RÉPUBLIQUE
FRANÇAISE
Liberté
Égalité
Fraternité

ANSSI

COLLECTION
CYBER CRISIS MANAGEMENT

ANTICIPATING AND MANAGING YOUR CYBER CRISIS COMMUNICATION

CAP'COM LE RÉSEAU DE LA COMMUNICATION PUBLIQUE ET TERRITORIALE

COLLECTION
CYBER CRISIS MANAGEMENT

GUIDE

ANTICIPATING AND MANAGING YOUR CYBER CRISIS COMMUNICATION

The French National Cyber Security Agency (ANSSI) is the national authority for the security of information systems. Attached to the Secretary-General for Defence and National Security, it carries out prevention, information, awareness and defence missions. ANSSI deals primarily with critical operators, both public and private.

CONTENTS

Editorial 6
Presentation 8

IN ANTICIPATION **10**

Step 1 (fact sheet 1): initiating dialogue with the cyber and IT teams outside of crisis periods 12
Step 2 (fact sheet 2): anticipating crisis scenarios and responses regarding the communication aspect 16
Step 3 (fact sheet 3): devising your cyber crisis response communication strategy 19
Step 4 (fact sheet 4): integrating the communication function when organising cyber crisis management 22
Step 5 (fact sheet 5): organising crisis communication 26
Step 6 (fact sheet 6): creating a dedicated toolbox for cyber crisis management 28
Step 7 (fact sheet 7): training your teams to manage the communication aspect 30

IN RESPONSE **34**

Step 1 (fact sheet 8): integrating the crisis management unit 36
Step 2 (fact sheet 9): carrying out your risk analysis regarding communication 40
Step 3 (fact sheet 10): preparing language elements to suit your target audiences 43
Step 4 (fact sheet 11): coordinating your organisation's communication 46
Step 5 (fact sheet 12): supporting institutional communication 48
Step 6 (fact sheet 13): capitalising on and seizing an opportunity for internal and external awareness raising 50

CHECKLIST **52**
GLOSSARY **53**

EDITORIAL

Over the years, computer attacks are increasing in their intensity and sophistication. Today, all organisations are aware that, one day or another, they risk coming under attack. More and more, they are preparing themselves for that eventuality. When that crisis does occur, however, we see all too often that the actions of communicators take a back seat. This is a mistake.

For global crisis management, it is indeed essential that the communication response works hand in hand with the technical response. Let's consider the unfortunately common case of a ransomware attack. With profound consequences on the workings of the organisation (work tools unavailable, data compromised, etc.), this type of attack is immediately visible and can attract strong media coverage. In a situation that can quickly escalate to alarming levels, acting upstream to include the communications function, both internal and external, becomes all the more vital in order to anticipate the reactions of media, politics and society... and to avoid adding one crisis to another.

The attackers themselves set about communicating by issuing press releases or organising press conferences! Hiding behind this communication is actually a leverage effect, reminding us that cyber attacks affect all business lines and all sectors.

This guide, which draws on the experience of the French National Cyber Security Agency (ANSSI), will not make you a cyber expert. The important thing here is to give you an understanding of the particular characteristics of cyber crises so that you can take better account of them within your own crisis communication strategy. With one key word: anticipation.

Guillaume Poupard
Director-General of ANSSI

The digital ocean can carry us far and wide. But it can also grow stormy. Hacking, and a good many other cyber attacks, can then cause us to lose our bearings. In an emergency, we all want to avoid rocking the boat. Public communicators will be much in demand, externally to communicate about the crisis and internally to convey information, to improvise new circuits, to maintain a listening ear.

We sometimes forget that communication in itself is not without risk. Reaching out to others means exposing ourselves as we remove the comfort of security. And yet dialogue, with all its uncertainties, amidst all the insecurity that surrounds it, is what allows us to stay connected in a state of mutual understanding, which is essential to the functioning of our society.

Accustomed as they are to the challenges of interaction, our communicators should therefore be mobilised at the very heart of operations in the event of a cyber attack, where inter-team understanding is key. Their knowledge of communication usage in times of crisis is a real asset and their expertise is crucial: making contact – with officers, citizens and elected officials – reformulating, popularising, restoring. In this, they should be recognised, themselves made aware of risk control, in a personal capacity also, and they must network to share their experiences.

Leading by example requires continuing competency and a humble attitude, like that of a sailor when putting out to sea. Faced with a cyber crisis, being able to count on everyone's individual skills is all-important in building effective, concerted solutions.

Yves Charmont
Delegate-General of Cap'Com

PRESENTATION

In the face of an attack, the technical nature of a cyber crisis can destabilise even the most experienced communicators, dealing with features, challenges and ecosystems that are sometimes very far removed from their core business activity.

Focussing on the particular characteristics of a cyber attack, this guide aims to show that good cyber crisis communication is primarily a reiteration of all the tools and reflexes we commonly apply to any crisis communication strategy.

What is this guide for?

Based on situations encountered by ANSSI since its formation in 2009 to provide assistance to victims, this guide aims to provide highly operational advice and recommendations in order to develop and then trigger the crisis communication component during a computer attack.

Although there is no magic recipe in crisis management, there are a number of reflexes and key concepts that can be integrated without delay by your organisation, whether private or public, in preparedness for a cyber crisis.

The recommendations in this guide are therefore also suitable for managing situations described as “sensitive”, which often precede a potential media crisis.

Who is it for?

This guide is intended for all people acting in the role of communicator during the management of a crisis. Depending on an entity's size and organisation, this may be a communication professional (Head of communications, communication officer or communication agency), but can also be other profiles (firm of professionals, legal expert, decision-maker), for lack of dedicated communicators. Depending on the situation, even the operational team can sometimes play the role of communicator.

While this guide is primarily intended for communication professionals, who have a key role to play in crisis management, it also aims to provide tools and advice to other technical and decision-making professionals called on to support our communicators.

What are the prerequisites?

This guide aims to provide insight into the particular characteristics of cyber crisis communication, as perceived by ANSSI. Its purpose is not to go into detail about how to develop a crisis communication strategy in general. Ideally, this task should be carried out and tested upstream in order to be able to adapt your organisation and tools to the specific nature of a cyber crisis.

This guide does, however, offer a few reminders of the basics of crisis communication to familiarise all readers with the concepts and key issues at stake for the communication function.

By the way, what is a cyber crisis?

A crisis of "cyber origin" is defined as the immediate and major destabilisation of the day-to-day operation of an organisation (cessation of activity, inability to deliver services, heavy financial losses, major loss of integrity, etc.) due to one or more malicious actions against its digital tools and services[1] (cyber attacks like ransomware, denial of service - DoS, etc.). This is a high-impact event, which cannot be dealt with by the usual processes and within the framework of the organisation's normal operations. By convention, we will use the term "cyber crisis" from here on.

1. To which are associated the organisation's IT systems and those of its service providers.

IN ANTICIPATION

STEP 1: initiating dialogue with the cyber and IT teams outside of crisis periods (fact sheet 1 – p. 12)

STEP 2: anticipating crisis scenarios and responses regarding the communication aspect (fact sheet 2 – p. 16)

STEP 3: devising your cyber crisis response communication strategy (fact sheet 3 – p. 20)

STEP 4: integrating the communication function when organising cyber crisis management (fact sheet 4 – p. 24)

STEP 5: organising crisis communication (fact sheet 5 – p. 26)

STEP 6: creating a dedicated toolbox for cyber crisis management (fact sheet 6 – p. 28)

STEP 7: training your teams to manage the communication aspect (fact sheet 7 – p. 30)

Managing your crisis communication effectively relies primarily on anticipation to enable rapid action and agility when a crisis does occur. Ahead of a crisis, in calmer times that are more conducive to reflection and change, there are seven steps to be adopted in sequence with the specific tempo of your own organisation, depending on its size and operation. The following practical fact sheets will help you prepare these steps.

STEP 1

INITIATING DIALOGUE WITH THE CYBER AND IT TEAMS OUTSIDE OF CRISIS PERIODS

When a cyber crisis occurs, the cyber and IT teams, including the Chief Information Security Officer (CISO)[2], are heavily involved alongside other crisis management players.

Becoming acquainted under these conditions can be complicated. However, as a communicator, you will not be the only one to "communicate": different information feeds will emerge from your organisation for employees, service providers, partners, etc. To ensure overall consistency on D-Day itself, it is essential to understand **the priorities, challenges and language of each business line.**

For greater ease, this dialogue will benefit from having been initiated ahead of any real crisis, in the upstream preparation phase. If the communicator needs to adapt to a specialised audience, the latter also needs to understand the overall context of the incident response, which may be subject to several sources of interference (media pressure including political, professional or social networks) adding a risk of a media or social crisis to the existing cyber crisis.

2. The CISO defines and develops the information security policy for a company, public institution or local authority.

First and foremost, you have to ask yourself the following questions: who is in charge of IT security within my organisation? Has any joint work already taken place to anticipate cyber risks? Has my organisation ever been the victim of a cyber attack?

In the absence of an internal team(s), local service providers or systems such as Cybermalveillance.gouv.fr[3] can provide some keys to understanding.

Recommendation

This mutual acculturation can take place in different forms: running dedicated workshops, defining an internal awareness-raising campaign (how about doing this during the French edition of the European Cyber Security Month, "Cybermoi/s", in October!) or organising cyber crisis management exercise(s)[4].

3. The Cybermalveillance.gouv.fr system aims to assist individuals, businesses, associations, local authorities and administrations that fall victim to cyber crime, and to inform them about digital threats and how to protect against them.
4. For more information, consult the ANSSI guide on *Organising a cyber crisis management exercise.*

ONE CRISIS, MULTIPLE ANGLES

The impacts of a cyber crisis may be visible immediately following the interruption of one or more services or the disruption of office tools.

	FROM THE PERSPECTIVE OF THE COMMUNICATOR
Questioning	For users, employees or even political or media commentators, there will be many questions: what happened? Who is responsible for the attack? What is the impact? As a customer or partner, could I be a victim myself? Why us? What are the internal IT services and the CISO doing? What is the image risk for our organisation? What is the financial impact for our organisation? The questions and the number of interlocutors mount up as the crisis unfolds. Cyber crises generate more anxiety when the subject remains relatively recent and poorly understood by the general public, leaving room for confusion (fear of a virus spreading, quick attribution to state actors, etc.).
Actions	Working under pressure, the communicator has to: ▸ Support the teams in charge of crisis management by taking charge of certain groups (internal, media) in order to let the operational teams manage the business impacts of the crisis. Often overlooked, internal communication is also fundamental when managing a crisis: employees directly or indirectly affected by the unfolding crisis need to be informed and reassured. ▸ Transmit information that is reliable, verified and adapted to the situation, based on the insight provided by cyber teams and crisis management. Understanding the incident and taking remedial action takes time though, which can be difficult to explain over several weeks, or even several months. ▸ Protect the entity's reputation: the role of communication is also to safeguard the entity's image, often tarnished by the crisis, and to ensure that it does not deteriorate further with the spread of rumours or false information.

When a crisis occurs, several actors come into play and offer a different interpretation of the unfolding crisis and its potential origin.

FROM THE PERSPECTIVE OF THE CYBER AND IT TEAMS

Questions will be stacking up quickly on the side of the cyber and IT teams: what exactly is going on? How was the attack able to get past the security measures in place? Could the attack spread to different IT systems within my organisation or to other entities via interconnections?

One of the characteristics of cyber attacks is that time taken for investigation and then remediation can be very long. The time frames for technical analyses unfortunately cannot be compressed. Although the effects of an attack are immediate, the work of the operational teams is long and tiresome, especially as they are working under pressure and with an often limited workforce.

Be aware also that there is usually a phase of denial followed by a phase of looking for culprits. It is important that you don't fall into this infernal spiral and instead concentrate on the analyses which will make it possible to recover critical services. As a second step only, it may be relevant to trace the origin of the attack.

Gaining an understanding of the incident is only the beginning of a long phase of remediation:

- understanding the situation: the teams launch investigations to determine the causes and extent of the attack;
- rebuilding the damaged IT systems in a controlled manner and back on solid ground, to avoid a replica of the attack;
- thoroughly reviewing the IT security measures in place in order to prevent another attempted attack from succeeding.

It may be several months before some organisations are able to safely reinstate their full range of services[5]. During this time, communication needs to be able to follow and accompany the teams in this long-distance race.

5. For more information, consult the ANSSI guide *Crisis of cyber origin: the keys to operational and strategic management.*

STEP 2

ANTICIPATING CRISIS SCENARIOS AND RESPONSES REGARDING THE COMMUNICATION ASPECT

Each organisation is required to conduct an analysis of the risks that threaten to destabilise its activities[6]. In the face of these risks, responses are provided, particularly in terms of communication. With the help of actors involved in crisis management, in particular the cyber and IT teams, several realistic crisis scenarios can be anticipated in order to reflect on the management processes regarding the crisis communication aspect.

This exercise is all the more useful to carry out for cyber crises as they seem difficult to tackle, due to their highly technical nature. Especially since there are different types of computer attacks, and as many different responses to provide. We wouldn't handle a (discreet) espionage operation in the same way as a (highly visible) ransomware or denial of service attack. Similarly, the way we approach an attack will depend on the context. The publication of financial results, of salary negotiations, of major events for the sector (election periods, product launch, etc.) are decisive elements to take into account. Finally, an attack with business impacts that are limited to the organisation alone is not handled in the same way as an attack that spreads to customers and/or partners. It is not possible to cover all scenarios, but putting in the work upstream will give you a reference framework to fall back on when the dreaded day arrives.

Recommendation

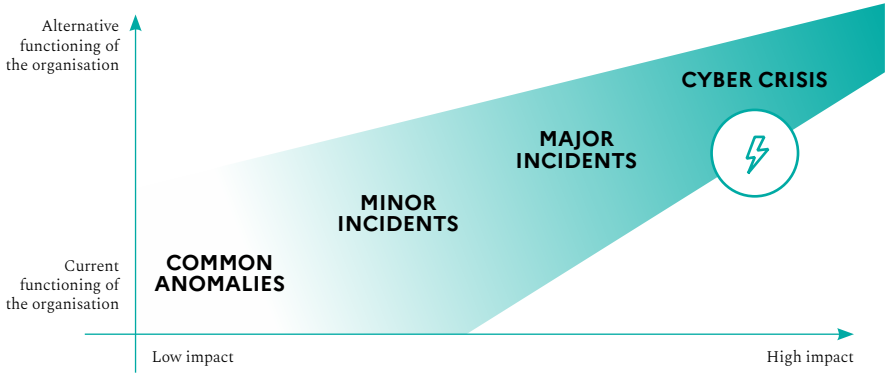
Beyond cyber scenarios, you could list major and sensitive events, as well as sensitive issues for your organisation and your sector that could influence your communication decisions.

6. To find out more, consult the EBIOS Risk Manager method.

GRAVITY SCALES IN CYBER SECURITY

We use the term "cyber crisis" when one or more malicious action(s) against the IT system generate(s) major destabilisation of the entity, having various and significant impacts, sometimes causing irreversible damage. ANSSI distinguishes between several levels of criticality, from a technical point of view:

POSITIONING A CYBER CRISIS FACED WITH EVENTS ADVERSELY AFFECTING THE BUSINESS ACTIVITIES OF AN ORGANISATION



It should be noted, however, that in terms of crisis communication, the criticality of a situation is also assessed, perhaps even more so, in terms of media, political, financial, commercial, internal and social pressure. Before an actual cyber crisis, organisations may have to manage sensitive situations related to digital issues such as, for example, data security (hosting, risk of data breach), choosing a service or a service provider that is potentially compromised or even a "normal" computer failure.

STEP 3

DEVISING YOUR COMMUNICATION STRATEGY IN RESPONSE TO A CYBER CRISIS

It is more beneficial to devise your crisis communication strategy outside of a crisis situation. Its primary aim is to serve as a reference and practical guide when managing a crisis, which is marked by stress, pressure and speed. Several steps can be identified:

1. Understanding the **context** in which the crisis is unfolding: this part is to be adapted to the actual situation experienced. Devising scenarios in advance is useful for referencing the questions to be asked on the day itself.

2. Defining **communication objectives** (see step 1 of the "In anticipation" section): this generally involves explaining the situation in an instructive manner, providing reassurance that the crisis is being managed effectively and protecting the entity's image and reputation.

3. Fully identifying your **targets**: these are the people your messages will be addressed to, whether they are internal (technical teams, management, employees, shareholders, service providers, customers, etc.) or external players (customers, partners, authorities, media, influencers, etc.).

4. Identifying **stakeholders**: these are players who may also be required to communicate on the situation (authorities, customers, service providers, etc.).

5. Designating and providing ongoing training for **spokesperson(s) representing** your organisation to external audiences, including the media, during a crisis.

6. Working on your **communication stances** (reactive vs. proactive, targeted vs. broad) as well as your main **messages**, in the form of language elements, as appropriate for the level of criticality of the crisis, the entity's exposure and/or the media, political, economic and/or social pressure generated.

7. Defining **the organisation of crisis communication** and identifying the **communication tools** available (press, web, directory).

Recommendation

To develop a crisis communication strategy that is consistent with the entity's identity, begin by examining your organisation's overall communication strategy.

INTEGRATING CYBER SCENARIOS WITHIN YOUR CRISIS COMMUNICATION STRATEGY

Based on scenarios developed together with the cyber and IT teams, you can prepare a crisis communication strategy in response to the situations identified, simply repeating the same steps, this time to include the codes and specific characteristics of the cyber field:

1. **Context:** anticipate a few questions, like what type of incident is it? What is the impact on services provided? What is my organisation's recent news (publication of results, major events, etc.)? The context section might take into account the answers to the questions posed on page 13 (critical services, etc.).

2. **Goals:** popularise technical vocabulary in order to provide clear and controlled information (security measures, results of initial analyses, etc.).

3. **Audience:** prioritise communications as relevant to the situation, particularly where there is a risk of spreading.

4. **Stakeholders**: integrate service providers, often called upon to assist in crisis management. Integrate specialist authorities (ANSSI, Data Protection Authority, cyber prosecution service, regulatory authorities), especially if you are subject to statutory obligations (OIV, OES, administrations). Create a press file with the media, journalists and main influencers of the cyber ecosystem, including those from the general press.

5. **Spokesperson**: train your spokesperson(s) in cyber issues.

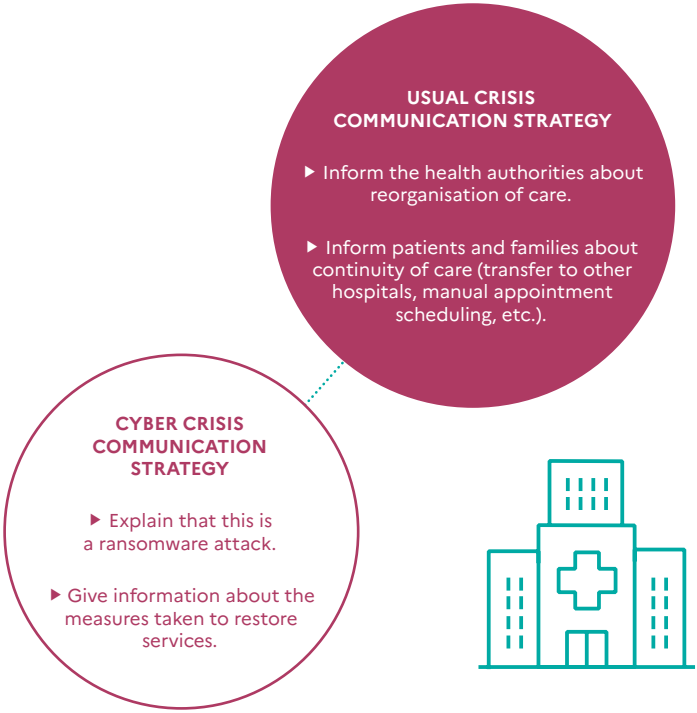
6. **Stances and messages**: engage with specialist teams to create a basic directory of popularised cyber vocabulary.

7. **Tools and organisation**: anticipate their unavailability!

Recommendation

The cyber crisis communication strategy allows you to respond to a single facet of the crisis, namely an explanation of the causes – of cyber origin – of the crisis. It works alongside other response strategies focusing on the management of business impacts that are more specific to your field of activity (malfunction or closure of a service, interruption to commercial relations, etc.).

Example of a hospital, victim to a ransomware attack that paralyses its office automation system:



STEP 4

INTEGRATING THE COMMUNICATION FUNCTION WHEN ORGANISING CYBER CRISIS MANAGEMENT

Whether or not this is a cyber crisis, crisis communication must be integrated within the organisation's overall crisis management system within the first few hours. As a communicator, you have several roles to play:

To alert: you keep an eye on what's trending, and on social and media reaction to hot topics related to your area of activity. The early signals of a crisis can come from media or social networks.

To react quickly: in a crisis, carefully worded messages adapted to different audiences, both internal and external, must be constructed quickly, with the support of the relevant business teams. You are already familiar with the diverse range of audiences for your organisation, whether internal or external (employees, managers, shareholders, board members, customers, media, partners, etc.), as well as the tools available to you. This expertise is invaluable when it comes to ensuring a good level of response.

To analyse and adapt: when managing a crisis, communication is not set in stone and you can adapt to suit the reactions of target audiences. This means a detailed analysis of the way different audiences perceive the situation and, where applicable, the messages sent out by your organisation.

This expertise is shared with other actors involved in crisis management within a number of dedicated units:

- **Strategy unit**, which brings together senior management and support professionals (legal, human resources, etc.). Communication can also be included here, as decisions affecting the image and reputation of an organisation are generally taken at decision-maker level.

- **Operational and technical units**, bringing together all the professionals involved in incident resolution in the longer term. Communications can rely on this unit to obtain up-to-date information on the operational situation.

Find comprehensive advice on organising crisis management in the dedicated guide[7].

Good crisis communication is no guarantee that everything will go smoothly – but poor management of crisis communication can only worsen an already difficult situation.

7. For more information, consult the ANSSI guide *Crisis of cyber origin, the keys to operational and strategic management.*

DESTABILISATION ATTACKS

A cyber crisis can take different forms depending on the motivations of the malicious actors. Some computer attacks, such as **DoS** or **website defacement** (see glossary) are primarily intended to destabilise the targeted organisation and damage its reputation.

These attacks have real business impacts, causing a failure to provide services, sometimes with significant financial cost. As they are relatively unsophisticated, they can be detected and stopped fairly quickly and they do not generally cause any long-term impact (such as loss of data or destruction of IT systems).

They do though have a high **symbolic and emotional impact**: they highlight the vulnerability of a service, or even raise a banner for hacktivists with intimidating messages.

There is a real gap between **the perception of the incident**, relayed via social networks and the media, **and the technical complexity** of the incident.

In this type of situation, "communication" expertise is key: the aim is to explain in an educational way the real impacts of the attack, which are generally moderate, in order to give rapid reassurance to audiences focussing on the issue. In the absence of appropriate and measured communication, these attacks can achieve their end goal of destabilisation by stirring up a media and social frenzy.

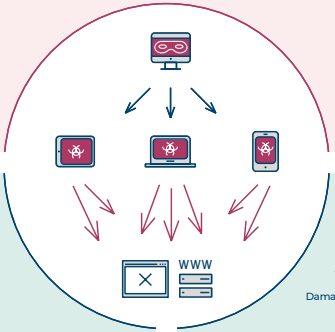
DDOS: DISTRIBUTED DENIAL OF SERVICE ATTACK

Access to the site you are viewing is disrupted

WHAT IS HAPPENING?

Many machines send a high number of requests to the service and overload it.

Your browsing on the site is slowed right down or made impossible.



Impact of the attack

- Integrity
- Authenticity
- Availability
- Confidentiality

Main motivation

- Damage to image
- Profit motivated
- Nuisance
- Demand
- Espionage

PHISHING

Are you being urged to communicate important information?
Don't fall into the trap.

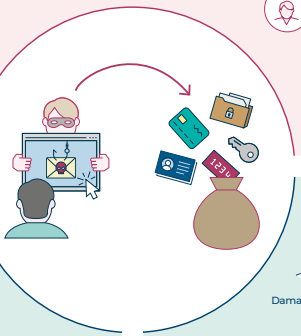
WHAT IS HAPPENING?

1. You receive a spoofed email.

The suspicious email prompts you to:
- click on an attachment or a spoofed link;
- communicate personal information.

2. The attacker impersonates a trusted person or third party.

The attacker is then able to:
- take control of your system;
- make use of your information.



Impact of the attack

- Integrity
- Authenticity
- Availability
- Confidentiality

Main motivation

- Damage to image
- Profit motivated
- Nuisance
- Demand
- Espionage
- Sabotage

STEP 5

ORGANISING CRISIS COMMUNICATION

Depending on the size (communications team or single contact person) and organisation of your entity (in-house or outsourced communication), you should pre-determine a specific crisis organisation for the communication function, including division of roles and tasks.

The key areas are:

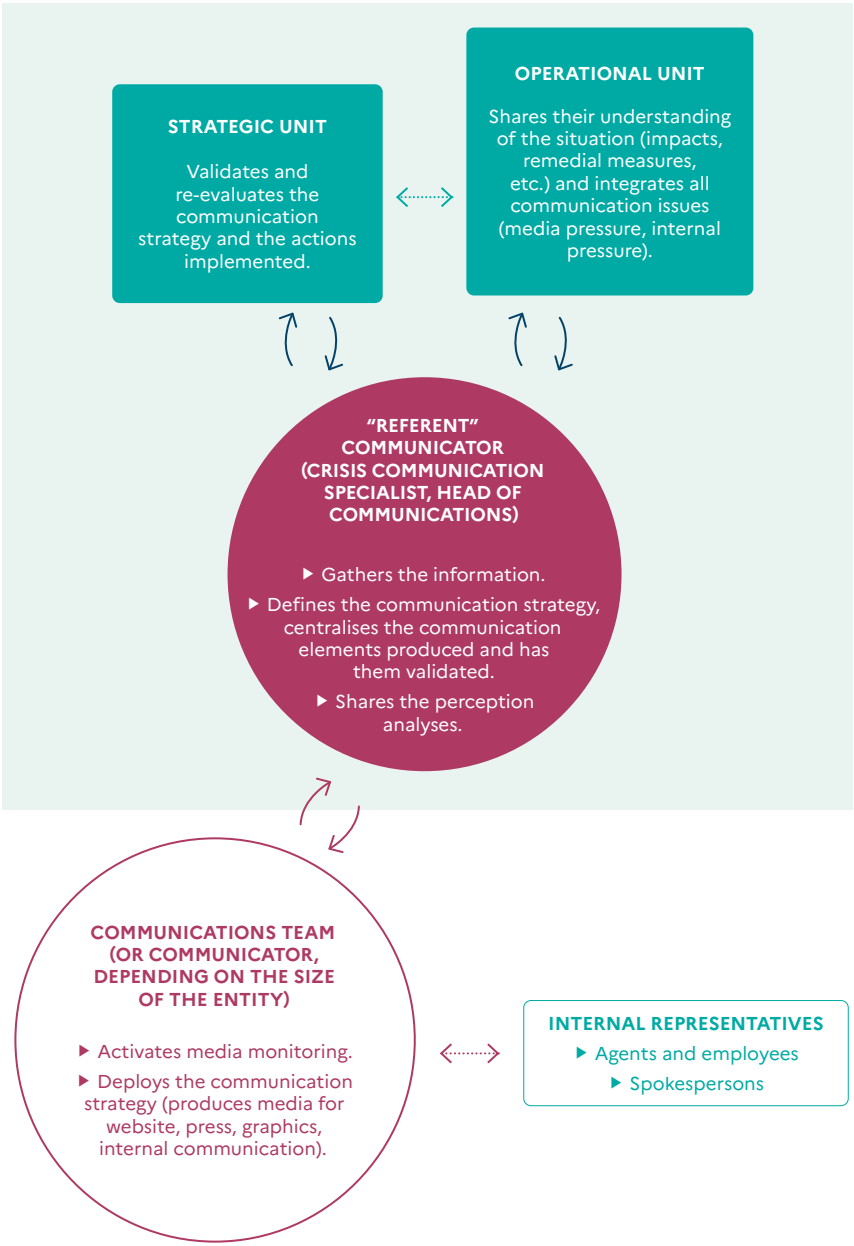
- **Coordination:** a communication representative attends the briefings of the operational and strategic units in order to include the perception aspect within the risk analysis and to validate the communication elements produced internally and externally. This individual also liaises with external stakeholders (relays, communicators, etc.).

- **Monitoring and perception:** media monitoring, covering the press and social networks, is set up and monitored by a dedicated person and serves as a basis for adapting the communication stance and messages throughout the crisis management.

- **Reaction:** members of the team in charge of press relations, coordinating social networks, website and internal communications will adapt and relay the messages to their respective audiences.

This organisation is feasible if the communication team is made up of several members. Where staff numbers are lower, these roles are still just as valid but must be adopted by a reduced number of people.

Crisis communication management system



STEP 6

CREATING A DEDICATED TOOLBOX FOR CYBER CRISIS MANAGEMENT

To allow crisis communication to be activated very quickly, it is very useful to create a "cyber crisis communication" toolbox in advance of any crisis. This contains:

- **The crisis communication strategy** (see step 3 of the "In anticipation" section).
- A diagram of your organisation's **crisis management system** and of its communication organisation (see steps 4 and 5 of the "In anticipation" section).
- **Steering tools:** a press file, account login credentials (social networks, mobile applications, website, Intranet, etc.), directories of crisis management actors, etc.
- **A glossary** or some form of catalogue of language elements on sensitive or crisis topics. This glossary can be compiled beforehand together with the IT teams.

This toolbox is then regularly updated with experience feedback, either real or fictitious (exercise).

Recommendation

Remember to have this toolbox on a separate USB key or an isolated server in case of a computer attack that paralyses your office tools. Also earmark a pool of PCs that are isolated from the network and keep a back-up paper copy of your crisis communication strategy documents.

THE 100% CYBER TOOLBOX

In preparing to deal with a cyber crisis, you can begin gathering useful materials and documents straight away, ready to be used on a turnkey basis in the event of a real crisis. For example, a "cyber" glossary can be devised with the operational teams using generic language elements, to be adapted to the crisis situation encountered on the day:

- **A clear and instructive definition of the most commonly occurring computer attacks:** DoS, ransomware, defacement. This definition would ideally include responses on the impacts of each attack (unavailability, potential data exfiltration and publication, loss of access to services, etc.).

- **A list of questions to anticipate:** has a complaint been filed? Do we need to make a General Data Protection Regulation (GDPR) type declaration to the national authority? Who is behind the attack?

You can put together an expanded press file listing which publications to monitor (specialist press, influencers) and contact details for specialist journalists, including the general press. The cyber community is made up of some very active, demanding and interested people who enjoy discussing technical elements, debating on social networks and commenting on official communications.

Recommendation

To create your toolbox, here are some resources in addition to the glossary included at the end of the guide:

- **ssi.gouv.fr (English version available)**
- **cybermalveillance.gouv.fr (French version only)**
- **Cybermoi/s campaigns**

STEP 7

TRAINING YOUR TEAMS TO MANAGE THE COMMUNICATION ASPECT

Crisis management exercises are an opportunity to test the resilience of your organisation and your tools in the face of a major attack that paralyses your information system. In particular, they allow you to automate certain actions which will then save you time in the event of a real incident, and in terms of communication as well.

Based on the scenarios defined among the teams, you can organise training sessions on several different scales:

- **A general exercise:** this type of exercise aims to test the entire crisis management system within your entity and allows you to verify the adequacy and effectiveness of the processes for dialogue between different units.

- **An exercise solely dedicated to communication:** whatever your setup (an in-house team of communicators or a service provider managing press relations, for example), this type of exercise allows you to test the coordination between the professional roles and the individuals undertaking them, and to familiarise them with the world of cyber security.

- **An exercise with external participants:** this exercise adds another layer of complexity by bringing in players external to the organisation (sector-specific regulator, customers, etc.).

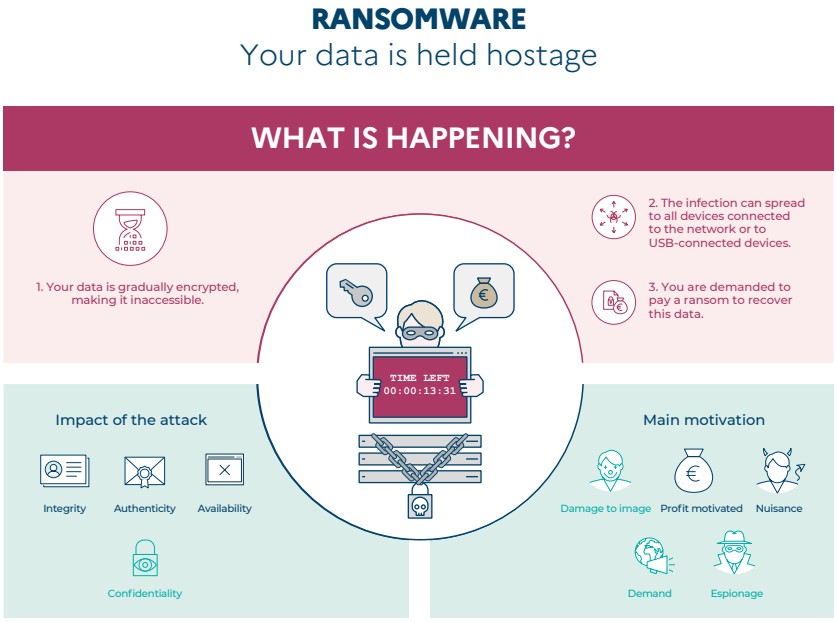
For a successful training session, it can be useful to simulate media pressure, either internally or via a service provider: fake media calls, fake dispatches or even fake social networks.

Exercises are effective when they go hand in hand with training upstream and feedback downstream to help teams make good progress[8].

8. For more information, consult the ANSSI guide on *Organising a cyber crisis management exercise.*

DEALING WITH A RANSOMWARE ATTACK

Ransomware attacks[9] (see glossary) are increasingly common and can affect any entity, regardless of its activity, nature or size. In terms of crisis communication, it is also a useful training exercise; this type of attack is visible, with immediate effects (unavailability) and sometimes a very long remediation time.



9. For more information, consult the ANSSI guide *Ransomware attacks, all concerned – How to prevent them and respond to an incident.*

▸ **Tempo:** the attack is generally visible almost immediately, calling for rapid action to determine your communication stance (proactive, reactive) and the messages you need to convey. On the technical side, managing the incident causes stress and heavy pressure on the technical and managerial teams, especially since the attackers often opt for periods with reduced staff numbers (weekends, public holidays, holiday periods).

In contrast, the remediation time remains long, with an often uncertain estimate of the time required to return to normal activity. It is therefore imperative to focus on the critical elements.

Recommendation

To limit the pressure, you will need to act quickly to provide responses to different audiences, starting with the definition of ransomware. It is also essential to be transparent and instructive about investigation and remediation times.

▸ **Emotional impact:** the attack is often accompanied by an intimidating message (skull and crossbones, countdown, threat) which can affect staff. Some cyber criminal groups are quick to establish their own public communication about the attack to increase pressure on the victim (threat of data disclosure, for example). The ransom demand alone will generate a surge of anxiety.

Recommendation

Internal, institutional and also managerial communication is essential to reassure your employees about the management of the crisis. In addition, ANSSI recommends that you do not pay the ransom. Payment offers no guarantee that data will be recovered intact and may even induce the author (or others) to subsequently perpetrate a new attack on a "good payer". Neither does paying the ransom avoid the workload required to return the IT system to normal service and to strengthen its level of security to prevent new attacks.

▸ **Tools:** the potential paralysis of traditional communication tools (press file, access to social network accounts or website, emails, etc.) makes it more difficult to implement communication actions swiftly, particularly internally (internal email, customers, etc.).

Recommendation

By acting upstream to anticipate degraded internal communication methods (telephone listing, posting, etc.), you will speed up the process when managing the crisis internally.

IN REACTION

STEP 1: integrating the crisis management unit (fact sheet 8 - p. 36)

STEP 2: carrying out your risk analysis regarding communication (fact sheet 9 - p. 40)

STEP 3: preparing language elements adapted to suit your target audiences (fact sheet 10 - p. 43)

STEP 4: coordinating your organisation's communication (fact sheet 11 - p. 46)

STEP 5: supporting institutional communication (fact sheet 12 - p. 48)

STEP 6: capitalising on and seizing an opportunity for internal and external awareness raising (fact sheet 13 - p. 30)

A crisis has now broken out: the crisis management units are in operation. The communication function is activated and you bring your expertise to help manage the crisis.

Once the crisis is established, crisis communication will need to be adapted to allow for consideration of situational factors for better decision-making. Here again, several steps follow in turn. Practical sheets detail these steps on the pages below.

STEP 1

INTEGRATING THE CRISIS MANAGEMENT UNIT

The communication and situation awareness component must be fully integrated into the decision-making of general management and technical teams. Be aware that intense pressure (media, politics) can have an effect on the teams, either positive or negative.

Integrating the crisis management unit(s) allow you to fulfil a two-fold objective:

- **Understanding the bigger picture:** the technical elements and their effects on the business lines and services/tools of your organisation.

- **Sharing your reflection process within the area of expertise that is communication:** internal, media or political reactions, prior to or subsequent to publications made by your organisation.

The end goal of the communicator is to protect the reputation and image of their organisation during and after a crisis.

Recommendation

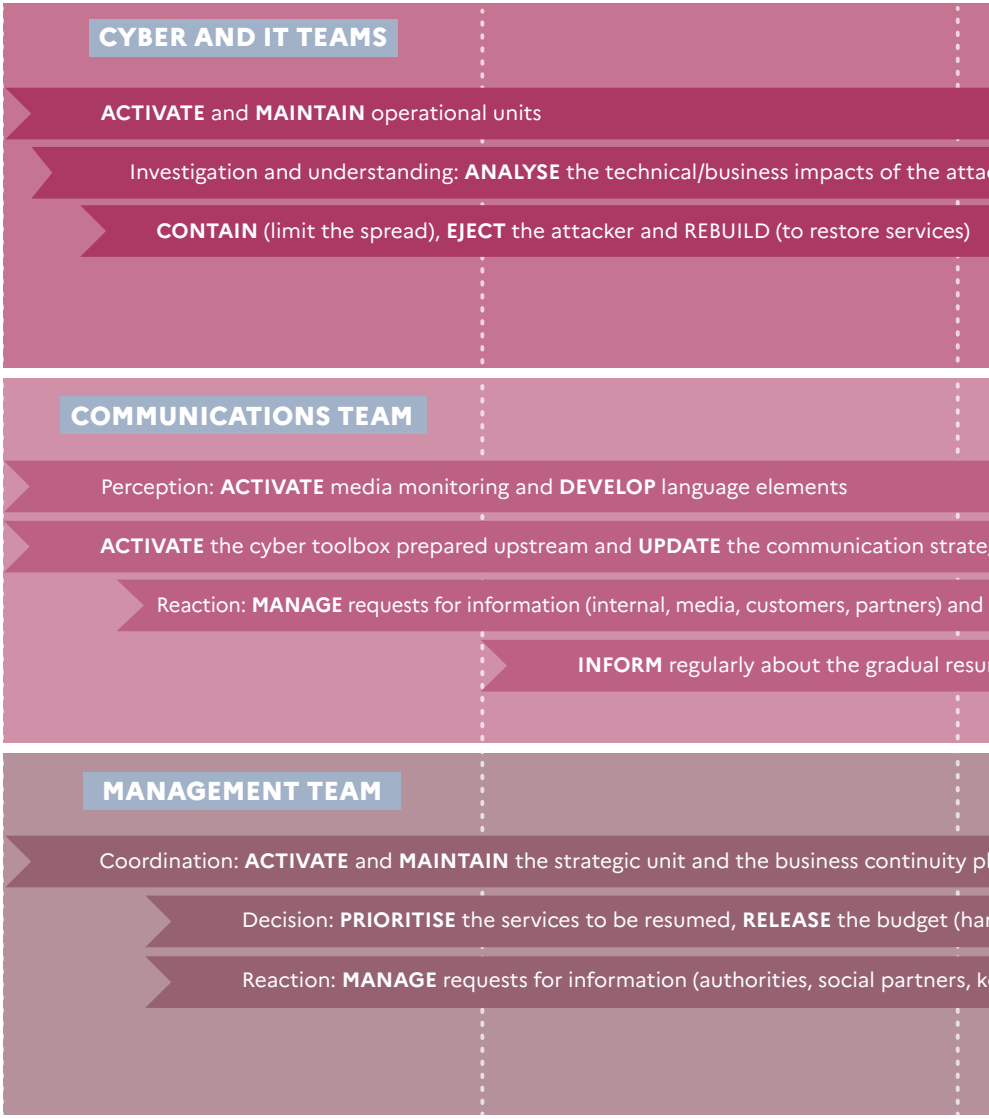
In order to ensure effective crisis management, the role of the communicator, within the strategic unit, is to ensure that the entity's outgoing communications fully respect the different tempos of the actors involved (cyber and IT teams, communications team, management team).

THE TIMELINE OF A RANSOMWARE ATTACK

The crisis can be read in different ways depending on the point of view adopted. Let's look at this fictitious example of a ransomware attack from three different angles: the communicator, the cyber and IT teams and the decision-maker. Remember: every situation is unique, and so the steps and time frames indicated should be adapted to suit the organisation and the nature of the attack.

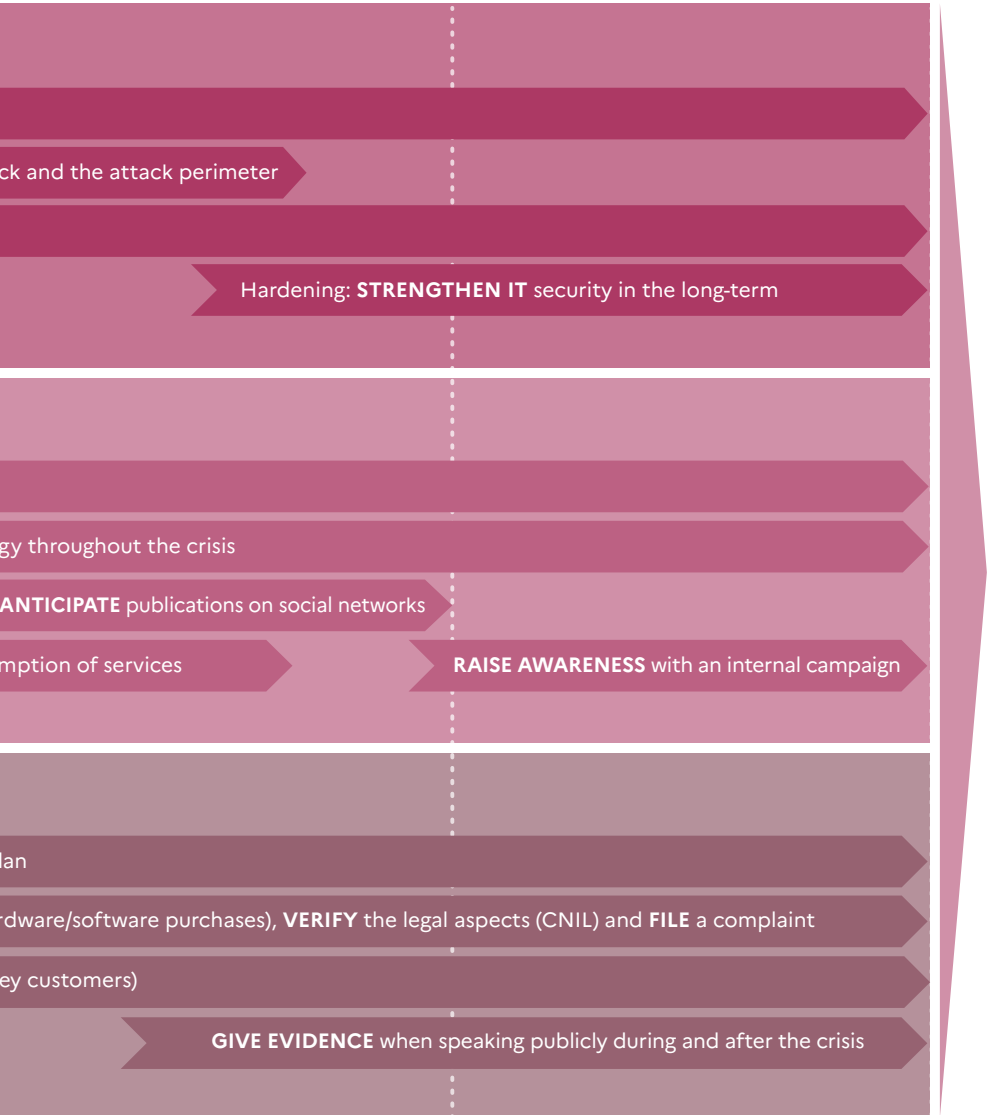
ONE ATTACK, THREE TEMPOS

D-0: day of the attack



In the context of this guide, this timeline is condensed over a few months.
In reality, the management of a crisis extends over a longer period of time.

D+4 MONTHS


ck and the attack perimeter
Hardening: **STRENGTHEN IT** security in the long-term
gy throughout the crisis
ANTICIPATE publications on social networks
mption of services
RAISE AWARENESS with an internal campaign
lan
rdware/software purchases), **VERIFY** the legal aspects (CNIL) and **FILE** a complaint
ey customers)
GIVE EVIDENCE when speaking publicly during and after the crisis

STEP 2

CARRYING OUT YOUR RISK ANALYSIS REGARDING COMMUNICATION

There is no single response to a crisis, whether cyber or not. The appropriate response depends on the facts, but also on the context at the time of the crisis (political, social, media, economic). The role of the communication function is to carry out a risk analysis in terms of image and reputation, considering audiences both internal and external to the entity and also in both the shorter and longer term.

To carry out your communication risk analysis, you can use the toolbox created earlier (see step 6 of the "In anticipation" section), which should be updated with regard to:

- **Facts established:** What happened? What are the actual impacts? What are the visible impacts? What are the risks and consequences of exposure to the crisis suffered by your company in the short and long term?

- **Context:** are there any cyber or sector-specific news topics to take into account? Who is doing the talking?

- **Current or anticipated reactions:** what are the initial reactions observed, internally or externally? How will your teams, customers or suppliers react if data leaks are established or when they learn that an attacker has penetrated your IT system?

Recommendation

Not communicating is an option, especially if an attack occurs at an intensely newsworthy time for the entity (product launch, election campaign, etc.).

First and foremost, this task is a cost/benefit analysis which requires, in each instance, an element of risk taking to be assumed by the decision maker in the short and medium term. On the basis of this analysis, the decision maker and their teams will be able to decide on the appropriate communication stance (proactive or reactive) to adopt.

In this case, the entity accepts the risk of information being leaked, even months later, and assumes the consequences of that disclosure. Reactive language elements should be prepared in any case.

EXAMPLE OF AN ESPIONAGE TYPE COMPUTER ATTACK

A cyber attack is not necessarily visible. Ransomware is just one possible type of attack. Attacks for espionage purposes are numerous, discreet, more sophisticated – and sometimes have disastrous consequences. For example, attackers have been able to break into information systems, for several years in some cases, in order to steal strategic information from a company.

When an attack of this type is detected, the communication aspect is approached differently, especially if the attack was detected by chance or at a very late stage. The communication risk analysis then asks the following questions:

- Is the attack likely to be visible? Does the attacker intend to publish the collected data?
- Who should I inform?
- Should we communicate widely? Internally? Externally?
- What is the reputational risk to my organisation if I disclose this attack?
- When should we talk about it? Is the attacker still active?

Some questions will take time to answer. If you opt not to communicate, then elements of responses should nevertheless be prepared and ready for circulation in case your communication stance were to change.

Recommendation

For this type of attack, the remediation component is often long, as the attacker has generally gained full control of the IT system. This will necessitate in-depth technical actions to eject the attacker and strengthen the security of the IT systems. And, in effect, you will need to support these actions with appropriate internal communication.

STEP 3

PREPARING LANGUAGE ELEMENTS ADAPTED TO SUIT YOUR TARGET AUDIENCES

With the risk analysis now carried out, you are ready to formulate and coordinate the messages to be sent out to the various audiences you have identified. Several parameters should be taken into account:

- **The level and quality of information is to be adapted to the target audience and reassessed throughout the crisis**. When managing a cyber crisis, technical analyses take time and impose a certain rhythm on communications, which ensures that the information transmitted is truthful and reliable.

- **The technicality of the information may also vary depending on the audience.** If you are addressing the generalist media and therefore a non-expert readership, you will need to simplify your information and show more of an instructive approach. Even when simplified, the information you send out must be truthful and reliable.

- **The pace of information transmission.** You need to occupy the media space to prevent other actors (experts, competitors) from expressing their views in your place. You will therefore need to provide visibility at each key stage, following the "battle rhythm" defined for crisis management in more general terms.

As a topic, cyber is now closely followed across the entire media spectrum, including non-specialist media. All communications relating to cyber must be well measured and well founded because they will be closely analysed by the community and relevant influencers.

WHAT SHOULD YOU SAY?

As every situation is unique, the messages will differ according to the situation and the target audience, both internal and external. Although it isn't easy to plan a typical message, several pieces of information will be expected:

▸ Explain the nature of the attack, in particular the impacts on the organisation, services or products of your entity.

▸ In the event of a data leak, explain in an instructive manner what this means for the customers or users affected and the actions they can take to protect themselves.

▸ Provide visibility on the actions implemented to restore your organisation's services and tools as quickly as possible. Be careful not to give too firm a resolution date: the complexity of computer attacks can lead to unforeseen delays.

▸ Be instructive about the time frame of investigations and remediation.

▸ Specify the measures taken in respect of authorities, as applicable:
- in the event of a data leak, a declaration to the national authority (e.g. CNIL);
- filing a complaint with specialist gendarmerie or police services.

The tone of your communications can also change with the crisis: educational, reassuring, authentic, calm. You will need to strike a balance between expert discourse (explanations around the incident) and assurances about the implementation of measures necessary for the resolution of the crisis.

Note that if the incident involves legal jurisdiction, certain specific elements cannot be disclosed without prior agreement of the competent investigating authority. In the event of a significant leak of personal data, the national authority may also send out recommendations regarding communications.

Finally, as with any crisis, it is better to adopt an empathetic tone in your message, especially if people are directly or indirectly affected.

Recommendation

Particular attention should be paid to your editorial choices (vocabulary, tone employed): be transparent, but be aware that it is more impactful to reassure than to opt for very anxiety-inducing terms. Similarly, using humour to ease tension is a risky choice: one person's perception of the incident will be very different to the next. Humour could be perceived as managing the crisis lightly, in contradiction to the criticality and the stress experienced by certain actors.

STEP 4

COORDINATING YOUR ORGANISATION'S COMMUNICATIONS

Three main types of communication can be identified when managing a cyber crisis:

- technical, expert, evolving and factual communication;
- institutional communication, controlled and validated by the decision-maker;
- political communication, led by the authorities.

The communication function is therefore not the only one issuing information throughout the crisis management process. Other actors intervene and address their own audiences:

- **technical teams;**
- **general management;**
- **professional roles in contact with external interlocutors** (customer services, legal services, etc.);
- identified **stakeholders**.

The role of the communication function is to coordinate the various feeds to ensure that the organisation's global communication is clear, controlled and coherent.

The communication function needs to have a comprehensive overview of the communication tools and the messages transmitted, including the social networks of senior managers or employees.

WHO ULTIMATELY HAS A COMMUNICATION ROLE?

Overview of the different lines of communication: objectives, priorities and challenges.

Communication

- **Message:** assessment of the situation, actions undertaken.
- **Audience:** employees, press, influencers, etc.
- **Medium:** appointment of a spokesperson, press, web, intranet, etc.

Technical teams

- **Message:** technical elements (markers), factual review of situation.
- **Audience:** Data Protection Officer (DPO), chain of command, counterparts (sector-specific CERT, CISO networks), authorities (CNIL/GDPR), service provider.
- **Medium:** emails, memos, meetings.

General management

- **Message:** situation management and business continuity.
- **Audience:** employees, authorities, customers, etc.
- **Medium:** email, press, telephone, etc.

Other professionals

- **Message:** situation management and business continuity; risk of spreading.
- **Audience:** customers, partners, prospective customers, etc.
- **Medium:** email, press, telephone, etc.

Other stakeholders

- ANSSI: sharing of technical information, institutional communication in the event of intervention.

- Sector-specific authorities, customers, partners and service providers: reassurance about their own situation.

STEP 5

SUPPORTING INSTITUTIONAL COMMUNICATION

Individual roles (entity, stakeholders) in terms of crisis communication must be clearly defined and shared by all. For better control of your message, it is often advised not to have multiple people conveying official institutional communication. Communication is responsible for managing certain specific audiences, including media, internal and social pressure. Two forms of communication are involved:

Internal communications

▸ **Goal:** to reassure and explain the situation. In the event of major work disruptions, to provide visibility on the actions taken and the anticipated return to normal activity.
▸ **Tools:** telephone listing/emails, meeting, Intranet, SMS campaign.
▸ **Your messages:**
- provide instructive information on the attack and the actions recommended and/or implemented to effectively emerge from the crisis;
- give practical instructions to employees so that they can work and provide visibility on forthcoming steps until the end of the crisis.

External communications

▸ **Goal:** to explain the situation throughout the crisis, the stages of management (understanding, remediation).
▸ **Tools:** identified spokesperson, press release, article on the website, relay on social networks, evolving language elements.
▸ **Your messages:**
- determine the level of information that needs to be provided to each recipient, depending on the impacts and the context;
- reassess with input from media and social monitoring.

TYPICAL QUESTIONS TO ANTICIPATE FROM JOURNALISTS

In the event of a computer attack, you may be contacted by your usual media contacts (sector-based press, national and/or regional general press) but also by the specialist press in information technology and more specifically in computer security.

Overview of typical questions asked by specialist journalists:

- What type of attack is it? What are the tactics, techniques and procedures?
- What are the direct consequences (technical, financial)? What are the indirect consequences? Spread? Lateral movement?
- Have your customers fallen victim? Are they sensitive customers?
- When did it happen? How long will this last? Is the attack still ongoing? When do you expect to return to normality or optimal operation?
- What are you doing today to repair the IT system?
- Has a complaint been filed? Has a GDPR declaration to the national authority been made?
- Are you being supported by ANSSI? By service providers?
- What measures are you going to put in place in the future?
- Who is the attacker? What are their motives? Did you pay the ransom?

STEP 6

CAPITALISING ON AND SEIZING AN OPPORTUNITY FOR INTERNAL AND EXTERNAL AWARENESS RAISING

A crisis is an opportunity, once under control, to identify areas for improvement (process, toolbox) and to remobilise teams on digital security topics.

For the communication component in particular, it is a potential starting point for an internal awareness-raising campaign on good IT practices to adopt, each at their own individual level. For inspiration, go to the ANSSI and Cybermalveillance.gouv.fr websites to find resources and ideas for your campaigns.

Sharing your experience can also serve to help other actors, within your sector of activity for example, to raise their awareness of the risks and the more technical measures to be implemented to prevent computer attacks.

Do not hesitate to share your experience to show how you were able to overcome this challenge and to play your part in strengthening security in France!

RECOMMENDATIONS FOR DEALING WITH RANSOMWARE

By way of example, the news reports an increase in ransomware attacks against all types of organisation. The French edition of the European Cyber Security Month, "Cybermoi/s", organised every year in October, is a great opportunity to conduct an internal awareness-raising campaign.

Recommendations

- back up your data;
- keep software and systems up to date;
- use anti-virus software and keep it updated;
- partition your information systems;
- limit user privileges and application permissions;
- control Internet access;
- implement log monitoring;
- assess the opportunity to take out cyber insurance.

Existing resources

- The ANSSI guide, produced in partnership with the Department of Criminal Affairs and Pardons (DACG) within the French Ministry of Justice; *Ransomware attacks, all concerned - How to prevent them and respond to an incident?*
- Cybermoi/s interactive comic strips, 2020 edition.
- Practical information on the Cybermalveillance.gouv.fr system.

CHECKLIST

- ☐ **Start preparing** your crisis communication toolkit now to deal with a computer attack.
- ☐ **Contact** the cyber and IT teams and the professionals involved in crisis management in general, to devise crisis scenarios and generic content, and to begin the discussion process.
- ☐ **Integrate** communication at the right level within your entity's global crisis management system to support staff teams and respond to internal and external requests during the crisis.
- ☐ **Take an interest** in the cyber security ecosystem: media, influencers, news, vocabulary.
- ☐ **Practise** and test the entire crisis management system, also including a simulated media pressure component for the communication section.
- ☐ **Approach** your CISO to raise your employees' awareness of cyber risks and good practices to adopt in order to avoid a cyber crisis.

GLOSSARY

CYBER SECURITY: providing resistance to events from cyber space likely to compromise the availability, integrity or confidentiality of the data stored, processed or transmitted and of the related services that these systems offer or make accessible.

TYPES OF ATTACKS

WEBSITE DEFACEMENT: alteration by a hacker of the appearance of a website, by modifying the content of its pages, often featuring slogans or images unrelated to the subject matter of the attacked site.

DENIAL OF SERVICE (DOS) OR DISTRIBUTED DENIAL OF SERVICE (DDOS): attacks aimed at making a service unavailable on the Internet by sending multiple requests until it becomes saturated, causing a breakdown or a severe degradation of the service.

ESPIONAGE: type of attack whereby an attacker discreetly gains a foothold into the victim's IT system to exfiltrate strategic information for the company. Such an attack, often sophisticated, can last several years before being detected.

PHISHING: fraudulent technique intended to deceive the Internet user by posing as a trusted third party (fake SMS, email, etc.) to prompt them to communicate personal data (access accounts, passwords, etc.) and/or bank details. This type of attack can be used for both an espionage attack and a ransomware attack.

RANSOMWARE: type of attack whereby a hacker executes malware on the victim's IT system, to encrypt all of its data, including backups, and demand a ransom in exchange for the decryption password. Additionally, it is not uncommon for the hacker to threaten to release previously exfiltrated data in order to increase the incentive to pay the ransom.

OPERATIONAL VOCABULARY

ATTRIBUTION OF A COMPUTER ATTACK: decision of the political authority, taken at the highest level, which aims to name the sponsor, generally a state, as responsible for this attack.

MALWARE: program developed for the purpose of harming an IT system. Note: viruses or worms are two known types of malware.

IDENTIFICATION OF A COMPUTER ATTACK: focuses on technical characterisation of the attacker's tools, techniques and tactics in order to determine their interests and working methods, to link them to known cyber attacks and finally, to identify a group of attackers or a sponsor. This technical work, which is given a variable level of certainty, then serves as a basis for determining possible attribution.

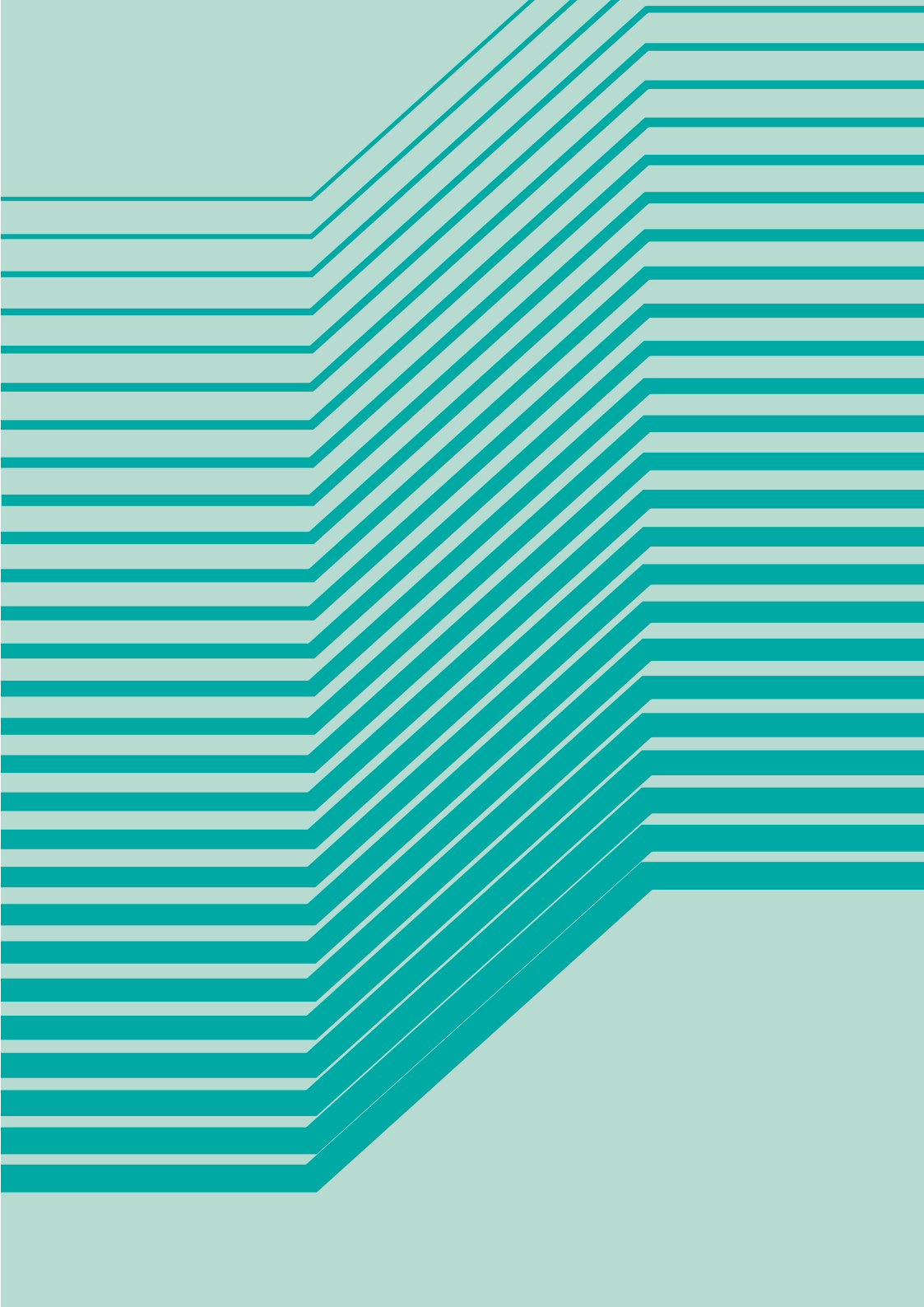
TECHNICAL MARKER OR INDICATOR OF COMPROMISE (IOC): technical information, such as the IP address of a malicious server or the name of a spoofed website, allowing an attack to be detected and characterised. The sharing of these elements of knowledge is particularly helpful in preventing future compromises. Conversely, such information is sometimes not to be communicated if the attack is the subject of criminal proceedings.

THE TACTICS, TECHNIQUES AND PROCEDURES (TTPS) OF AN ATTACKER OR GROUP OF ATTACKERS: equates to the attacker's signature, the method of operation they use to target and attack their victims.

GENERAL DATA PROTECTION REGULATION (GDPR): regulates the processing of personal data within the territory of the European Union. The CNIL in particular is in charge of handling complaints and developing new compliance tools to guarantee the protection of personal data for all.

VECTOR OF ATTACK: means of access used by a malicious actor to exploit security flaws and gain access to a server or device (attachments, Internet pages, unpatched vulnerabilities).

VULNERABILITY: security flaw that could affect a software product, an IT system or even a hardware component. It can serve as a gateway for malicious actors if they manage to exploit it. Vulnerabilities are generally corrected during updates or by patches published by software editors.



COLLECTION
CYBER CRISIS MANAGEMENT

"When a cyber crisis occurs, the actions of communicators all too often take a back seat. This is a mistake. For global crisis management, it is essential that the communication response works hand in hand with the technical response."

Guillaume Poupard, Director-General of ANSSI

In the face of an attack, the technical nature of a cyber crisis can destabilise even the most experienced communicators: dealing with the specific characteristics of the cyber field can be far removed from their core business activity.

Produced in partnership with Cap'Com and drawing on extensive experience in cyber crisis communication, this guide will support you in designing and deploying your communication strategies in the event of a computer attack.

Version 1.0 – March 2022 - **ANSSI-PA-091-EN**

ISBN : 978-2-11-167120-1 (papier)
ISBN : 978-2-11-167121-8 (numérique)
Dépôt légal : mars 2022

AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION
ANSSI — 51, boulevard de la Tour-Maubourg — 75 700 PARIS 07 SP — France
www.ssi.gouv.fr — communication@ssi.gouv.fr