Cyber Incident Response Plan Template

Version:

Signed:

Version	Date	Author	Contributors.	Comments
1.0	May 2020	Amar Singh		Ready for Public Release

Copyright and Disclaimer

Attribution-NonCommercial-ShareAlike 4.0 International (CC BY-NC-SA 4.0)

This is a human-readable summary of (and not a substitute for) the license. Disclaimer.

You are free to:

Share — copy and redistribute the material in any medium or format

Adapt — remix, transform, and build upon the material

The licensor cannot revoke these freedoms as long as you follow the license terms.

Under the following terms:

Attribution — You must give appropriate credit, provide a link to the license, and indicate if changes were made. You may do so in any reasonable manner, but not in any way that suggests the licensor endorses you or your use.

NonCommercial — You may not use the material for commercial purposes.

ShareAlike — If you remix, transform, or build upon the material, you must distribute your contributions under the same license as the original.

No additional restrictions — You may not apply legal terms or technological measures that legally restrict others from doing anything the license permits.

[Pre-Reading]

How to Read and Use This Document

[You can delete this whole section titled Pre-Reading after reading it. Don't forget to print or save another copy for future reference. You can also delete any text in **[ ]** like this paragraph. Please feel free to change any text especially text in {change}].

The only thing we ask of you, please do not sell this template. You can use it in your own company.

To obtain maximum value from this document, please read this full section. However, please start by reading our blog (click here) on what should and should not be in a response plan. Please return to this document once you have read the blog.

Further Reading

In addition to the guidance in our various blogs, you can also enrol in our UK Government-certified training (more details are here). Furthermore, if you so wish, you should review and read the following

- ISO 27001:2013
- NIST'S Computer Security Incident Handling Guide SP-800-62r2
- NIST's Cyber Security Framework

NCSC-Certified Training

Our Cyber Incident Planning & Response (CIPR) course is NCSC-Certified. (More info) The NCSC or National Cyber Security Centre is an organisation of the United Kingdom Government that provides advice and support for the public and private sector in how to avoid computer security threats. Based in London, it became operational in October 2016, and its parent organisation is GCHQ.

What is a plan?

Condensed from various dictionaries, a plan is a list of actions to achieve one or more objectives. A plan can be as simple as 'ABC' or as complex as a combination of multiple *trigonometry* formulae with hundreds of pages.

We prefer easy-to-read and understandable plans. Importantly, the plan (or plans) must be easy to refer to during a crisis or emergency. Why? quite simply, that's when you really need to reference them.

We implore you NOT to fall for the 'complexity makes you sound knowledgeable' school of thought. This convoluted ideology produces entangled documents that look scholarly and are more suited for academia than practical real-life incidents.

Remember this saying - "Any darn fool can make something complex; it takes a genius to make something simple."

What is a Cyber Incident Response Plan (CIRP)?

In our opinion a CIR plan should achieve two things. A Cyber Incident Response Plan is what it says on the tin. A response plan. The plan should help an organisation respond and recover from a cyber-attack (and a cyber-crisis).

In a bit more detail, a cyber incident response plan should help you:

- During an incident so you know whom to call, who can authorise critical actions, who goes to the press, which third-party to call for forensics, the members of the crisis management team etc. This 'during an incident' is also known as the Golden Hour - something we cover in our UK Government NCSC-Certified Cyber Incident Planning & Response training here.
- After an incident, you should know what to say, how to manage and communicate with the press, where to turn for professional legal advice, specific post-incident tests to carry out etc. Our certified CIPR course covers these and other topics.

Our Cyber Incident Response Plans

Our advice is to keep your plans short and easy to comprehend. To align with our philosophy, the incident response plan template that you have downloaded is concise and easy to read and should help you in creating a plan that is specific to your business.

This is a template document but unlike the regular 'find-this-text' and 'replace-it-with-your-company-name' templates, this document is also designed to support, help and educate you in creating your own effective cyber response plan.

Oh, one more thing. The reality is that this type of a document is only going to be referenced during a cyber-attack or cyber-crisis.

Crisis Management App

A key and important step in successfully managing a crisis is that you MUST ensure you log all decisions and record all calls made during and after the crisis. Furthermore, to be able to rapidly respond to an incident, you need immediate (stress IMMEDIATE) access to key documentation (processes, procedures, playbooks, checklists, contact lists etc) so you can take the necessary actions, on time. In addition, you also need a secure chat feature where you can securely communicate with key stakeholders. Finally, you should be able to centrally manage all of this with one app.

One more thing. Rather than getting people to DIAL-IN, try to obtain a service that can DIAL OUT to the stakeholders.

Document Structure

1. It is our opinion that you should create a document that is easy to refer to. What does that mean? (See below) Please keep in mind that a document that you can't find in under a minute and/or that takes you ages to read is as useful as a chocolate teapot.

2. Digging deeper into this, if we told you, during an emergency phone call, to refer to **Section**: Document Structure, **Paragraph** 2.a.i - you would be able to do that straight away.

    a. **Metrics**: That's a policy and/or a strategic requirement. Yes, there should be a reminder and reference to metrics.

        i. **Forms**: We are not going to include forms in this template, but we will refer to them in this document.

What is NOT included in this template

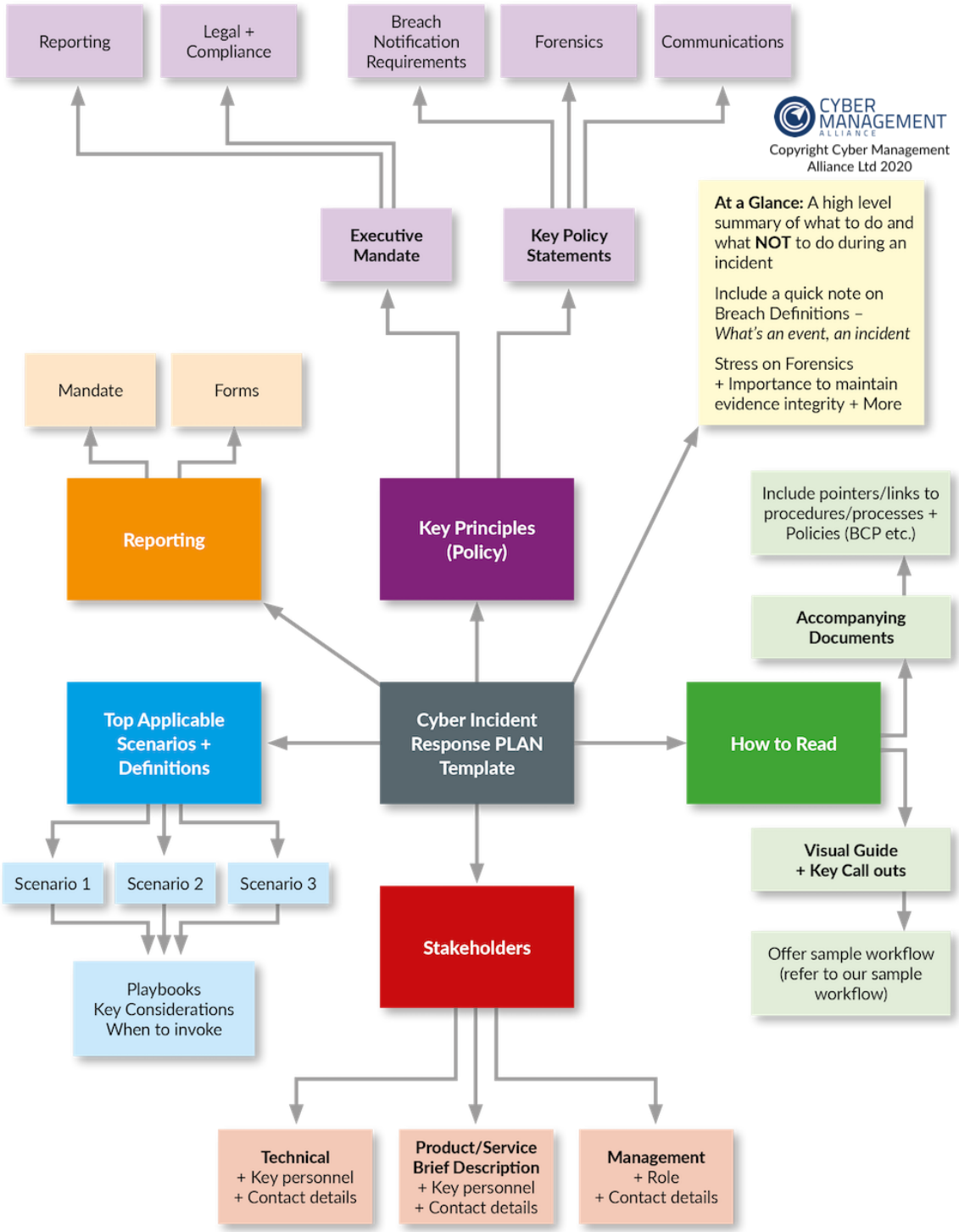
What we are not covering in this template includes the following:

- **Metrics**: That's a policy and/or a strategic requirement. Yes, there should be a reminder and reference to metrics.
- **Forms**: We are not going to include forms in this template, but we will refer to them in this document.
- Referring to the various standards and guidance (including NIST's Cyber Security Framework, NIST incident handling guide) we don't discuss 'preparation' as it's not relevant for a plan. This plan is about how you **respond** to and **recover** from a cyber-attack.

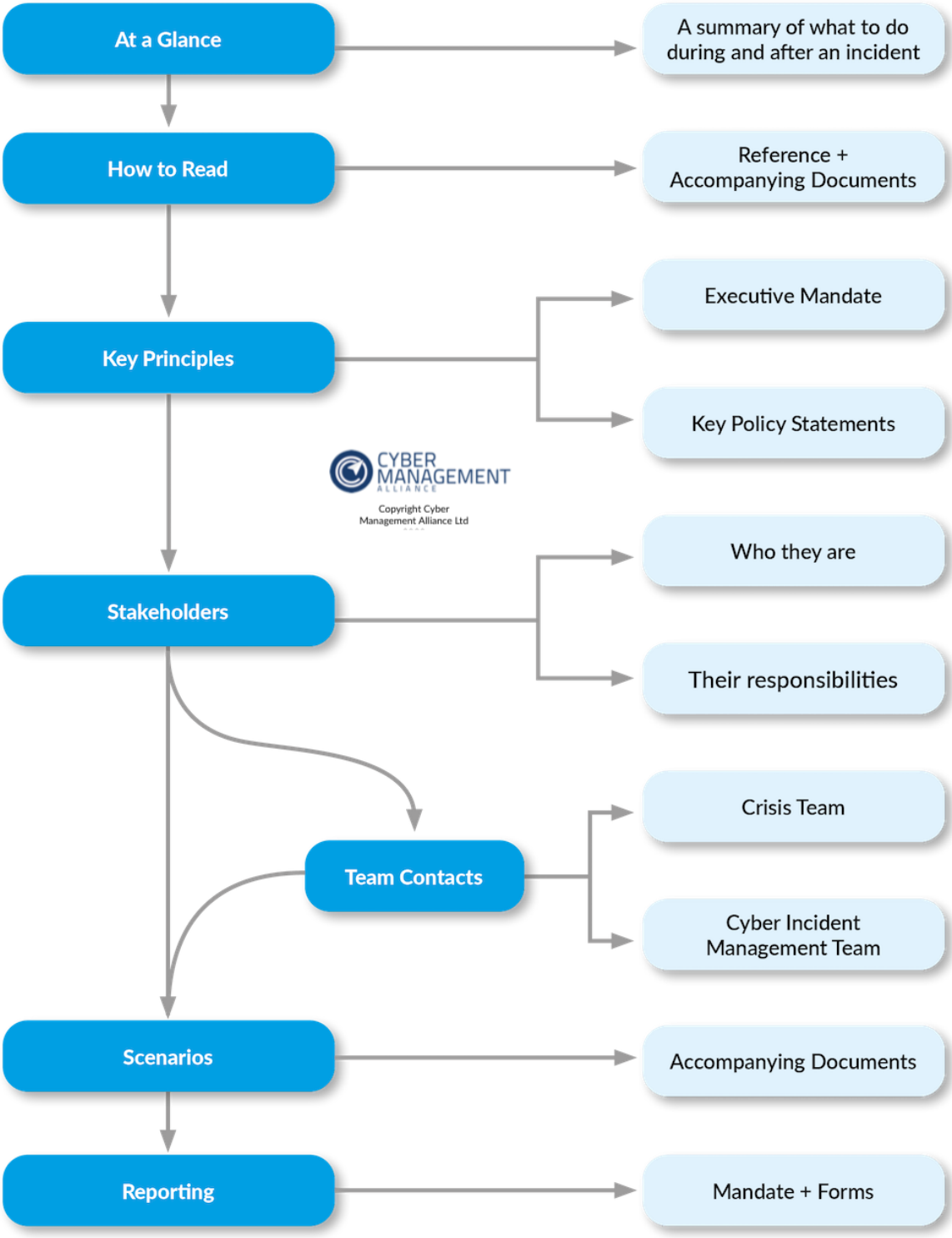
Remember, you can delete the Pre-Reading Section above.

This page is intentionally blank. Feel free to delete it.

.



Navigation



At a Glance

Review this checklist first

- **Internal** Crisis **Communications**: Do not use email. Use CM-Alliance's Crisis Management App. Avoid Emotions.
- **Evidence**: **Do NOT Delete**. **Do NOT Change.** Preserve & Protect.
- **Timelines & Audit:** LOG everything. Record ALL Decisions. Everyone creates their own timeline.
- **Ask what** data and/or critical systems have been compromised.
- **DO NOT Call it a BREACH:** Remember NOT to use data breach in your communications UNTIL you have all the facts.
- **FACTS**: Insist on factual answers to your questions. If someone isn't sure with their answer, get them to check again.
- **Communications External:** Make sure you read the comms policy. No one makes any statement to the public.
- **Communications Internal:** Keep staff informed with an accurate version of the event. Sooner or later, they will find out from external media.
- **Regulators**: Ensure you let the regulators know ONCE you have all the facts.
- **Playbooks**: Ensure you know your scenarios and the respective playbooks.
- **Takedown**: Issue immediate take-down notices to websites (like Twitter, LinkedIn, pastebin etc) that may be used to expose your data.
- **Taxonomy**: Use the same vocabulary across teams when describing attacks and when communicating.
- **Crisis Management APP:** Use the CM-Alliance crisis management app for convening conference calls and accessing documents and initial checklists

Credentials

Please note that credentials to all critical systems (1) have two-factor authentication enabled and (2) are ONLY accessible via the Password Vault.

Break-Glass procedures are here and must only be invoked during an emergency. Remember to document everything.

Emergency & Change Control

There are established change control procedures for regular changes and for emergencies. If, during exceptional circumstances, where you are unable to follow the procedures, you must make an informed decision about your actions. Remember to document everything. An audio timeline of your decisions, the context and your actions are acceptable.

Evidence, Forensics & Timelines

It is mandatory for all those involved in all phases of an incident to ensure the collection and preservation of the integrity of the evidence.

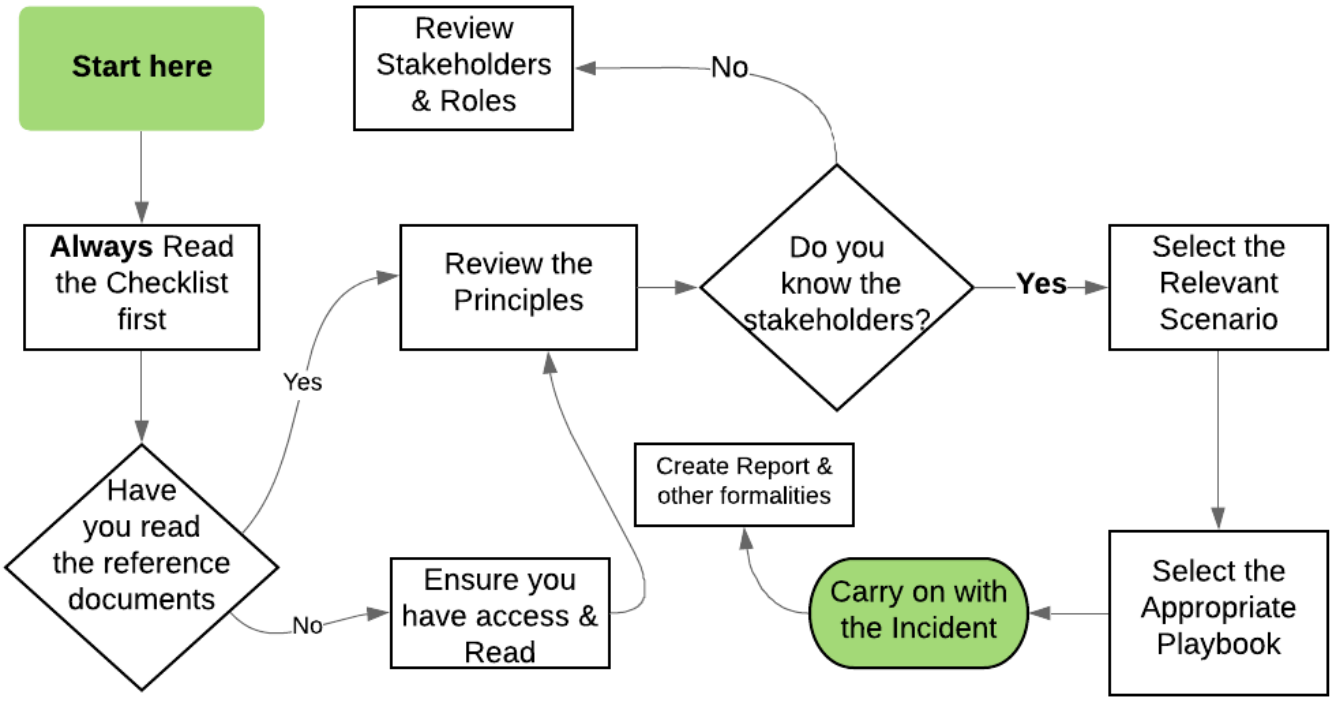
Own up

To err is human. If you make a mistake during or immediately after an incident it’s ok to admit it and own up to the action(s) immediately.

How to Read

In summary (refer also to the image):

- Read the Checklist in the 'At a Glance' section.
- Ensure you know where the key documents are and that you have access to them.
- You should ensure you understand the Key Principles set out by the Executive.
- It's always very useful to know the key stakeholders and teams that are part of the incident response, incident management and the CRISIS management team.
- After this, you need to figure out the closest applicable scenario and invoke the playbook(s) for that scenario.
- Don't forget, record everything so you can create post-incident reports and timelines.



Accompanying Documents

This table lists documents that are related to this document. Ensure you have access to them before an incident.

Name of Document	Location	Notes
Playbook Repository	Click here	This should be the first place you look for playbooks. These playbooks should have contacts for 3rd parties and specialists retained for specific systems.
Stakeholders	Click here.	All stakeholders and contact details are here.
Crisis Management App	Click here	If you have NOT already, ensure you download and install the CM-Alliance crisis management app.
Forensics, Privileged Users & Other policies	Click here	Repository of the latest & approved policies.
BREAK Glass	Click here	Important: This procedure should ONLY be implemented in the most critical and exceptional cases.
Critical Systems	Click here	This link takes you to details of the critical systems their owners and other critical information about them.

Key Principles

At {Cyber Management Alliance Ltd} the following are executive mandates that must be followed

1. **Forensics & Evidence Integrity:** You MUST store and protect from ANY change (authorised or unauthorised), all evidence before, during and after an incident. Tampering with evidence is illegal and a serious breach of your employment contract.

2. **Transparency**: As an organisation we MUST maintain maximum transparency with our clients, regulators and staff. To do this, we must be able to rely fully on the audit trail the log data we are collecting.

3. **Breach Notification:** You must NOT label any event/incident a data breach until you have all the available evidence and facts.

4. **Need to Know**: Until you are told otherwise, you MUST use the company approved Crisis Management App for Crisis related activities (comms, chat, etc)

5. **Privacy**: Maintaining the Privacy of Staff and our Customers is of utmost importance and we MUST do everything to ensure we do NOT impact our data subjects as a result of our actions during and after an incident.

6. **Business Operations**: To ensure the business remains profitable, we must ensure ZERO to Minimal disruption during and after an incident.

7. **Health & Safety**: Our staff are our most important asset. We must ensure we protect our staff's mental and general health. Especially relevant during and after a cyber-attack.

8. **Cyber Resilience**: We expect maximum protection from cyber-attacks. However, we understand that 100% security is NOT possible. We must strive for rapid detection and rapid response.

9. **Physical Copies**: Ensure you print and keep a copy of this plan, the contact details and other key documents. You **must safely secure these** documents. Do not carry these printed documents around.

Critical Apps & Systems

This list is regularly updated, and MAY not include all the critical systems. Always ask if you are not sure.

- HR system and Database
- Core CRM system hosted in the Cloud.
- Database ABC
- Core RJA system

To access details of the critical systems, their owners and more, see the accompanying documents section.

Communications

All internal and external communications MUST be approved by the {Corporate PR department.} They are contactable by email and 24x7 by phone {+44 208 123 4568}. Only use this phone if you need immediate and URGENT assistance and permission.

Templates: Most scenarios have a communications template that you can use. It makes it easier if you review the template, fill it in and then engage the {PR department.}

Teams & Stakeholders

There are 5 key teams listed below.

- The Response Team: The CSIRT Team or the Cybersecurity Incident Response Team is responsible for a range of tasks including but not limited to fix, reconfigure, rebuild and restore.
- The Cyber Incident Management Team: The Cyber Incident Management team is a smaller group of stakeholders that oversees the management of all cyber incidents.
- The Crisis Management Team: Only revoked during a crisis (should be kept informed of major incidents) this team will have a representative from the Cyber Incident Management team.
- Product & System Owners: Each of our products and critical systems has their own owners. These resources know their systems and products and are best placed to advice on business impact.
- Third Parties, Vendors & Partners: Ensure you check for retained specialists during the incident. Reach out to specific vendors where necessary.

From the RACI model (Responsible, Accountable, Consulted & Informed)

- Keep the Crisis Management team informed.
- The CSIR Team are most responsible for response and recovery.
- The Incident Management Team is consulted and accountable.
- Product and systems owners should be informed (and where possible, seek their authorisation) when making changes to their system(s).

Contacting Stakeholders

Use our CM-Alliance Crisis Management App to access the contact details of the various stakeholder groups. This list contains sensitive confidential information and it is your responsibility to maintain this confidentiality.

- Unless absolutely necessary **DO NOT directly contact stakeholders**. Instead use the App's Crisis management Calling Tool that will dial the necessary resources. This will ensure all calls are RECORDED.
- Avoid corporate CHAT apps for discussing anything related to an incident.

Scenarios

This section is about scenarios. Pick the scenario that closely resembles the attack you are facing. Regardless of scenario, please note:

Human Error: Remember, misconfiguration and other human errors are often a leading root cause of a data-breach.

Forensics & **Evidence**: Ensure you keep this topic on the top of your mind.

Detect & **Analyse**: Ensure you review the common attack vectors (email, phishing, web etc) when carrying out your analysis and investigations of the incident. **Triage**: Correct and accurate triage is important. Keep checking if triage has been done and if it has been done correctly.

Containment: You must endeavour to contain the attack as quickly as possible. **Speed is of the essence**. (malware, ransomware, or whatever the attack)

Eradicate: Your next focus must be to eradicate the problem. Keep in mind that modern attacks don't just INFECT one device. Ensure you seek for a full cleanse.

Look Back: Remember to ask and seek context about an incident. Ask that IT reviews any previous incidents that are linked.

Scenario	Playbook(s)	Comments
Malware (generic)	Click here	Use this for generic malwares NOT highlighted by threat intel feeds.
Phishing (generic)	Click here	Remember to check ALL STAFF inboxes for the malicious link/attachment.

Scenario	Playbook(s)	Comments
Denial of Service - Website	Click here	Check with vendor to ensure no further compromises.
Denial of Service - Internal	Click here	Attacker could be in the network.
Malware Incident - HR systems	Click here Click here	Remember to check for rootkits.
GDPR Data-Breach: Client	Click here	Do not take actions that further compromise client privacy.
GDPR Data-Breach: Staff	Click here	Do not take actions that further compromise staff privacy.
Core CRM - Data Breach	Click here	Remember to contact the 3rd party.