



**SMEs Edition**



# CYBER CRISIS COMMUNICATION

**BE PREPARED REDUCE THE IMPACT**

# DISCLAIMER

Copyright © European Union Agency for Cybersecurity (ENISA), 2024

This document and information contained in this document may be excerpted, copied, printed, republished, made available to the public by wire or wireless means and/or otherwise provided to third parties only under the condition that the source and copyright owner is clearly stated as follows:

“Source: ENISA Cyber Crisis Communication Toolbox, Copyright © European Union Agency for Cybersecurity (ENISA), 2024”. If you do republish we would be grateful if you link back to the ENISA website [www.enisa.europa.eu](http://www.enisa.europa.eu). No part of this document, including any part of the information contained therein, in whichever format, whether digital or otherwise, may be altered, edited or changed without prior express and written permission of the European Union Agency for Cybersecurity (ENISA), to be requested via email to “[access-documents@enisa.europa.eu](mailto:access-documents@enisa.europa.eu)”, clearly stating the element (document and/or information) and term of use requested.

The present document is being distributed without warranty of any kind, either express or implied in relation to its content and/or use and the views expressed herein do not necessarily represent the opinions or the stated policy of ENISA. To the extent permitted by the applicable law, ENISA shall not be liable for any damages arising from the content and use of the present document.



# STEPS OVERVIEW



## ● Plan

1. Risk, situation, target of communication assessment
2. Clear target, messages, roles and communication protocols

## ● Execute the Plan

1. How to communicate about a cyber crisis
2. How to manage media inquiries
3. How to test the plan

## ● Monitor and Evaluate

1. What to measure and monitor & how
2. How to draw lessons learnt from internal or other players' in your sector cyber crisis experiences

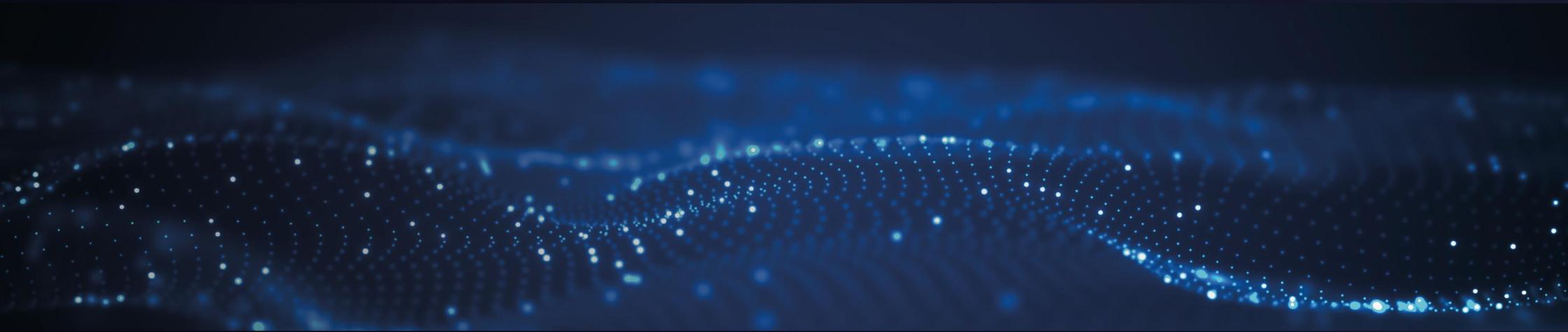
# BASIC PRINCIPLES



1. **Do conduct regular risk assessments** to identify potential vulnerabilities and threats.
2. **Do establish clear communication protocols and roles.**
3. **Do communicate timely, clearly and transparently** with stakeholders, incl. customers, partners, employees.
4. **Do adapt the granularity, focus and channels** for communication for each target audience.
5. **Do ask for help** and expert advise if in doubt.
6. **Do use the crisis experience** to improve your organisation, resilience, procedures.



7. **Don't panic.** Use a set of tools, procedures, good examples developed in calm times.
8. **Don't cover, ignore or omit** real cybersecurity incidents.
9. **Don't delay in responding** to a cyber crisis or fail to communicate with stakeholders in a timely and transparent manner.
10. **Don't rely solely on technology** to protect your organisation from cyber threats - employee training and incident response planning are also critical components of a comprehensive cybersecurity strategy.



# PLAN

# TASK #1 RISK ANALYSIS

Area	Question	Answer	Note	Guide	
Criticality	Do you operate in critical sectors?	Yes		The more critical and sensitive data you process, the bigger the likelihood and impact of potential cyber crisis. Adequate level of planning and testing of cyber crisis communication is required. In addition, make sure such processes, systems and data is subject to strict security measures and monitoring (incl. automated alerts).	
	Do you supply critical processes or infrastructure	No			
Sensitivity	Do you store, collect, or process sensitive data?				
	Do you process data of political or economic importance for a country?				
Regulatory	Do you have compliance requirements linked to cyber incident communication or crisis plan?				Ensure regulatory requirements are detailed and clearly integrated in your cyber crisis communication plan. Special attention to be paid on who (responsibility within the organisation), when (deadline), how (template, mandatory fields, flags to allow for identification of relevant incidents) and what (criticality, impact, type) of incidents need to be notified to the regulator.
Impact	Is a damage to people health, life or well being possible?				Same as criticality, the higher the impact the more robust and detailed planning and testing of cyber crisis communication is required. Adequate measures to prevent the damage and severe impact to internal and external stakeholders and your own business are to be planned, implemented, and tested.
	How many people would be impacted in the case of a cybersecurity crisis?				
	Could you go out of business in the case of a cyber crisis?				
Reputation	How important is the public perception, customer trust, and business partnerships for our business?			Different company types (eg. public entities) and stages of development (startup, fundraising, under M&A for instance) would have different sensitivity to public perception. Sensitive moments would require better preparedness and resources for possible cyber crisis communication, due to anticipated high public, shareholders, investors, and media interest. As such, possible reputation damage from a cyber crisis should be evaluated and adequately addressed in the cyber crisis communication plan.	
Lessons learnt	Do you have access to knowledge on the impact, best practices and lessons learned from past cyber crises in your own company or sector of activity?			Never miss an opportunity to learn from a crisis. What companies in your sector have done well or not so well to respond to cyber crises? What have your own testing or crisis handling experience taught you? Can you use the crisis to better focus protection priorities? Use this criteria as an option to highlight key lessons learnt. If no knowledge is available, you may need to run and test a few procedures before finalising your cyber crisis communication plan V1, based on lessons learnt.	

# TASK #2 DEFINE OBJECTIVES

- ① **Protect the organisation's reputation**
- ② **Provide timely and accurate information**
- ③ **Inform customers or stakeholders (employees, suppliers, partners, regulators)**

Outline how and when each stakeholder group will be notified of the incident, and what information will be shared to demonstrate transparency, empathy, and a proactive approach to resolving the cyber incident.
- ④ **Mitigate the impact of the crisis**

Includes strategies for mitigating financial impacts, such as developing contingency plans, prioritising business-critical functions.

# TASK #2 DEFINE OBJECTIVES

- 5 Manage media relations**

Provide accurate and timely information to the media, coordinate media interactions, and proactively manage the organisation's public image through effective media engagement.
- 6 Coordinate crisis response efforts**

Define how different departments within the organisation will collaborate, and how external partners and vendors will be involved in the response effort.
- 7 Learn from the crisis**

A crisis is an opportunity to learn and improve your cyber resilience. The plan could outline processes for gathering feedback, conducting post-incident assessments, and using the insights gained to refine the communication strategies and enhance future crisis response capabilities.
- 8 Prepare for the worst, hope for the best**

Prepare for a complete blackout scenario, where all systems are offline/inaccessible. Ensure separate copy of the crisis comms plan, contacts and communication mean should be envisaged (offline, on paper, at different location).

# TASK #3 ASSESS THE SITUATION

## Define the Nature and Extent of Incidents

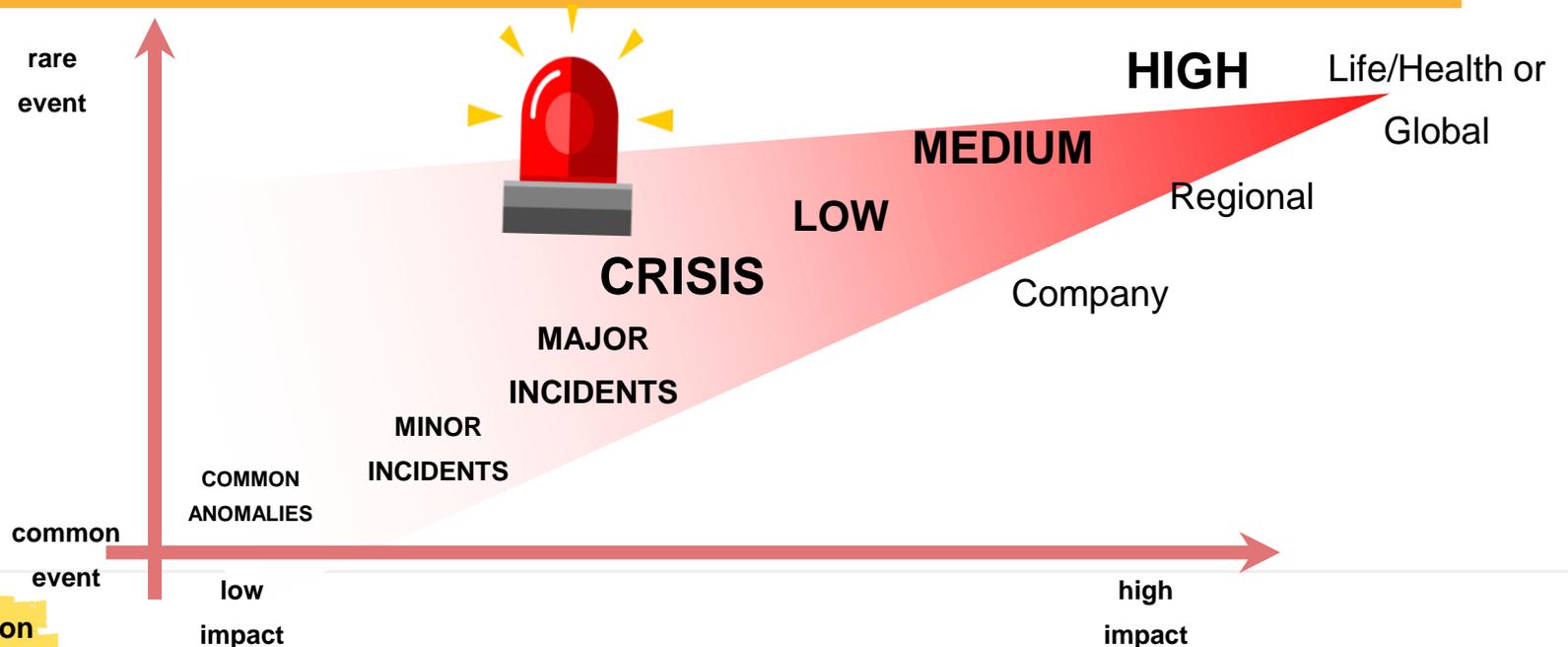
Define a structured assessment of the incident **root cause**, **scope**, **severity**, incl:

- **Source:** internal or external systems, data, processes
- **Type:** unavailability, confidentiality, integrity of systems and data
- **Potential to:**
  - a. impact the **safety** and wellbeing of people
  - b. impact the **existence** or **reputation** of the organisation
  - c. bring **political** implications
  - d. cause **legal** or **contractual** implications or **non-compliance** with applicable rules
- **Severity level:** can be high, medium or low as per the organisation matrix

## Who is assessing?

Depending on the scale and complexity of the incident, cybersecurity experts, forensic analysts, legal counsel, and other relevant professionals can be involved.

## POSITIONING A CYBER CRISIS



# CHOOSE TARGET GROUP



Target group is the stakeholders who may be affected by a cyber incident, such as employees, customers, partners, suppliers, regulatory authorities, the media. Which stakeholders are included in the plan will depend on the nature of the business operations, the types of sensitive data the organisation handles, and the regulatory requirements for the industry in which it operates. Consider each group's specific needs and concerns. For example, employees may require detailed information about the incident and what steps are being taken to mitigate it, while customers may be concerned about the impact and protection measures for their own services, technology, and data. Regulatory authorities will likely be interested in showing compliance with relevant regulations, while the media may focus on the scale of the incident impact.

# DEVELOP KEY MESSAGES



**ACE** the below to communicate effectively with stakeholders, build trust, and navigate the crisis with transparency and confidence.

**Accuracy & transparency:** information is verified, factually correct, and free from speculation.

**Customised and clear language:** use simple and straightforward language for the messages to be easily comprehended and remembered. Address the unique needs of each stakeholder group, by targeting the message focus, level of details, channels.

**Empathy and assurance** should be incorporated into the key messages. Acknowledge impacted stakeholders' concerns and provide assurances on your commitment to resolving the issue, protecting affected individuals, and preventing future incidents.

# TASK #5 APPOINT THE ROLES

## Create a Crisis Communications Team

Compile a team with the following roles / skills / functions: incident coordinator, spokesperson, technical, legal, HR, management, with clear roles and responsibilities. Incident coordinator takes the leading role, needs to make decisions quick and based on data collected from the team.

- **Incident coordinator** orchestrates the incident response and is in capacity to take quick decisions to handle the incident.
- **Spokesperson** is the single point of contact for the organisation and takes care of the media relations. It can be the CEO, a company executive, or someone else who possesses strong communication skills. The ability of the spokesperson to humanise the company and present the mistakes as manageable plays a pivotal role in maintaining support from stakeholders.
- **Technical expert** have deep knowledge of the SME's IT infrastructure and can advise on technical issues related to the incident.
- **Legal advisor** ensures that communications comply with data protection and other legal requirements.
- **HR representative** ensures smooth communication with employees and that their needs are met.

## FORMALISE A CRISIS COMMUNICATION TEAM CONTACT LIST

Role	Name	Position	Email	Mobile
Incident Coordinator				
Spokesperson				
Legal Counsel				
HR representative				
Technical experts				

# TASK #6 SET RULES OF ENGAGEMENT

## **Establish Internal Communication Protocols**

Develop clear procedures, outlining the steps and protocols for sharing information within the organisation, ensuring consistent and accurate messages to speed up the process, minimise confusion and prevent misinformation spread.

Provide guidelines on the types of information that can or cannot be shared internally & externally and establish approval processes for sensitive or strategic messages to ensure only appropriate and authorised information is communicated, reducing unintended consequences or misrepresentation.

Raise awareness within the organisation on the main points of the crisis communication plan, including clear roles and responsibilities, and the above protocols for cyber crisis communication.

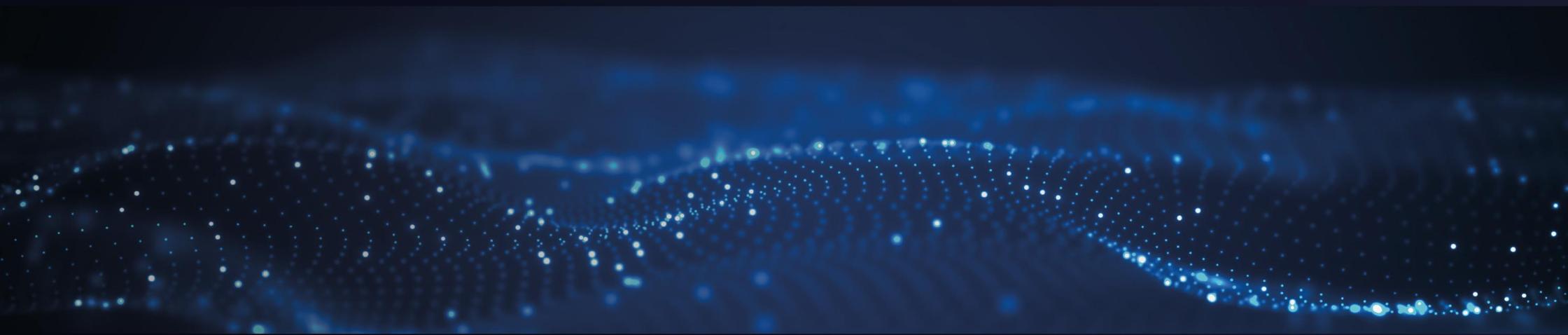
## **External Stakeholder Communication**

Ensure proactive communication with external stakeholders, based on priority, with timely updates on the incident status, its impact, and the steps being taken to address it. This includes addressing stakeholders' concerns and managing their expectations regarding the resolution and recovery process. Proactive damage control, as a crisis plan cornerstone, involves taking pre-emptive measures to minimise the impact of a crisis and mitigate potential risks to effectively address vulnerabilities and enhance the organisation's resilience to cyber threats.

## **Media Relations**

Designate a spokesperson, with adequate communication skills, training and experience, to represent the organisation and handle interviews and other media engagements. Develop model press materials to support interactions with incident announcement, summary of its impact and ongoing response efforts. Q&A documents can anticipate common questions and provide well-crafted answers for consistent messaging.





EXECUTE THE PLAN

# PRINCIPLES FOR CRISIS MESSAGE DESIGN

➤ **Tailor messages to different stakeholders:** Provide each group with necessary information, guidance and support.

➤ **Provide perspective:** Place the situation into context.

➤ **Communicate what the organisation knows:** Provide factual information only, without judgment, emotion or guessing.

➤ **Action-oriented:** Detail the steps being taken to remedy the situation and avoid it happening again to reassure key stakeholders

➤ **Show empathy:** It is important to express concern for any affected parties, whether internal or external; take responsibility and apologise if it is demonstrably at fault.

➤ **Stay clear and transparent:** Responses should be timely, accurate and consistent, even if under external media and stakeholders' pressure.

➤ **Provide ongoing updates:** Acknowledge the need for ongoing communication to maintain engagement and reassure stakeholders that the issue is being addressed.

# PRINCIPLES FOR CRISIS COMMUNICATIONS

➤ **Act Swiftly and decisively:** As soon as the incident is identified, activate the crisis communication plan, delays lead to speculation, misinformation and reputational damage.

➤ **Establish clear lines of communication:** Provide contact information, such as dedicated hotlines or email addresses, to facilitate communication and ensure that queries and concerns are addressed promptly.

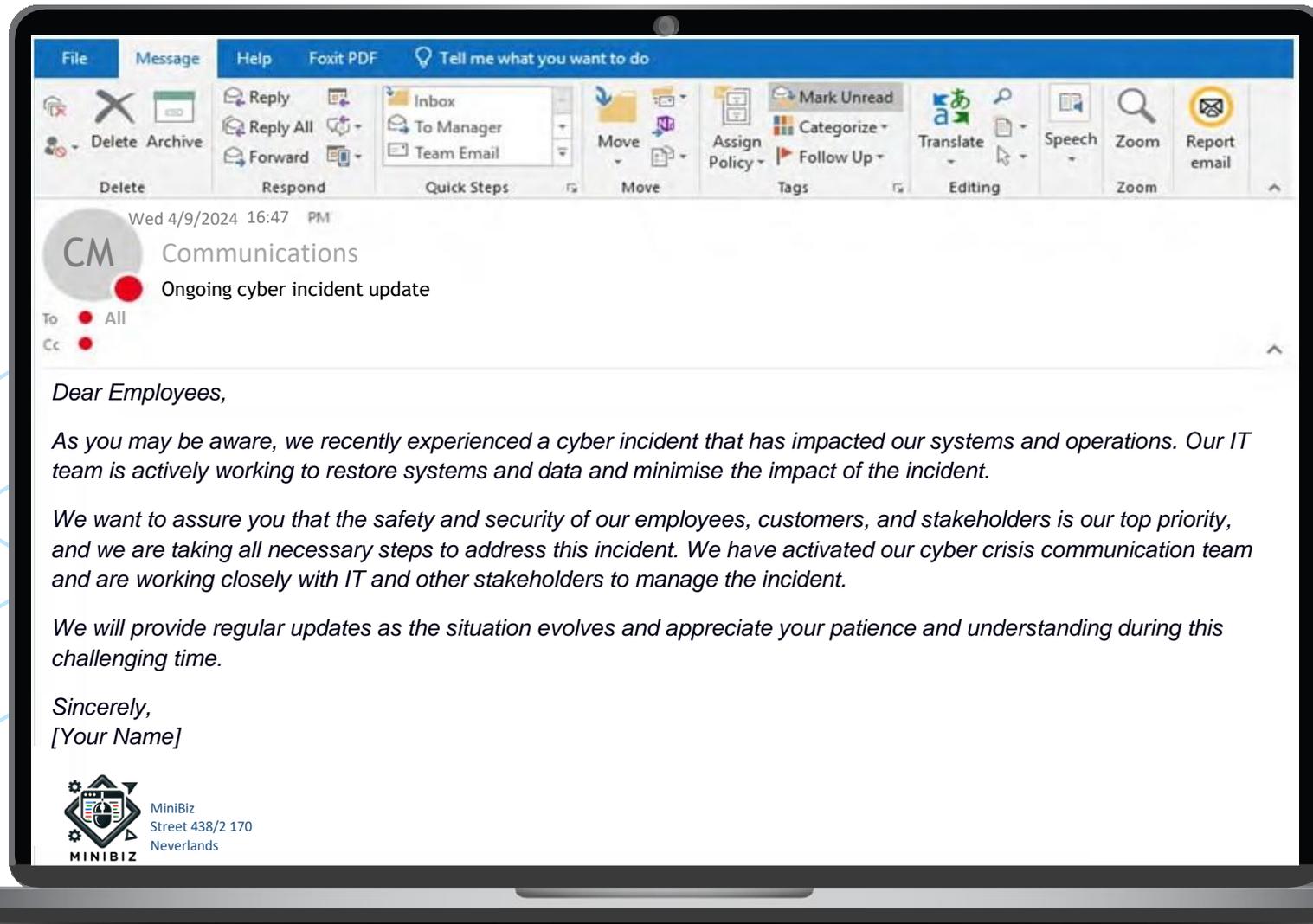
➤ **Acknowledge the crisis:** Do not try to hide if/when there is an incident developing, but be careful not to take the ownership or responsibility for a crisis that is not the organisation's responsibility

➤ **Manage media effectively:** Maintain a proactive approach in managing media inquiries, providing accurate information, and promptly correcting any inaccuracies or misleading reports.

➤ **Leverage social media and online platforms:** Monitor relevant hashtags and keywords to stay aware of public sentiment and address any emerging issues or misinformation proactively.

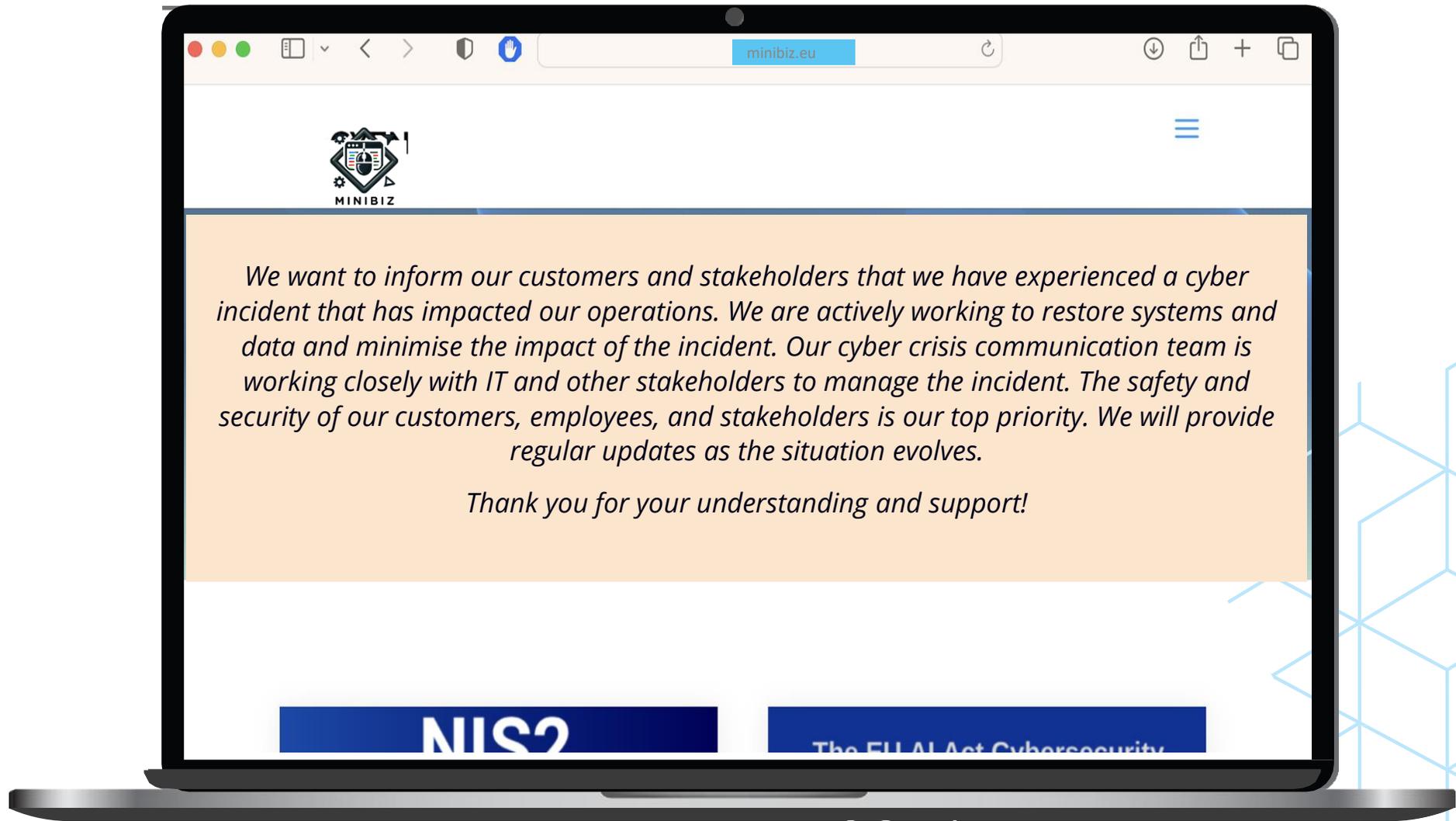
➤ **Gather feedback after the crisis is resolved to capture findings and comments**

# Example: Internal Email Communication



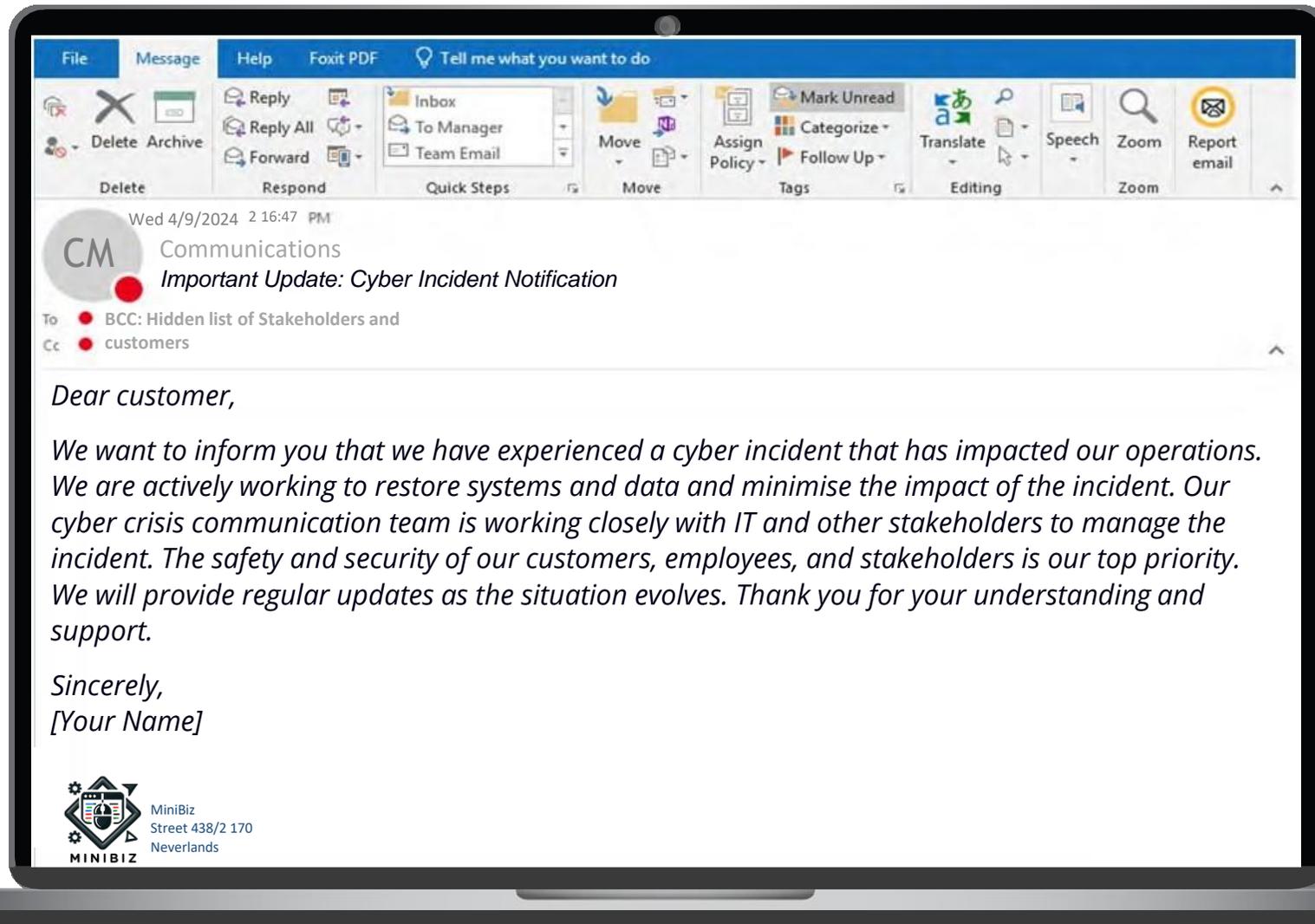
EMAIL TEMPLATE

## Example: News Communication



NEWS TEMPLATE

# Example: External Email Communication

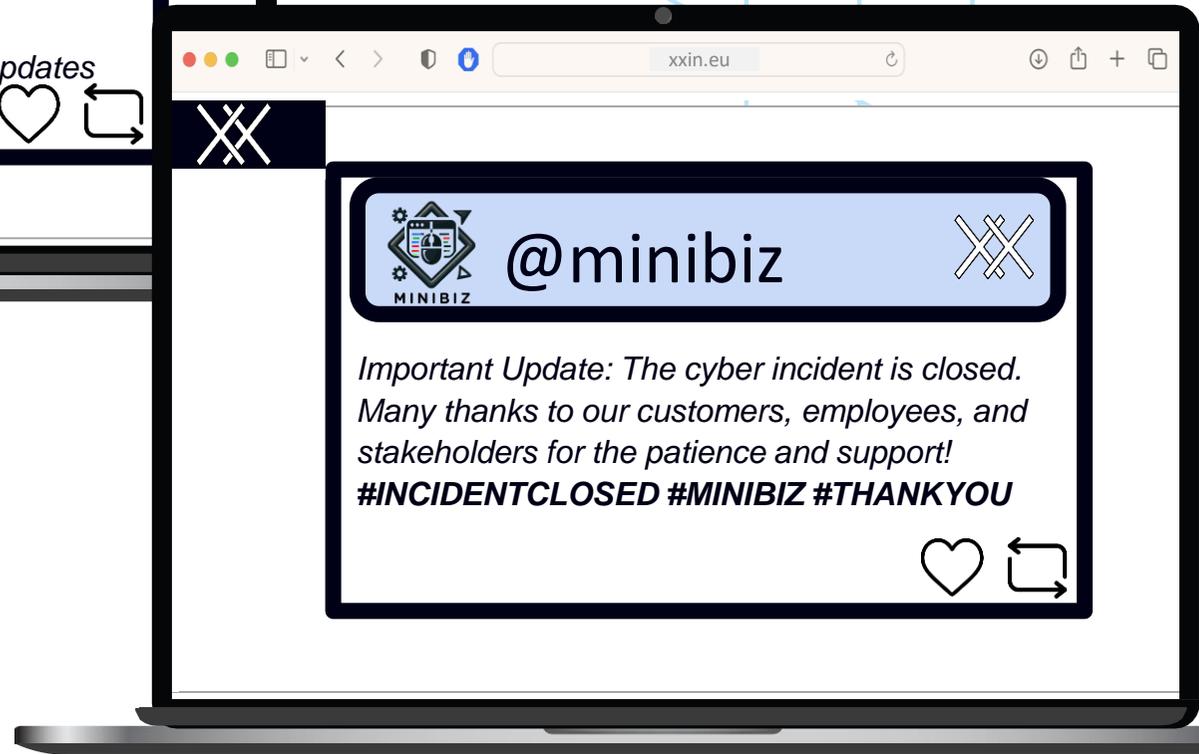


EMAIL TEMPLATE

# Example: Social Media Communication



NEWS TEMPLATE



UPDATE TEMPLATE

# EXERCISE THE PLAN

## TYPE OF EXERCISES

**Tabletop:** A discussion-based exercise to simulate a crisis scenario involving the cyber crisis communication team. Participants analyse hypothetical scenarios, review the communication plan, and practice decisions and communication efforts.

**Functional:** Hands-on exercise that simulate the cyber crisis operational response with internal AND external participants. The scenario unfolds gradually, allowing participants to engage in real-time decision-making, communication, and coordination activities.

**Full-Scale:** A real-life crisis simulation exercise, often conducted in a realistic setting with a broader range of participants, incl. external partners, vendors, authorities, involving strategies for media engagement, public response, and stakeholder interaction.

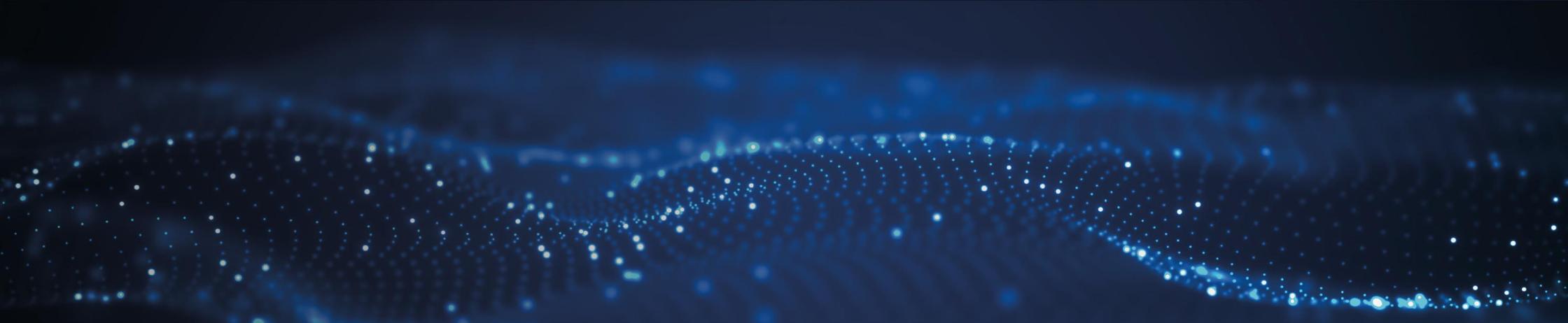
### Good practice

**Invite external observers, communication or crisis management experts,** to oversee the exercise and assist in evaluating the performance, identify gaps and areas for fine-tuning.



# EXAMPLES OF A CYBER CRISIS EXERCISE SCENARIO

Scenario	Objective	Simulation, run an ongoing cyber crisis scenario where:
<b>Internal communication services (email, teams, skype) are inaccessible or untrusted/compromised</b>	Practice effective communication and collaboration within the team in the absence of usual communication channels	Critical information promptly needs to be discussed, disseminated within the team and shared to stakeholders, including to the public/press, but not through the usual communication channels. Each expert should apply their chosen communication methods and strategy to effectively convey the message.
<b>Ransomware attack in the middle of holiday period</b>	Exercise the backup and alternate system	It is 25 December, you need to respond to a ransomware attack, but some of the key stakeholders and crisis communication team members are away with no stable internet connection.
<b>Inaccessible organisation assets (network, laptop, communication channels)</b>	Access a backup of company crisis communication plans, systems, information.	You need to collaborate without the usual communication channels and gain access to important information for the smooth and timely crisis communication plan execution.



**MONITOR**

**&**

**EVALUATE**

## SOCIAL MEDIA MONITORING

**Monitor discussions and sentiment related to the cyber incident online.**

Organisations should actively track social media channels, forums, and other relevant online platforms to identify emerging issues, rumours, or misinformation circulating about the incident. By promptly addressing any inaccuracies, clarifying information, and responding to concerns raised by the online community, organisations can help mitigate the potential negative impact and maintain a positive reputation. **This ongoing evaluation allows for agile decision-making and the ability to adapt communication strategies as the cyber crisis unfolds.**



## GATHER FEEDBACK

Actively seek feedback from internal and external stakeholders. Encourage customers to share their experiences and concerns openly, ensuring that their voices are heard. Analyse feedback by look for patterns, common themes, and emerging issues that could indicate the extent of the crisis's impact on customers. This analysis can provide valuable insights into the specific areas that need immediate attention and mitigation efforts.

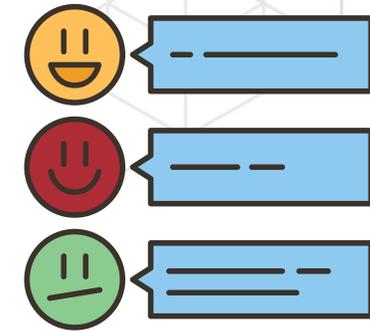
Insights from the members of the crisis communication team, IT department, executive management, and other relevant departments can provide valuable perspectives on what worked well and what could be improved.



## Post incident review

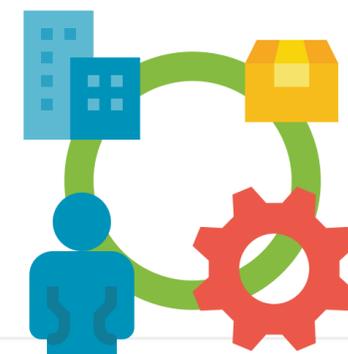
Capture the lessons learned and refine the cyber crisis communication plan thorough assessment of the organisation's response to the cyber incident, including the effectiveness of its communication.

By analysing the strengths and weaknesses of the communication plan, organisations can improve their procedures and raise awareness amongst the personnel on the lessons learnt reflected in procedure reviews. Regular post-incident reviews foster a culture of continuous improvement, enabling organisations to continually enhance their crisis communication capabilities and better prepare for future cyber crises.



# REAL EXAMPLES

**Shop supply chain attack in 2023:** As a result of a ransomware attack to one of the IT services providers in Sweden, a number of SMEs were severely impacted (closing stores, stopping deliveries, interrupting content productions). Certain companies resorted to a cyber crisis communication plan to inform their customers of the ongoing disruption. An example is a shop, a chain of stores and e-commerce, who published a press release explaining the technical details of the incident, the impact on clients, the current actions to resolve the issue and acknowledge the inconvenience for clients.



# REAL EXAMPLES

**SME:** In 2017, an individual raised an inquiry through the company official corporate website. Their query pertained to the circumstances surrounding their spouse departure from their 11-year managerial role at one of the company establishments. In response, the company opted for a restrained approach, refraining from providing a public statement. This decision was influenced by considerations surrounding matters of personal privacy and the potential for the company to become engaged in a defensive stance. Rather than engaging in immediate communication, the company opted for a strategy of allowing the situation to naturally dissipate over time.



# REAL EXAMPLES

**Telecommunication company attack in 2015:** A UK-based telecommunications company experienced a cyber-attack that exposed customer data. The company crisis communication response involved swift acknowledgment of the breach and transparent communication with customers. The CEO appeared in media interviews, addressing the issue directly and reassuring customers about the steps being taken. The company also offered support to affected customers and took measures to enhance its cybersecurity. While the company faced criticism for the breach, its proactive communication helped mitigate the damage to its reputation.

