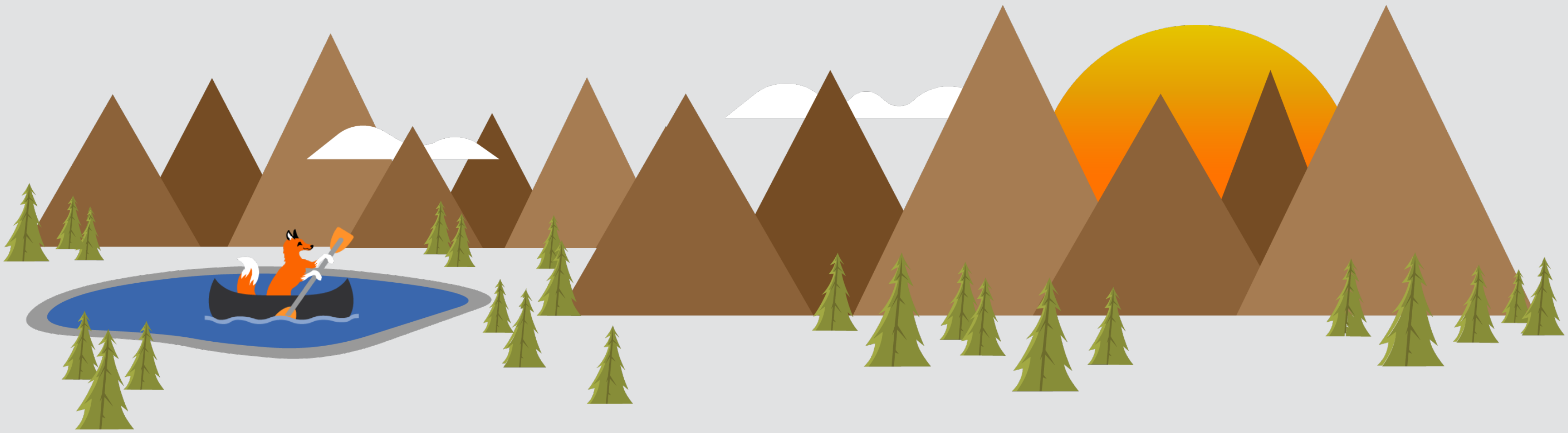
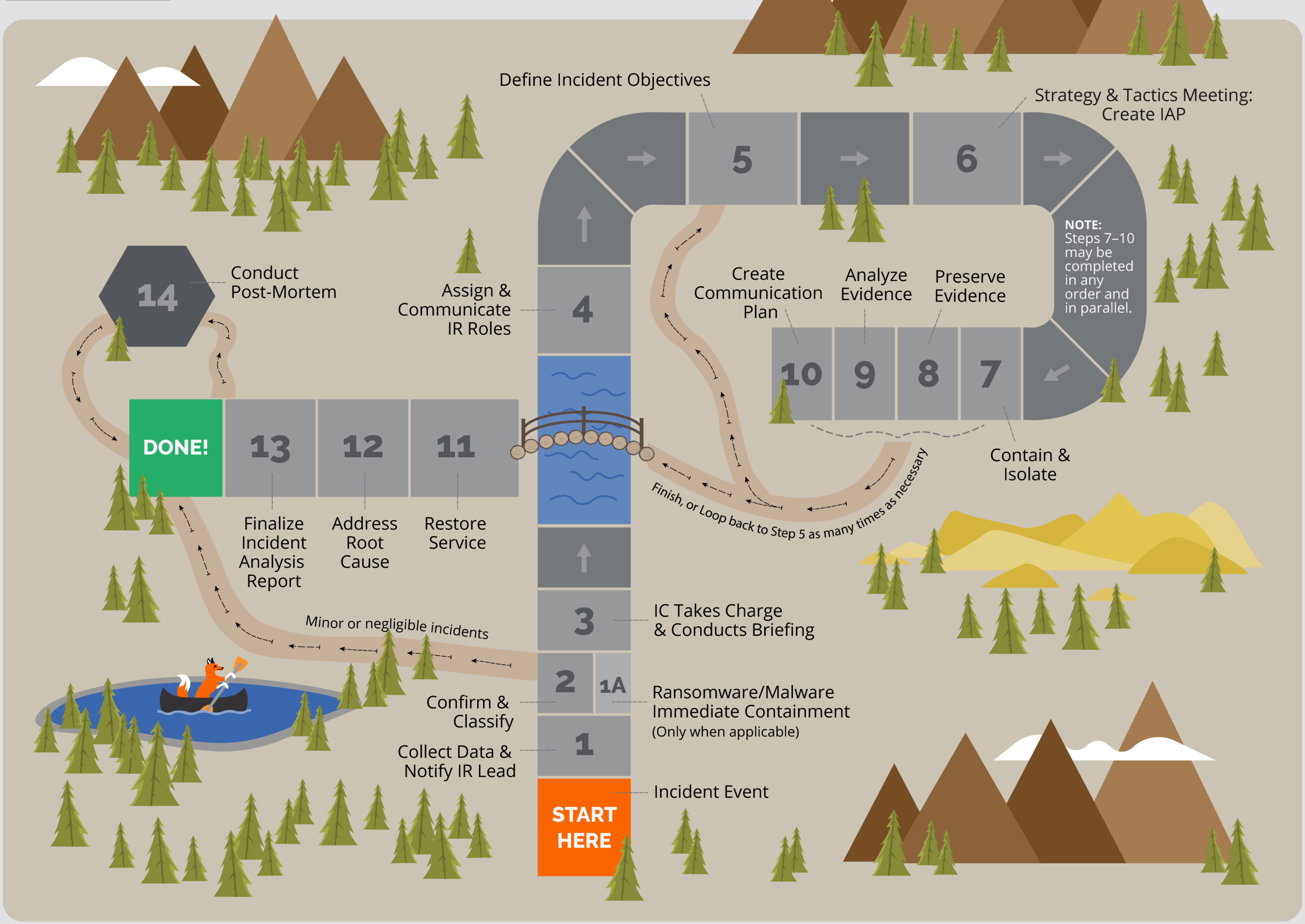
Cybersecurity Incident Response Plan

A Step-by-Step Guide



Cybersecurity Incident Response Path



START HERE

Incident Event

1 Collect Data & Notify IR Lead

2 Confirm & Classify

1A Ransomware/Malware Immediate Containment (Only when applicable)

3 IC Takes Charge & Conducts Briefing

4 Assign & Communicate IR Roles

5 Define Incident Objectives

6 Strategy & Tactics Meeting: Create IAP

7 Contain & Isolate

8 Preserve Evidence

9 Analyze Evidence

10 Create Communication Plan

NOTE: Steps 7–10 may be completed in any order and in parallel.

Finish, or Loop back to Step 5 as many times as necessary

11 Restore Service

12 Address Root Cause

13 Finalize Incident Analysis Report

DONE!

14 Conduct Post-Mortem

Minor or negligible incidents

IR Roles

Role Assignments

Standing Roles

Role		Name	Phone	Email
IRL	**Incident Response Leader** (#1)			
	Incident Response Leader (#2)			
	Incident Response Leader (#3)			
	Incident Response Leader (#4)			

Mandatory Roles (Core IR Staff, to be assigned in Step 4)

Role		Name	Phone	Email
IC	**Incident Commander**			
-	**IT Support/Operations Representative**			
-	**Cybersecurity Representative**			
-	**Legal and Compliance Representative**			

Optional Roles (to Be Assigned as Needed in Step 4)

Role		Name	Phone	Email
PIO	**Public Information Officer**			
-	**Safety Officer**			
-	**Liaison Officer**			
-	**Operations Section Chief**			
-	**Planning Section Chief**			
-	**Logistics Section Chief**			
-	**Finance/Admin Section Chief**			

Additional Optional Contacts

Role		Name	Phone	Email
-	**Third-Party IR Vendor**			
-	**Management Contact**			
MSP	**Managed Services Provider**			
-	**Cybersecurity Insurance Provider**			

Step 1

Data Collection & IR Lead Notification

Typical Duration
1 hour

Max Duration
2 hours

Above All Else...
Life safety is ALWAYS priority #1. Make sure everyone is in a safe location. Don't hesitate to call 911 if there is a life-safety issue.

Responsible Party

Typical: IT Operations/Security Team

Complete These Tasks

- ☐ Escalate suspected incident to Incident Response Leader (IRL) immediately.
  - Is ransomware/malware believed to be spreading throughout the network? If yes, dispatch team to execute Step 1A in parallel to Steps 1 and 2.
- ☐ Open the Incident Response Kit and grab the Incident Handling Ledger (IHL).
- ☐ Record the current time and time stamps for currently known incident events.
- ☐ Gather incident details from incident reporter on how the incident was identified, what systems/data might be involved, when the incident occurred, and who is aware of the incident.
- ☐ Record these details in the IHL Initial Intake Summary. Then fill out Sections A – D.
- ☐ Collect any evidence already obtained by the incident reporter, and provide this to the IRL.
- ☐ For any existing physical evidence, establish chain of custody.
- ☐ Seal evidence within evidence bags from within the Incident Response Kit to maintain integrity of physical evidence.

Achieve These Objectives

- ☐ IRL is aware of suspected incident.
- ☐ All incident background data, evidence, and documentation has been collected and provided to the IRL.

Guidance/Process Support

Any individual that fields a potential incident report should focus on confirming incident details, filling out the Incident Handling Ledger, and escalating immediately to the Incident Response Leader.

To maintain an accurate and complete chain of custody:

- Limit the number of individuals handling evidence.
- Confirm that all names, identification numbers, and dates are listed on the chain of custody documents.
- Ensure the chain of custody documents are signed by the first person who came in contact with/obtained the evidence.
- Ensure the chain of custody document details the collection location, time/date collected, and description and condition of the item(s).
- Ensure all evidence packaging is properly sealed and marked prior to submission.
- Obtain signed or otherwise secure property transfer receipts upon transfer of evidence. One copy of the receipt should be given to the recipient, with one retained by the transferring party.

***NOTE:** Following this IR plan means you will NOT be making any changes to the environment until a plan is agreed upon in Step 6 – unless immediate containment is necessary and Step 1a is added to the response. Trust the process!*

Things You'll Need

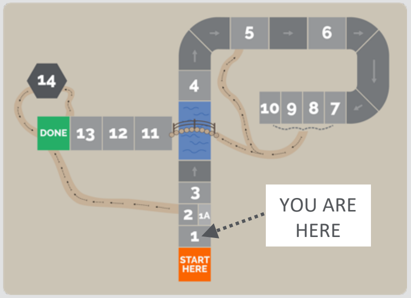
- ☐ Incident Response Kit
- ☐ Time-stamp reference

See Also

- Org chart
- Phone list

What's with the P?

The incident response path diagram used on page 2 and throughout this plan is based on the FEMA Incident Command System Planning P (or Planning Cycle). This P establishes a continuum for Incident Action Planning in emergency and non-emergency operations.



Step 1A (in parallel with Step 1)

Ransomware/Malware Immediate Containment

Typical Duration
4 hours
Max Duration
72 hours

Above All Else...
Move quickly but carefully. Containment actions at this stage can make or break the rest of the response and recovery efforts.

Responsible Party

IT Operations/Security Team

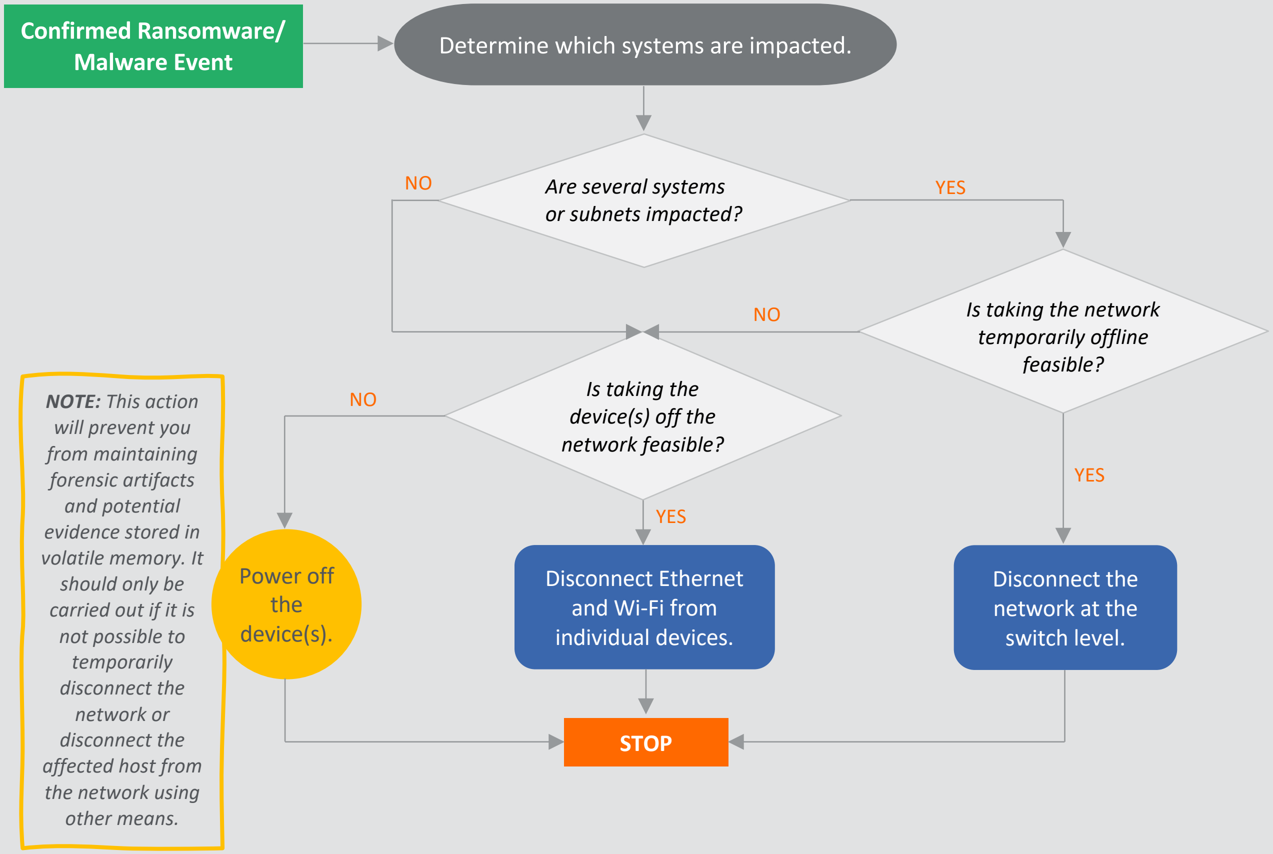
Complete These Tasks

- ☐ Determine which systems were impacted, and ***immediately*** isolate them.

Achieve These Objectives

- ☐ Active spread of ransomware or malware is contained.

Guidance/Process Support



Confirmed Ransomware/ Malware Event

Determine which systems are impacted.

Are several systems or subnets impacted?

NO

YES

Is taking the network temporarily offline feasible?

NO

YES

Is taking the device(s) off the network feasible?

NO

YES

Power off the device(s).

Disconnect Ethernet and Wi-Fi from individual devices.

Disconnect the network at the switch level.

STOP

NOTE: *This action will prevent you from maintaining forensic artifacts and potential evidence stored in volatile memory. It should only be carried out if it is not possible to temporarily disconnect the network or disconnect the affected host from the network using other means.*

See Also

- CISA Ransomware Guide: https://rule4.io/CISA-ransomware

Step 2

Initial Verification: Confirm & Classify

Typical Duration
30 minutes

Max Duration
1 hour

Above All Else...
When in doubt, engage your Third-Party IR Vendor immediately!

Responsible Party

Incident Response Leader

Complete These Tasks

- ☐ Review incident details documented in Incident Handling Ledger (IHL) Sections A – D, such as indicators, involved parties/systems, witnesses or other sources, date of events, and known disclosures.
- ☐ Classify incident according to ***Classification Matrix*** based on known incident details, and document confirmation steps in IHL Sections E and I.
- ☐ Use classification to execute prescribed response from ***Immediate Response Matrix***.

Achieve These Objectives

- ☐ Incident is confirmed and accurately classified.
- ☐ Third-Party IR Vendor is engaged, if appropriate.
- ☐ Incident Commander is assigned and alerted.

Guidance/Process Support

Classification Matrix

Level	Test/Criteria
Critical	Targeted cybersecurity attacks or loss of publicly available online service. Known exposure or loss of sensitive data, successful/wide-ranging phishing/spear-phishing resulting in data loss/fraud.
Significant	Website defacement or damaging unauthorized changes to a system. Potential/suspected but unconfirmed exposure or loss of sensitive data (e.g., lost unencrypted laptop), successful phishing/ spear-phishing resulting in no expected data loss/exposure.
Moderate	Suspected compromise where impact is unknown. Multiple reports of unusual/unexpected behavior. Virus or malware outbreak.
Minor	Unsuccessful DoS attack, the majority of network monitoring alerts, loss of encrypted laptop, unsuccessful phishing/spear-phishing campaign detected.
Negligible	Isolated antivirus alert, spam email, or false positive.
Baseline	Cyber events that require no investigation and are not cyber incidents.

Immediate Response Matrix

Level	Response
Critical	Assign and alert Incident Commander, on-call resource/team, and management. Engage Third-Party IR Vendor to assist. Continue to Step 3.
Significant	Assign and alert IC and on-call resource/team. Continue to Step 3.
Moderate	Assign and alert IC and on-call resource/team. Continue to Step 3.
Minor	Monitor impact. Follow appropriate non-IR procedures. STOP HERE.
Negligible	No immediate response. Follow up as normal trouble ticket for any outstanding resolution. STOP INCIDENT RESPONSE HERE.
Baseline	No immediate response. STOP INCIDENT RESPONSE HERE.

Things You'll Need

- ☐ IRK (handed off from Step 1)
- ☐ IHL (handed off from Step 1)

See Also

- On-call schedule

Step 3

IC Takes Charge & Conducts Briefing

Typical Duration
1 hour
Max Duration
1 hour

Above All Else...
Focus on communicating the current state of the incident to the IR staff as it's understood at the time. Working quickly is critical to containment!

Responsible Party

Incident Commander

Complete These Tasks

- ☐ Transfer command from Incident Response Leader to Incident Commander.
- ☐ **Immediately** schedule initial briefing. Scheduling should occur within minutes of completing Step 2.
- ☐ Establish the Incident Command Post and communicate location/call-in details to IR staff and on-call resource/team.
- ☐ Establish location to store incident data, and document in Incident Handling Ledger Section F.
- ☐ Assess and invite attendees based on availability and appropriateness for role. Include Third-Party IR Vendor (if engaged).
- ☐ Prepare initial management briefing (using Management Briefing Template).

Achieve These Objectives

- ☐ Management is briefed on incident.
- ☐ IHL ownership is transferred to IC (or documented delegate).
- ☐ Incident Command Post is established and communicated.
- ☐ On-call resource/team is engaged and participating.
- ☐ Immediate resource needs are identified.

Guidance/Process Support

The IHL should be the primary reference for this meeting, where the Incident Commander will communicate:

- ☐ Current state of the incident
- ☐ Classification, and why the incident was classified as such
- ☐ Initial evidence identified
- ☐ Any immediate response, desired or otherwise, already taken/initiated
- ☐ Any concerns, risks, or mitigating factors that currently exist
- ☐ Immediate resource needs

Things You'll Need

- ☐ Management Briefing Template
- ☐ Phone/computer for conferencing/ communicating
- ☐ Location for briefing, if in person
- ☐ Org chart

14
DONE
13
12
11
5
6
4
10
9
8
7
3
2
1A
1
START HERE
YOU ARE HERE

Step 4

Assign & Communicate Incident Response Roles

Typical Duration
30 minutes
Max Duration
1 hour

Above All Else...
Make decisions; don't get caught up in finding the exact right fit for each role.

Responsible Party

Incident Commander

Complete These Tasks

- ☐ Assign and communicate IR roles and responsibilities, and document on p. 3 and in the Incident Handling Ledger.

Achieve These Objectives

- ☐ Roles are assigned.
- ☐ Responsibilities are clearly understood.

Guidance/Process Support

Assign appropriate roles and populate into the table on p. 3.

NOTE: *Especially in smaller cybersecurity incidents, individuals may occupy more than one role.*

Incident Commander

Core IR Staff

IT Support/Operations Representative
Leads IT response actions as directed by the Incident Commander and action plan.

Cybersecurity Representative
Provides cybersecurity-specific guidance and expertise.

Legal and Compliance Representative
Oversees the legal affairs and interests of the organization.

Command Staff
Only activated if needed

Public Information Officer
Interfaces with the public, media, and others needing incident information.

Safety Officer
Monitors incident operations and advises on matters related to health and safety.

Liaison Officer
Serves as IC's point of contact for orgs not included in command structure.

General Staff
Assigned functional authority

Operations Section Chief
Conducts operations to reach incident objectives. Establishes tactics and directs all operational resources.

Planning Section Chief
Supports the incident action planning process by tracking resources, collecting and analyzing information, and maintaining documentation.

Logistics Section Chief
Arranges for resources and needed services to support achievement of incident objectives. (Resources can include personnel, equipment, teams, supplies, and facilities.)

Finance/Admin Section Chief
Monitors costs related to the incident. Provides accounting, procurement, time recording, and cost analyses.

Things You'll Need

- ☐ ICP location and/or conference bridge information
- ☐ Identified staff

Step 5

Define Incident Objectives

Typical Duration
30 minutes

Max Duration
1 hour

Above All Else...

Document clear objectives and use them as a guide.

Responsible Party

Incident Commander

Complete These Tasks

- ☐ Define incident objectives as a group according to SMART principles.
- ☐ Document objectives in Incident Handling Ledger Sections E – L.

Achieve These Objectives

- ☐ Objectives are defined, approved, and documented.
- ☐ Objectives are understood by all staff.

Guidance/Process Support

In this step, it's important to stay focused on defining **OBJECTIVES**, not straying into strategies and tactics (yet). Keep these definitions in mind:

- **Incident objectives** – state what will be accomplished, what is the desired outcome

  Example: Stop the spread of hazardous materials from a tanker truck accident into the lake by 16:00 UTC today.
- Strategies – establish the general plan or direction for accomplishing the objectives

  Example: Employ barriers.
- Tactics/Action Items – specify how the strategies will be executed

  Example: Use absorbent damming materials to construct a barrier between the downhill side of the accident scene and Nimmo Lake.

Define objectives based on the current operational period, understanding that they may change as the incident evolves and evidence is reviewed, and use the SMART principles:

Specific — *Is it precise and unambiguous?*

Measurable — *How will it be measured and judged complete?*

Achievable — *Is it feasible and attainable?*

Relevant — *Does it apply to the current situation?*

Time-Based — *What is the time frame?*

Things You'll Need

- ☐ IHL (in-progress version)
- ☐ ICP location and/or conference bridge information

See Also

- Compliance program documentation

YOU ARE HERE
14
DONE
13
12
11
4
5
6
10
9
8
7
3
2
1A
1
START HERE

Step 6

Strategy & Tactics Meeting: Create Incident Action Plan

Typical Duration
1 hour
Max Duration
2 hours

Above All Else…
The IAP should describe what resources are performing what actions on what timeline.

Responsible Parties

- Incident Commander
- Operations Section Chief
- Planning Chief

Complete These Tasks

☐ Define incident ***strategies*** and ***action items*** required to achieve incident objectives.

☐ Assign responsibility for action items.

☐ Define the Operational Period (timeline for regrouping and updating the IAP as appropriate).

☐ Create the Incident Action Plan and document within Incident Handling Ledger Sections E – L.

☐ Document required resources in IHL Section G.

☐ Identify any impacts and risks in IHL Section I.

☐ Engage law enforcement.

☐ Engage cybersecurity insurance provider.

Achieve These Objectives

☐ Strategies and action items are defined in an Incident Action Plan.

☐ Incident action items are assigned to resources for execution.

☐ IAP is documented in the IHL.

☐ Management strategy brief is complete or underway.

☐ Law enforcement is engaged if appropriate.

☐ Cybersecurity insurance provider is engaged if appropriate.

Guidance/Process Support

The Incident Action Plan (IAP) should be focused on immediate, near-term actions, and will be revisited and revised through the Planning P cycle.

- It is often difficult to obtain situational awareness at the beginning of an incident, which can be chaotic, so this initial plan is often developed very quickly and with incomplete information.
- Incident action planning is more than just producing an IAP; it provides a consistent rhythm and structure to *an* incident and is the vehicle by which the incident response team communicates their expectations and provides clear guidance to those managing the incident.
- Capture action items or tactical steps in the IAP. Ensure responsibilities are clearly articulated!

Strategies	vs.	Tactics
Definition: Establish the general plan or direction for accomplishing incident objectives.		**Definition:** Specific action items that are detailed and specific; how the strategies will be executed.
Examples: Determine the extent of the malware spread; Ensure no staff members are speaking with media or outside parties.		**Examples:** Review audit log for login failures in LogRhythm; Send org-wide communication to *all-staff@example.com* mailing list

IMPORTANT: *Steps 7–10 may be completed in any order and in parallel. Before you finalize your IAP and move on from Step 6, determine the order of the next batch of steps.*

Things You'll Need

☐ ICP location and/or conference bridge information

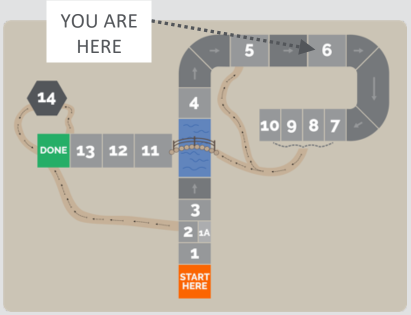
☐ IHL (in-progress version)

☐ Org chart and phone list

☐ SME representative for systems identified in scope

See Also

- System/tool inventory
- Compliance program documentation



Step 7

Contain & Isolate

REMEMBER

Steps 7 – 10 may be completed in any order, and in parallel. Loop back to Step 5 if necessary (and repeat loop as many times as needed).

Typical Duration
4 hours

Max Duration
72 hours

Above All Else...

Prioritize locking down/protecting unaffected highly sensitive systems and data first!

Responsible Party

Operations Section Chief

Complete These Tasks

- ☐ Execute Incident Action Plan containment and isolation action items.
- ☐ Record all changes to systems in Incident Handling Ledger Section N.
- ☐ Assess appropriate response to changes in approach dictated by attempts to contain/isolate.
- ☐ Execute necessary additional containment steps.
- ☐ Execute any initial communication steps outlined in the IAP.
- ☐ Document efforts.

Achieve These Objectives

- ☐ Incident is sufficiently contained and potential of additional impact to systems and users is minimized.
- ☐ Evidence integrity has not been compromised as part of the containment process (see Step 8 for guidance).

Guidance/Process Support

This step is focused exclusively on containment/isolation, **not investigation**. This is **critical** to keep in mind, as any attempts to investigate could impact evidence viability.

Containment strategies (see Step 6) will differ depending on the type of incident.

Level	Isolation Steps
Critical	Affected systems must be immediately isolated from other systems and outside connectivity.
Significant	Incident Commander makes decision about which systems (if any) must be isolated.
Moderate	IC makes decision about which systems (if any) must be isolated.

Containment activities could include:

- ☐ Blocking (and logging) of unauthorized access
- ☐ Blocking malware sources (e.g., email addresses and websites)
- ☐ Closing particular ports and mail servers
- ☐ Changing system administrator passwords where compromise is suspected
- ☐ Firewall filtering
- ☐ Relocating website home pages
- ☐ Isolating systems

What is containment?

Stopping contamination and removing risk.

NOTE: *Some containment activities may have already been completed in Step 1.*

Things You'll Need

- ☐ IAP (created in previous step)
- ☐ Incident Command Post location and/or conference bridge information
- ☐ Incident Handling Ledger (handed off from previous step)

See Also

- Password vault
- IT operations Wiki

14
DONE
13
12
11
4
5
6
10
9
8
7
3
2
1A
1
START HERE
YOU ARE HERE

Step 8

Preserve Evidence

REMEMBER

Steps 7 – 10 may be completed in any order, and in parallel. Loop back to Step 5 if necessary (and repeat loop as many times as needed).

Typical Duration
2 weeks

Max Duration
6 weeks

Above All Else...

When in doubt, engage your Third-Party IR Vendor to assist with evidence preservation, even if forensic capture requirements are unclear.

Responsible Party

Operations Section Chief

Complete These Tasks

□ Preserve evidence to support analysis efforts in accordance with the Incident Action Plan, including documenting chain of custody using tools/forms provided in the Incident Response Kit.

□ If forensic capture was not already initiated, assess again whether forensic capture is required using the additional criteria outlined in the IAP.

□ If required (and not already engaged), engage Third-Party IR Vendor immediately.

Achieve These Objectives

□ Chain of custody is established for all evidence.

□ Forensically sound copies of evidence are collected.

Guidance/Process Support

Preservation steps will vary depending on the severity and specifics of the incident. Use the table below to determine appropriate preservation steps.

Level	Preservation Steps
Critical	Immediately establish physical incident ledger and chain of custody. Immediate freeze on all backup and data retention purge activity. Engage a third party to perform forensic capture of all involved systems.
Significant	Establish physical incident ledger and chain of custody. IC makes decision about which systems (if any) must be forensically captured (internal or third-party team can perform capture).
Moderate	Establish physical incident ledger, and ensure log, configuration data, and breach specimens are retained.

When preserving evidence on targeted systems/devices, **DO NOT**:

X Turn ON a device if it is turned OFF.

X Charge a device if it is not charged.

X Plug anything into the device.

X Open any applications, files, or pictures on the device, which could accidentally cause data to be lost or overwritten.

X Copy anything to or from the device.

X Trust anyone without forensics training to investigate or view files on the original device. They might cause the deletion of data or the corruption of important information.

When preserving evidence on targeted systems/devices, **DO**:

◊ Physically secure the device.

◊ Take a picture of the piece of evidence (front, back, etc.) to prove its condition.

◊ Ensure that investigators know the PIN/password pattern of the device.

◊ Immediately establish a physical incident ledger and chain of custody.

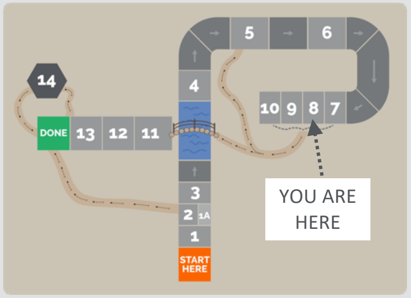
◊ Immediately freeze all backup and data retention purge activity.

Things You'll Need

□ Incident Response Kit (handed off from previous steps)

See Also

- ACPO Digital Forensics Guidelines: https://rule4.io/ACPO-forensics



Step 9

Analyze Evidence

REMEMBER

Steps 7 – 10 may be completed in any order, and in parallel. Loop back to Step 5 if necessary (and repeat loop as many times as needed).

Typical Duration
3 weeks

Max Duration
6 months

Above All Else...

Focus on gaining confidence through review of evidence that isolation and containment efforts were successful.

Responsible Party

Operations Section Chief

Complete These Tasks

- □ Review evidence preserved in Step 8 for indicators of breach and/or malicious activity.
- □ Work with subject matter experts on action items identified in the Incident Action Plan to identify root cause, scope of incident, impact, and identity of attacker.
- □ Document findings in Incident Handling Ledger Sections G, J, and L, and determine additional next steps for outstanding remediation activities.
- □ Prepare briefing for the IR staff and management.

Achieve These Objectives

- □ The root cause and scope of the incident are clearly understood.
- □ A detailed briefing has been created in preparation for IR staff and management meeting.

Guidance/Process Support

Responsibilities and approach for analyzing incident evidence:

Level	Analysis Steps
Critical	Analyze evidence and identify appropriate mitigation steps. Produce at a minimum: (1) incident timeline based on data analysis, (2) evidence manifest, and (3) root cause analysis.
Significant	Analyze evidence and identify mitigation steps. Produce an incident summary that contains an evidence manifest (if evidence was captured) and a root cause analysis.
Moderate	Identify team members who will analyze incident and document.

The following analysis activities should occur:

- Examine alerts and events from DS, IPS, DLP, or SIEM.
- Examine preserved evidence from impacted systems.
- Correlate the alerts/everts with network data (including from cloud providers).
- Compare them against threat intelligence. All types of event logs should be included in this review, including:
    - ○ Firewall/router logs (including proxy servers)
    - ○ Technical security monitoring logs and alerts (e.g., IDS or DLP software)
    - ○ Traditional server and workstation logs
    - ○ Business application audit logs
    - ○ Web server logs
    - ○ DNS and DHCP logs covering all devices
    - ○ Email history and archives
    - ○ Internet usage logs
    - ○ Network data
    - ○ Building access logs

Things You'll Need

- □ Incident Command Post location and/or conference bridge information
- □ IHL (handed off from previous step)
- □ Evidence preserved in Step 9

Step 10

Create Communication Plan

REMEMBER: Steps 7 – 10 may be completed in any order, and in parallel. Loop back to Step 5 if necessary (and repeat loop as many times as needed).

Typical Duration
2 hours

Max Duration
8 hours

Above All Else...

Obtain legal review of all external communication plans.

Responsible Party

- Public Information Officer
- Legal and Compliance Representative

Complete These Tasks

☐ Investigate reporting requirements based on outcome of the incident response investigation.

☐ Create a communication plan that encompasses both internal and external stakeholders, and takes into account legal and regulatory reporting requirements.

☐ Obtain approval for the communication plan from the Incident Commander and management.

☐ Execute the communication plan (see the Emergency Communications templates).

Achieve These Objectives

☐ Legal and regulatory reporting requirements are addressed in the communication plan.

☐ Incident Commander understands and approves the plan.

☐ Internal and external stakeholders have received relevant and appropriate communication regarding the incident.

Guidance/Process Support

Here are some key questions to consider:

- What are our reporting requirements?
- Who do I report to?
- What do I report?
- In what format do I report?
- What is the objective of reporting?

Once these questions have been addressed, the actual reporting itself should include:

- A full description of the nature of the incident, its history, and what actions were taken to recover.
- A realistic estimate of the financial cost of the incident, as well as other impacts on the business, such as damage to reputation, loss of management control, or impaired growth.
- Recommendations regarding enhanced or additional controls required to prevent, detect, remediate, or recover from cybersecurity incidents more effectively.

This notification process should also include any particular authorities that the organization has a mandate to report to, which may include:

Data Type	Associated Notification/ Communication Statute	Notes
Personally Identifiable Information/Privacy	General Data Protection Regulation (GDPR)	https://rule4.io/GDPR
Cardholder Data	Payment Card Industry Data Security Standard (PCI DSS)	https://rule4.io/PCI-DSS
Protected Health Information	The HIPAA Breach Notification Rule, 45 CFR §§ 164.400-414	https://rule4.io/HIPAA-breach

Things You'll Need

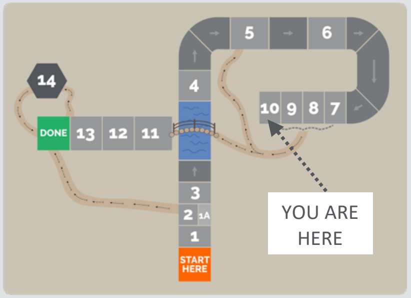
☐ Incident Command Post location and/or conference bridge information

☐ Incident Handling Ledger (in-progress version)

☐ Emergency Communications templates (Users, Internal Team, and Public)

See Also

- Documented notification requirements for jurisdictions and customers



Step 11

Restore Service

⇉ *REMEMBER*

Steps 11 – 13 may be completed in parallel.

Typical Duration
4 weeks

Max Duration
12 months

Above All Else...

Ensure life-safety systems are prioritized in restoration activities.

Responsible Party

Operations Section Chief

Complete These Tasks

- ☐ Assess appropriate restoration action items based on results of evidence analysis and the Incident Action Plan.
- ☐ Obtain approval of the Incident Commander for restoration action items.
- ☐ Assign restoration action items to appropriate section leads and resources.
- ☐ Assign priorities to restoration efforts aligned with impact and risk to the organization.
- ☐ Execute restoration action items.
- ☐ Perform security review and validation for any restored services before they are brought back online.

Achieve These Objectives

- ☐ Systems and data have been restored to a reasonable prior state.
- ☐ Restoration action items have been defined, approved, and assigned.

Guidance/Process Support

Restoration activities could include, but are not limited to:

- Rebuilding infected systems (often from distribution media or other known “clean” sources).
- Replacing compromised files with clean versions.
- Removing temporary constraints imposed during the containment period.
- Resetting credentials on compromised accounts.
- Installing patches.
- Tightening network perimeter security, including firewall rulesets.
- Testing systems thoroughly, including security controls.
- Confirming the integrity of business systems and controls.

Things You’ll Need

- ☐ Incident Command Post location and/or conference bridge information
- ☐ Results of evidence analysis and the Incident Action Plan
- ☐ Incident Handling Ledger (in-progress version)

See Also

- Disaster restoration procedures
- System provisioning procedures
- Backup procedures

5
6
4
14
10
9
8
7
DONE
13
12
11
3
2
1A
1
START HERE
YOU ARE HERE

Step 12

Address Root Cause

⇉ *REMEMBER*

Steps 11 – 13 may be completed in parallel.

Typical Duration
2 weeks

Max Duration
12 months

Above All Else…

Seek to understand what events led to the incident.

Responsible Party

- Incident Commander
- Relevant subject matter experts

Complete These Tasks

- ☐ Identify primary vector for breach.
- ☐ Identify pre-incident conditions that led to incident.
- ☐ Identify individuals (including organization personnel) who played a role in conditions that led to the incident.
- ☐ Identify systems, devices, or software that led to the breach or enabled the primary vector.
- ☐ Identify processes or procedures that that led to the breach or enabled the primary vector.
- ☐ Develop, document, and execute a plan that would prevent this root cause in the future.

Achieve These Objectives

- ☐ There is a clear understanding of root cause.
- ☐ The root cause has been mitigated such that it could not occur again.

Guidance/Process Support

Activities to address the root cause issues could include, but are not limited to:

- Changing credentials.
- Installing patches.
- Tightening network perimeter security, including firewall rulesets.
- Testing systems thoroughly, including security controls.
- Addressing personnel issues.
- Addressing technology lifecycle management issues.

It is critical to separate *causes* from *symptoms and effects*.

By repeatedly asking the question "Why" (five times is a good rule of thumb), you can peel away the layers. Although this technique is called "5 Whys," you may need to ask the question fewer or more than five times before you find the core issue.

Things You'll Need

- ☐ Incident Handling Ledger (in-process version)

5
6
14
4
10
9
8
7
DONE
13
12
11
3
2
1A
1
START HERE
YOU ARE HERE

Step 13

Finalize Incident Analysis Report

⇉ ***REMEMBER***
Steps 11 – 13 may be completed in parallel.

Typical Duration
2 hours

Max Duration
4 hours

Above All Else…
Document the facts, not emotions or opinions.

Responsible Party

Incident Commander

Complete These Tasks

- ☐ Complete a detailed incident analysis report focused on what occurred and when, the response, the end result, and a root cause (if identified).
- ☐ Present the Incident Report to management.

Achieve These Objectives

- ☐ An Incident Analysis Report has been completed and presented to leadership.
- ☐ The Incident Analysis Report is stored with a retention limit that meets regulatory and compliance requirements.

Guidance/Process Support

The Incident Analysis Report should be written without opinion or bias, and as if it were going to be used in a legal proceeding (because sometimes they are!). The Incident Analysis Report template offers structure and guidance, but here are some additional guidelines:

- Timestamp and date references throughout the report must be standardized.
- Include evidence screenshots if available, with numbered captions.

Things You'll Need

- ☐ Incident Handling Ledger (for reference)
- ☐ Incident Analysis Report Template

5
6
14
4
10
9
8
7
DONE
13
12
11
3
2
1A
1
START HERE
YOU ARE HERE

Step 14

Post-Mortem

Typical Duration
90 minutes
Max Duration
3 hours

Above All Else...
Understand that incidents are high-pressure, stressful situations. Focus on solutions and improvement, not failures or casting blame.

Responsible Party

Incident Commander

Complete These Tasks

- □ Review key aspects of the Incident Report and work as a team to answer the post-mortem questions.
- □ Identify opportunities for improvements to process, tools, structure, and training.
- □ Assign post-mortem action items to appropriate team members.

Achieve These Objectives

- □ Clear, actionable tasks to improve the incident response process are identified.
- □ Responsibilities for executing improvements are assigned.
- □ IR Plan changes are documented (if any).

Guidance/Process Support

Post-mortem attendees should include:

- All IR staff
- Staff with relevant insights:
  - ○ SMEs
  - ○ DR team
  - ○ Cybersecurity program owner

The goal of the post-mortem should be to answer the following questions:

- Were resources/tools sufficient to handle the incident?
- How much time passed between incident communication and confirmation? Between confirmation and resolution? Confirmation and containment? Containment and recovery?
- Could we have identified the incident sooner? How?
- Are there opportunities to automate or improve processes to mitigate this type of incident in the future?
- Did IR training sufficiently prepare the response team for this type of incident?
- Was the IR Plan consulted and followed during the incident? What should be updated?
- What can we do better next time?
- What was learned from recovery?

Things You'll Need

- □ Incident Report
- □ Incident Post-Mortem Template

YOU ARE HERE
14
DONE
13
12
11
4
5
6
10
9
8
7
3
2
1A
1
START HERE

Glossary

Key Terms

Term	Definition
Attack Vector	A path or means by which a hacker can gain access to a computer or network server in order to deliver a payload or malicious outcome.
Chain of Command	The orderly line of authority within the ranks of incident management and operations.
Chain of Custody	The chronological documentation or paper trail that records the sequence of custody, control, transfer, analysis, and disposition of materials, including physical or electronic evidence.
Command Staff	A group of incident personnel that the Incident Commander assigns to support the command function at an ICP. Command Staff often include a PIO, a Safety Officer, and a Liaison Officer, who have assistants as necessary. Additional positions may be needed, depending on the incident.
Forensic Capture	To capture evidence in such a way as to maintain the integrity of the system state, often in the context of using said data in the court of law.
General Staff	A group of incident personnel organized according to function and reporting to the Incident Commander. General Staff consists of the Operations Section Chief, Planning Section Chief, Logistics Section Chief, and Finance/Administration Section Chief.
Incident	An occurrence, natural or manmade, that necessitates a response to protect life or property.
Incident Action Plan (IAP)	An oral or written plan containing the objectives established by the IC and addressing tactics and action items in support of achieving incident objectives during the operational period (usually 12-24 hours).
Incident Commander (IC)	The individual responsible for on-scene incident activities, including developing incident objectives and ordering and releasing resources. The IC has overall authority and responsibility for conducting incident operations.
Incident Command Post (ICP)	The location (virtual and/or physical) from which the incident response is managed.
Incident Handling Ledger (IHL)	A document found in the Incident Response Kit that is used to physically record all incident details.
Incident Response Kit	A kit containing tools and guidance to assist with successful incident response activities, including forensics (physical and digital).
Incident Response Leader (IRL)	The first point of escalation for a potential incident, until they select an IC to take over.
Operational Period	The period of time scheduled for execution of a given set of tactical actions as specified in the Incident Action Plan. Operational Periods can be of various lengths, although usually not over 24 hours.
Post-Mortem	A process intended to help improve the incident handling process and identify gaps in knowledge and tooling through an analysis of each incident shortly after it occurs.
Subject Matter Expert (SME)	An authority in a particular area or topic.
Threat Agent	Any entity that may have a negative impact on the system. This may be a malicious user who wants to compromise the system's security controls; however, it could also be an accidental misuse of the system or a more physical threat like fire or flood.
Vulnerability	A weakness that makes the system susceptible to attack or damage.

NOTES

[1] These glossary definitions are pulled from ICS-300 training materials at https://rule4.io/ICS-training.

[2] This plan is loosely based on FEMA's National Incident Management System (NIMS). For more information, visit https://rule4.io/FEMA-NIMS.

Cybersecurity Incident Handling Ledger

Organization Name (if applicable): ____

Initial Intake (description and details):

Ticket # __________________________ **Third-Party Ticket/Reference #** _______________________

The following individual(s) are the primary client contact(s) for this incident response and are authorized to discuss the incident.

Primary Authorized Contact(s):

Contact Information:

□ **Yes**
□ **No**
□ **N/A**

Does the third party have an existing incident response plan that must overlay this response? (e.g., defined communication paths or procedures)? If so, obtain a copy of this plan from the above contact(s) for review and integration into the response.

Section Completed By: ______________________________ **Contact Information:** ______________________________

Current Date (YYYY-MM-DD) and Time (24-hour UTC): ____

Source of Time Reference: ____

A. Who reported this incident, and how did they become aware of it?

Section Completed By: ______________________________ **Contact Information:** ______________________________

Current Date (YYYY-MM-DD) and Time (24-hour UTC): ____

Source of Time Reference: ____

B. What is known about the incident? (Users, systems, software, hardware involved? Time events occurred?)

Section Completed By: ________________________________ **Contact Information:** ________________________________

Current Date (YYYY-MM-DD) and Time (24-hour UTC): ____

Source of Time Reference: ____

C. What actions have been taken to this point? (Who performed these actions and when?)

Name	**Action**	**Date** (YYYY-MM-DD)	**Time** (24-hour UTC)

Section Completed By: ______________________________ **Contact Information:** ______________________________

Current Date (YYYY-MM-DD) and Time (24-hour UTC): ____

Source of Time Reference: ____

D. Who is aware of this incident (name, organization if not internal, notes)?

Name	Organization (if not internal)	Notes

Section Completed By: ________________________________ **Contact Information:** ________________________________

Current Date (YYYY-MM-DD) and Time (24-hour UTC): ____

Source of Time Reference: ____

E. What steps were taken/data was collected to confirm the incident?

Section Completed By: ______________________________ **Contact Information:** ______________________________

Current Date (YYYY-MM-DD) and Time (24-hour UTC): ____

Source of Time Reference: ____

F. Where is data associated with IR efforts being stored (screenshots, logs, etc.)?

Section Completed By: ______________________________ **Contact Information:** ______________________________

Current Date (YYYY-MM-DD) and Time (24-hour UTC): ____

Source of Time Reference: ____

G. What controls are in place to protect that data/does additional effort need to be applied?

Section Completed By: ______________________________ **Contact Information:** ______________________________

Current Date (YYYY-MM-DD) and Time (24-hour UTC): ____

Source of Time Reference: ____

H. What risk does this incident pose to the organization?

Section Completed By: ______________________________ **Contact Information:** ______________________________

Current Date (YYYY-MM-DD) and Time (24-hour UTC): ____

Source of Time Reference: ____

I. What vulnerability caused the initial exposure and how should it be secured?

Section Completed By: _______________________________ **Contact Information:** _______________________________

Current Date (YYYY-MM-DD) and Time (24-hour UTC): ____

Source of Time Reference: ____

J. How and when should service be interrupted and restored?

Section Completed By: ______________________________ **Contact Information:** ______________________________

Current Date (YYYY-MM-DD) and Time (24-hour UTC): ____

Source of Time Reference: ____

K. Should evidence be gathered to attempt to pursue the attacker or further analyze the incident?

Section Completed By: ______________________________ **Contact Information:** ______________________________

Current Date (YYYY-MM-DD) and Time (24-hour UTC): ____

Source of Time Reference: ____

L. What entities should be notified, when, and by whom?

Name	Phone/Email	Notify When...	To Be Notified By

Section Completed By: ________________________________ **Contact Information:** ________________________________

Current Date (YYYY-MM-DD) and Time (24-hour UTC): ____

Source of Time Reference: ____

M. Record all changes made during this phase of incident handling:

Date (YYYY-MM-DD)	**Time** (24-hour UTC)	**Change/Description**

Section Completed By: ______________________________ **Contact Information:** ______________________________

Current Date (YYYY-MM-DD) and Time (24-hour UTC): ____

Source of Time Reference: ____

Incident Contact List

Name	Department	Phone/Email	Incident Functions/Notes

Post-Incident Actions

Use this section to capture details of actions following the incident (e.g., client data requests, destruction of media, evidence return requests).

Overflow Notes

Section Continued (e.g., B): ____________

Page Continued From: ___________

Section Continued (e.g., B): ____________

Page Continued From: ___________

Section Continued (e.g., B): ___________

Page Continued From: __________

Section Continued (e.g., B): ___________

Page Continued From: __________

Section Continued (e.g., B): ___________

Page Continued From: __________

Section Continued (e.g., B): ___________

Page Continued From: __________

Evidence Manifest

Kit# - Item #	Item Description
0001-001	
0001-002	
0001-003	
0001-004	
0001-005	
0001-006	
0001-007	
0001-008	
0001-009	
0001-010	
0001-011	
0001-012	
0001-013	
0001-014	
0001-015	

Kit# - Item #	Item Description
0001-016	
0001-017	
0001-018	
0001-019	
0001-020	
0001-021	
0001-022	
0001-023	
0001-024	
0001-025	
0001-026	
0001-027	
0001-028	
0001-029	
0001-030	

Incident Briefing for Management

Date: ______________________

Ticket # ______________________________

Third-Party Ticket/Reference # _____________________________

Background

Classification

The Incident Response Leader and Incident Commander have classified this incident as:

Incident Classification Matrix

Level	Test/Criteria
Critical	Targeted cybersecurity attacks or loss of publicly available online service. Known exposure or loss of sensitive data, successful/wide-ranging phishing/spear-phishing resulting in data loss/fraud.
Significant	Website defacement or damaging unauthorized changes to a system. Potential/suspected but unconfirmed exposure or loss of sensitive data (e.g., lost unencrypted laptop), successful phishing/spear-phishing resulting in no expected data loss/exposure.
Moderate	Suspected compromise where impact is unknown. Multiple reports of unusual/unexpected behavior. Virus or malware outbreak.

Impacted Systems & Users

Initial Evidence Identified

Response (To Date)

Action	Full Name of Actor	Date & Time

Current Known State

Concerns/Mitigating Factors

INTERNAL TEAM

Emergency Communications

Incidents and their impacts will vary widely and are often the product of unexpected or unique circumstances. While there is no one-size-fits-all message that should be used for incident communications, a general structure can be applied to any situation.

The following templates are intended to be used as a starting point for emergency communications. They should not be used without applying critical thought to the given situation and audience.

Initial Communication

Use this initial communication template as a starting point to create a message to the internal team for any incident.

> [[Your Organization Name]] Team:
>
> This is an URGENT message. Please read carefully.
>
> We have reason to believe that events have occurred that possibly put the organization's [[data/safety]] at risk.
>
> At this time, we do not know or cannot yet disclose the cause or other details about the situation. [[Investigating Authority]] is investigating and will work with [[Relevant Officials]] to provide updated information as soon as possible.
>
> To help minimize the risk resulting from this situation, please stay alert for further updates through [[chat/email]], and follow the instructions of [[Relevant Officials]].
>
> The next update will [[give specific information about when and how the next update will be given]].
>
> Thank you,
>
> [[Your Organization Name]] Leadership

Subsequent Messages

When more information is available, send updates to your team. Adapt the following basic structure to the event:

1. Expression of empathy
2. Who/what/when/why/where/how
3. What we do *not* know
4. Process to get answers
5. Clarifying facts/call for action
6. Statement of commitment
7. Referrals (for more information)
8. Next scheduled update

PUBLIC

Emergency Communications

Incidents and their impacts will vary widely and are often the product of unexpected or unique circumstances. While there is no one-size-fits-all message that should be used for incident communications, a general structure can be applied to any situation.

The following templates are intended to be used as a starting point for emergency communications. They should not be used without applying critical thought to the given situation and audience.

Initial Communication

Use this initial communication template to create a message to the public. This text is written for a data breach scenario, but can be adjusted or customized for other incident types (such as service interruption without data exposure).

[[DATE]]

To the [[Your Organization Name]] [[Community/User]]:

Recently, we have investigated and responded to a cybersecurity incident that may have exposed some of our customers' user information. In addition to this public announcement, we are sending direct emails to users whose account might be impacted. We take the protection and proper use of customer information very seriously, and this outreach is meant to explain what happened and the steps any affected users can take to protect their personal information.

What happened?

We became aware of this data incident on [[DATE]] from [[SOURCE OF REPORT(S)]] and immediately began investigating. Soon after we discovered the data breach due to [[CAUSE]], we took a series of actions to protect user accounts and ensure our environment was secure. We were able to confirm that other [[Your Organization Name]] systems were unaffected, and we contacted [[law enforcement/government officials]].

At this time, [[discussion of what data was exposed and what was not]]. We are providing this notice out of an abundance of caution because some of account data was potentially accessed by the perpetrator of this cybersecurity incident.

What type of information was involved?

The account-related data that the perpetrator gained access to includes some or possibly all of the following:

- [[DATA (e.g., Username)]]
- [[DATA (e.g., Password)]]

What are we doing to prevent [[e.g., any future breach of data]]?

Upon discovery of the cybersecurity attack, we immediately [[ACTION (e.g., secured the servers and patched the vulnerability)]]. We also conducted a digital forensic investigation to confirm that no other systems were affected, and we have taken additional measures to fortify our network against similar attacks in the future. [[List any additional improvements or implementations to improve security.]]

Our customers' happiness, and the privacy and security of their information, is extremely important to us, and we sincerely regret any inconvenience or stress this incident may have caused.

Thank you,

[[NAME]]

[[Your Organization Name]] CEO

AFFECTED USERS

Emergency Communications

Incidents and their impacts will vary widely and are often the product of unexpected or unique circumstances. While there is no one-size-fits-all message that should be used for incident communications, a general structure can be applied to any situation.

The following templates are intended to be used as a starting point for emergency communications. They should not be used without applying critical thought to the given situation and audience.

Initial Communication

Use this initial communication template to create a message to users. This text is written for a data breach scenario, but can be adjusted or customized for other incident types (such as service interruption without data exposure).

[[DATE]]

Dear [[Your Organization Name]] User:

Recently, we have investigated and responded to a cybersecurity incident that may have exposed some of our customers' user information. In addition to this public announcement, we are sending direct emails to users whose account might have been impacted. We take the protection and proper use of your information very seriously, and this outreach is meant to explain what happened and the steps you can take to protect your personal information.

What happened?

We became aware of this data incident on [[DATE]] from [[SOURCE OF REPORT(S)]] and immediately began investigating. Soon after we discovered the data breach due to [[CAUSE]], we took a series of actions to protect user accounts and ensure our environment was secure. We were able to confirm that other [[Your Organization Name]] systems were unaffected, and we contacted [[law enforcement/government officials]].

At this time, [[discussion of what data was exposed and what was not]]. We are providing this notice out of an abundance of caution because some of account data was potentially accessed by the perpetrator of this cybersecurity incident.

What type of information was involved?

The account-related data that the perpetrator gained access to includes some or possibly all of the following:

- [[DATA (e.g., Username)]]
- [[DATA (e.g., Password)]]

What are we doing to prevent [[e.g., any future breach of data]]?

Upon discovery of the cybersecurity attack, we immediately [[ACTION (e.g., secured the servers and patched the vulnerability)]]. We also conducted a digital forensic investigation to confirm that no other systems were affected, and we have taken additional measures to fortify our network against similar attacks in the future. [[List any additional improvements or implementations to improve security.]]

What can you do?

We encourage all [[Your Organization Name]] users to change their account password, and to change it to something with high complexity. Please also continue to be vigilant against potential email phishing attacks or other forms of cyber fraud.

Your happiness, and the privacy and security of your information, is extremely important to us. We sincerely regret any inconvenience or stress this incident may have caused you.

Thank you,

[[NAME]]

[[Your Organization Name]] CEO

Incident Analysis Report

Ticket # ________________

Situation Overview

Evidence Collection & Inventory

The following items were signed into investigator custody via a chain of custody form for investigation and analysis, and custody was maintained until the items were returned to the owner as noted.

Serial #	Description of Item (model, condition, marks/scratches, etc.)	Date & Time Signed Into Custody	Date and Time Returned to

Mitigation Actions

Involved Party Interviews

Evidence Review

Incident Timeline

Date	Time	Event

Recommendations

Conclusions

Appendix: Identifier Mapping

Identifier	Full Name
Individual 1	
Individual 2	
Individual 3	
Individual 4	
Individual 5	
Individual 6	
Individual 7	
Individual 8	

Incident Post-Mortem

Ticket # ____

Third-Party Ticket/Reference # (if applicable) ____

Brief Incident Description

Instructions

After completing an incident report and presenting it to management, hold a post-mortem session focused on the following tasks:

- Review key aspects of the incident report and collaborate to answer the post-mortem questions below.
- Identify opportunities for improvement to process, tools, structure, and training.
- Assign action items to appropriate team members.
- This session will improve the incident handling process and is an opportunity to identify gaps in knowledge and tooling. Focus on improvements and moving forward, not on casting blame.
- Have the Incident Report and Incident Handling Ledger handy for reference as you answer the post-mortem questions.

Post-Mortem Questions

1. Were resources/tools sufficient to handle the incident?

2. How much time passed between the following stages of the incident (in minutes, hours, or days as appropriate)?

Starting Point	End Point	Time Lapsed	Comments
Communication	Confirmation		
Confirmation	Resolution		
Confirmation	Containment		
Confirmation	Recovery		

If they are not already defined, it may be useful to define goals for these periods, to set a benchmark to work toward for future response (e.g., 10 minutes between communication and confirmation).

3. Could we have identified the incident sooner? How?

4. Are there opportunities to automate or improve processes to mitigate this type of incident in the future?

5. Did IR training sufficiently prepare the response team for this type of incident?

6. Was the IR plan reviewed/followed/consulted during the incident? What should be updated?

7. What can we do better next time?

8. What was learned from recovery?

Post-Mortem Actions

#	Action	Owner	Planned Completion Date
1			
2			
3			
4			
5			
6			
7			
8			
9			
10			
11			
12			
13			
14			