

cyber

# Cyber security incident response plan template

Table of Contents

[Introduction 2](file:///C%3A%5CUsers%5CU1100879%5CDesktop%5CVictor%20Word%20Template%20-%20Booklet.docx#_Toc71210698)

[Main Incident Response Plan 3](#_Toc71210700)

[Quick Start Guide 4](#_Toc71210702)

[Handling an incident 14](#_Toc71210702)

 [Additional information (Legal, PR, HR guidance) 24](#_Toc71210703)

[Appendices (contacts, template forms) 27](#_Toc71210704)

Introduction

This template is designed to help you create a basic incident response plan.

The plan may be tailored to your business/organization and is broken into three components:

* A ‘Quick start guide’ at the beginning with key information required to kick off an incident response; many businesses will find this sufficient for handling of most incidents.
* A full detailed incident response plan, in the event that additional detail is desired; additionally it is beneficial for meeting some audit requirements.
* An appendix with additional useful forms and templates.

There are some parts of the plan which need completing, such as relevant contact details of various teams who would assist with incident response.

#### Incident response

An incident response plan is a useful document in handling incidents, however good incident response requires more than just a plan. It requires rehearsals, suitable technology and evidence availability (e.g. log data), good backups and system/network documentation, experienced responders (in-house or external) and often input from many teams around the business (from technical to HR, PR, Legal).

A risk assessment identifying the most critical areas of the business that require prioritization in the event of a cyber incident needs to be formulated to inform your incident response plan. These critical areas could include critical data assets, applications and infrastructure.

You may also want to create playbooks with specific guidance on different types of incidents – e.g. data breach, ransomware, other malware, and denial of service.

Cyber security incident response plan

## <Company><Date>

#### Quick start guide



#### First steps



#### Key contact information

|  |  |  |
| --- | --- | --- |
| team | typical reason for involvement/contact | contact details |
| CSIRT team | Any cyber/computer incident | (EMAIL / PHONE / OTHER) |
| Incident response vendor | To perform or support technical investigation of a cyber/computer security incident  | (EMAIL / PHONE / OTHER) |
| IT security | To support investigation and remedial activities | (EMAIL / PHONE / OTHER) |
| Legal / compliance | Breach of sensitive data and/or when regulators or law enforcement are involved | (EMAIL / PHONE / OTHER) |
| PR / Comms | Incident requires comms with media/public | (EMAIL / PHONE / OTHER) |
| HR | Employee is suspected of malicious activity; or potentially breach of staff data | (EMAIL / PHONE / OTHER) |
| Crisis team / Senior mgmt. / Execs | Major incidents (see priority table) | (EMAIL / PHONE / OTHER) |
| Cyber insurance provider | Should be informed for any incident which may become a claim. Can also offer technical, legal, PR support as required on any incident | (EMAIL / PHONE / OTHER) |
| (TO COMPLETE AS NEEDED) |  | (EMAIL / PHONE / OTHER) |
| (TO COMPLETE AS NEEDED) |  | (EMAIL / PHONE / OTHER) |
| (TO COMPLETE AS NEEDED) |  | (EMAIL / PHONE / OTHER) |

#### Emergency numbers of incident calls:

|  |  |  |
| --- | --- | --- |
| name | conf bridge |  |
| Conf bridge #1 | (NUMBER AND CODE) |  |
| Conf bridge #2 | (NUMBER AND CODE)  |  |
| (OTHER – E.G. WHATSAPP / HIPCHAT / ALTERNATIVE EMAIL) |  |  |

#### Classification

|  |  |
| --- | --- |
| classification | description |
| Data breach | Data has been leaked or exposed in some way that is not meant to be and/or data has been accessed by an unauthorized party. This could be anything from someone having emailed data to the wrong person to an attacker stealing data from the network.  |
| Denial of service | An attack which affects service availability – such as website or mobile app being taken down by floods of traffic.  |
| Fraud / scam | Someone has been convinced to make a fraudulent payment or provide information as part of a scam.  |
| Ransom / extortion | There is a demand for payment (or some sort of action but usually payment) to stop some ongoing or imminent attack.  |
| System / data damage | Systems / data are damaged – often making them unusable. The most common cyber event of this type is ransomware.  |
| Malware | Malware has been discovered on the network – potentially spreading / has spread. Should consider whether it is ‘common’ malware or something more targeted along with the spread and potential motive of the attacker.  |
| Unauthorized access | Some type of unauthorized access has been discovered – this could be to the network in general or to specific data sets. This could also be by an employee or contractor; not necessarily an external party.  |

Prioritization
The incident manager may alter the priority as more information is determined; if unsure, raise to the crisis team(s) for review.

|  |  |
| --- | --- |
| priority | description / example |
| Critical (P1) - **RAISE TO CRISIS TEAM** | Severe impact and often damage increasing rapidly / limited resolution options.* Large number of (>40%) staff unable to work, critical work impacted
* Critical business systems are down with no known resolution
* Significant volume of sensitive (PII / intellectual property) data has been breached
* Large number of customers are affected and/or acutely disadvantaged in some way
* The financial impact of the incident is likely to exceed (INSERT VALUE – E.G. $100,000) – consider business interruption as well as costs for handling the incident.
* Widespread virus outbreak across all systems causing damage to data and systems
* Major reputational damage / significant impact to share price/company value

 |
| Medium (P2) - **INFORM CRISIS TEAM** | * Number of (<40%) staff are unable to work (in non-critical roles)
* Non-critical systems are down; or critical systems are down but with possible resolution
* Some (non-sensitive) data has been breached, or there is a potential, but low, risk that a small amount of sensitive data has been breached
* Small number (<50) of customers are affected and/or disadvantaged in a minor way
* Known virus / malware on several (<10) non-critical machines – low risk
* The financial impact of the incident is limited, but still of note (E.G. $50,000)
 |
| Low (P3) | * A few staff are impacted / unable to work – e.g. 1-5 people in non-critical roles
* Non-critical systems are down for <1 hour; or critical systems are down for <15 minutes
* Minor virus / malware on 1-2 (non-critical) machines
 |

Additional resources – e.g. playbooks

(INSERT PREFERENCES TO ANY SPECIFIC ADDITIONAL RESOURCES WHICH MAY BE USEFUL)

Incident record form

This form is a simple template for recording key incident information – it can be used as the initial incident notification / record and used for updates or handovers.

**For large and complicated incidents, it may also be worth mapping out the attack in a diagram and/or creating a timeline of events to understand all aspects of it and ensure nothing is missed.**

|  |  |
| --- | --- |
| INCIDENT REF/TITLE: | START DATE: |
| UPLOAD DATE: | **AUTHOR:** |
| INCIDENT STILL LIVE? Yes/No |
| INCIDENT SUMMARY: |

**Affected systems/users (refer to separate spreadsheet/file if needed)**

|  |  |  |  |
| --- | --- | --- | --- |
| Machine name | ip address | username | purpose/function/role |
| System: mspsrv012 | 1.2.3.4 | NA – all | Internal file server |
| Unknown | Unknown | Jharris | Finance |

**Known indicators of compromise / signatures (refer to separate spreadsheet/file if needed)**

|  |  |  |
| --- | --- | --- |
| type | name | notes |
| File | Bad.exe | Main malware executable |
| Network account | Adminuser1 | Admin account used by attacker |

|  |
| --- |
| **Current status:**(What actions have been taken; what is in progress; what is known) |
| **Next steps (any urgent actions / questions):**(very important if being used as a handover) |

**Actions (or refer to action tracker)**

|  |  |  |  |
| --- | --- | --- | --- |
| actions ref | action | assigned to | due date |
|  |  |  |  |
|  |  |  |  |

Checklist

#### Triage / Start response

* Validate the incident – is it real, what is known?
* Assign an incident manager and assemble team
* Inform your insurer and engage third parties as required
* Start incident record – document facts, key decisions etc.
* Obtain technical information regarding the environment (e.g. architecture diagrams).

#### Contain / Mitigate

* Take action to preserve evidence if required (e.g. isolate machine but not turn it off or start taking action on the system; alternatively this may just be making sure certain logs are not overflowing/overwriting etc.)
* Consider if any immediate action is possible to lower the risks/reduce impact
* Ensure you consider the risks and benefits of these actions vs others/doing nothing
* Plan and prioritize before implementing actions if many are required
* Consider additional logging/monitoring where appropriate
* Document findings, actions and key decisions, and report upwards as required.

#### Investigate

* Plan and prioritize tasks
* Assign tasks to relevant people/teams and track progress
* Regularly review findings and determine:
	+ New (or changes to existing) tasks
	+ Further mitigation/containment actions and/or steps for remediation plan
* Document findings, actions and key decisions, and report to others as required.

#### Remediate

* Plan remediation actions if required – e.g. if timings are important
* Ensure monitoring is in place if required while implementing actions
* Implement remediation actions
* Confirm remediation success – e.g. monitoring
* Document findings, actions and key decisions, and report to others as required.

#### Recover

* Continue with any non-critical investigation actions (e.g. historical activity) if required
* Restore/recover data or any other action required to return to ‘BAU’
* Document final status and report to others as required
* Ensure all external reporting is complete where required (e.g. customers, regulators).

#### Lessons Learned

* Invite all relevant parties to review (may require separate sessions)
* Review incident using the form in the Appendix
* Assign any actions to relevant people/teams
* Agree incident close down.

Introduction

#### Scope & Purpose

This plan is applicable to anyone who may be involved in handling a cyber or IT security related incident. The purpose of the document is to provide guidance on handling any incident of this type.

As well as maintaining this plan, staff should also review or carry out the following:

* Other relevant incident documents (playbooks, business continuity/disaster recovery/crisis management plans);
* Running incident exercises/rehearsals, testing processes and systems all work as expected;
* Maintaining and improving in-house tools and capabilities as required;
* Reviewing availability of in-house and third parties;
* Maintaining and improving communication facilities;
* Following up on previous post-incident reviews;
* Maintaining logs and reviewing retention policies;
* Testing and reviewing BC/DR capabilities.

|  |  |
| --- | --- |
| other relevant documents | location |
| (E.G. BUSINESS CONTINUITY PLAN) |  |
| (E.G. DISASTER RECOVERY PLAN) |  |
| (E.G. CRISIS COMMS PLAN) |  |
| (E.G. NETWORK DIAGRAM/INFO) |  |
| (E.G. RELATED PLAYBOOKS – DDOS, DATA BREACH, RANSOMWARE ETC) |  |

#### Computer/Security Incident Response Team (CSIRT)

Contact details available in Appendix A.

The primary team who handles IT/security/cyber incidents consists of those in the below table. It is the responsibility of this CSIRT to handle all cyber/computer security related incidents; raising these to more senior teams and involving other teams as required.

|  |  |
| --- | --- |
| CSIRT team | key contact information |
| (TO COMPLETE AS NEEDED – MAY BE SPECIFIC CSIRT TEAM, OR MAYBE A TEAM WHICH IS FORMED AS A COMBINATION OF IT, SECURITY ETC) |  |

The following departments/people may also be involved in incidents depending on the type:

|  |  |
| --- | --- |
| team | typical reason for involvement |
| System admins / owners | Knowledge and/or authority for the systems in question |
| Network admins / owners | Knowledge and/or authority for the network aspects in question |
| Human resources | Risk to staff data or concern about a malicious employee activity |
| Public relations / marketing | The incident may, or has already, become public knowledge |
| Compliance / Audit / Legal | If there may be regulatory or contractual reporting requirements, or if civil/criminal proceedings may be required |
| Customer services | If there may be customer communications / risk of customer contact re the incident |
| Security (physical/bldg.) | If the incident involves any breach of physical security |
| Crisis management teams | If the incident is (PRIORITY 1/2) |
| (TO COMPLETE AS NEEDED) |  |

#### Reporting of incidents

Incidents are typically discovered and reported via the following routes:

All staff must report incidents to: (LINE MANAGER / EMAIL / PHONE / OTHER).

Handling an incident

The below diagram shows the high level view of the incident lifecycle. Note that some stages may cycle round and/or occur at the same time depending on the type of incident.



#### Triage

Any incident which is raised to the CSIRT must be triaged to determine if it requires this plan to be invoked. Note that a key initial consideration should be whether or not it may be a false positive. Below are some key classifications of an incident; note that some may fall into several categories.

##### CLASSIFICATION & PRIORITIZATION

Classifications are as follows:

|  |  |
| --- | --- |
| classification | description |
| Data breach | Data has been leaked or exposed in some way that is not meant to be and/or data has been accessed by an unauthorized party. This could be anything from someone having emailed data to the wrong person to an attacker stealing data from the network.  |
| Denial of service | An attack which affects service availability – such as website or mobile app being taken down by floods of traffic.  |
| Fraud / scam | Someone has been convinced to make a fraudulent payment or provide information as part of a scam.  |
| Ransom / extortion | There is a demand for payment (or some sort of action but usually payment) to stop some ongoing or imminent attack.  |
| System / data damage | Systems / data are damaged – often making them unusable. The most common cyber event of this type is ransomware.  |
| Malware | Malware has been discovered on the network – potentially spreading / has spread. Should consider whether it is ‘common’ malware or something more targeted along with the spread and potential motive of the attacker.  |
| Unauthorized access | Some type of unauthorized access has been discovered – this could be to the network in general or to specific data sets. This could also be by an employee or contractor; not necessarily an external party.  |

The following questions should be applied to prioritize the incident:

* Is there any chance of the finding being a false alarm?
* What services or systems are currently impacted?
* Who is affected (staff, customers, partners) and how many?
* Is there any risk of sensitive data being breached?
* How long is the issue expected to continue?
* Is there any public aspect to the incident (e.g. website defaced, data online)?
* Is there any known action to mitigate/contain the risk or threat?
* What is the potential impact (e.g. if no action is taken quickly could it worsen)?

**(THE** **BELOW TABLE CAN BE UPDATED WITH SPECIFICS WHICH APPLY TO THE BUSINESS IN QUESTION – THERE MAY BE A SPECIFIC CRITICAL SYSTEM OR CERTAIN CATEGORIES OF CUSTOMERS FOR EXAMPLE. ALSO NOTE THAT IF YOU HAVE TIERS OF CRISIS TEAM (E.G. BRONZE, SILVER, GOLD) YOU COULD ADD IN DETAILS ABOUT WHICH LEVEL TO INFORM RATHER THAN JUST ‘CRISIS TEAM’)**

|  |  |
| --- | --- |
| priority | description / example |
| Critical (P1) - **RAISE TO CRISIS TEAM** | Severe impact and often damage increasing rapidly / limited resolution options.* Large number of (>40%) staff unable to work, critical work impacted
* Critical business systems are down with no known resolution
* Significant volume of sensitive (PII / intellectual property) data has been breached
* Large number of customers are affected and/or acutely disadvantaged in some way
* The financial impact of the incident is likely to exceed (INSERT VALUE – E.G. $100,000) – consider business interruption as well as costs for handling the incident.
* Widespread virus outbreak across all systems causing damage to data and systems
* Major reputational damage / significant impact to share price/company value

 |
| Medium (P2) - **INFORM CRISIS TEAM** | * Number of (<40%) staff are unable to work (in non-critical roles)
* Non-critical systems are down; or critical systems are down but with possible resolution
* Some (non-sensitive) data has been breached, or there is a potential, but low, risk that a small amount of sensitive data has been breached
* Small number (<50) of customers are affected and/or disadvantaged in a minor way
* Known virus / malware on several (<10) non-critical machines – low risk
* The financial impact of the incident is limited, but still of note (E.G. $50,000)
 |
| Low (P3) | * A few staff are impacted / unable to work – e.g. 1-5 people in non-critical roles
* Non-critical systems are down for <1 hour; or critical systems are down for <15 minutes
* Minor virus / malware on 1-2 (non-critical) machines
 |

#### Start response

Assuming the incident is deemed to require invoking the incident response process the following steps should be taken.

1. Create incident record
2. Assign an incident manager

The incident manager should then:

1. Escalate and/or inform any senior teams who need to be told
2. Engage relevant teams and individuals and assign tasks
3. Arrange for any required wider communications (e.g. staff or customers)
4. Set up or diarize any regular meetings/communications/reviews which may be required
5. Update incident record and ensure it is maintained
6. Obtain technical information regarding the environment (e.g. architecture diagrams)

#### Create incident record

Create a record of the incident **(INSERT DETAILS OF ANY RELEVANT INCIDENT TRACKING/RECORD SYSTEM)**

#### Assign incident manager

|  |  |
| --- | --- |
| important contact details |  |
| IR team/manager | (EMAIL / PHONE / OTHER (e.g. hipchat group) |
| Crisis mgmt. team | (EMAIL / PHONE / OTHER (e.g. hipchat group) |
| Incident conference bridge | (EMAIL / PHONE / OTHER (e.g. hipchat group) |

An **incident manager** should be assigned to project manage the breach. This individual should oversee the day to day running of the response and remediation, including ensuring the right people are involved and regularly report to any senior management as required.

It may also be required to assign a **technical recovery lead** who will oversee the technical response and recovery of the incident and report to the incident manager for larger incidents.

#### Escalate to senior teams

In some cases an incident may require escalating to a more senior crisis team, either for their awareness or for them to take the lead. The incident manager is responsible for this decision and process if it has not already occurred.

Any P1 incident should be immediately raised to the crisis team. The crisis team should be informed of any P2 incident – but they may not take over leading it; they may just wish to be kept informed. **[UPDATE THIS PARAGRAPH AS NEEDED]**

#### Engage teams (and individuals) and assign tasks

The incident manager should engage the relevant people/teams as required and assign tasks to them. Note this could include anyone across the business as well as external suppliers. This may require a meeting with various parties to agree on the tasks and determine the highest priorities.

All contact details are in Appendix A; below shows the common contacts for cyber incidents:

|  |  |
| --- | --- |
| important external contact details (further contact details in appendix a) |  |
| Internal IS / investigation support | (EMAIL / PHONE / OTHER) |
| Incident response vendor | (EMAIL / PHONE / OTHER) |
| Internal legal support | (EMAIL / PHONE / OTHER) |
| Legal support vendor | (EMAIL / PHONE / OTHER) |
| Internal PR support | (EMAIL / PHONE / OTHER) |
| PR / Crisis mgmt. vendor | (EMAIL / PHONE / OTHER) |

#### Prioritization of tasks

In a large investigation, tasks must be prioritized as it is rare that all can be progressed at once. The priority for the response should be considered and agreed – for example the priority is often to stop the attack; but may be closely followed by determining data loss or how the attack came in. Certain tasks may also be reliant on others being completed first.
**A simple actions tracker is available in Appendix C.**

#### Wider communications (staff/customers/regulators)

In some cases, communications may need to go out to staff or customers (or potentially other parties). This should always be carefully considered in a security related incident as sending out too much information could be detrimental overall. However there are situations where it will need to be considered, for example:

* Critical services/systems are unavailable (in this case it can likely be limited communication saying the service is temporarily down and people are working on it)
* Sensitive personal data has been breached (may not be proven at this point however)
* Staff or customers are required to do something different – e.g. work from home.

**Refer to ‘Additional information’ on required reporting.**

#### Wider communications (staff/customers/regulators)

The incident manager should arrange for any of the following as required:

* Conference calls/meetings to review status of the incident and agree on tasks
* Potential times/dates for any key decisions or findings

#### Record incident

The incident manager is responsible for ensuring the incident is documented throughout the incident. (This may be by assigning a scribe in larger incidents).

#### Evidence preservation

Depending on the type of incident it may be important to preserve evidence – for example if a case may be likely to go to court (such as a criminal case against an employee / ex-employee).
If this may be the case this should be considered at the very beginning of the incident before action is taken which may impact the evidence. **Further guidance can be found in ‘Additional information’ below.**

Note that evidence preservation can impact mitigation and recovery actions so the benefits and risks should be considered.

#### Contain / mitigate

Always consider if any evidence needs preserving before starting to take actions which impact it – see above.

Containing the attack and/or mitigating risks is critical throughout; and should always be considered from the beginning. Key points to consider are:

* What possible actions are there to mitigate or contain the incident/risk?
* What are the impacts of those actions compared to the incident impact?
* Is it better to wait for any further findings before taking action?
* Who/what may be behind the attack or the nature of the incident?

Typical actions may include isolating systems, resetting accounts, and removing any malicious software or access routes. It is also important to consider non-technical actions; for example communications that may help manage any public fall out; or alternative systems/processes staff could use.

**Document tasks and plan; ensure tasks are assigned to relevant teams and people. Ensure regular calls / meetings are planned, as required, to review status and findings and provide updates.**

#### Investigate

Note that containment/mitigation actions may occur throughout this stage; and some investigation may also continue through remediation.

#### Prioritization of tasks

In a large investigation, tasks must be prioritized as it is rare that all can be progressed at once. The priority for the response should be considered and agreed – for example the priority is often to stop the attack; but may be closely followed by determining data loss or how the attack came in.

#### Correlation of findings and regular reviews

For any complicated incident (definitely any P1 or P0 incidents) it is important to ensure that findings are correlated and reviewed – they may highlight an aspect that was not previously known or an incorrect assumption. Findings may also need to be regularly discussed and reported to inform other actions such as media handling or notifications to staff.

#### Communications

As findings come out, it may be required to further communicate downtimes/findings relating to any breach of data etc.

**Document tasks and plan; ensure tasks are assigned to relevant teams and people. Ensure regular calls/meetings are planned, as required, to review status and findings.**

#### Remediate

Remediation should aim to fully stop any live incident or attack. In some cases the attack may have been remediated by containment and mitigation actions; however often there may still be further actions to take following the investigation findings.

#### Remediation plan

If there are many remedial actions required it may be useful to document and agree a plan with timings and assigned actions to ensure everything is completed. In some cases this will not be necessary as actions may simply be to block one endpoint or take one machine offline – for example.

**Document tasks and plan; ensure tasks are assigned to relevant teams and people. Ensure regular calls/meetings are planned, as required, to review status and findings.**

#### Confirm remediation

In some incidents it is important to continue a period of monitoring (or enhanced/focused monitoring) in case of re-occurrence / anything new starting as a reaction to the remediation. This may be technical monitoring (e.g. network traffic, user accounts) or it may be monitoring social media, paste/data leak sites etc. This may continue whilst recovery is ongoing.

#### Recover

The recovery phase is typically after remediation is complete, or at least after the incident is suitably contained. This is to limit the risk of damage/loss occurring to newly recovered systems. Recovery actions may include:

* Restoring of data onto newly cleaned systems;
* Putting systems back online;
* Providing further messaging to affected parties.

Note that less critical investigation may still be continuing at this stage; for example if investigating all attacker actions and data exfiltration on a system was less critical to remediation it may happen at this stage, with the critical investigation leading to remediation occurring first.

#### Reporting

If not started/completed already, any regulatory, staff, customer, or public reporting should be considered if it is required.

**Document decisions and plan; ensure tasks are assigned to relevant people as required. This may also be the time to document the whole incident – if not completed throughout.**

#### Post incident review (lessons learned)

The incident should be kept open until all other stages are agreed complete and the post incident review has been completed.

The priority issues that an organization should consider when conducting a post incident review are listed below:

* Perform detailed investigation when immediate incident contained and remediated
* Incident reporting to relevant business stakeholders and authorities
* Update key information, controls and processes
* Post incident review considerations
* Lessons learned – communication and action
* Use threat intelligence to inform incident response plan

The above points are expanded upon below:

##### PERFORMING A DETAILED INVESTIGATION CAN INCLUDE:

Performing problem cause analysis

* Identify root cause of incident
* Perform a business impact assessment. Consider this in terms of financial, reputational, management or compliance impact
* Consider reporting to police and carry out sufficient evidential preservation to enable sufficient investigation to identify the threat actors.

##### INCIDENT REPORTING TO RELEVANT BUSINESS STAKEHOLDERS AND AUTHORITIES:

* What are the reporting requirements? Are there any statutory legal requirements?
* Who do I report to?
* What do I report?
* How do I report it?
* What is the objective of reporting?

These questions should be answered and ideally form part of the incident response plan. Once answered, the reporting should include the following information:

* A full background of the incident, a timeline of the incident and current status of the incident
* A business impact assessment in terms of:
	+ The financial cost of the incident (best estimate)
	+ Assessment of reputational harm
	+ Loss of management control
	+ Impaired growth of the business
* Effective recommendations for added or enhanced controls to prevent, detect, remediate or recover from a cyber incident.

##### UPDATE KEY INFORMATION, CONTROLS AND DOCUMENTS

Following a cyber incident, it is important to update your cyber security incident response approaches, controls and related documents. Areas to consider include:

* Cyber security incident management methodologies or processes
* Cyber security incident management preparatory activities
* Management controls (e.g. training and awareness activity)
* Technical controls (e.g. patching, log configuration, firewall whitelisting/blacklisting), use of intrusion prevention/detection tools
* Business continuity or crisis management arrangements
* Internal IT auditing.

Special attention should be paid to the configuration of:

* Poorly designed web applications
* Misconfigured systems
* Internet downloads
* Personal devices (tablets/smartphones)
* Authorized third parties (e.g. customers, suppliers, business partners).

##### POST INCIDENT REVIEW CONSIDERATIONS

The following points should be considered as part of the review:

* How did management and staff perform during the incident? Were the documented incident response procedures followed? Were they adequate?
* What information was needed sooner?
* Were any actions taken during the incident that could/may have hindered the recovery?
* Could any unforeseen events have been prevented?
* What could have been done differently by the personnel responding to the incident?
* How could information sharing internally and externally be improved?
* What remedial actions can prevent similar incidents in the future?
* What precursors or indicators should be watched for in the future to detect similar incidents?
* How can results be fed back into our risk assessment methodology?
* What lessons have we learned?

##### LESSONS LEARNED – COMMUNICATION AND ACTION

* It is very important to document, communicate and build on lessons learned
* Share key issues and good practice across the business
* Communications should be clear and concise focused on problem resolution and control improvement
* An action plan should be created that explains how the organization will leverage lessons learned
* Actions should be specifically assigned to a named person, prioritized with a scheduled completion date.

##### USE THREAT INTELLIGENCE TO INFORM INCIDENT RESPONSE PLAN

* Analysis of the trends of current cyber security incidents
* Use analysis to inform response plan
* Assign a budget for information security that is proportionate to threat faced. The organization needs to understand potential costs and impact of a cyber incident.

The incident manager should invite the relevant people to the review, which may include external vendors. Please refer to the lessons learned template in Appendix C.

**Document results from review and ensure any longer term improvements are assigned to relevant teams and people with clear timeframes for completion.**

#### Closure

The incident manager should agree the final closure of the response actions, along with agreement from upper management as required.

Additional information

#### Legal and regulatory considerations

##### IMPORTANT CONTACT DETAILS (FURTHER CONTACT DETAILS IN APPENDIX A)

|  |  |
| --- | --- |
| TEAM | contact details |
| Legal | Email/Phone |
| Regulatory/Compliance | Email/Phone |
| Data Protection Officer(s) | Email/Phone |

If there is any evidence of the following; the legal and compliance teams should be informed so that they can make decisions around what is required:

* Exposure of personal, or sensitive personal, information – this could include:
	+ Addresses
	+ Financial information
	+ Social Security numbers
	+ Healthcare information
* Sensitive supplier/client data (e.g. intellectual property of theirs which you hold) – there may be reporting requirements in supplier/client contracts.

You should also consider informing PR/customer relations teams in case notifications are required.

Key considerations:

* Is the data (fully or partially) encrypted or redacted?
* What is the likelihood of the data theft/exposure? Is there definite proof?
* How much data been stolen/exposed?
* If there is no legal or regulatory requirement, what is the risk and potential impact of notifying vs. not notifying?

#### Data breach reporting requirements

(ENTER IN SPECIFIC LEGAL REQUIREMENTS)

#### Evidential capture of data

Evidential capture of data is capturing and preserving data to strict legal standards such that it can be presented in a court case or other legal situation – e.g. by maintaining the chain of custody and ensuring evidence isn’t altered in any way. While some effort to stop evidence being lost is useful in many cases, full ‘evidential’ preservation is often not required.

**NOTE:** Evidence preservation can impact recovery – for example, taking a system offline where there is no failover/backup to use instead. This therefore needs considering, along with whether there may be any other sources of evidence which are more practical to preserve.

Consider whether evidence preservation may be required in cases such as:

* An employee suspected of wrong doing that could lead to a court case
* Activity where it is likely the criminal will be caught – in most cyber-attacks this is not the case, however if an ex-employee is suspected or it’s a targeted ransom/data breach and you have involved the police, it may be required.

#### Guidance

Although you must refer to specific country laws and company policies, key considerations when capturing evidentially (and serve as useful good practice) are commonly along the lines of the following:

* As much as possible, take no action to affect the data or system in any way (best course is likely to isolate the machine – but do not turn it off).
* Ensure it is stored somewhere secure.
* Keep a detailed record of all actions taken with dates and times – such that these actions could be recreated precisely if required. This should include a ‘chain of custody’ document to detail clearly who had the evidence at all times, including any handovers between people.
* Ideally have two people present, with one serving to witness the actions taken.

#### PR and customer communications

##### IMPORTANT CONTACT DETAILS (FURTHER CONTACT DETAILS IN APPENDIX A)

|  |  |
| --- | --- |
| TEAM | contact details |
| PR Team | Email/Phone |
| Customer Relations | Email/Phone |

When an incident may become public knowledge or external parties are affected/need to be notified, it is important to get communications right to help minimize reputational damage. This could include data breach or just downtime of public systems.

Decisions made in this area will likely be guided by any technical findings and legal/regulatory requirements.

#### HR teams / workers councils

##### IMPORTANT CONTACT DETAILS (FURTHER CONTACT DETAILS IN APPENDIX A)

|  |  |
| --- | --- |
| TEAM | contact details |
| HR Team | Email/Phone |

Where there is a chance that an employee is involved in the incident, or employee data may be affected by an incident, HR should be involved.

#### Informing your insurer

##### IMPORTANT CONTACT DETAILS (FURTHER CONTACT DETAILS IN APPENDIX A)

|  |  |  |
| --- | --- | --- |
| Report via [Victor Response mobile app](https://victorinsuranceus.com/Content/Industries/Cyber/Pages/Victor_Response_-_Mobile_App.aspx)CFC Cyber Claims and Incident Response hotline | USA | (844) 677 4155 |
| CFC Cyber Claims email(for non-urgent incidents) | cyberclaims@cfcunderwriting.com  |  |

There are in-house and external incident response specialists who may be able to provide you with immediate assistance in event of a cyber-attack, including putting you in touch with specialist investigators if the incident cannot be handled in-house/with existing vendors and remote support. The [Victor Response mobile app](https://victorinsuranceus.com/Content/Industries/Cyber/Pages/Victor_Response_-_Mobile_App.aspx) is the easiest method to gain immediate support in the event of a live incident. Alternatively, you may call the hotline to gain access to this support.

To submit a cyber claim, provide the following:

* Date of incident
* Nature of the incident
* Type of data / systems affected
* Steps taken so far to remediate the incident
* Any incurred or estimated costs to handle the incident and recover.

Appendix A – Contact details

##### INTERNAL

|  |  |
| --- | --- |
| key group contact info: |  |
| Incident Response Team |  |
| Incident conference bridges |  |
| Escalation details – e.g. crisis team/execs |  |

|  |  |
| --- | --- |
| incident managers |  |
| Incident Lead Primary: | Incident Lead Secondary: |
| Direct Dial: | Direct Dial: |
| Mobile: | Mobile: |
| Email: | Email: |

|  |  |
| --- | --- |
| it |  |
| IT Primary: | IT Secondary: |
| Direct Dial: | Direct Dial: |
| Mobile: | Mobile: |
| Email: | Email: |

|  |  |
| --- | --- |
| security  |  |
| Security Primary: | Security Secondary: |
| Direct Dial: | Direct Dial: |
| Mobile: | Mobile: |
| Email: | Email: |

|  |  |
| --- | --- |
| legal |  |
| Legal Primary: | Legal Secondary: |
| Direct Dial: | Direct Dial: |
| Mobile: | Mobile: |
| Email: | Email: |

|  |  |
| --- | --- |
| public relations |  |
| PR Primary: | PR Secondary: |
| Direct Dial: | Direct Dial: |
| Mobile: | Mobile: |
| Email: | Email: |

|  |  |
| --- | --- |
| risk and compliance |  |
| Risk and Compliance Primary: | Risk and Compliance Secondary: |
| Direct Dial: | Direct Dial: |
| Mobile: | Mobile: |
| Email: | Email: |

|  |  |
| --- | --- |
| human resources |  |
| HR Primary: | HR Secondary: |
| Direct Dial: | Direct Dial: |
| Mobile: | Mobile: |
| Email: | Email: |

|  |  |
| --- | --- |
| customer services |  |
| Customer Services Primary: | Customer Services Secondary: |
| Direct Dial: | Direct Dial: |
| Mobile: | Mobile: |
| Email: | Email: |

|  |  |
| --- | --- |
| internal audit |  |
| Internal Audit Primary: | Internal Audit Secondary: |
| Direct Dial: | Direct Dial: |
| Mobile: | Mobile: |
| Email: | Email: |

##### EXTERNAL

|  |  |
| --- | --- |
| forensics/incident response |  |
| Contact: | Company: |
| Direct Dial: |  |
| Mobile: |  |
| Email: |  |

|  |  |
| --- | --- |
| legal counsel |  |
| Contact: | Company: |
| Direct Dial: |  |
| Mobile: |  |
| Email: |  |

|  |  |
| --- | --- |
| public relations |  |
| Contact: | Company: |
| Direct Dial: |  |
| Mobile: |  |
| Email: |  |

|  |  |
| --- | --- |
| insurance company |  |
| Contact: | Company: |
| Direct Dial: |  |
| Mobile: |  |
| Email: |  |

|  |  |
| --- | --- |
| notification/credit/identity monitoring |  |
| Contact: | Company: |
| Direct Dial: |  |
| Mobile: |  |
| Email: |  |

Appendix B – Incident checklist

##### TRIAGE / START RESPONSE

* Validate the incident – is it real, what is known?
* Assign an incident manager and assemble team
* Inform your insurer and engage third parties as required
* Start incident record – document facts, key decisions etc.

##### CONTAIN / MITIGATE

* Take action to preserve evidence if required (e.g. isolate machine but do not turn it off or start taking action on the system; alternatively this may just be making sure certain logs are not overflowing/overwriting etc.)
* Consider if any immediate action is possible to lower the risks/reduce impact
* Ensure you consider the risks and benefits of these actions vs. others/doing nothing.
* Plan and prioritize before implementing actions if many are required
* Consider additional logging/monitoring where appropriate
* Document findings, actions and key decisions, and report upwards as required.

##### INVESTIGATE

* Plan and prioritize tasks
* Assign tasks to relevant people/teams and track progress
* Regularly review findings and determine
	+ New (or changes to existing) tasks
	+ Further mitigation/containment actions and/or steps for remediation plan
* Document findings, actions and key decisions, and report to others as required

##### REMEDIATE

* Plan remediation actions if required e.g. if timings are important
* Ensure monitoring is in place if required while implementing actions
* Implement remediation actions
* Ongoing monitoring for a period if required to confirm incident is fully remediated
* Document findings, actions and key decisions, and report to others as required.

##### RECOVER

* Continue with any non-critical investigation actions (e.g. historical activity) if required
* Restore/recover data or any other action required to return to, “BAU”
* Document final status and report to others as required
* Ensure all external reporting is complete where required (e.g. customers, regulators).

##### LESSONS LEARNED

* Invite all relevant parties to review (may require separate sessions)
* Review
	+ How the response went and possible improvements
	+ The incident and determine security improvements which may be required
* Document review and actions. Assign actions to relevant people/teams.

Appendix C – Forms

##### INCIDENT RECORD

This form is a simple template for recording key incident information – it can be used as the initial incident notification/record and used for updates or handovers.

**For large and complicated incidents it may also be worth mapping out the attack in a diagram and/or creating a timeline of events to understand all aspects of it and ensure nothing is missed.**

|  |  |
| --- | --- |
| Incident record |  |
| Incident Ref/title: | Start date: |
| Update date: | Author: |
| Incident still live? Yes/No |  |
| Incident summary: |

Affected systems/users (refer to separate spreadsheet/file if needed)

|  |  |  |  |
| --- | --- | --- | --- |
| machine name | ip address | username | purpose/function/role |
|  |  |  |  |
|  |  |  |  |

**Known indicators of compromise/signatures (refer to separate spreadsheet/file if needed)**

|  |  |  |
| --- | --- | --- |
| typE | name | notes |
|  |  |  |
|  |  |  |

|  |
| --- |
| current status |
| (What actions have been taken; what is in progress; what is known) |

|  |
| --- |
| next steps (any urgent actions/questions) |
| (Very important if being used as a handover) |

 **Actions (or refer to action tracker)**

|  |  |  |  |
| --- | --- | --- | --- |
| actions REf | action | assigned to | due date |
|  |  |  |  |
|  |  |  |  |

##### ACTION TRACKER

This simple template can be used to track the status of various actions:

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| ref | date created | action | priority | assignee | due date | status | notes |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |

##### LESSONS LEARNED

The following template can be used to capture lessons learned following the incident response.

|  |  |
| --- | --- |
| INCIDENT REF/TITLE: | MEETING DATE: |
| INCIDENT SUMMARY: | **ATTENDEES:** |

##### LESSONS LEARNED – INCIDENT

* How could the incident have been prevented? (Or should it have been?)
* How could the incident have been detected earlier?
* Are there security improvements that would assist with preventing or detecting this type of incident?

##### LESSONS LEARNED – INCIDENT HANDLING

* Could anything have been improved regarding the initial reporting/notification of the incident?
* Was the incident response plan (or any other plan) followed – why not/did it work?
* Were there issues with managing the incident – e.g. anything that could’ve been done differently?
* Were there any issues with investigation – e.g. missing data for analysis?
* Were there any issues with mitigation/containment/remediation?
* Were there any difficulties with full recovery of systems/data/BAU?
* Is there anything else which could have gone better?

##### ACTIONS

|  |  |  |  |
| --- | --- | --- | --- |
| actions REf | action | assigned to | due date |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |



Visit us at victorinsurance.com to learn more.

Visit us at victorinsuranceus.com to learn more.

Visit us at victorinsuranceus.com to learn more.

Visit us at victorinsuranceus.com to learn more.

© 2023 Victor Insurance Managers LLC
Victor Insurance Services LLC in MN | DBA in CA and NY: Victor Insurance Services | CA Ins. Lic. #0156109

This document is for illustrative purposes only and is not a contract. It is intended to provide a general overview of the program described. Please remember only the insurance policy can give actual terms, coverage, amounts, conditions and exclusions. Program availability and coverage are subject to individual underwriting criteria.

© 2022 Victor Insurance Managers Inc.

This document is for illustrative purposes only and is not a contract. It is intended to provide a general overview of the program described. Please remember only the insurance policy can give actual terms, coverage, amounts, conditions and exclusions. Program availability and coverage are subject to individual underwriting criteria.

© 2022 Victor Insurance Managers Inc.

This document is for illustrative purposes only and is not a contract. It is intended to provide a general overview of the program described. Please remember only the insurance policy can give actual terms, coverage, amounts, conditions and exclusions. Program availability and coverage are subject to individual underwriting criteria.

© 2022 Victor Insurance Managers Inc.