Incident Response Plan (Template)

Introduction

This Incident Response Plan exists to ensure that we consistently handle information security events in an effective and efficient manner. By doing so we can minimise negative consequences to the organisation, our staff, customers and other people we hold data on.

Three principles underpin our Incident Response Plan. They're called out here, right at the beginning, to serve as a reminder for every incident:

1. Assert what you know (or believe) to be true in a way that can be proved (do not assume!)
2. Failed assertions help to rule out what it *isn't* just as correct ones let you close in on a cause
3. Look for the simplest answer to the problem

Ackowledgements

Based upon the Cydea IR Plan template under the Creative Commons Attribution 4.0 International Public License. More information and updates are available from https://cydea.tools/ir-plan/

Coordinating our response

We primarily use Slack to coordinate our response to cyber security events. We also use a conference call for update calls. If an issue is classified as a S1 or S2 we will create a channel in Slack specifically for that issue and include the relevant individuals and assign roles at that time.

Slack:	https://YOURORG.slack.com/incident-response
Conference call:	+44 1234 567 890, meeting ID: 123456#
One-click join:	+44 1234 567 890,,,123456#

Alternative communication methods may be used or required if, for example, email or Slack accounts are believed to have been compromised and are unavailable, or their use would tip-off an adversary.

Phone numbers, email and other details on individuals and our key suppliers can be found in key contacts.

Roles and responsibilities

We do not have a standing incident response team. We form virtual, cross-functional teams from security, IT and other departments to tackle issues as they arise. **Incident response activities are to take priority over day-to-day responsibilities.**

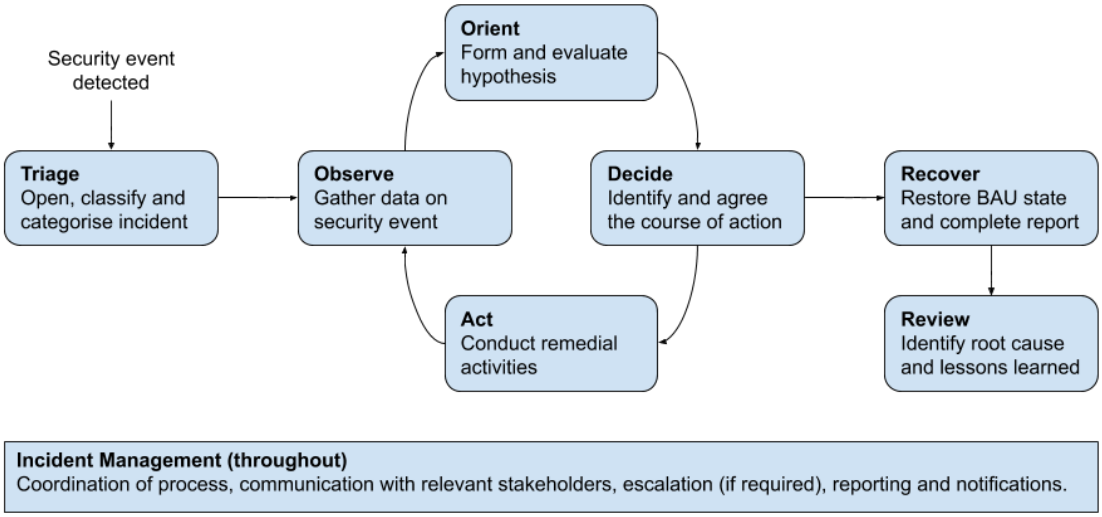
Roles are assigned on a case-by-case basis and the breakdown below outlines the typical responsibilities:

- **Senior Management** are available to support critical decisions such as taking an important system offline
- **Triage Manager (TM)** is responsible for reviewing security alerts, identifying if the security alert warrants mobilising the incident response process.
- **Incident Manager (IM)** is responsible for having an oversight of the entire incident, keeping track of progress and ensuring updates are being made within the team and out to the wider business as required.
- **Technical Lead (TL)** takes the lead on technical aspects of response and recovery (and frees up the Incident Manager to focus on coordinating the overall response.) Depending on the size and scale they may deal with the incident or will call on and coordinate investigators and infrastructure team members from a technical standpoint.
- **Investigators/Analysts/SMEs** perform analysis and help to deliver on the actions required to remediate and recover from the incident. (May include third-party resources.)
  These individuals will assist the IM or TL with assigned actions during the incident
- **IT & Infrastructure** play a critical role completing technical activities to contain and remediate issues in IT infrastructure. (May include third-party suppliers.)
  These individuals will assist the IM or TL with assigned actions during the incident
- **Other Department Leads** provide input and take actions on non-IT aspects of a response, such as ***legal***, ***media relations***, ***customer services*** and ***human resources***.
- **Third parties** may be involved depending on the type and severity of incident. Commonly these may be ***cyber insurers***, ***vendor IR teams***, ***PR/comms specialists***, ***surge call centres***, ***identity protection companies***.

Incident response process

Overview

Our Incident Response process follows the principles of an ‘OODA loop’ of: observe, orient, decide, act shown below. This gives the flexibility to handle a wide variety of situations and scenarios.



Specific information on each stage can be found below:

- Incident Management
- Triage
- Observe
- Orient
- Decide
- Act
- Recover
- Review

Playbooks

For some high-impact or frequent scenarios, we have taken this general approach and tailored it to the specific activities so that we have confidence that we are effectively and efficiently responding to these situations.

Our playbooks include:

- List of your playbooks (this may be more suited to an appendix.)

Incident Management

*Overall coordination of the incident response process is the responsibility of the **Incident Manager**. They are responsible for establishing and maintaining the 'heartbeat' of the incident, ensuring the stakeholders are kept abreast of relevant information in a timely manner, escalating the incident where appropriate, and reporting the outcomes.*

When a security incident is declared an Incident Manager is assigned. Their primary activities include:

- Tracking, assigning tasks and correlating all findings, and communications, to make sure that relevant information, hypotheses and decision points are documented
- Mobilising a response team to fulfil the necessary roles and responsibilities
- Arranging of regular update meetings or calls, and involvement of relevant teams

- Escalating serious incidents to senior management
- Ensuring the incident is communicated appropriately (to the team, wider business, other stakeholders)
- Ensuring that the full incident lifecycle is covered from initial discovery through to close down
- Ensuring that discussions remain objective and factual in nature

Record keeping of what was known and why decisions were taken is very important - as incidents may last for days or weeks, and require handover between multiple Incident Managers - and also in cases which may later be reviewed by regulators or courts. This may include criminal activity, personal or sensitive data breaches, and computer misuse. It is also critical for effective post-incident reviews.

Incident Management Checklist

- ❑ Setup 'heartbeat' checkpoints at an appropriate time interval
- ❑ Identify resources required to be part of Virtual IR Team
- ❑ Consider the need for Law Enforcement involvement
- ❑ Consider the need to notify data protection officer and regulator

Triage

*Triage is the responsibility of the **Triage Manager**, who may seek input from **Technical Lead** or **Other Department Leads**.*

The initial purpose of the triage stage is to ascertain if the security event that has been detected warrants being treated as a security incident, or is a false positive.

The Triage Manager may be filled by day-to-day operational staff reviewing security alerts from detection technology or someone from a team assigned on an ad-hoc basis to review what's known in the first instance. It is their role to sound the alarm if they believe it warrants mobilisation of formal incident response. (They may go on to become the Incident Manager.)

All security events should be logged and triaged to support trend analysis and understanding the effectiveness of security countermeasures. False-positive security events can be closed following triage.

Where a security event warrants further investigation a security incident should be opened and the rest of this process be followed.

As part of triage, all security incidents must be assigned a severity and category. Depending on the severity of the incident an escalation may be required.

Useful points to consider when triaging a security incident are:

- Who reported or what led to the discovery of the event?
- Where (systems, networks, users) does the event affect?
- What are the consequences of the event?
- How was it discovered?

- What are the related, and potentially expose, devices, systems or networks?
- Has the source(s) of the events been identified?

Triage Checklist

- ❑ Log the incident
- ❑ Record the source of the incident
- ❑ Record details and what is known about the incident
- ❑ Form a working hypothesis for the incident
- ❑ Assign an incident severity
- ❑ Assign an incident category
- ❑ Escalate or notify (as required)
- ❑ Mobilise Virtual IR Team based on type and severity of the incident
- ❑ Consider the need for third-party support
- ❑ Consider need for Legal involvement
- ❑ Consider the need to notify any customer(s)

Incident Severity

When determining the severity of an incident we consider the confidentiality, integrity, and availability of data and systems that have been affected.

1. **Confidentiality** - Has sensitive data been accessed, leaked or stolen?
2. **Integrity** - Has data or systems been altered such that they cannot be trusted?
3. **Availability** - Is the availability of data or systems impacted?

We assign incidents a severity level on a four-point scale from S1 (most severe) to S4 (least severe.)

Examples and definitions of our S1-S4 levels can be found in the severity matrix.

Incident Categorisation

To aid our understanding of the consequences of a risk event we also categorise our security incidents. This also allows us to build situational awareness of the types of incidents which we are most commonly experiencing.

We use the risk events outlined in the *Open Information Security Risk Universe* as that allows commonality between our IR and risk management approaches.

Please refer to the list of incident categories.

Escalation

The severity level will inform how quickly the incident needs to be handled and who it might need to be escalated to.

Details of the escalation requirements can be found for each corresponding severity level in the severity matrix. Contact details of Senior Management can be found in key contacts.

Delegation of authority

Cyber security incidents can evolve rapidly. It may not always be practical to wait for decision-makers to be available, or they may wish to delegate authorisation for common tasks.

We have established clear deputies for key contacts that are empowered to take decisions on their behalf. Details of Senior Management can be found in key contacts.

In addition, the following authorities are granted to the Technical Lead, under the following circumstances:

- E.g. Technical Lead may carry out any and all remedial actions, without further authorisation, for S3 and S4 incidents.
- Etc

Observe

*The **Technical Lead** and **Investigators/Analysts** or **IT & Infrastructure** are responsible for capturing and collating data that support the investigation of a security incident.*

Data and logs should be sourced from data sources relevant to the investigation and that will help to understand 'what has, or is, happening?'

Observation may involve detailed technical analysis to take large volumes of data (obtained from raw log files, or captured disk images) and conduct forensics to pull out important data points.

Observe Checklist

- ❏ Identify what data is required to support testing the hypothesis
- ❏ Record the working hypothesis in the incident log
- ❏ Confirm which assets and data sources are in scope
- ❏ Gather direct observations (or request from supplier)
- ❏ Collate outside data (e.g. OSINT)

Orient

*The **Incident Manager** collates the data from the Observe stage and, with the **Technical Lead** and **Investigators/Analysts**, evaluates the scenario.*

Contextual information, such as asset information, company plans, and external/open-source intelligence may be used to help understand the landscape.

Observations need to be analysed to understand what they tell you about the situation and help prioritise the response. The analysis at this stage takes 'data' and turns it into 'information.' Important questions include, for example, 'is this an active event still unfolding?' or 'is action needed immediately to prevent further consequences?'

The aim of this stage is to form a provable hypothesis: something that further observation or action can test. It is important to assert the objective facts rather than adopt subjective assumptions.

> *"Never attribute to malice, that which is adequately explained by stupidity."* – Hanlon's Razor

> *"When you have eliminated the impossible, whatever remains, however improbable – must be the Truth."* – Sherlock Holmes

When forming and reviewing hypotheses the Analysis of Competing Hypothesis (ACH) method can be used to conduct a structured review of hypotheses, identifying which observations are *consistent*, *inconsistent* or *not applicable*. A template matrix and more details on this method are provided in Annex E.

Once the hypothesis is formed then decisions that need to be made in order to take the next steps can be identified.

Orient Checklist

- ❑ Analyse the data to inform the understanding of what has, and is, going on
- ❑ Describe any new hypotheses that explain the causes of the event
- ❑ Combine observed data to understand the context
- ❑ Test the observations against the proposed hypothesis (consistent, inconsistent, n/a)
- ❑ Record results in incident log
- ❑ Identify the activities, and decision points, required to progress the incident

Decide

***Senior Management**, or the **Incident Manager** with appropriate delegated authority, make the required decisions based upon the context established in the previous stage. The **Incident Manager** records the decisions and justifications for the course of action.*

Decisions should, where possible, be small in nature to preserve agility when dealing with evolving situations and so that the effects of any actions can be observed and actions pivoted if required.

Decide Checklist

- ❑ Convene 'heartbeat' call
- ❑ Report the known-facts from observations and orientation of the incident in plain English, wherever possible, e.g.:
  - ❑ What happened?
  - ❑ What does this mean for us?
  - ❑ What have we done?
  - ❑ What are we doing next?
- ❑ Confirm the severity and categorisation of the incident are still appropriate
- ❑ Discuss each decision point
- ❑ Record the outcome in the incident log

- ❏ Agree on the timeframe for the next decision point

Act

*The **Technical Lead** with support from **Other Department Leads** and **Investigators/Analysts** and **IT & Infrastructure** act on the decisions made in the previous stage to further the investigation or remedy of the situation.*

It is important that actions be logged so that any cause/effect can be tracked and any ‘red herring’ subsequent security events discounted from the hypothesis.

During the ‘act’ stage teams will try to contain the threat and eradicate any actors that have infiltrated the organisation’s environment.

Where action may have a side effect on authorised user behaviour it is important that they are informed to help minimise further business disruption.

Actions may include:

- Isolation of systems (can include critical systems, virtual machines, websites)
- Reset of credentials and ability to block or lockdown remote access
- Blocking in/outbound traffic and emails
- Removing malicious files (clean or rebuild machines, clean user profiles, using AV, or deploying scripts)
- Resetting domain admin and service accounts, and estate wide resets
- Remotely isolate or quarantine machines or parts of the network
- Remotely block or remove malicious files and/or processes
- Block or alert on specific patterns (e.g. traffic patterns)
- Monitoring of network and host activity to confirm actions have been successful

The success or failure of every action should always be ascertained, especially before moving to recovery. The results form a data point when circling back to the ‘observe’ stage.

Act Checklist

- ❏ Plan the activities required to achieve the objective
- ❏ Communicate the plan with affected stakeholders
- ❏ Record details of the actions taken and the results achieved
- ❏ Communicate progress to the Incident Manager

Recover

*The **Incident Manager** is recommending a ‘green light’ to **Senior Management** to resume business as usual activities once the **Technical Lead** and any **Other Department Leads** confirm that the business environment has returned to a clean and fit state.*

Once the security incident is believed to have been contained and consequences understood the primary goal becomes a return to ‘business as usual.’

Depending on the severity and scale of the incident this may be a brief set of checks, or a far more involved process.

For malware or system compromise events that may involve returning systems to a ‘clean’ and ‘known good’ state. This may involve applying further risk mitigations or security countermeasures to prevent or reduce the frequency that similar events occur in the future, such as configuration changes or applying security patches to harden the security posture.

All recovery efforts should be closely monitored so that you can respond quickly in the event of recurrence and confidently ‘sign-off’ systems back to live operations.

Any legal, regulatory, media and customer matters should also be finalised.

Recover Checklist

- ❑ Confirm that the events are believed to have been successfully contained
- ❑ Plan activities required in order to restore affected systems and assets to BAU state
- ❑ Request any backups needed (NB: data-only backups, rather than snapshots, reduce the risk of reintroducing threats)
- ❑ Communicate recovery plan to stakeholders
- ❑ Implement recovery plan
- ❑ Review systems to confirm operating as expected / ‘clean state’
- ❑ Make a return to BAU operations recommendation to Senior Management
- ❑ Close the incident disband the Virtual IR Team

Review

*The **Incident Manager** is responsible for arranging a ‘**post-incident review’** following the successful recovery from an incident, attended by members of the **Virtual Incident Response Team** (both in-house and third-party suppliers.)*

Following the recovery phase, it is important to review the incident to fully understand the root causes of the events, where security monitoring and countermeasures may be improved, and other lessons learned. The output of post-incident reviews can also be used by the cyber security team to inform their cyber risk assessment.

Post-incident Reviews are conducted without blame or finger-pointing to encourage open and honest participation so that lessons can be learned and improvements identified. Failing to create the right open, safe environment may cause participants to withhold information crucial to preventing events from occurring again.

It is important to consider the people, process and technology aspects, and ‘what went well’ as well as ‘even better if,’ to continually improve the organisation’s capabilities. It is as important to recognise the good as it is to address any gaps.

The post-incident review will consider two lenses, including the:

- circumstances that led to the events themselves (“pre-event”)
- effectiveness and efficiency of the response activities (“post-event”)

Pre-event considerations (non-exhaustive!)

- Is this a common trend of similar events we are experiencing?
- What would have prevented the incident from occurring?
- How could we have detected the events sooner?
- Is this something considered by our cyber risk assessment?

Post-event considerations (non-exhaustive!)

- Was our response successful? (e.g. 1-10)
- What would have made our response more effective?
- How could we have made our response more efficient?
- Did we make a sound hypothesis?
- What was the key thing that led to us understanding the incident?
- Should we create, or update, a playbook for this scenario?
- Did anything hamper our response?
- Was any data or information difficult to obtain?
- Were the right people and tools available?
- Did we have any communication issues?

Review Checklist

- ❑ Identify stakeholders needed for post-incident review (inc. third-parties)
- ❑ Consider the need for independent facilitation
- ❑ Arrange a mutually convenient time for post-incident review
- ❑ Share incident report with attendees
- ❑ Discuss ‘what went well’ and ‘even better if’
- ❑ Do not ‘point fingers’ or assign blame to individuals
- ❑ Record the lessons learned and any further action points

Legal, regulatory and contractual requirements

We hold personal data of our employees and within some customers data sets. We are subject to specific regulatory reporting requirements.

Contractual and customer requirements

Details of any contractual or customer reporting/notification requirements.

Personal data breach

If a personal data breach is suspected we need to consider whether this poses a risk to the affected persons.

This will involve considering the likelihood and severity of the risk to people’s rights and freedoms, following the breach. Legal support should be sought as part of this assessment.

If this assessment deems that it's likely there will be a risk then we must notify the Information Commissioner's Office (ICO); if it's unlikely then we do not have to report.

A personal data breach that is reportable to the ICO is automatically considered an S1 incident.

We do not need to report every breach to the ICO.

Further information on reporting a personal data breach can be found on the ICO website: https://ico.org.uk/for-organisations/report-a-breach/

Law enforcement and evidential handling

If the decision is made to undertake any legal proceedings (e.g. to prosecute a criminal) then there will also be a requirement to engage relevant law enforcement agencies. This (along with any civil cases) requires careful handling of evidence.

Details of any evidential handling requirements.

Annexes

Key contacts

Incident Management

Slack:	https://YOURORG.slack.com/incident-response
Conference call:	+44 1234 567 890, meeting ID: 123456#
One-click join:	+44 1234 567 890,,,123456#

Third-party support

We have an agreement with (Cydea, or another party ;-)) to provide subject matter expertise in the event of an incident.

They can be contacted at:

- +44 203 920 7900
- https://cydea.com/#contact

Senior Management

Name	Contact	Deputy
Jane Director	jane@email.com 01234 567 890 07890 123 456 (24x7)	Bob Manager
Bob Manager	bob@email.com 01234 567 890 07890 123 456 (24x7)	Jo Leader
Jo Leader	jo@email.com 01234 567 890 07890 123 456 (24x7)	Bob Manager

Virtual IR team members

Name	Contact	Deputy

Other departmental leads

Name	Contact	Deputy
Legal		
Finance		
Human Resources		

Outsource IT provider

Name	Contact	Notes
ACME, Inc	support@email.com 01234 567 890	Available 08:00 - 18:00, Monday-Friday. Account ID: ABC12345
Other Contact		

Other key suppliers

Name	Contact	Notes

Severity matrix

When assessing the severity of an incident we consider the scale of the events, the type of systems and data involved, and the consequences. The severity matrix below helps to consistently apply severity ratings to incidents and includes some examples.

<table>
<tr><td rowspan="2">Severity</td><td colspan="2">Definition, escalation and typical cadence criteria...</td></tr>
<tr><td>… in-hours</td><td>… out-of-hours</td></tr>
<tr><td rowspan="2">S1</td><td colspan="2">Over 80% of staff unable to work
CRITICAL SYSTEM offline with no known resolution
High risk to / definite breach of sensitive client or personal data
Severe reputational damage - likely to impact business long term</td></tr>
<tr><td>Senior Management notified by phone within 60 minutes of triage.
Meeting cadence 4 hours.</td><td>Senior Management notified by phone within 60 minutes of triage.
Meeting cadence 12 hours.</td></tr>
<tr><td rowspan="2">S2</td><td colspan="2">50% of staff unable to work
Risk of breach of personal or sensitive data
Non critical systems affected, or CRITICAL SYSTEM affected with known (quick) resolution
Potential serious reputational damage</td></tr>
<tr><td>Senior Management notified by message within 4 hours of triage.
Meeting cadence 8 hours.</td><td>Senior Management notified by phone within 4 hours of triage.
Meeting cadence 12 hours.</td></tr>
<tr><td rowspan="2">S3</td><td colspan="2">Small/individual team unable to work
Possible breach of small amounts of non-sensitive data
Low risk to reputation
Small number of non-critical systems affected with known resolutions</td></tr>
<tr><td>Senior Management notified by message within 1 day of triage.
Meeting cadence daily.</td><td>Not required.</td></tr>
<tr><td rowspan="2">S4</td><td colspan="2">Minimal, if any, impact
One or two non-sensitive / non-critical machines affected</td></tr>
<tr><td>Not required.</td><td>Not required.</td></tr>
</table>

Working hours

Working hours are defined as: Monday-Friday, 09:00 - 17:00. All other times are considered ‘out-of-hours.’

Incident categorisation

Incidents may be triggered by events that are inside or outside our scope of control.

External risk events that occur outside your scope of control:

- **Supplier incident** - service compromise, breach or unavailability
- **Regulatory change** - unforeseen rules change
- **Security research** - critical vulnerability published

Internal risk events that occur inside your scope of control:

- **Abusive content** - harmful, child, sexual or violent speech or content, harassment
- **Malware** - ransomware, worm, spyware, rootkits, etc
- **Availability interruption** - denial of service or sabotage
- **Information gathering** - reconnaissance activities, network scanning or sniffing
- **Social engineering** - phishing, bribes and other (physical) threats
- **Information breach** - unauthorised access to, or sharing, modification or deletion of system/information
- **Fraud** - theft of money or misappropriation of company resources
- **System intrusion** - software exploit, SQL injection, XSS, use of stolen credentials
- **Governance failure** - process or audit failure

These categories are based upon those of the *Open Information Security Risk Universe* (https://oisru.org/).

Data sources

Details of specific systems and contacts for obtaining relevant data.

Asset and configuration information:

- IT Assets
- Software configuration (authorised software packages)

External network communications:

- Network traffic – metadata and packet capture (firewalls, IDS/IPS, proxies, DHCP, DNS)
- Emails - email logs, full email files, audit logs for the email systems

Web-facing systems:

- Web logs and potentially similar host logs to above

Authentication and access:

- Account activity - domain controller and active directory logs
- Remote logins - as above plus potentially RDP, VPN and similar

Internal network activity:

- Local system activity - event logs, antivirus logs, any other host security software logs, and full images or memory dumps of the systems

Other systems and specialist software may also need to be considered:

- Information storage (document management systems and databases)
- Financial systems
- Operational technology systems – you should consider what logs and evidence exist for these
- Cloud service-specific logs

Analysis of Competing Hypotheses

This method in this annex is intended to support the objective assessment of evidence and observations. The hypothetical causes of the incident are detailed on one axis with evidence on the other side of the matrix.

Each piece of evidence is declared to be **Consistent (C)**, **Inconsistent (I)** or **Not Applicable (N)** for each hypothesis.

By weighing up the supporting consistencies, detracting inconsistencies and ignoring data points that are not applicable the most likely of the competing hypothesis can be identified.

Hypotheses

ID	Description	Status
Hypothesis 1	*Jaffa Cakes are cake*	
Hypothesis 2	*Jaffa Cakes are biscuits*	
...		

ACH Table

ID	Evidence / data point	Hypothesis 1	Hypothesis 2	...
1	Ingredients are similar to a fluffy sponge than crisp biscuit	C	I	
2	They harden when stale (like a cake)	C	I	
3	Displayed in the biscuits aisle not the bakery section	I	C	
4	The name ‘cake’ is	N	N	
...				

C = Consistent; I = Inconsistent; N = Not applicable.