $$ | Data lost but manually recoverable | Potential for reputational harm due to service outages |
| 2Medium | Multiple roles | Customer-facing services degraded | Single application unavailable | <$ | Data lost but digitally recoverable | Limited potential for reputational harm |
| 1Low | Single role | No customer impact | No interruption | No cost | No data lost | No reputational impact |

Observed functional impacts may not all align with the table above. Use best judgment when triaging an incident and adjust as more information becomes available.

Notification Thresholds

The appropriate staff and teams should be notified based on the severity of an incident. Observation of the communication thresholds is critical to reducing alert fatigue. The escalation threshold template provided below identifies required and recommended notifications based on the incident severity. In rapidly evolving situations, the severity may increase quickly, and additional individuals may need to be notified and back briefed.

[Customize the Notification Escalation Thresholds table to fit the needs of your organization. For example, if your organization has an Executive Director instead of an Organization Head or Chief Official, feel free to replace the positions in the table.]

| Threshold | Notification Recommended | Notification Considered |
| --- | --- | --- |
| 4Emergency | * [Name of position being notified]
* Organization Head or Chief Official
* Council or Commissioners Court
* All positions at the High and lower threshold
 | * [Name of position being notified]
 |
| 3High | * [Name of position being notified]
* Legal Counsel
* Human Resources
* Public Information Officer
* All positions at the Medium and lower threshold
 | * [Name of position being notified]
* Emergency Management
* Law Enforcement
 |
| 2Medium | * [Name of position being notified]
* Incident Coordinator
* Incident Response Core Team
* IT Director
* All positions at the Low threshold
 | * [Name of position being notified]
* Deputy Director
 |
| 1Low | * [Name of position being notified]
* Help Desk
* IT Manager
 | * [Name of position being notified]
 |

Situation Notifications

In addition to the escalation thresholds, some situations require immediate notification to specific positions. These situations and points of contact are listed below.

[Customize the Notification Situations table to fit the needs of your organization.]

| Situation | Point of Contact Notified |
| --- | --- |
| [Situation] | * [Name of position being notified]
 |
| Breach of Customer or Employee Information | * Privacy Officer
* Legal Counsel
* Public Information Officer
 |
| Critical Business Process Offline | * Business Unit Leader(s)
* Organization Head
 |
| Ransom Demand | * Organization Head
* Chief Elected Official
* Legal
 |

Services Restoration Priority Worksheet

The services restoration policy below identifies the services and systems used by the organization to conduct its internal and external operations. Prioritization of the importance or criticality of services and systems is paramount to supporting restoration priorities during incident response and recovery activities. These services and systems may be listed and prioritized as part of the business continuity or disaster recovery planning process.

[Consider the restoration priority for your organization using the sample classifications below:

* Priority 1: Critical services or systems, and life safety or public safety systems.
* Priority 2: Core business functions and services that enable the operation of the entity.
* Priority 3: Routine business functions and services that support operations.
* Priority 4: Non-production services or functions that do not impact end users.]

Services Restoration Policy

[The table below provides a consolidated list to guide service restoration.]

| Priority | Service/System | Function and Details | End User |
| --- | --- | --- | --- |
| 1 | [Domain controllers] | [Authentication – Active Directory] | [Internal and External] |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
| 2 |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
| 3 |  |  |  |
|  |  |  |  |
|  |  |  |  |
| 4 |  |  |  |
|  |  |  |  |
|  |  |  |  |

Hardware and Software Inventory

[Your organization should track its IT resources, including computers, servers, mobile devices, IP phones, internet connected devices, and approved and managed software. This inventory allows IT or the organization’s managed service provider to track devices to maintain and provide a starting point for prioritizing disaster recovery efforts.]

Hardware Tracking

[You should consider using a hardware tracking spreadsheet that inventories your organization’s current hardware.

Complete and maintain the following hardware asset tracking sheet. Customize the table, including headers, as appropriate.

Typically, a hardware tracking spreadsheet will capture a combination of the following:

* Asset Number.
* Current Status.
* Assigned Employee.
* Asset Type.
* Model.
* Manufacturer.
* Location.
* Description.
* Date Issued.
* Date Returned.]

| Asset Number | Assigned Employee | Asset Type | Model | Manufacturer | Serial Number |
| --- | --- | --- | --- | --- | --- |
| [XXXXX] | [Jane Doe] | [Laptop] | [Model | [Dell] | [XXXXX] |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

Software Tracking

[Complete and maintain the following software tracking sheet. Customize the table, including headers, as appropriate. The Center for Internet Security (CIS) provides additional an [hardware and software asset tracking spreadsheet](https://www.cisecurity.org/white-papers/cis-hardware-and-software-asset-tracking-spreadsheet/) if needed.]

| Software Use | Name | Software Description | License Type | Version | Software Key | Purchase Date | Billing Cycle |
| --- | --- | --- | --- | --- | --- | --- | --- |
| [End User] | [Adobe Lightroom] | [Photo Editor] | [Service] | [X.X] | [In Console] | [MM/DD/YYYY] | [Monthly] |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |

Data Classification Process

[Your organization should classify its data according to a defined schema. The process of data classification provides your organization insight into the risks associated with data breaches in addition to informing the implementation of appropriate security controls before an incident occurs.

DIR has developed a [Data Classification Template](https://dir.texas.gov/resource-library-item/data-classification-template) for state agencies to use as a guide. All organizations may leverage this template to support the data classification process.

The table below identifies the responsibilities of sample data professionals who may work with data at your organization. These roles likely have different responsibilities, dependent upon data classification. These roles may be different than traditional incident response roles since these activities are largely conducted before an incident occurs.

This table can modified to suit your organization’s needs.]

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Role | Public | Sensitive | Confidential | Regulated |
| Data Custodian | • Ensure systems support access controls which enforce data classification. |
| Data Owner | • Identify the classification level of data.• Review audit logs. |
| Information Security Officer, Legal and/or Privacy Office | • Develop and maintain information security policies, procedures, and guidelines. • Provide guidance on data classifications |
| Managers |  | • Ensure users are aware of data classification requirements.• Monitor user activities to ensure compliance. |
| Users |  | • Identify data and label where appropriate. • Properly dispose of data in accordance with the records retention policy. |

Internal Communication and Reporting

[Below are two examples of how an initial notification of a cybersecurity incident may look. The first table-based example provides for consistent structure and form, while the second text-based example provides for a more comprehensive and adaptable approach.

At minimum, initial notification to management should provide a brief summary of the incident, focusing on business impacts, current and planned actions, and resources needed for resolution of the incident.

Both templates can be modified to suit your organization’s needs. They can be used either individually or together.]

Table-Based Internal Management Cybersecurity Incident Alert

|  |  |
| --- | --- |
| [Organization] Internal Cybersecurity Incident Alert | **TLP: RED** |
| Alert Date and Time | [Month DD, 20xx, 12:00 a.m. / p.m.] |
| Incident Name/Number | [Descriptive name or numbered naming convention] |
| Type | [Ransomware, Malware Infection, Data Breach, DDoS, or other attack type] |
| Incident Details | [Provide a summary (in less than 6 lines) of the incident impacts. Include what happened, when it occurred, when and how it was discovered, and any additional high-level details appropriate for senior management notification. Consider using the 5 Ws (who, what, when, where, and why) and Impacts] |
| Public Impacts | [Status of Public Website, Payment Processing, Public Data Systems, Public Safety Answering Point, Supervisory Control and Data Acquisition (SCADA) Systems, or other public-facing system] |
| Internal Impacts | [Status of organization email, phone system, computer workstations, internal document and records storage, public safety, or other internal systems] |
| Current Containment Activities |
| 1. [List major activities taken to contain impacts]
 |
| Planned Actions |
| 1. [List major actions planned to further contain and eradicate active threat]
 |
| Supporting Actions or External Assistance Requests |
| [List any supporting actions or external requests needed to facilitate incident response activities] |
| Next Scheduled Update | [Month dd, 20xx at 12:00 a.m./p.m. or as conditions warrant] |

Text-Based Internal Management Cybersecurity Incident Alert

Organization Information

Notification Made to

* [Name of person or team being notified]

Notification Made by

* [Name of person making the notification]

Incident Information

Type of Incident

* [Ransomware, malware infection, data breach, etc.]

Date and Time

* [MM/DD/YYY HH:MM AM/PM]

Incident Name/Tracking Number

* [Provide a short name for referencing the incident internally]

Incident Impact

* [Provide a brief list of internal processes or services that are impacted by this incident]
* [Provide a brief list of external processes or services that are impacted by this incident]

Executive Summary

* [Provide a brief summary (in less than six lines) of the incident impacts. Include what happened, when it occurred, when and how it was discovered, and any additional high-level details appropriate for senior management notification. Consider using the 5 Ws and Impacts]

Incident Containment And Resource Management

Current Containment Action Items

* [Provide a brief list of major action items taken to contain the impact of the incident]

Planned Containment Action Items

* [Provide a brief list of planned action items for containing the impact of the incident]

Supporting Action Items

* [Provide a brief list of any supporting actions or external requests needed to facilitate incident response activities]

Next Steps

Next Notification Expected

* [MM/DD/YYY HH:MM AM/PM]

Daily Situational Report

[Leadership should receive consistent, frequent updates per your incident response plan’s reporting schedule.

Below are two examples of how a daily situational report notification for a cybersecurity incident may look. The first table-based example provides for consistent structure and form, while the second text-based example provides for a more comprehensive and adaptable approach.

At minimum, daily situational reports to management should provide a brief incident update, list any accomplishments, and focus on current and planned actions to resolve the incident.]

Table-Based Internal Management Daily Situational Report

|  |  |
| --- | --- |
| [Organization] IRT Daily SitRep — Containment, Eradication, and Recovery | **TLP: AMBER** |
| Report Date and Time | [Month DD, 20xx, 12:00 a.m. / p.m.] |
| Incident Name/Number | [Descriptive name or numbered naming convention] |
| Current Priorities | [Current priority of incident response team] |
| BLUF | [(Bottom Line Up Front) – Define the most relevant activities associated with this report.] |
| Key Action Items | [Provide a summary of the progress made on each of the identified incident objectives or by organization unit, such as website restoration or application and developer activities.] |
| Accomplishments  |
| 1. [List recent activities and progress made by the incident response team since the last report.]
 |
| Planned Activities/Next Steps |
| 1. [List the next planned activities to support incident response.]
 |
| Supporting Resources |
| 1. [List the internal and external resources (by group) supporting the incident response.]
 |
| Next Scheduled Update | [Month DD, 20xx at 12:00 a.m./p.m. or as conditions warrant] |

Text-Based Internal Management Daily Situational Report

Organization Information

Notification Made to

* [Name of person or team being notified]

Notification Made by

* [Name of person making the notification]

Report Information

Report Date and Time

* [MM/DD/YYY HH:MM AM/PM]

Incident Name/Tracking Number

* [Provide a short name for referencing the incident internally.]

Bottom Line Up Front (BLUF)

* [Provide a brief summary (in less than six lines) of the incident impacts. Include what happened, when it occurred, when and how it was discovered, and any additional high-level details appropriate for senior management notification. Consider using the 5 Ws and Impacts.]

Incident Containment And Resource Management

Accomplishments

* [Provide a brief list of action items accomplished in containing the impact of the incident.]

Planned Action Items

* [Provide a brief list of planned action items for containing the impact of the incident.]

Supporting Action Items

* [Provide a brief list of any supporting actions or external requests needed to facilitate incident response activities.]

Next Steps

Next Notification Expected

* [MM/DD/YYY HH:MM AM/PM]

Post-Incident After-Action Review and Improvement Plan

Post-Incident After-Action Review Report

[Use the sections below to capture post-incident comments captured in a hot wash or after-action review. Customize the content in brackets with your own details and information.]

|  |  |
| --- | --- |
| Item | Description |
| Cyber Incident | [Use your organization’s naming convention for the incident.] |
| Dates and Times | [Indicate, at a minimum, the start/end dates/times of the incident. Include a full incident chronology if available.] |
| Description | [Give a brief description of the incident.] |
| Impact | [What was the impact to the organization?] |
| Detection | [How was the incident detected?] |
| Metrics | [Enter any related metrics such as mean time to incident discovery, cost of recovery, time from detection to containment, etc.] |
| Incident Cost | [What was the cost in time, materials, human resources, and lost productivity to the organization in dollar figures? These could range from time and resources, equipment replacement costs, organization downtime, idle employee time, backlog catchup overtime, etc.] |

Lessons Learned Questions

[The following table provides learning and improvement questions to assess the incident response.]

| Question | Response |
| --- | --- |
| Were documented policies and procedures followed? |  |
| Were the procedures adequate? |  |
| Were all features, policies, and processes examined to identify all contributing factors that caused this incident? |  |
| What information was needed sooner? |  |
| Were any steps taken that might have inhibited recovery? |  |
| What actions could the organization do differently if a similar incident occurs? |  |
| How could information sharing (in/out) with other organizations have been improved? |  |
| What corrective actions can prevent or lower the likelihood of similar incidents in the future? |  |
| What precursors or indicators of compromise should be watched in the future to speed up detection? |  |
| What additional tools or resources are needed to address future incidents? |  |

Root Cause Analysis Questions

[The following table provides questions for incident response root cause analysis.]

| Question | Response |
| --- | --- |
| What could have prevented the incident? |  |
| Was damage caused prior to detection? |  |
| Is the incident a recurrence of a previous incident? |  |
| Were all features, policies, and processes examined to identify all contributing factors that caused this incident? |  |
| Was there a difference between the initial impact assessment and the final impact assessment? |  |
| Were there any leading-edge indicators of detection that were missed? |  |

Response Strengths

[You can use this section to identify areas of the response that went well, including processes that worked as—or better than—intended and other strengths your organization identified during the response.]

[Our organization] identified these areas as strengths in our response to the incident. Strengths should be identified and captured as best practices.

|  |  |
| --- | --- |
| Strength | Description |
|  |  |
|  |  |
|  |  |

Response Improvement Opportunities

[Our organization] identified these areas for improvement in our response to the incident. Areas for improvement should be captured and analyzed to prevent the issue from recurring. Corrective actions for each area for improvement can be documented in the next section.

|  |  |
| --- | --- |
| Area of Improvement | Description |
|  |  |
|  |  |
|  |  |

Corrective Action Plan

This corrective action plan has been developed for [organization] because of the [incident name] Cyber Incident.

| Improvement | Corrective Action | Responsible Stakeholder | Start Date | End Date | Notes or Limitations |
| --- | --- | --- | --- | --- | --- |
| [Improvement One] | [Corrective Action] | [Name/Org] | [MM/DD/YY] | [MM/DD/YY] | [As needed] |
| [Corrective Action] |  |  |  |  |
| [Corrective Action] |  |  |  |  |
| [Improvement Two] | [Corrective Action] |  |  |  |  |
| [Corrective Action] |  |  |  |  |
| [Corrective Action] |  |  |  |  |
| [Improvement Three] | [Corrective Action] |  |  |  |  |
| [Corrective Action] |  |  |  |  |
| [Corrective Action] |  |  |  |  |
| [Improvement Four] | [Corrective Action] |  |  |  |  |
| [Corrective Action] |  |  |  |  |
| [Corrective Action] |  |  |  |  |
| [Improvement Five] | [Corrective Action] |  |  |  |  |
| [Corrective Action] |  |  |  |  |
| [Corrective Action] |  |  |  |  |

1. NIST Risk Management Framework for Information Systems and Organizations [↑](#footnote-ref-2)