Incident Response Plan for {{COMPANY_NAME}}

Author: {{AUTHOR_NAME}}, {{AUTHOR_EMAIL}}

Revision {{REVISION_NUMBER}}, Released {{RELEASE_DATE}}

Abstract

This incident response plan is based on the concise, directive, specific, flexible, and free plan available on Counteractive Security's Github and discussed at www.counteractive.net

It was last reviewed on {{REVIEW_DATE}}. It was last tested on {{TEST_DATE}}.

Contents

Incident Response Plan for {{COMPANY_NAME}}

Author: {{AUTHOR_NAME}}, {{AUTHOR_EMAIL}}

Revision {{REVISION_NUMBER}}, Released {{RELEASE_DATE}}

This incident response plan is based on the concise, directive, specific, flexible, and free plan available on Counteractive Security's Github and discussed at www.counteractive.net

It was last reviewed on {{REVIEW_DATE}}. It was last tested on {{TEST_DATE}}.

```
TODO: Customize this plan template for your organization using
instructions at https://github.com/counteractive/incident-response-plan-template.
For incident response services, or help customizing, implementing,
or testing your plan, contact us at contact@counteractive.net or
at (888) 925-5765.
```

Assess

1. **Stay calm and professional.**
2. Gather pertinent information, *e.g.*, alarms, events, data, assumptions, intuitions (**observe**).
3. Consider impact categories, below (**orient**), and determine if there is a possible incident (**decide**):
4. Initiate a response if there is an incident (**act**). If in doubt, initiate a response. The incident commander and response team can adjust upon investigation and review.

Assess Functional Impact

What is the direct or likely impact on your mission? (*e.g.*, business operations, employees, customers, users)

- Mission/business degradation or failure: **incident!**
- None: assess information impact.

Assess Information Impact

What is the direct or likely impact on your information/data, particularly anything sensitive? (*e.g.*, PII, proprietary, financial, or healthcare data)

- Information accessed, taken, changed, or deleted: **incident!**
- None: handle via non-incident channels (*e.g.*, support ticket).

Every team member is empowered to start this process. If you see something, say something.

`TODO: Customize categories/severities as necessary. This simple example (incident vs. no incident) is based on impact categories in NIST SP 800-61r2.`

Initiate Response

Name the Incident

Create an simple two-word phrase to refer to the incident—a codename—to use for the incident file and channel(s). `TODO: Customize incident naming procedure.`

Assemble the Response Team

1. Page the on-duty/on-call Incident Commander. `TODO: Add Incident Commander call list or procedure`
2. **Do not** discuss the incident outside the response team unless cleared by the Incident Commander
3. Launch and/or join the response chat at {{RESPONSE_CHAT}}. `TODO: Add response chat launch procedure.`
4. Launch and/or join the response call at {{RESPONSE_PHONE}} and/or {{RESPONSE_VTC}}. `TODO: Add response call launch procedure.`
5. Prefer voice call, chat, and secure file exchange over any other methods.
6. **Do not** use primary email if possible. If email is necessary, use sparingly or use {{ALTERNATE_EMAIL}}. Encrypt emails when any participant is outside the {{ORGANIZATION_DOMAIN}} domain. `TODO: Add alternative email details and procedure, e.g., on-demand Office 365 or GSuite`

7. **Do not** use SMS/text to communicate about the incident, unless to tell someone to move to a more secure channel.
8. Invite on-duty/on-call responders to the response call and response chat.
    - Invite the security team. `TODO: Add security team contact list or procedure.`
    - Invite a SME for affected teams and systems. `TODO: Add team SME contact list or procedure.`
    - Invite executive stakeholders and legal counsel at earliest opportunity, but prioritize operational responders. `TODO: Add executive stakeholder contact list or procedure.`
9. *OPTIONAL:* Establish an in-person collaboration room ("war room") for complex or severe incidents. `TODO: Add collaboration room procedure.`

Reference: Response Team Structure

- Command Team
    - Incident Commander
    - Deputy Incident Commander
    - Scribe
- Liaison Team
    - Internal Liaison
    - External Liaison
- Operations Team
    - Subject Matter Experts (SMEs) for Systems
    - SMEs for Teams/Business Units
    - SMEs for Executive Functions (*e.g.*, Legal, HR, Finance)

`TODO: Modify role structure as necessary.`

Reference: Response Team Contact Information

Response Team Role	Contact Information
Incident Commander pager	{{INCIDENT_COMMANDER_PAGER_NUMBER}}
Incident Commander pager url	{{INCIDENT_COMMANDER_PAGER_URL}}
Incident Commander roster	{{INCIDENT_COMMANDER_ROSTER}}
Security team roster	{{SECURITY_TEAM_ROSTER}}
Team SME roster	{{TEAM_SME_ROSTER}}
Executive roster	{{EXECUTIVE_ROSTER}}

`TODO: Customize response team contact information. Include contact procedures in rosters, which can be static or dynamic.`

Establish Battle Rhythm

Conduct Initial Response Call

1. Conduct initial call using the initial response call structure
2. Follow instructions from the Incident Commander. If the on-duty/on-call Incident Commander does not join the call **within {{INCIDENT_COMMANDER_RESPONSE_SLA}}** and you are a trained incident commander, take command of the call.
3. Follow the instructions for your role.
4. Follow the call and chat, and comment as appropriate. If you are not a SME, filter input through the SME for your team if possible.
5. **Keep the call and chat active throughout the incident for event-driven communication.**
6. Schedule updates **every {{UPDATE_FREQUENCY}}** on the active bridge.

Reference: Initial Response Call Structure

- INCIDENT COMMANDER (IC): My name is [NAME], I am the Incident Commander. I have designated [NAME] as Deputy, and [NAME] as Scribe. Who is on the call?
- SCRIBE: [Takes attendance]
- IC: [If missing key personnel] Deputy, please page [MISSING PERSONNEL].
- IC: [Asks questions to understand situation, symptoms, scope, vector, impact, and timeline from the incident reporter, applicable SMEs for systems and business units]
- SMEs: [Brief answers to IC's questions]
- IC:[If this is an incident]:
  - At this time, the incident summary is as follows: [reiterates summary]. The Investigation team will be led by [NAME], the Remediation team will be led by [NAME], and the Communication team will be led by [NAME]. They will coordinate team membership and report to me. SMEs, please report to your appropriate team leader.
  - What investigation, remediation, or communication steps have already been taken? [this should be a short list, but needs to come out now]
  - This call and chat will remain up and available until incident closure, please use it for all incident related communications. Provide real-time status updates in the chat, if possible. Are there any questions or remaining inputs? [answers questions]

  - Team leaders, please proceed with your planned actions. We will reconvene at [UPDATE_TIME] to discuss the status. Thank you.
- IC: [If this is not an incident]: At this time, these facts do not rise to the level of an incident. I will coordinate directly with the incident reporter for follow-on actions. Thank you for your time.

Reference: Call Etiquette

- Join both the call and chat.
- Keep background noise to a minimum.
- Keep your microphone muted until you have something to say.
- Identify yourself when you join the call; State your name and role (*e.g.*, "I am the SME for team x").
- Speak up and speak clearly.
- Be direct and factual.
- Keep conversations/discussions short and to the point.
- Bring any concerns to the Incident Commander (IC) on the call.
- Respect time constraints given by the Incident Commander.
- **Use clear terminology, and avoid acronyms or abbreviations. Clarity and accuracy is more important than brevity.**

Conduct Response Update

- Conduct scheduled updates using the update call structure every {{UPDATE_FREQUENCY}} on the active bridge. `TODO: Customize update frequency and scripts; recommend no more than twice daily.`
- Adjust frequency as necessary.
- Coordinate independent updates (*e.g.*, executive, legal) as required, but as infrequently as practicable.

Reference: Response Update Call Structure

- INCIDENT COMMANDER (IC): Since our last scheduled update, the incident summary is as follows:
  - [Impact]
  - [Vector]
  - [Summary update]
  - [Timeline update]
- IC: Investigation team, please provide a brief update
  - INVESTIGATION LEAD: [Investigative activities or "nothing to report"]
  - What is your recommended investigations plan?
  - What investigation actions need tasking or approval? [listen, gain consensus, task/approve]
- IC: Remediation team, please provide a brief update

  - REMEDIATION LEAD: [Remediation activities or "nothing to report"]
  - What is your recommended remediation strategy? Strong objections? [listen, gain consensus, task/approve]
  - What remediation actions need tasking or approval?
- IC: Communication team, please provide a brief update:
  - COMMUNICATIONS LEAD: [Communication activities or "nothing to report"]
  - What is your recommended communication strategy? Strong objections? [listen, gain consensus, task/approve]
  - What communication actions need tasking or approval?
- IC: This call and chat will remain up and available until incident closure, please use it for all incident related communications. Provide real-time status updates in the chat, if possible. Are there any questions or remaining inputs? [answers questions]
- IC: Team leaders, please proceed. We will reconvene in [] to discuss the status. Thank you.

Monitor Scope

- Monitor the scope of the response to ensure it does not exceed the Incident Commander's span of control.
- If an incident gets sufficiently complex, and there are sufficient responders, consider spinning off sub-teams.

Create Sub-Teams

- In preparation for complex incidents, three sub-teams are pre-defined: Investigation, Remediation, and Communication, generally responsible for those response functions. `TODO: Customize sub-team structure if necessary.`
- Create a call bridge and chat for each sub-team.
- The Incident Commander will designate team leaders, who report to the IC, and team members, who report to their team leader. *Team leaders do not have to be trained as incident commanders, however some leadership experience is preferable.*
- The Incident Commander may adjust the purpose or name of the sub-teams as necessary.
- If you wish to switch teams, ask your **current team leader**. **Do not** ask the Incident Commander, or the leader of the other team(s). Use the chain of command.

Split Incident

If an incident turns out to be two or more distinct incidents:

- Establish a new incident file.
- Track and coordinate investigation, remediation, and communication in the appropriate file.
- Consider establishing sub-teams for each incident.
- **Maintain one top-level Incident Commander**, to coordinate low-density, high-demand assets and maintain unity of command.

Investigate

Investigate, remediate, and communicate in parallel, using separate teams, if possible. The Incident Commander will coordinate these activities. Notify the Incident Commander if there are steps the team should consider.

Create Incident File

1. Create a new incident file at {{INCIDENT_FILE_LOCATION}} using the incident name. Use this file for secure storage of documentation, evidence, artifacts, *etc.*
   - Provision secure digital storage.
   - Provision secure file exchange.
   - Obtain physical storage.
   - Share the incident file location on the call and chat.
   - `TODO: Customize and automate file location and procedure`
2. Document the functional and information impact, if known (see Assess). `TODO: Customize impact categories, if necessary.`
3. Document the vector, if known (*e.g.,* web, email, removable media). `TODO: Customize vector list, if necessary.`
4. Document the incident summary: a brief overview of the vector, impact, investigation, and remediation situation, if known.
5. Document the incident timeline, including attacker activity and responder activity. `TODO: Add timelines of varying details, as necessary.`
6. Document investigation, remediation, and communication steps. Document activities independently so they can be combined and reused, if possible.
7. Track significant information such as:
   - **Evidence**, with time of collection, source, chain of custody, *etc.*
   - **Affected systems**, with how and when system was identified, and summary of effect (*e.g.*, has malware, data accessed).
   - **Files of interest**, such as malware or data files, with system and metadata.

- **Accessed and taken data**, with filenames, metadata, and time of suspected exposure.
- **Significant attacker activity**, such as logins and malware execution, with time of the event.
- **Network-based indicators of compromise (IOCs)**, such as IP addresses and domains.
- **Host-based IOCs**, such as filenames, hashes, and registry keys.
- **Compromised accounts**, with scope of access and time of compromise.

`TODO: Customize incident documentation procedure, including spreadsheets, databases, forms, systems, and templates, if necessary.`

Collect Initial Leads

1. Interview incident reporter(s).
2. Collect initial supporting data (*e.g.*, alarms, events, data, assumptions, intuitions) in the incident file.
3. Interview SME(s) with domain or system expertise, to understand technical detail, context, and risk.
4. Interview SME(s) in affected business unit, to understand mission/business impact, context, and risk.
5. Ensure leads are relevant, detailed, and actionable.

Reference: Response Resource List

Resource	Location
Critical information list	{{CRITICAL_INFO_LIST_LOCATION}}
Critical asset list	{{CRITICAL_ASSET_LIST_LOCATION}}
Asset management database	{{ASSET_MGMT_DB_LOCATION}}
Network map	{NETWORK_MAP_LOCATION{}}
SIEM console	{{SIEM_CONSOLE_LOCATION}}
Log aggregator	{{LOG_AGGREGATOR_CONSOLE}}

`TODO: Complete critical information and asset lists ("crown jewels"). This is incredibly important to effective response.`

`TODO: Customize response resource list`

Update Investigative Plan and Incident File

1. Review and refine incident impact.
2. Review and refine incident vector.
3. Review and refine incident summary.
4. Review and refine incident timeline with facts and inferences.
5. Create hypotheses: what may have happened, and with what confidence.
6. **Identify and prioritize key questions** (information gaps) to support or discredit hypotheses.
    - Use the MITRE ATT&CK matrix or similar framework to develop questions.
        - ATT&CK for Enterprise, including links to Windows, Mac, and Linux specifics.
        - ATT&CK Mobile Profile for mobile devices.
    - Use interrogative words as inspiration:
        - **When?**: first compromise, first data loss, access to x data, access to y system, *etc.*
        - **What?**: impact, vector, root cause, motivation, tools/exploits used, accounts/systems compromised, data targeted/lost, infrastructure, IOCs, *etc.*
        - **Where?**: attacker location, affected business units, infrastructure, *etc.*
        - **How?**: compromise (exploit), persistence, access, exfiltration, lateral movement, *etc.*
        - **Why?**: targeted, timing, access x data, access y system, *etc.*
        - **Who?**: attacker, affected users, affected customers, *etc.*
7. **Identify and prioritize witness devices and strategies** to answer key questions.
    - Consult network diagrams, asset management systems, and SME expertise
    - Check the Response Resource List)
8. Refer to incident playbooks for key questions, witness devices, and strategies for investigating common or highly damaging threats.

The investigative plan is critical to an effective response; it drives all investigative actions. Use critical thinking, creativity, and sound judgment.

Reference: Attacker Tactics to Key Questions Matrix

Attacker Tactic	The way attackers ...	Possible Key Questions
Reconnaissance	... learn about targets	How? Since when? Where? Which systems?

Attacker Tactic	The way attackers ...	Possible Key Questions
Resource Development	... build infrastructure	Where? Which systems?
Initial Access	... get in	How? Since when? Where? Which systems?
Execution	... run hostile code	What malware? What tools? Where? When?
Persistence	... stick around	How? Since when? Where? Which systems?
Privilege Escalation	... get higher level access	How? Where? What tools?
Defense Evasion	... dodge security	How? Where? Since when?
Credential Access	... get/create accounts	Which accounts? Since when? Why?
Discovery	... learn our network	How? Where? What do they know?
Lateral Movement	... move around	How? When? Which accounts?
Collection	... find and gather data	What data? Why? When? Where?
Command and Control	... control tools and systems	How? Where? Who? Why?
Exfiltration	... take data	What data? How? When? Where?
Impact	... break things	What systems or data? How? When? Where? How bad?

See the MITRE ATT&CK page for more insight and ideas.

Create and Deploy Indicators of Compromise (IOCs)

Emphasize **dynamic and behavioral** indicators alongside static fingerprints.

- Create IOCs based on initial leads and analysis.
- Create IOCs using an open format supported by your tools (*e.g.*, STIX 2.0), if possible. `TODO: Customize IOC format as necessary.`

- Use automation, if possible. `TODO: Add IOC deployment/revocation procedure.`
- **Do not** deploy unrelated, un-curated "feeds" of IOCs; these can cause confusion and fatigue.
- Consider all IOC types:
  - Network-based IOCs such as IP or MAC addresses, ports, email addresses, email content or metadata, URLs, domains, or PCAP patterns.
  - Host-based IOCs such as paths, file hashes, file content or metadata, registry keys, MUTEXes, autoruns, or user artifacts and permissions.
  - Cloud-based IOCs such as log patterns for SaaS or IaaS deployments
  - Behavioral IOCs (a.k.a., patterns, TTPs) such as process tree patterns, heuristics, deviation from baseline, and login patterns.
- Correlate various IOC types, such as network and host-based indicators on the same systems(s).

Identify Systems of Interest

1. Validate whether they are relevant.
2. Categorize the reason(s) they are "of interest": has malware, accessed by compromised account, has sensitive data, etc. Treat these as "tags", there may be more than one category per system.
3. Prioritize collection, analysis, and remediation based on investigative needs, business impact, *etc.*

Collect Evidence

- Prioritize based on the investigative plan
- Collect live response data using {{LIVE_RESPONSE_TOOL}}. `TODO: Customize live response tools and procedure.`
- Collect relevant logs from system(s) (if not part of live response), aggregator(s), SIEM(s), or device console(s). `TODO: Customize log collection tools and procedure.`
- Collect memory image, if necessary and if not part of live response, using {{MEMORY_COLLECTION_TOOL}}. `TODO: Customize memory collection tools and procedure.`
- Collect disk image, if necessary, using {{DISK_IMAGE_TOOL}}. `TODO: Customize disk image collection tool and procedure.`
- Collect and store evidence in accordance with policy, and with proper chain of custody. `TODO: Customize evidence collection and chain of custody policy.`

Consider collecting the following artifacts as evidence, either in real time (_e.g., via EDR or a SIEM) or on demand:

Example Useful Artifacts

`TODO: Customize and prioritize useful artifacts.`

- Running Processes
- Running Services
- Executable Hashes
- Installed Applications
- Local and Domain Users
- Listening Ports and Associated Services
- Domain Name System (DNS) Resolution Settings and Static Routes
- Established and Recent Network Connections
- Run Key and other AutoRun Persistence
- Scheduled tasks and cron jobs
- Artifacts of past execution (e.g., Prefetch and Shimcache)
- Event logs
- Group policy and WMI artifacts
- Anti-virus detections
- Binaries in temporary storage locations
- Remote access credentials
- Network connection telemetry (e.g., netflow, firewall permits)
- DNS traffic and activity
- Remote access activity including Remote Desktop Protocol (RDP), virtual private network (VPN), SSH, virtual network computing (VNC), and other remote access tools
- Uniform Resource Identifier (URI) strings, user agent strings, and proxy enforcement actions
- Web traffic (HTTP/HTTPS)

Analyze Evidence

- Prioritize based on the investigative plan
- Analyze and triage live response data
- Analyze memory and disk images (*i.e.*, conduct forensics)
- Analyze malware
- *OPTIONAL:* Enrich with research and intelligence
- Document new indicators of compromise (IOCs)
- Update the case file

Example Useful Indicators

`TODO: Customize and prioritize useful indicators.`

- Unusual authentication behavior (*e.g.*, frequency, systems, time of day, remote location)

- Non-Standard formatted usernames
- Unsigned binaries connecting to the network
- Beaconing or significant data transfers
- PowerShell command line requests with Base64-encoded commands
- Excessive RAR, 7zip, or WinZip activity, especially with suspicious file names
- Connections on previously unused ports.
- Traffic patterns related to time, frequency, and byte count
- Changes to routing tables, such as weighting, static entries, gateways, and peer relationships

Iterate Investigation

Update the investigative plan and repeat until closure.

Remediate

Investigate, remediate, and communicate in parallel, using separate teams, if possible. The Incident Commander will coordinate these activities. Notify the Incident Commander if there are steps the team should consider

Update Remediation Plan

1. Review the incident file at {{INCIDENT_FILE_LOCATION}} using the incident name
2. Review applicable playbooks.
3. Review the Response Resource List).
4. Consider which attacker tactics are in play in this incident. Use the MITRE ATT&CK list (*i.e.*, Persistence, Privilege Escalation, Defense Evasion, Credential Access, Discovery, Lateral Movement, Execution, Collection, Exfiltration, and Command and Control), or similar framework.
5. Develop remediations for each tactic in play, as feasible given existing tools and resources. Consider remediations to Protect, Detect, Contain, and Eradicate each attacker behavior.
6. Prioritize based on timing strategy, impact, and urgency.
7. Document in incident file.

Use information security (infosec) frameworks as inspiration, but **do not use incident remediation as a substitute for an infosec program with an appropriate framework.** Use them to supplement one another.

Protect

> "How can we stop tactic X from happening again, or reduce risk? How can we improve future protection?"

Use the following as a starting point for protective remediation:

- Patch applications.
- Patch operating systems.
- Update network and host IPS signatures.
- Update endpoint protection/EDR/anti-virus signatures.
- Reduce locations with critical data.
- Reduce administrative or privileged accounts.
- Enable multi-factor authentication.
- Strengthen password requirements.
- Block unused ports and protocols at segment and network boundaries, both inbound and outbound.
- Whitelist network connections for critical servers and services.

Detect

> "How can we detect this on new systems or in the future? How can we improve future detection and investigation?"

Use the following as a starting point for detective remediation:

- Enhance logging and retention for system logs, particularly critical systems.
- Enhance logging for applications, including SaaS applications.
- Enhance log aggregation.
- Update network and host IDS signatures using IOCs.

Contain

> "How can we stop this from spreading, or getting more severe? How can we improve future containment?"

Use the following as a starting point for containment remediation:

- Implement access lists (ACLs) at network segment boundaries
- Implement blocks at the enterprise boundary, at multiple layers of the OSI model.
- Disable or remove compromised account access.
- Block malicious IP addresses or networks.
- Black hole or sinkhole malicious domains.
- Update network and host IPS and anti-malware signatures using IOCs.
- Remove critical or compromised systems from the network.

- Contact providers for assistance (*e.g.*, internet service providers, SaaS vendors)
- Whitelist network connections for critical servers and services.
- Kill or disable processes or services.
- Block or remove access for external vendors and partners, especially privileged access.

Eradicate

> "How can we eliminate this from our assets? How can we improve future eradication?"

Use the following as a starting point for eradication remediation:

- Rebuild or restore compromised systems and data from known-good state.
- Reset account passwords.
- Remove hostile accounts or credentials.
- Delete or remove specific malware (difficult!).
- Implement alternative vendors.
- Activate and migrate to alternate locations, services, or servers.

Choose Remediation Timing

Determine the timing strategy—when remediation actions will be taken—by engaging the Incident Commander, the system SMEs and owners, business unit SMEs and owners, and the executive team. Each strategy is appropriate under different circumstances:

- Choose **immediate** remediation when it is more important to immediately stop attacker activities than to continue investigating. For example, ongoing financial loss, or ongoing mission failure, active data loss, or prevention of an imminent significant threat.
- Choose **delayed** remediation when it is important to complete the investigation, or important not to alert the attacker. For example, long-term compromise by an advanced attacker, corporate espionage, or large-scale compromise of an an unknown number of systems.
- Choose **combined** remediation when both immediate and delayed circumstances apply in the same incident. For example, immediate segmentation of a sensitive server or network to meet regulatory requirements while still investigating a long-term compromise.

Execute Remediation

- Assess and explain risks of remediation actions to stakeholders. `TODO: Customize remediation risk approval procedure, if necessary.`

- Immediately implement those remediation actions with little or no affect on the attacker (sometimes called "posturing actions"). For example, many of the protection and detection actions above are good candidates.
- Schedule and task remediation actions according to the timing strategy.
- Execute remediation actions in batches, as events, for maximum effectiveness and minimum risk.
- Document execution status and time in the incident file, especially for temporary measures.

Iterate Remediation

Update the remediation plan and repeat until closure.

Communicate

Investigate, remediate, and communicate in parallel, using separate teams, if possible. The Incident Commander will coordinate these activities. Notify the Incident Commander if there are steps the team should consider

All communication must include the most accurate information available. Display integrity. Do not communicate speculation.

Communicate Internally

Notify and Update Stakeholders

- Communicate with stakeholders as part of the initial and update calls, as well as via event-driven updates on the call and chat.
- Coordinate independent updates (*e.g.*, executive, legal) as required, but as infrequently as practicable, to keep the focus on investigation and remediation.
- Focus on the best assessment of the vector, impact, summary, and highlights of the timeline including remediation steps. Do not speculate.

Notify and Update Organization

- **Do not** notify or update non-response personnel until cleared by the Incident Commander, particularly if there is a risk of an insider threat.
- Coordinate updates for teams or the entire organization with executives and business leadership.
- Focus on the best assessment of the vector, impact, summary, and highlights of the timeline including remediation steps. Do not speculate.

Create Incident Report

- Upon incident closure, capture information in the incident file for distribution using the format at {{INCIDENT_REPORT_TEMPLATE}}. **If the vector, impact, summary, timeline, and activity reports are complete, this can be fully automated.**
- Distribute the incident report to the following: {{INCIDENT_REPORT_RECIPIENTS}}.
- `TODO: Customize incident report creation and distribution, if necessary`

Communicate Externally

Notify Regulators

- **Do not** notify or update non-response personnel until cleared by the Incident Commander.
- Notify regulators (*e.g.*, HIPAA/HITRUST, PCI DSS, SOX) if necessary, and in accordance with policy.
- Coordinate requirements, format, and timeline with {COMPLIANCE_TEAM{}}.

Notify Customers

- **Do not** notify or update non-response personnel until cleared by the Incident Commander.
- Coordinate customer notifications with {{COMMUNICATIONS_TEAM}}.
- Include the date in the title of any announcement, to avoid confusion.
- **Do not** use platitudes such as "we take security very seriously". Focus on facts.
- Be honest, accept responsibility, and present the facts, along with the plan to prevent similar incidents in future.
- Be as detailed as possible with the timeline.
- Be as detailed as possible in what information was compromised, and how it affects customers. If we were storing something we shouldn't have been, be honest about it. It'll come out later and it'll be much worse.
- **Do not** discuss external parties that might have caused the compromise, unless they've already publicly disclosed, in which case link to their disclosure. Communicate with them independently (see Notify Vendors)
- Release the external communication as soon as possible. Bad news does not get better with age.
- If possible, contact customers' internal security teams before notifying the public.

Notify Vendors and Partners

- **Do not** notify or update non-response personnel until cleared by the Incident Commander.
- If possible, contact vendors' and partners' internal security teams before notifying the public.
- Focus on the specific aspects of the incident that affect or implicate the vendor or partner.
- Coordinate response efforts and share information if possible.

Notify Law Enforcement

- **Do not** notify or update non-response personnel until cleared by the Incident Commander.
- Coordinate with {{EXECUTIVE_TEAM}} and {{LEGAL_TEAM}} prior to interacting with law enforcement
- Contact local law enforcement at {{LOCAL_LE_CONTACT}}.
- Contact FBI at {{FBI_CONTACT}} or via the Internet Crime Complaint Center (IC3).
- Contact operators for any systems used in the attack, their systems may also have been compromised.

Contact External Response Support

- Contact {{INCIDENT_RESPONSE_VENDOR}} to help in assessing risk, incident management, incident response, and post-incident support.
- Contact {{PUBLIC_RELATIONS_VENDOR}} for help with PR and external communication.
- Contact {{INSURANCE_VENDOR}} for help with cyber insurance.

Share Intelligence

- Share IOCs with Infragard if applicable.
- Share IOCs with your servicing ISAC through {{ISAC_CONTACT}}, if applicable.

Recover

`TODO: Customize recovery steps.`

`TODO: Specify tools and procedures for each step, below.`

Recovery is typically governed by business units and system owners. Take recovery actions only in collaboration with relevant stakeholders.

1. Launch business continuity/disaster recovery plan(s): *e.g.*, consider migration to alternate operating locations, fail-over sites, backup systems.
2. Integrate security actions with organizational recovery efforts.

Playbooks

The following playbooks capture common investigation, remediation, and communication steps for particular types of incident.

`TODO: Create additional playbooks for highly likely or highly damaging incident types.`

Playbook: Website Defacement

Investigate, remediate (contain, eradicate), and communicate in parallel!

Assign steps to individuals or teams to work concurrently, when possible; this playbook is not purely sequential. Use your best judgment.

Investigate

1. Immediately take the defaced server offline for further investigation
    - This is especially important if the defacement is insulting or triggering in any way. Remove this from the public eye as quickly as possible to avoid harm as well as to mitigate business impact.
    - The defacement message may also contain false information that could mislead users or put them at risk.
    - Taking the server offline will allow a deeper investigation of the defacement. This may be necessary as the hacker may have dove depper into the organization accessing application servers, databases, etc.
2. Determine the system's source of vulnerability that was used by the attacker. Common exploits include:
    - SQL injection attakcs
        - This kind of attack occurs when an attacker interferes with an application's queries to the database. Therefore, this can lead to unauthorized access to private or sensitive data. Read more about SQL injection attacks here
    - Remote File Inclusion (RFI) attacks

    - This kind of attack exploits an application's referencing function to upload malware from a remote URL. Read more about RFI attacks here
  - webshells
    - More about web shells and website defacement here
  - poor web application design
    - javascript hacks
    - PHP/ASP hacks
    - Here's more on hacking with javascript
  - other methods of detection include:
    - Checking the server logs
      * look through the web page's access log and error log for any suspicious or unfamiliar activity
      * of course, it is also a good idea to check the IDS or IPS firewall logs, if available
    - Checking files with static content
    - Scanning databases for malicious content
    - Checking links present in the page
3. Collect any clues as to who the hacker is or what organization they are working for. Consider the following questions:
   - What did the defacement portray? Did it include an obvious message?
   - Did the defacement seem harmless or intentional? Could the hacker be a kid messing around or a professional group working with a motive?
   - Does it seem like your organization was targeted? Who may want to target your organization?
   - What did the hacker hope to accomplish?
   - Consult here to learn more about the types of hackers that may have attacked your webpage.
4. Collect other important information from the page that has been defaced such as:
   - a screenshot of the defacement
   - the domain and IP address of the page
   - details of the web server
   - page's source code
     - analyze this carefully to identify the problem and ensure that it is on a server belonging to the company
   - name or any information on the attacker
5. There are also tools available to aid in both detection and log analysis. A few are listed below:
   - Weblog Expert
   - Sawmill
   - Deep Log Analyzer

`TODO: Expand investigation steps, including key questions and strategies, for website defacement.`

Remediate

- **Plan remediation events** where these steps are launched together (or in coordinated fashion), with appropriate teams ready to respond to any disruption.
- **Consider the timing and tradeoffs** of remediation actions: your response has consequences.

Contain `TODO: Customize containment steps, tactical and strategic, for website defacement.`

`TODO: Specify tools and procedures for each step, below.`

1. Backup all data stored on the web server for forensic purposes.
2. As previously mentioned, make sure to take the defaced page's server down temporarily while investigation occurs.
    - You should have an error page prepared for this situation that informs user and/or employees that maintenance is undereway and the page they sought will return shortly. You may even wish to have a backup website prepared where you may publish content while investigation and remediation are underway and have your temporary error page redirect users to this backup site.
    - Check your network architecture map. If the breach is another system on the network, take that down and investigate it.
3. Once the source of the attack has been determined, apply the necessarily steps to ensure this will not happen again. This may include modifying code or editing access rights.
    - Reference the "Investigate" section for common sources of vulnerability.
    - If this is outside of your domain, simply ensure that you have given the appropriate personnel all the information on the attack that you have and allow experts to do their job.

Recover

`TODO: Customize recovery steps for defacement`

`TODO: Specify tools and procedures for each step, below`

1. Remove the hacker's message and replace with original, legitimate content. If data was lost in the attack, reference backups and restore the original page as much as possible.
    - Check backups for indicators of compromise
    - Consider partial recovery and backup integrity testing
2. Consider asking users to change their login credentials if the web server has user authentication.

3. After implementing risk avoidance measures (as recommended below), restore your server showing the original page content.
4. If necessary and/or applicable, prepare an apology/explanation of the attack that occurred for users or anyone who witnessed the defacement. Ensure that is it clear that the defacement content does not reflect your organization in any way.

Risk Avoidance `TODO: Communicate with other employees to ensure that everyone understands and contributes to the following steps, where applicable`

1. Use as few plug-ins as necessary. Hackers target websites that are vulnerable and have many sources of entry. You can limit these sources of entry by only using what you need and removing any unused or old plug ins and software. It is also important to update these as soon as possible.
2. Closely monitor and mandate access to administrative content. Only allow individuals access to what they need access to. This will reduce the chance of human error leading to cyber attacks. There are more DIY methods of prevention mentioned in this article (steps 6-12) and in resource #4 at the end of this playbook.
3. Regularly check for malware on your site by scanning the source code. Look for scripts, iframes, or URLs that look unfamiliar and make sure to also scan URLs that do look familiar.
4. There are many highly reputable automated website scanners that will not cost any of your time and will thoroughly scan your site for vulnerabilities regularly. Here is a link to popular scanners.
5. Defend against common points of exploitation such as SQL injections and XSS attacks. This article includes best practices to defend these attacks.
6. Install defacement detection programs so that if an attack were to occurr again, you would be prepared and respond quickly. Here is an article that summarizes some of 2020's best monitoring services.
7. Discuss with your employees the importance of keeping administrative access limited and confidential and inform them of these steps to avoid incidents including regular cybersecurity awareness training.

Reference: Remediation Resources `TODO: Specify financial, personnel, and logistical resources to accomplish remediation`

Communicate

`TODO: Customize communication steps for defacement`

`TODO: Specify tools and procedures (including who must be involved) for each step, below, or refer to overall plan`

1. Escalate incident and communicate with leadership per procedure
2. Document incident per procedure (and report if applicable)
3. Communicate with internal and external legal counsel per procedure, including discussions of compliance, risk exposure, liability, law enforcement contact, *etc.*
4. Communicate with users (internal)
    1. Communicate incident response updates per procedure
    2. Communicate impact of incident **and** incident response actions (e.g., containment: "why is the file share down?")
    3. Communicate requirements: "what should users do and not do?"

5. Communicate with customers
    1. Focus particularly on those whose data was affected
    2. Generate required notifications based on applicable regulations (particularly those that may consider defacement a data breach or otherwise requires notifications) `TODO: Expand notification requirements and procedures for applicable regulations`
6. Contact insurance provider(s)
    1. Discuss what resources they can make available, what tools and vendors they support and will pay for, *etc.*
    2. Comply with reporting and claims requirements to protect eligibility
7. Consider notifying and involving law enforcement. TODO: Link the following bullets to actual resources for your organization
    1. Local law enforcement
    2. State or regional law enforcement
    3. Federal or national law enforcement
8. Communicate with security and IT vendors TODO: Link the following bullets to actual resources for your organization
    1. Notify and collaborate with managed providers per procedure
    2. Notify and collaborate with incident response consultants per procedure

Resources

Reference: User Actions for Suspected Defacement Attack `TODO: Customize steps for users dealing with suspected defacement`

1. Stay calm, take a deep breath.
2. Disconnect your system from the network `TODO: include detailed steps with screenshots, a pre-installed tool or script to make this easy ("break in case of emergency"), consider hardware network cut-off switches`
3. Take pictures of the page you see using your smartphone showing the things you noticed: the defacement message and any other changes to the usual site.

4. Take notes about the problem(s) using the voice memo app on your smartphone or pen-and-paper. Every little bit helps! Document the following:
    1. What did you notice?
    2. When did it first occur, and how often since?
    3. What data do you typically access?
    4. Who else have you contacted about this incident, and what did you tell them?
5. Contact the help desk and be as helpful as possible.
6. Be patient: allow the IT personnel get it under control, you may be protecting others from harm! **Thank you.**

Reference: Help Desk Actions for Suspected Defacement Attack `TODO: Customize steps for help desk personnel dealing with suspected defacement`

1. Stay calm, take a deep breath.
2. Open a ticket to document the incident, per procedure. `TODO: Customize template with key questions (see below) and follow-on workflow`
3. Use your best judgement on which steps to prioritize (i.e. if the defacement left harmful or triggerring content, prioritize taking down the server immediately).
4. Ask the user to take pictures of their screen using their smartphone showing the things they noticed.
5. Take notes about the problem(s) using the voice memo app on your smartphone or pen-and-paper. If this is a user report, ask detailed questions, including: 1. What did you notice?
    1. When did it first occur, and how often since?
    2. What data do you typically access?
    3. Who else have you contacted about this incident, and what did you tell them?
6. Ask follow-up questions as necessary. **You are an incident responder, we are counting on you.**
7. Get detailed contact information from the user (home, office, mobile), if applicable.
8. Record all information in the ticket, including hand-written and voice notes.
9. Quarantine affected users and systems. `TODO: Customize containment steps, automate as much as possible`
10. Contact the security team and stand by to participate in the response as directed: investigation, remediation, communication, and recovery.

Additional Information

1. A helpful and detailed paper on defacement detection

2. 10 tools for better website monitoring and security
3. 2019 Website Threat Research Report with helpful statistics
4. Article including DIYs and Best practices to prevent website defacement## Playbook: Identity and Access Compromise

Investigate, remediate (contain, eradicate), and communicate in parallel!

Assign steps to individuals or teams to work concurrently, when possible; this playbook is not purely sequential. Use your best judgment.

Investigate

`TODO: Expand investigation steps, including key questions and strategies, for identity and access compromise.`

1. TODO

Remediate

- **Plan remediation events** where these steps are launched together (or in coordinated fashion), with appropriate teams ready to respond to any disruption.
- **Consider the timing and tradeoffs** of remediation actions: your response has consequences.

Contain `TODO: Customize containment steps, tactical and strategic, for identity and access compromise.`

`TODO: Specify tools and procedures for each step, below.`

- TODO

`TODO: Consider automating containment measures using orchestration tools.`

Eradicate `TODO: Customize eradication steps, tactical and strategic, for identity and access compromise.`

`TODO: Specify tools and procedures for each step, below.`

- TODO

Reference: Remediation Resources `TODO: Specify financial, personnel, and logistical resources to accomplish remediation.`

Communicate

`TODO: Customize communication steps for identity and access compromise`

`TODO: Specify tools and procedures (including who must be involved) for each step, below, or refer to overall plan.`

In addition to the general steps and guidance in the incident response plan:

1. TODO

Recover

`TODO: Customize recovery steps for identity and access compromise.`

`TODO: Specify tools and procedures for each step, below.`

In addition to the general steps and guidance in the incident response plan:

1. TODO

Resources

Additional Information

1. "Title", Author Last Name (Date)

Playbook: Phishing

Investigate, remediate (contain, eradicate), and communicate in parallel!

Assign steps to individuals or teams to work concurrently, when possible; this playbook is not purely sequential. Use your best judgment.

Investigate

`TODO: Expand investigation steps, including key questions and strategies, for phishing.`

1. **Scope the attack** Usually you will be notified that a potential phishing attack is underway, either by a user, customer, or partner.
   - Determine **total number of impacted users**
   - Understand **user actions** in response to the phishing email (*e.g.*, did they download the attachment, visit the spoofed site, or give out any personal or business information such as credentials)

- Find the potentially related activity. Check:
  - social media
  - any possibly suspicious emails
  - emails with links to external and unknown URLs
  - non-returnable or non-deliverable emails
  - any kind of notification of suspicious activity

2. **Analyze the message** using a safe device (i.e., **do not** open messages on a device with access to sensitive data or credentials as the message may contain malware), determine: `TODO: Specify tools and procedure`
   - who received the message
   - who was targeted by the message (may be different than "successful" recipients)
   - email address of the sender
   - subject line
   - message body
   - attachments (**do not open attachments** except according to established procedures)
   - links, domains, and hostnames (**do not follow links** except according to established procedures)
   - email metadata including message headers (see below)
     - sender information from the 'from' field and the X-authenticated user header
     - all client and mail server IP addresses
   - note "quirks" or suspicious features
3. **Analyze links and attachments** `TODO: Specify tools and procedure`
   - use passive collection such as nslookup and whois to find IP addresses and registration information
   - find related domains using OSINT (*e.g.*, reverse whois) on email addresses and other registration data
   - submit links, attachments, and/or hashes to VirusTotal
   - submit links, attachments, and/or hashes to a malware sandbox such as Cuckoo, Hybrid Analysis, Joe Sandbox, or VMray.
4. Categorize the type of attack. `TODO: Customize categories and create additional playbooks for common or high-impact phishing types`
5. **Determine the severity.** Consider:
   - whether public or personal safety is at risk
   - whether personal data (or other sensitive data) is at risk
   - any evidence of who is behind the attack
   - number of affected assets
   - preliminary business impact
   - whether services are affected
   - whether you are able to control/record critical systems

`TODO: Expand investigation steps, including key questions and`

`strategies, for phishing.`

Remediate

- **Plan remediation events** where these steps are launched together (or in coordinated fashion), with appropriate teams ready to respond to any disruption.
- **Consider the timing and tradeoffs** of remediation actions: your response has consequences.

Contain `TODO: Customize containment steps, tactical and strategic, for phishing.`

`TODO: Specify tools and procedures for each step, below.`

- Contain affected accounts
  - change login credentials
  - reduce access to critical services, systems, or data until investigation is complete
  - reenforce multi-factor authentication (MFA)
- Block activity based on discovered indicators of compromise, *e.g.*:
  - block malicious domains using DNS, firewalls, or proxies
  - block messages with similar senders, message bodies, subjects, links, attachments, *etc.*, using email gateway or service.
- Implement forensic hold or retain forensic copies of messages
- Purge related messages from other user inboxes, or otherwise make inaccessible
- Contain broader compromise in accordance with general IR plan
- Consider mobile device containment measures such as wiping via mobile device management (MDM). Balance against investigative/forensic impact.
- Increase detection "alert level," with enhanced monitoring, particularly from related accounts, domains, or IP addresses.
- Consider outside security assistance to support investigation and remediation
- Confirm relevant software upgrades and anti-malware updates on assets.

Reference: Remediation Resources `TODO: Specify financial, personnel, and logistical resources to accomplish remediation`

Communicate

`TODO: Customize communication steps for phishing`

`TODO: Specify tools and procedures (including who must be involved) for each step, below, or refer to overall plan`

1. Escalate incident and communicate with leadership per procedure
2. Document incident per procedure (and report)
3. Communicate with internal and external legal counsel per procedure, including discussions of compliance, risk exposure, liability, law enforcement contact, *etc.*
4. Communicate with users (internal)
    1. Communicate incident response updates per procedure
    2. Communicate impact of incident **and** incident response actions (e.g., containment: "why is the file share down?")
    3. Communicate requirements: "what should users do and not do?"

5. Communicate with customers
    1. Focus particularly on those whose data was affected
    2. Generate required notifications based on applicable regulations (particularly those that may consider phishing a data breach or otherwise requires notifications) `TODO: Expand notification requirements and procedures for applicable regulations`
6. Contact insurance provider(s)
    1. Discuss what resources they can make available, what tools and vendors they support and will pay for, *etc.*
    2. Comply with reporting and claims requirements to protect eligibility
7. Consider notifying and involving law enforcement TODO: Link the following bullets to actual resources for your organization
    1. Local law enforcement
    2. State or regional law enforcement
    3. Federal or national law enforcement
8. Communicate with security and IT vendors TODO: Link the following bullets to actual resources for your organization
    1. Notify and collaborate with managed providers per procedure
    2. Notify and collaborate with incident response consultants per procedure

Recover

`TODO: Customize recovery steps for phishing`

`TODO: Specify tools and procedures for each step, below`

1. Launch business continuity/disaster recovery plan(s) if compromise involved business outages: *e.g.*, consider migration to alternate operating locations, fail-over sites, backup systems.
2. Reinforce training programs regarding suspected phishing attacks. Key suspicious indicators may include:
    - misspellings in the message or subject
    - phony-seeming sender names, including mismatches between display name and email address

- personal email addresses for official business (e.g., gmail or yahoo emails from business colleagues)
- subject lines marked "[EXTERNAL]" on emails that look internal
- malicious or suspicious links
- receiving an email or attachment they were not expecting but from someone they know (contact sender before opening it)
- reporting suspicious activity to IT or security

3. Ensure that IT and security staff is up to date on recent phishing techniques.
4. Determine if any controls have failed when falling victim to an attack and rectify them. Here is a good source to consider following a phishing attack.

Resources

Reference: User Actions for Suspected Phishing Attack `TODO: Customize steps for users dealing with suspected phishing`

1. Stay calm, take a deep breath.
2. Take pictures of your screen using your smartphone showing the things you noticed: the phishing message, the link if you opened it, the sender information.
3. Take notes about the problem(s) using the voice memo app on your smartphone or pen-and-paper. Every little bit helps! Document the following:
    1. What did you notice?
    2. Why did you think it was a problem?
    3. What were you doing at the time you detected it?
    4. When did it first occur, and how often since?
    5. Where were you when it happened, and on what network? (office/home/shop, wired/wireless, with/without VPN, *etc.*)
    6. What systems are you using? (operating system, hostname, *etc.*)
    7. What account were you using?
    8. What data do you typically access?
    9. Who else have you contacted about this incident, and what did you tell them?
4. Contact the help desk using the phishing hotline or the phishing report toolbar and be as helpful as possible.
5. Be patient: the response may be disruptive, but you are protecting your team and the organization! **Thank you.**

Reference: Help Desk Actions for Suspected Phishing Attack `TODO: Customize steps for help desk personnel dealing with suspected phishing`

1. Stay calm, take a deep breath.

2. Open a ticket to document the incident, per procedure. `TODO: Customize template with key questions (see below) and follow-on workflow`
3. Ask the user to take pictures of their screen using their smartphone showing the things they noticed: the phishing message, the link if you opened it, the sender information, *etc.* If this is something you noticed directly, do the same yourself.
4. Take notes about the problem(s) using the voice memo app on your smartphone or pen-and-paper. If this is a user report, ask detailed questions, including:
    1. What did you notice?
    2. Why did you think it was a problem?
    3. What were you doing at the time you detected it?
    4. When did it first occur, and how often since?
    5. What networks are involved? (office/home/shop, wired/wireless, with/without VPN, *etc.*)
    6. What systems are involved? (operating system, hostname, *etc.*)
    7. What data is involved? (paths, file types, file shares, databases, software, *etc.*)
    8. What users and accounts are involved? (active directory, SaaS, SSO, service accounts, *etc.*)
    9. What data do the involved users typically access?
    10. Who else have you contacted about this incident, and what did you tell them?
5. Ask follow-up questions as necessary. **You are an incident responder, we are counting on you.**
6. Get detailed contact information from the user (home, office, mobile), if applicable.
7. Record all information in the ticket, including hand-written and voice notes.
8. Quarantine affected users and systems. `TODO: Customize containment steps, automate as much as possible`
9. Contact the security team and stand by to participate in the response as directed: investigation, remediation, communication, and recovery.

Additional Information

1. Anti-Phishing Attack resources
2. Methods of Identifying a Phishing attack
3. Phishing Email Examples
4. Anti-Phishing best practices ## Playbook: Ransomware

Investigate, remediate (contain, eradicate), and communicate in parallel! Containment is critical in ransomware incidents, prioritize accordingly.

Assign steps to individuals or teams to work concurrently, when possible; this

playbook is not purely sequential. Use your best judgment.

Investigate

`TODO: Expand investigation steps, including key questions and strategies, for ransomware.`

1. **Determine the type** of ransomware (*i.e.,* what is the family, variant, or flavor?)[1]
    1. Find any related messages. Check:
        - graphical user interfaces (GUIs) for the malware itself
        - text or html files, sometimes opened automatically after encryption
        - image files, often as wallpaper on infected systems
        - contact emails in encrypted file extensions
        - pop-ups after trying to open an encrypted file
        - voice messages
    2. Analyze the messages looking for clues to the ransomware type:
        - ransomware name
        - language, structure, phrases, artwork
        - contact email
        - format of the user id
        - ransom demand specifics (*e.g.*, digital currency, gift cards)
        - payment address in case of digital currency
        - support chat or support page
    3. Analyze affected and/or new files. Check:
        - file renaming scheme of encrypted files including extension (*e.g.*, `.crypt`, `.cry`, `.locked`) and base name
        - file corruption vs encryption
        - targeted file types and locations
        - owning user/group of affected files
        - icon for encrypted files
        - file markers
        - existence of file listings, key files or other data files
    4. Analyze affected software or system types. Some ransomware variants only affect certain tools (*e.g.*, databases) or platforms (*e.g.*, NAS products)
    5. Upload indicators to automated categorization services like Crypto Sheriff, ID Ransomware, or similar.
2. **Determine the scope:**
    1. Which systems are affected? `TODO: Specify tool(s) and procedure`
        - Scan for concrete indicators of compromise (IOCs) such as files/hashes, processes, network connections, etc. Use endpoint protection/EDR, endpoint telemetry, system logs, etc.

- Check similar systems for infection (*e.g.*, similar users, groups, data, tools, department,configuration, patch status): check IAM tools, permissions management tools, directory services, *etc.*
- Find external command and control (C2), if present, and find other systems connecting to it: check firewall or IDS logs, system logs/EDR, DNS logs, netflow or router logs, *etc.*

2. What data is affected? (*e.g.*, file types, department or group, affected software) `TODO: Specify tool(s) and procedure`
   - Find anomalous changes to file metadata such as mass changes to creation or modification times. Check file metadata search tools
   - Find changes to normally-stable or critical data files. Check file integrity monitoring tools

3. **Assess the impact** to prioritize and motivate resources
   1. Assess functional impact: impact to business or mission.
      - How much money is lost or at risk?
      - How many (and which) missions are degraded or at risk?
   2. Assess information impact: impact to confidentiality, integrity, and availability of data.
      - How critical is the data to the business/mission?
      - How sensitive is the data? (*e.g.*, trade secrets)
      - What is the regulatory status of data (*e.g.*, PII, PHI)
4. **Find the infection vector.** Check the tactics captured in the Initial Access tactic of MITRE ATT&CK[4]. Common specifics and data sources include:
   - email attachment: check email logs, email security appliances and services, e-discovery tools, *etc.*
   - insecure remote desktop protocol (RDP): check vulnerability scanning results, firewall configurations, *etc.*
   - self-propagation (worm or virus) (check host telemetry/EDR, system logs, forensic analysis, *etc.*)
   - infection via removable drives (worm or virus)
   - delivered by other malware or attacker tool: expand investigation to include additional attacker tools or malware

Remediate

- **Plan remediation events** where these steps are launched together (or in coordinated fashion), with appropriate teams ready to respond to any disruption.
- **Consider the timing and tradeoffs** of remediation actions: your response has consequences.

Contain `TODO: Customize containment steps, tactical and strategic, for ransomware.`

`TODO: Specify tools and procedures for each step, below.`

In ransomware situations, containment is critical. Inform containment measures with facts from the investigation. Prioritize quarantines and other containment measures higher than during a typical response.

Quarantines (logical, physical, or both) prevent spread *from* infected systems and prevent spread *to* critical systems and data. Quarantines should be comprehensive: include cloud/SaaS access, single-sign-on, system access such as to ERP or other business tools, *etc.*

- Quarantine infected systems
- Quarantine affected users and groups.
- Quarantine file shares (not just known-infected shares; protect uninfected shares too)
- Quarantine shared databases (not just known-infected servers; protect uninfected databases too)
- Quarantine backups, if not already secured
- Block command and control domains and addresses
- Remove vector emails from inboxes
- Confirm endpoint protection (AV, NGAV, EDR, *etc.*) is up-to-date and enabled on all systems.
- Confirm patches are deployed on all systems (prioritizing targeted systems, OSes, software, *etc.*).
- Deploy custom signatures to endpoint protection and network security tools based on discovered IOCs

`TODO: Consider automating containment measures using orchestration tools.`

Eradicate `TODO: Customize eradication steps, tactical and strategic, for ransomware.`

`TODO: Specify tools and procedures for each step, below.`

- Rebuild infected systems from known-good media
- Restore from known-clean backups
- Confirm endpoint protection (AV, NGAV, EDR, *etc.*) is up-to-date and enabled on all systems.
- Confirm patches are deployed on all systems (prioritizing targeted systems, OSes, software, *etc.*).
- Deploy custom signatures to endpoint protection and network security tools based on discovered IOCs
- **Watch for re-infection:** consider increased priority for alarms/alerts related to this incident.

Reference: Remediation Resources `TODO: Specify financial, personnel, and logistical resources to accomplish remediation.`

Communicate

`TODO: Customize communication steps for ransomware`

`TODO: Specify tools and procedures (including who must be involved) for each step, below, or refer to overall plan.`

1. Escalate incident and communicate with leadership per procedure
2. Document incident per procedure
3. Communicate with internal and external legal counsel per procedure, including discussions of compliance, risk exposure, liability, law enforcement contact, *etc.*
4. Communicate with users (internal)
    1. Communicate incident response updates per procedure
    2. Communicate impact of incident **and** incident response actions (e.g., containment: "why is the file share down?"), which can be more intrusive/disruptive during ransomware incidents
    3. Communicate requirements: "what should users do and not do?" See "Reference: User Actions for Suspected Ransomware," below
5. Communicate with customers
    1. Focus particularly on those whose data was affected
    2. Generate required notifications based on applicable regulations (particularly those that may consider ransomware a data breach or otherwise requires notifications (*e.g.*, HHS/HIPAA)) `TODO: Expand notification requirements and procedures for applicable regulations`
6. Contact insurance provider(s)
    1. Discuss what resources they can make available, what tools and vendors they support and will pay for, *etc.*
    2. Comply with reporting and claims requirements to protect eligibility
7. Communicate with regulators, including a discussion of what resources they can make available (not just boilerplate notification: many can actively assist)
8. Consider notifying and involving law enforcement
    1. Local law enforcement
    2. State or regional law enforcement
    3. Federal or national law enforcement
9. Communicate with security and IT vendors
    1. Notify and collaborate with managed providers per procedure
    2. Notify and collaborate with incident response consultants per procedure

Recover

`TODO: Customize recovery steps for ransomware.`

`TODO: Specify tools and procedures for each step, below.`

> **We do not recommend paying the ransom:** it does not guarantee a solution to the problem. It can go wrong (*e.g.*, bugs could make data unrecoverable even with the key). Also, paying proves ransomware works and could increase attacks against you or other groups.[2, paraphrased]

1. Launch business continuity/disaster recovery plan(s): *e.g.*, consider migration to alternate operating locations, fail-over sites, backup systems.
2. Recover data from known-clean backups to known-clean, patched, monitored systems (post-eradication), in accordance with our well-tested backup strategy.
   - Check backups for indicators of compromise
   - Consider partial recovery and backup integrity testing
3. Find and try known decryptors for the variant(s) discovered using resources like the No More Ransom! Project's Decryption Tools page.
4. Consider paying the ransom for irrecoverable critical assets/data, in accordance with policy `TODO: Expand and socialize this decision matrix`
   - Consider ramifications with appropriate stakeholders
   - Understand finance implications and budget
   - Understand legal, regulatory, and insurance implications
   - Understand mechanisms (*e.g.*, technologies, platforms, intermediate vendors/go-betweens)

Resources

Reference: User Actions for Suspected Ransomware `TODO: Customize steps for users dealing with suspected ransomware`

1. Stay calm, take a deep breath.
2. Disconnect your system from the network `TODO: include detailed steps with screenshots, a pre-installed tool or script to make this easy ("break in case of emergency"), consider hardware network cut-off switches`
3. Take pictures of your screen using your smartphone showing the things you noticed: ransom messages, encrypted files, system error messages, *etc.*
4. Take notes about the problem(s) using the voice memo app on your smartphone or pen-and-paper. Every little bit helps! Document the following:
   1. What did you notice?
   2. Why did you think it was a problem?

3. What were you doing at the time you detected it?
4. When did it first occur, and how often since?
5. Where were you when it happened, and on what network? (office/home/shop, wired/wireless, with/without VPN, *etc.*)
6. What systems are you using? (operating system, hostname, *etc.*)
7. What account were you using?
8. What data do you typically access?
9. Who else have you contacted about this incident, and what did you tell them?

5. Contact the help desk and be as helpful as possible
6. Be patient: the response may be disruptive, but you are protecting your team and the organization! **Thank you.**

Reference: Help Desk Actions for Suspected Ransomware `TODO: Customize steps for help desk personnel dealing with suspected ransomware`

1. Stay calm, take a deep breath.
2. Open a ticket to document the incident, per procedure `TODO: Customize template with key questions (see below) and follow-on workflow`
3. Ask the user to take pictures of their screen using their smartphone showing the things they noticed: ransom messages, encrypted files, system error messages, *etc.* If this is something you noticed directly, do the same yourself.
4. Take notes about the problem(s) using the voice memo app on your smartphone or pen-and-paper. If this is a user report, ask detailed questions, including:
    1. What did you notice?
    2. Why did you think it was a problem?
    3. What were you doing at the time you detected it?
    4. When did it first occur, and how often since?
    5. What networks are involved? (office/home/shop, wired/wireless, with/without VPN, *etc.*)
    6. What systems are involved? (operating system, hostname, *etc.*)
    7. What data is involved? (paths, file types, file shares, databases, software, *etc.*)
    8. What users and accounts are involved? (active directory, SaaS, SSO, service accounts, *etc.*)
    9. What data do the involved users typically access?
    10. Who else have you contacted about this incident, and what did you tell them?
5. Ask follow-up questions as necessary. **You are an incident responder, we are counting on you.**
6. Get detailed contact information from the user (home, office, mobile), if applicable

7. Record all information in the ticket, including hand-written and voice notes
8. Quarantine affected users and systems `TODO: Customize containment steps, automate as much as possible`
9. Contact the security team and stand by to participate in the response as directed: investigation, remediation, communication, and recovery

Additional Information

1. "Ransomware Identification for the Judicious Analyst", Hahn (12 Jun 2019)
2. No More Ransom! Project, including their Crypto Sheriff service and their Q&A
3. ID Ransomware service
4. MITRE ATT&CK Matrix, including the Initial Access and Impact tactics

Playbook: Supply Chain Compromise

Investigate, remediate (contain, eradicate), and communicate in parallel!

Assign steps to individuals or teams to work concurrently, when possible; this playbook is not purely sequential. Use your best judgment.

Investigate

`TODO: Expand investigation steps, including key questions and strategies, for supply chain compromise.`

1. TODO

Remediate

- **Plan remediation events** where these steps are launched together (or in coordinated fashion), with appropriate teams ready to respond to any disruption.
- **Consider the timing and tradeoffs** of remediation actions: your response has consequences.

Contain `TODO: Customize containment steps, tactical and strategic, for supply chain compromise.`

`TODO: Specify tools and procedures for each step, below.`

- TODO

TODO: Consider automating containment measures using orchestration tools.

Eradicate TODO: Customize eradication steps, tactical and strategic, for supply chain compromise.

TODO: Specify tools and procedures for each step, below.

- TODO

Reference: Remediation Resources TODO: Specify financial, personnel, and logistical resources to accomplish remediation.

Communicate

TODO: Customize communication steps for supply chain compromise

TODO: Specify tools and procedures (including who must be involved) for each step, below, or refer to overall plan.

In addition to the general steps and guidance in the incident response plan:

1. TODO

Recover

TODO: Customize recovery steps for supply chain compromise.

TODO: Specify tools and procedures for each step, below.

In addition to the general steps and guidance in the incident response plan:

1. TODO

Resources

Additional Information

1. "Title", Author Last Name (Date)

Roles

The following are the descriptions, duties, and training for each of the defined roles in an incident response.

`TODO: Customize roles, descriptions, duties, and training, if necessary.`

Structure of Roles

- Command Team
  - Incident Commander
  - Deputy Incident Commander
  - Scribe
- Liaison Team
  - Internal Liaison
  - External Liaison
- Operations Team
  - Subject Matter Experts (SMEs) for Systems
  - SMEs for Teams/Business Units
  - SMEs for Executive Functions (*e.g.*, Legal, HR, Finance) During larger complex incidents, the role structure may be adjusted to account for the creation of sub-teams. Read about how we handle complex incidents for more information.

This is a **flexible structure**: every role will not be filled by a different person for every incident. For example, in a small incident the Deputy might act as the Scribe and Internal Liaison. The structure is flexible and scales based on the incident.

Wartime vs. Peacetime

On incident response calls ("wartime"), a different organizational structure overrides normal operations ("peacetime"):

- The Incident Commander is in charge. No matter their rank during peacetime, they are now the highest ranked individual on the call, higher than the CEO.
- Primary responders (folks acting as primary on-call for a team/service) are the highest ranked individuals for that service.
- Decisions will be made by the IC after consideration of the information presented. Once that decision is made, it is final.
- Riskier decisions can be made by the IC than would normally be considered during peacetime.
- The IC may go against a consensus decision. If a poll is done, and 9/10 people agree but 1 disagrees. The IC may choose the disagreement option despite a majority vote. Even if you disagree, the IC's decision is final. During the call is not the time to argue with them.
- The IC may use language or behave in a way you find rude. This is wartime, and they need to do whatever it takes to resolve the situation,

so sometimes rudeness occurs. This is not personal, and something you should be prepared to experience if you've never been in a wartime situation before.
- You may be asked to leave the call by the IC, or you may even be forcibly kicked off a call. It is at the IC's discretion to do this if they feel you are not providing useful input. Again, this is not personal and you should remember that wartime is different than peacetime.

Role: All Participants

Description

All participants in an incident response have the responsibility to help resolve the incident according to the incident response plan, under the authority of the Incident Commander.

Duties

Exhibit Call Etiquette

- Join both the call and chat.
- Keep background noise to a minimum.
- Keep your microphone muted until you have something to say.
- Identify yourself when you join the call; State your name and role (*e.g.*, "I am the SME for team x").
- Speak up and speak clearly.
- Be direct and factual.
- Keep conversations/discussions short and to the point.
- Bring any concerns to the Incident Commander (IC) on the call.
- Respect time constraints given by the Incident Commander.
- If you join only one channel (call or chat), do not actively participate, as it causes disjoined communication.
- **Use clear terminology, and avoid acronyms or abbreviations. Clarity and accuracy is more important than brevity.**

Reference: Common Voice Procedure Standard radio voice procedure **is not required**, however you may hear certain terms (or need to use them yourself). Common phrases include:

- **Ack/Rog:** "I have received and understood"
- **Say Again:** "Repeat your last message"
- **Standby:** "Please wait a moment for the next response"
- **Wilco:** "Will comply"

Do not invent new abbreviations; favor being explicit over implicit.

Follow the Incident Commander The Incident Commander (IC) is the leader of the incident response process.

- Follow instructions from the incident commander.
- Do not perform any actions unless the incident commander has told you to do so.
- The commander will typically poll for strong objections before tasking a large action. Raise objections if you have them.
- Once the commander has made a decision, follow that decision (even if you disagreed).
- Answer any questions the commander asks you in a clear and concise way. Answering "I don't know" is acceptable. Do not guess.
- The commander may ask you to investigate something and get back to them in X minutes. Be ready with an answer within that time. Asking for more time is acceptable, but provide the commander an estimate.

Training

Read and understand the incident response plan, including the roles and playbooks.

Role: Incident Commander (IC)

Description

The Incident Commander (IC) acts as the single source of truth of what is currently happening and what is going to happen during an major incident. The IC is the highest ranking individual on any incident call, regardless of their day-to-day rank. They are the decision maker during an incident; they delegate tasks and listen to subject matter experts to resolve the incident. Their decisions made as commander are final.

Your job as an IC is to evaluate the situation, provide clear guidance and coordination, recruiting others to gather context/details. **Do not perform any investigation or remediation:** delegate these tasks.

Duties

Resolve the incident as quickly and as safely as possible using the incident response plan as a framework: lead the team to investigate, remediate, communicate. Use the Deputy to assist you, and delegate to relevant liaisons and experts (SMEs) at your discretion.

1. Help prepare for incidents,
    - Setup communications channels for incidents.

    - Funnel people to these communications channels when there is a major incident.
    - Train team members on how to communicate during incidents and train other Incident Commanders.
2. Drive incidents to resolution,
    - Get everyone on the same communication channel.
    - Collect information from team members for their services/area of ownership status.
    - Collect proposed repair actions, then recommend repair actions to be taken.
    - Delegate all repair actions, the Incident Commander is NOT a resolver.
    - Be the single authority on system status
3. Facilitate calls and meetings,
    - Gain consensus (Poll During a Decision)
    - Provide status updates
    - Reduce scope (dismiss attendees when possible)
    - Spin off sub-teams
    - Transfer command when necessary
    - Sign off calls
    - Maintain order
    - Get straight answers
    - Handle executive swoop such as
        - Overriding the Incident Commander
        - Anti-motivation
        - Information requests
        - Questioning severity
    - Handle disruptive or belligerent responders
4. Post Mortem,
    - Creating the initial template right after the incident so people can put in their thoughts while fresh.
    - Assigning the post-mortem after the event is over, this can be done after the call.
    - Work with Team Leads/Managers on scheduling preventive actions.

The Incident Commander uses some additional call procedures and lingo:

- Always announce when you join the call if you are the on-call IC.
- **Do not** let discussions get out of hand. Keep conversations short.
- Note objections from others, but your call is final.
- If anyone is being actively disruptive to your call, kick them off.
- Announce the end of the call.
- After an incident, communicate with other training Incident Commanders on any debrief actions you feel are necessary.

Use clear terminology, and avoid acronyms or abbreviations. Clarity and accuracy is more important than brevity.

Training

- Read the incident response plan, including all roles and playbooks.
- Participate in an incident response exercise.
- Shadow a current incident commander without actively participating, keeping your questions until the end.
- Reverse shadow a current incident commander. Respond to incidents with the current IC there to take over if necessary.
- *OPTIONAL:* facilitation training
- *OPTIONAL:* Refer to Incident Responders as Facilitators (and Therapists) and the PagerDuty Incident Commander training for more ideas and discussion.

Prerequisites There is no seniority or business-unit prerequisites to become an Incident Commander, it is a role open to anyone with the training and ability. Before you can be an Incident Commander, it is expected that you meet the following criteria:

- Excellent verbal and written **communication skills**.
- **High-level knowledge** of business infrastructure and functions.
- Excellent critical thinking, judgment, and decision-making.
- Flexibility and ability to **listen to expert feedback**, modifying plans as necessary.
- **Participated in at least two incident responses**.
- Gravitas, ability to **take command**, and **willingness to kick people off a call** to remove distractions, even if it's the CEO.

Deep technical knowledge is not required! Incident Commanders do not require deep technical knowledge of our systems. Your job as Incident Commander is to coordinate the response, not make technical changes. Don't think you can't be an Incident Commander just because you're not in the engineering department.

Graduation Upon completion of training, add yourself to the Incident Commander roster.

Role: Deputy Incident Commander (Deputy)

Description

A Deputy Incident Commander (Deputy) is a direct support role for the Incident Commander (IC). The Deputy enables the IC to focus on the problem at hand, rather than worrying about documenting steps or monitoring timers. The deputy supports the IC and keeps them focused on the incident. As a Deputy, you will be expected to take over command from the IC if they request it.

Duties

1. Bring up issues to the Incident Commander that may otherwise not be addressed (keeping an eye on timers that have been started, circling back around to missed items from a roll call, etc).
2. Be a "hot standby" Incident Commander, should the primary need to either transition to a SME, or otherwise have to step away from the IC role.
3. Manage the incident call, and be prepared to remove people from the call if instructed by the Incident Commander.
4. Monitor the status of the incident, and notify the IC if/when the incident escalates in severity level.
5. Monitor timers:
   - track how long the incident has been running
   - notify the IC every X minutes so they can take actions (*e.g.*, "IC, be advised the incident is now at the 10 minute mark.")
6. Monitor task deadlines (e.g., "IC, be advised the timer for [TEAM]'s investigation is up.")

Training

- Read and understand the incident response plan, including the roles and playbooks.

Prerequisites

- Be trained as an Incident Commander.

Role: Scribe

Description

A Scribe documents the timeline of an incident as it progresses, and makes sure all important decisions and data are captured for later review. The Scribe should focus on the incident file, as well as follow-up items for later action.

Duties

1. Ensure the incident call is being recorded.
2. Note in chat and in the file timelines: important data, events, and actions, as they happen. Specifically:
   - Key actions as they are taken
   - Status reports when one is provided by the IC

    - Any key call-outs either during the call or at the ending review
3. Update the chat with who the IC is, who the Deputy is, and that you're the scribe (if not already done).

Scribing is more art than science. The objective is to keep an accurate record of important events that occurred, Use your judgement and experience. But here are some general things you most definitely want to capture as scribe.

- The result of any polling decisions.
- Any followup items that are called out as "We should do this..", "Why didn't this?..", etc.

Training

Read and understand the incident response plan, including the roles and playbooks.

Prerequisites

- Excellent verbal and written **communication skills**.
- Anyone can act as a scribe during an incident, and are chosen by the Incident Commander at the start of the call.
- Typically the Deputy will act as the Scribe

Training Process

- Read the incident response plan, including all roles and playbooks.
- *OPTIONAL:* Parallel the actions of a scribe during an incident or exercise, and seek feedback from the actual Scribe and Incident Commander.

Role: Subject Matter Expert (SME)

Description

A Subject Matter Expert (SME) is a domain expert or designated owner of a team, component, or service (an "area"). You are there to support the incident commander in identifying the cause of the incident, suggesting and evaluation investigation, remediation, and communication actions, and following through on them as tasked.

Duties

1. Diagnose common problems within your area of expertise.
2. Rapidly fix issues found during an incident.

3. Concise communication:
    - Condition: What is the current state of your area? Is it healthy or not?
    - Actions: What actions need to be taken if your area is not in a healthy state?
    - Needs: What support do you need need to perform an action?
4. Participate in the investigation, remediation, and/or communication phases of the response.
5. Announce all suggestions to the incident commander, it is their decision on how to proceed, do not follow any actions unless told to do so.

If you are on-call for any team, you may be paged for an incident and will be expected to respond as a subject matter expert (SME) for your team, component, or service. Anyone who is considered a "domain expert" can act as a SME for an incident. Typically the team's primary on-call will act as the SME for that team.

Prepare for On-Call Period

1. Be prepared, by having already familiarized yourself with our incident response policies and procedures.
2. Make sure you have set up your alerting methods in accordance with our on-call procedure.
3. Check you can join the incident call. You may need to install a browser plugin.
4. Be aware of your upcoming on-call time and arrange swaps around travel, vacations, appointments, etc.
5. If you are an Incident Commander, make sure you are not on-call for your team at the same time as being on-call as Incident Commander.

During On-Call Period

1. Have your laptop and Internet with you at all times during your on-call period (office, home, a MiFi, a phone with a tethering plan, etc).
2. If you have important appointments, you need to get someone else on your team to cover that time slot in advance.
3. When you receive an alert for an incident, you are expected to join the incident call and chat as quickly as possible (within minutes).
4. You will be asked questions or given actions by the Incident Commander. Answer questions concisely, and follow all actions given (even if you disagree with them).
5. If you're not sure about something, bring in other SMEs from your team that can help. **Never hesitate to escalate**, if necessary.
6. Do not blame. This incident response process is completely blameless: blaming is counter productive and distracts from the problem at hand. After-action review will identify places we can all improve.

Training

- Read and understand the incident response plan, including the roles and playbooks.

Role: Liaison

Description

Liaisons interact with other teams or stakeholders, outside the incident response team. These often include:

- External Liaison: responsible for interacting with customers, either directly, or via public communication.
- Internal Liaison: responsible for interacting with internal stakeholders. Whether it's notifying an internal team of the incident, or mobilizing additional responders within the organization.

Duties

External or Customer Liaison

1. Post any publicly facing messages regarding the incident (Twitter, etc).
2. Notify the IC of any customers or media coverage reporting affects of the incident.
3. Provide customers with the external message from the post-mortem once it is completed.
4. Contact or interact with external stakeholders such as vendors, partners, law enforcement, *etc.*
5. **Do not** feel responsible for creating every message: work with the Incident Commander and other stakeholders.
6. As appropriate, keep customers informed during an incident.
7. Act as a voice for our customers to the Incident Commander, as this is useful for IC decision making.
8. Gaining message approval after you have crafted the public message: copy the message into chat and wait for verbal/written confirmation from the IC before proceeding.

Tips for Public Messages

- Prepare a default message in advance that can be used for the initial update if the scope of the issue is unknown.
- Be honest. Do not lie or guess.
- Describe our progress in resolving the incident.
  - *"We are aware of an incident. . . "*

  - *"We are investigating delayed notifications..."*
  - *"A fix has been applied and is currently being deployed..."*
  - *"The issue has been resolved..."*
- Be clear about how the incident is affecting customers. This is the primary piece of information customers will care about.
- Provide workarounds customers can use until the incident is resolved.
- Don't estimate resolution times.
- Provide the appropriate level of detail.

Internal Liaison

1. Page SME's or other on-call personnel as instructed by the Incident Commander.
2. Notify or mobilize other teams within the organization (e.g. Finance, Legal, Marketing), as instructed by the Incident Commander.
3. Track and anticipate SMEs on the call.
4. Interact with stakeholders and provide status updates as necessary.
5. Interact with internal stakeholders to answer their questions, to keep the primary call distraction free.
6. Provide regular status updates to the executive team, giving an executive summary of the current status.

Training

Read and understand the incident response plan, including the roles and playbooks.

Prerequisites

- Excellent verbal and written **communication skills**.
- *OPTIONAL:* Customer support training.
- *OPTIONAL:* Corporate communication or marketing training.

Conduct an After Action Review (AAR)

1. Schedule an After Action Review (AAR) meeting within {{AAR_SLA}} and invite the attendees listed at {{AAR_ATTENDEES}}. Always include the following:
   - The incident commander.
   - Service owners involved in the incident.
   - Key engineer(s)/responders involved in the incident.

2. Designate an AAR owner who will investigate the incident in advance of the meeting to prepare, looking into the incident process itself including reviewing notes and reports.

Conduct the AAR Meeting

Document answers to the following key questions:

1. **What happened?** Create a timeline, supported with data or other artifacts. **Avoid blame. Find facts.**
2. **What was supposed to happen?**
   - Detail deviations from process, procedure, or best practice, including SME assessments.
   - Identify ways the incident could have been detected sooner, or responded to more effectively
3. **What were the root causes?** Find root cause to things that happened and to things that should have happened.
4. **How can we improve?** Capture action items *with assignees and due dates*. Consider:
   - Stop: what should we stop doing?
   - Start: what should we start doing?
   - Continue: what should we keep doing?

Communicate AAR Status and Results

The AAR owner, in coordination with the Internal Liaison, will communicate the status of the AAR (see below)

Status Descriptions

Status	Description
Draft	AAR investigation is still ongoing
In Review	AAR investigation has been completed, and is ready to be reviewed during the AAR meeting.
Reviewed	AAR meeting is over and the content has been reviewed and agreed upon.If there are additional "External Messages", the communications team will take action to prepare.

Status	Description
Closed	No further actions are needed on the AAR (outstanding issues are tracked in tickets).If no “External Messages”, skip straight to this once the meeting is over.If there are additional “External Messages”, communications team will update AAR Closed once sent.

Communicate the results of the AAR internally and finalize the AAR documentation.

About

This template was developed by the team at Counteractive Security, to help all organizations get a good start on a concise, directive, specific, flexible, and free incident response plan. Build a plan you will actually use to respond effectively, minimize cost and impact, and get back to business as soon as possible.

License

Instructions

Customize this plan template for your own organization. Instructions are available in the project’s README. For professional assistance with incident response, or with customizing, implementing, or testing your plan, please contact us by email or phone.

References and Additional Reading

- NIST Computer Security Incident Handling Guide (NIST)
- CERT Societe Generale Incident Response Methodologies
- NIST Cybersecurity Framework
- Incident Handler’s Handbook (SANS)
- Responding to IT Security Incidents (Microsoft)

- Defining Incident Management Processes for CSIRTs: A Work in Progress (CMU)
- Creating and Managing Computer Security Incident Handling Teams (CSIRTS) (CERT)
- Incident Management for Operations (Rob Schnepp, Ron Vidal, Chris Hawley)
- *Incident Response & Computer Forensics, Third Edition* (Jason Luttgens. Matthew Pepe. Kevin Mandia)
- *Incident Response* (Kenneth R. van Wyk, Richard Forno)
- The Checklist Manifesto (Atul Gawande)
- The Field Guide to Understanding Human Error (Sidney Dekker)
- Normal Accidents: Living with High-Risk Technologies (Charles Perrow)
- Site Reliability Engineering (Google)
- Debriefing Facilitation Guide (Etsy)
- Every Minute Counts: Leading Heroku's Incident Response (Blake Gentry)
- Three Analytical Traps in Accident Investigation (Dr. Johan Bergström)
- US National Incident Management System (NIMS) (FEMA)
- Informed's NIMS Incident Command System Field Guide (Michael J. Ward)
- Advanced PostMortem Fu and Human Error 101 (Velocity 2011)
- Blame. Language. Sharing.