Crisis Management *Playbook*

Components of effective crisis management

WHAT DO YOU NEED?

This playbook is the third instalment in our series on managing cybersecurity events, completing the progression from notification management to incident management and now crisis management. Where an incident can often be resolved through established technical and operational response mechanisms, a crisis extends further in scope, severity, and impact. True crises can disrupt essential business functions, often draw the attention of employees, customers, regulators, and the media, and demand difficult decisions from executive leaders.

In this guide, you will find practical, actionable advice for managing such high-pressure situations. It dives into the most important components of effective crisis management, including:

Preparation of crisis management processes and procedures

Coordination of key stakeholders across technical, business and legal roles

Effective **communication** with incomplete information and under scrutiny

The ability to **recover** and build **resilience** for the future

Breached? Call our emergency hotline: +31 70 222 0000

Crisis management essentials

TURNING UNCERTAINTY INTO STRUCTURE

A cyber crisis is not a matter of *if* anymore, it is a matter of *when*. The variety, speed and sophistication of cyber threats mean that even organizations with robust defenses can find themselves blindsided by a critical incident. Without preparation, decision-making becomes reactive, fragmented, and error-prone. In the heat of a crisis, delays often cost money, reputation, and trust.

An effective crisis management framework turns uncertainty into structured action. When roles are clear, priorities agreed upon, and communication pathways established, a team can respond almost instinctively; reducing harm, preserving business continuity, and restoring normal operations faster. Preparation also ensures alignment across legal, technical, and business domains, which is essential for compliance, stakeholder confidence, and operational resilience.

The goal of this playbook is to ensure that when a cyber crisis strikes, your organization executes a well-practiced plan, not a desperate improvisation, so that you and your team can keep calm, and trust the process.

What not to do

Fair warning: even with preparation, it's easy to make missteps under pressure. The wrong actions can amplify the damage of a cyber crisis rather than contain it. Before we unpack what you should do, it's worth being clear about what you should avoid.

Do not:

- Start restoring before securing investigation material.
- Improvise untested workarounds.
- Underestimate the power of effective and efficient crisis communication, internal and external.
- Be a to-do hoarder.

Checklist(s)

KEY TASKS FOR CRISIS READINESS

To make your life easier, lists are the way to go. On the next page, you will find a list of the things you need to do to ensure that there is a crisis management process in place. The table indicates the identifier, a description of the action, whether it has been implemented (including date/time), and room for comments. While it's recommended to implement every single task item, you may not be able to do so due to time constraints or conflicting business priorities. *Table 1* is therefore a reminder and to-do list to check if each individual component has been implemented or will be implemented in the future.

Depending on your current level of incident readiness, implementing all the actions listed in *Table 1* might be a time consuming endeavour. If this feels unachievable, it's best to focus on the basics in the short term. At an absolute minimum, consider implementing the following action items.

Essential action items ✅

- Create contact lists of key stakeholders (internal service owners, executives, Legal, Comms, HR, BCP, IT ops, external IR/forensics, PR, cloud providers, regulators, law enforcement, cyber insurance) with primary/deputy, mobile, and out-of-band methods. Conduct quarterly verification with a timestamp to ensure these details remain up-to-date.
- Map service & asset owners to systems, data classifications, RTO/RPO, runbooks, and dependencies.
- Ensure you have access and/or credentials vault for emergency use (break-glass), with dual control and audit.
- Create an offline pack - export critical registers to an encrypted USB and create a sealed print copy.

#	Action	Finish date	Comments
CM01	Create a crisis management process, process owner, and an overview of the required roles in the crisis management team.		
CM02	Create a list of contacts per role, at least two.		
CM03	Create a decision tree to determine which roles are required for which type of incident priority and who is in charge.		
CM04	Create a guideline that prioritizes by type of incident (battlecards & playbooks).		
CM05	Create a communication matrix and determine the frequency per incident priority.		
CM06	Make a list of digital emergency response companies.		
CM07	Create an out-of-band communication channel.		
CM08	Create a risk register template.		
CM09	Maintain stakeholder map: regulators/supervisory authorities, law enforcement, customers, investors, cyber insurance, critical suppliers. (Consult Legal for jurisdiction-specific obligations such as EU data-protection notifications.)		
CM10	Arrange mandate/budgets before a P1-P3 incident occurs.		
CM11	Practice the entire incident management process on a regular basis.		
CM12	Create a big-bang playbook.		
CM13	Create holding statement(s) template(s).		

Table 1 - Crisis management checklist

Escalation managers

WHO TRIGGERS & LEADS ESCALATION?

Once an incident is considered high-priority (priority 1 or 2), the situation could be escalated to an escalation manager. The escalation manager can reassess the incident and kickstart crisis management. The actual escalation manager may differ per asset in the organization. If your organization is smaller, it could also be the same person for multiple areas of expertise. Furthermore, a backup will have to be defined for each escalation manager and, where possible (as people go on holiday, get sick, or are stuck in other matters), a third contact should be provided.

Note: *This is most relevant to large companies with operations across multiple locations/countries. It is unlikely that companies with 500 employees or less will have a dedicated escalation manager. Nevertheless it's always good to appoint someone to this role.*

Domain	Name	Contact details	Backup escalation manager
Network environment			
Office 365			
Azure			
Backups			

Table 2 - Escalation managers

Communication channels

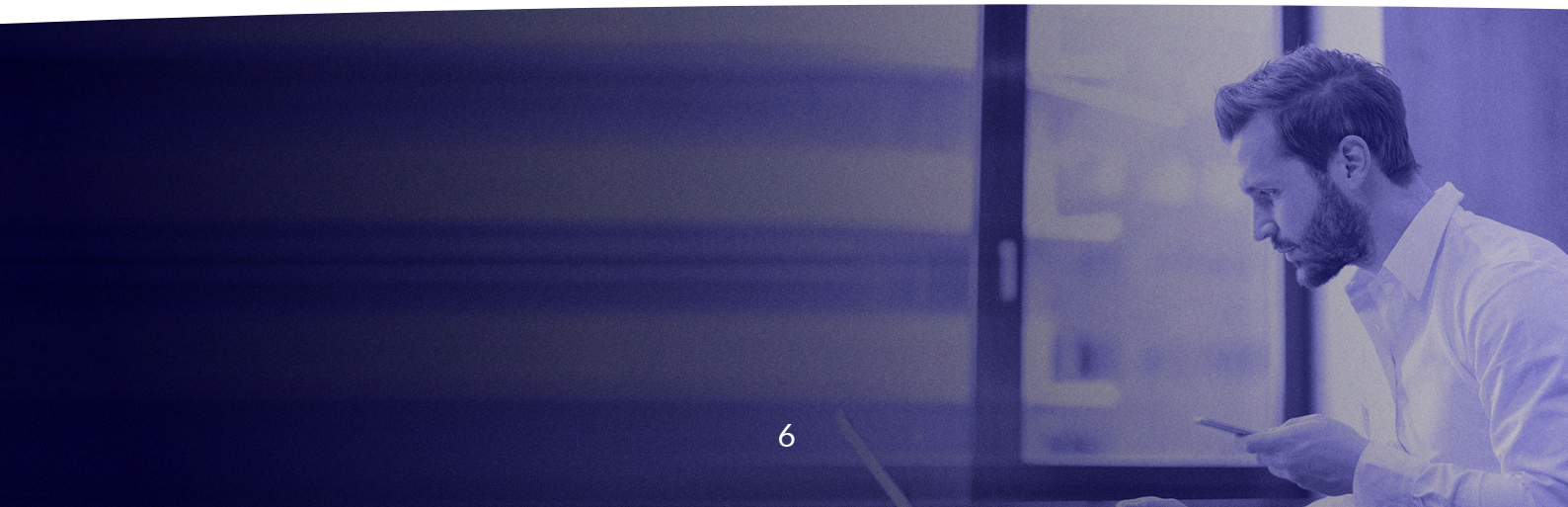
FOR INTERNAL USE

Communication is essential during crisis management. It is recommended to have several communication channels in place, including a backup channel in case primary systems fail - for example, due to an outage or a ransomware attack. These channels should meet certain requirements: the ability to add or remove participants quickly to avoid overcrowding, and options for automatic message deletion after a set period to maintain security and limit unnecessary data retention. Preferably, these channels exist prior to an incident, so as not to waste time when one occurs.

Communication channel	Name of the channel	Purpose of the channel
Microsoft Teams		Main communication channel for chat and storage of documents, research results, etc.
WhatsApp / Signal		Back up the communication channel when Microsoft Teams is unavailable.
Email group		Main communication channel for other communications, such as emailing external parties and sharing with the crisis management team.

Table 3 - Communication channels for crisis management

Note: *Use the empty rows to fill in additional communication channels specific to your own organization.*



Crisis Management Team (CMT)

CORE ROLES & RESPONSIBILITIES

Once an escalation manager - or someone else who is eligible - labels the situation a crisis and those who need to know are informed following the proper channels, it is time to engage the crisis team. In *Table 4*, an overview can be found of the roles, names and contact details that should be part of the crisis team. Please note that it might not be necessary to involve all roles from the start of the crisis. It is, however, critical that all roles are assigned, and can be included when required. A multidisciplinary team ensures comprehensive coverage. Involvement depends on crisis classification - not every incident needs the full roster. Ultimately, the Crisis Manager decides who to engage.

Role	Name	Contact info	Backup contact
Crisis manager *Overall coordination, authority to approve major actions.*			
Technical lead *Root cause analysis, containment, recovery guidance.*			
Legal counsel *Regulatory obligations, liability mitigation, evidence handling.*			
HR representative *Internal staff communications, sensitive personnel issues.*			
Business continuity lead *Impact on operations, prioritization of business services.*			
Communications lead *Media handling, stakeholder messaging, social media monitoring.*			
Executive sponsor *Strategic oversight, executive decision authority.*			
External advisors *Incident Response (IR) firms, forensic analysts, PR agencies.*			

Table 4 - Overview of members of the crisis management team

Effective CMT meetings

A GUIDE FOR STRUCTURED DISCUSSIONS

Why streamline your CMT meetings?
In a fast-moving cyber crisis, unstructured meetings become gravity wells for time: people chase technical rabbit holes, repeat status, or argue priorities while the clock keeps ticking. Streamlining the CMT rhythm preserves tempo, reduces cognitive overload, and turns partial information into timely, defensible decisions. A crisp format also keeps legal, communications, and business continuity aligned with the technical plan. We recommend using the SADIE (or BOBOC)[1]framework to help with this.

How SADIE or 'BOBOC' works (5–15 minutes), is explained in the image below. Everyone at the table provides their input in all five rounds, starting with situational awareness. Once everyone has provided their input regarding objective facts and information, you go round the table again to determine what this means. Based on the interpretation of facts, you come to a decision. Then it is time to determine who is going to execute that decision, and finally, in the last round you decide how you will evaluate and monitor for the outcomes.

Operating rules — do and do not.
Run BOBOC in your CMT with a timebox (usually 5–15 minutes) and a small quorum:

- Crisis Manager (chair)
- Technical Lead
- Legal
- Communications
- BCP/Operations
- others only if essential

Share a single **Common Operating Picture** on screen; no slide decks. Require a **note-taker** to capture decisions, actions, and assumptions with review times.

Park unresolved deep-dive items into the relevant workstream ("parking lot") with named owners and return-times.

SADIE a.k.a 'BOBOC'

1. **Situational Awareness**

Gather objective facts and information to build a clear understanding of the situation.

2. Assessment & Analyse

Analyse and interpret the information to assess risks, causes and priorities.

3. Decision making

Choose a justified and appropriate course of action based on the analysis.

4. Implementation / Follow up

Execute the decision with clear coordination and actions.

5. Evaluation / monitoring

Evaluate the outcomes and adjust as necessary based on results.

[1] SADIE/BOBOC: Beeldvorming (Situation Assessment); Oordeelsvorming (Judgement/Analysis); Besluitvorming (Decision-Making); Opdracht (Assignment); Controle (Control).

Things to do ✅	Things to avoid 🚨
• Arrive with pre-reads • State confidence levels • Make reversible decisions quickly and flag which ones need re-validation • End with a clear external/internal message and an exact time for the next checkpoint • Call on roles in the same order each time to build cadence • Re-classify severity only with stated evidence and rationale	• Turning the meeting into a technical troubleshooting session • Debating attribution or root cause before containment • Allowing decisions to go unlogged • Promising timelines you cannot control

Priorities & Stakeholders

MANAGING INTERESTS DURING A CRISIS

Now that you have established fluent communication and meeting processes, you still need to determine the tone of voice of your messaging, and the priorities for your actions. During a crisis, you have to manage different types of stakeholders. Throughout the crisis, the stakeholders that need to be managed differ, which is why it is important to constantly re-evaluate which stakeholders need to be managed, but also to determine the corresponding course of action. *Figure 1* provides an overview of the different stakeholder groups, which are defined as follows:

- **[Controllers]:** entities that ensure that a company complies with standards when dealing with cyber incidents;
- **[Supporters]:** entities that help a business respond to a cyberattack;
- **[Value chain]:** entities that are at the core of the business;
- **[Adversaries and external stakeholders]:** entities that (may) work against a company.

Figure 1 - Stakeholder management

Stakeholder management

- During an incident, you have to deal with a lot of stakeholders. The amount of stakeholders and the actual stakeholders themselves differ per phase of the investigation.
- The stakeholders influence, to a large extent, your priorities during an incident.
- Do note that stakeholder management is not a static thing, it is continuously evolving during the incident.

Crisis management matrix

PRIORITY-BASED RESPONSE

Depending on the priority and severity of the incident, certain aspects may differ, including: the frequency of communication updates, whether there is a dedicated war room, reporting lines, and budget approval ceilings.

- **[Update frequency]:** Update frequency describes how often crisis management is updated by different stakeholders in the organization about the status of the incident. This can be an update from the external security partner about the investigation, an update regarding communication about the latest press release, or, for example, a HR update about the organizational impact and communication related to it. Please note that setting an update interval should be done prudently. Requiring an update too often will not leave enough time to actually do the work. Too little will result in a loss of control over the incident;

- **[War-room]:** The higher the priority of an incident, the more important it is to have a dedicated war room available where the members of the crisis management team can focus on the incident and communicate directly with each other. Preferably, this is a physical space where the crisis management team is gathered, but if this is not possible (due to an intercontinental crisis) a combination of a physical space/virtual space may be the best solution;

- **[Reporting lines]:** Reporting lines are particularly important and can vary by priority of an incident. If it is a lower priority, it is sufficient to update an escalation manager on the status of the incident, if it is a high priority (i.e. P1 or P2), C-level should be involved;

- **[Budget approval ceiling]:** During an incident, you want to avoid a lengthy budget approval process to hire external expertise. Therefore, it is recommended to have budget approval ceilings for the crisis management team, allowing them to sign incident-related proposals without relying too much on an approval chain or the involvement of tenders, for example.

Table 5 contains the crisis management matrix, including the frequency of the communication, the War-room, reporting lines, and budget approval cap per incident priority level.

Part	P1	P2
Update frequency	Per ___ hour(s)	Daily
War room	Yes/ No	Yes / No
Reporting line	CEO	CFO, CIO, or department manager
Budget approval ceiling	€_____/week	€_____/week

Table 5 - Crisis management matrix

External support

TRUSTED PARTNERS

Depending on the severity and (potential) impact of the incident, external assistance may be required. *Table 6* provides an overview of possible external parties which can be contacted.

Organization	Contact	Contact details	Type of company
Hunt & Hackett		+31 70 222 0000	CERT support
Accountant			
External IT			
PR/Communications			

Table 6 - External team contact details

Holding statement (external)

A CLEAR, FACTUAL RESPONSE

A holding statement stabilizes expectations when facts are still emerging. It signals that the crisis plan is active, establishes a cadence for updates, and buys time for investigation while minimizing legal and reputational risks from speculation or inconsistent messaging. You can prepare this or more versions prior to an incident.

What does it look like?
Keep it short (about 75–150 words), strictly factual, and empathetic. Use plain language, state what you know with confidence, and tell audiences exactly when and where the next update will appear. Offer a practical next step (support channel, workaround) and have Legal, the Communications Lead, and the Executive Sponsor review it before release.

What to avoid?
Avoid overpromising or downplaying. Do not speculate on root cause, attacker identity, or impact totals, and avoid categorical claims (e.g., “no data accessed”) unless evidenced. Skip vague platitudes unless paired with concrete actions, and never include technical indicators, internal ticket numbers, or privileged legal strategy.

Structure it as: a precise acknowledgement of the issue; concrete actions taken (activation, specialists engaged); current impact if safe to share; guidance for recipients; and the update cadence with a single public source of truth. An example can be found below.

> *We are investigating a cybersecurity incident affecting [systems/services]. Upon detection at [time, timezone], we activated our crisis response, engaged specialized partners, and are working to contain the issue. We will provide updates at [cadence/location]. If you have questions, contact [contact].*

How to reach people?
First of all, determine your audience. Who do you want to reach, and where does this group look for information. Is this on socials, the website, or anywhere else? Publish simultaneously on the website/status page, customer portal, and press room, and push to mailing lists and support teams.

Employee FAQ

CONSISTENT GUIDANCE FOR STAFF

An employee FAQ gives everyone one place to find clear, consistent guidance during a crisis. It reduces noise to IT/SOC/HR, discourages risky improvisation, and keeps messaging legally safe and aligned.

Write it in a direct, empathetic tone. Start with what happened and what is currently impacted (or when/where the next update will be posted). Tell people whether to keep working and how to use approved workarounds. Clarify that personal devices and personal email are not permitted for company data. Explain that password/MFA changes will be requested only when needed and through a named channel. Show how to report suspicious emails, chats, or calls via the phishing button or ticketing link.

Set expectations on communication: who may speak externally (designated spokespeople only), how often updates will come, and which channels to watch (e.g., intranet status page with follow-up email/Teams summaries). Tell people where they can pose their questions or share concerns. Commit to updating the FAQ as new facts emerge.

Distribute the FAQ via a single intranet incident page (source of truth), pinned in Teams/Slack and linked from an intranet banner and the VPN/login portal. After major updates, send an all-staff summary that links back to the page. Provide manager talking points for team stand-ups, consider a short video message from the Crisis Manager, and have SMS/phone-tree fallbacks if email/IM are degraded. Version the FAQ with timestamps and an owner, and retire outdated guidance promptly.

Example questions:

1. What happened?
2. What should I do?
3. What not to do? (phishing, sharing screenshots)
4. How we will update you?
5. What are the relevant support channels?

Conclusion

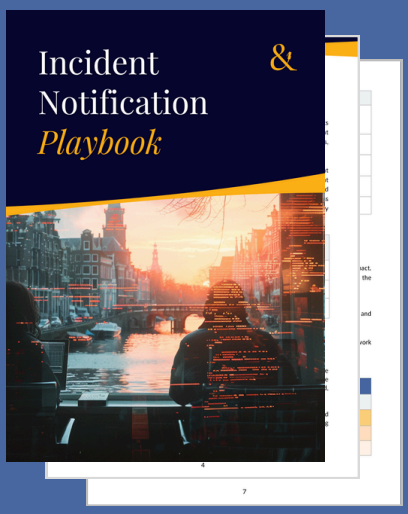
CRISIS MANAGED

Crisis management is where preparation and coordination are truly put to the test. This playbook is the third in our *Incident Response* series, which aims to provide practical guidance and tools to handle cybersecurity disruptions at every stage - from initial notification through to crisis response.

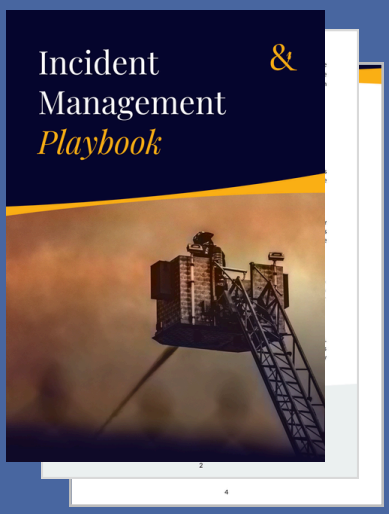
Just remember: reading about what you *should do* is one thing; actually *doing* it is another. Don't forget to translate your learnings into hands-on practice. The more your team trains together, the more instinctive and coordinated your response will be when a real crisis hits. If you're considering working with an external security partner, look for one who will support this through **fire drills**, **tabletop exercises**, and other **practical sessions** to help you build a well-oiled response machine.

At Hunt & Hackett, our **Incident Response Retainer (IRR)** does exactly that, combining 24/7 SLA-backed support, an innovative cloud-based IR lab, and a thorough incident readiness approach to help organizations adeptly navigate cyber incidents and build resilience over time. We also like to share our learnings with the general public, offering (free) crisis workshops and incident readiness tabletops through our **CyberConnect series**. No matter where you are on your incident response journey, the key is to keep building, practicing, and refining — because readiness is never truly finished.

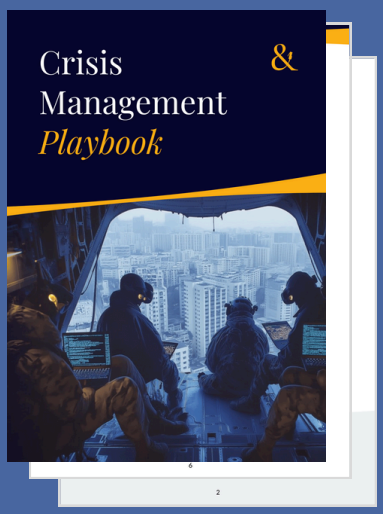
Part 1



Part 2



Part 3



HUNT & HACKETT

Hunt & Hackett was founded in 2020 by Ronald Prins (co-founder Fox-IT) and Jurjen Harskamp (former executive Fox-IT). Hunt & Hackett is a privately-owned Dutch company based in The Hague, the Netherlands, and governed by stringent national and European standards on privacy and security. A fast-growing team of highly experienced security specialists and upcoming talents is protecting customers against their sector- and organisation-specific threat landscape, including the most sophisticated APTs.

Want to know more?

Join one of our CyberConnect roundtables

Questions or want to get in touch?

+31 70 22 0000

info@huntandhackett.com

www.huntandhackett.com