

COLLECTION
CYBER CRISIS MANAGEMENT

ANTICIPATING AND MANAGING YOUR CYBER CRISIS COMMUNICATION



GUIDE

**ANTICIPATING AND
MANAGING YOUR CYBER
CRISIS COMMUNICATION**

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

often that the actions of communicators take a back seat. This is

communication is actually a leverage effect, reminding us that cyber attacks affect all business lines and all sectors.

Guillaume Poupard
Director-General of ANSSI

contact – with officers, citizens and elected officials – reformulating,

all-important in building effective, concerted solutions.

Yves Charmont
Delegate-General of Cap'Com

PRESENTATION

a reiteration of all the tools and reflexes we commonly apply to any

What is this guide for?

a number of reflexes and key concepts that can be integrated without

managing situations described as “sensitive”, which often precede

Who is it for?

during the management of a crisis. Depending on an entity's size and

What are the prerequisites?

By the way, what is a cyber crisis?

A crisis of “cyber origin” is defined as the immediate and major (cessation of activity, inability to deliver services, heavy financial losses, major loss of integrity, etc.) due to one or more malicious

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 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

STEP 1

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

Chief Information Security Officer (CISO)

“communicate”: different information feeds will emerge from your

the priorities, challenges and language of each business line.

For greater ease, this dialogue will benefit from having been initiated

which may be subject to several sources of interference (media

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

joint work already taken place to anticipate cyber risks? Has my



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

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

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 services⁵. 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

of salary negotiations, of major events for the sector (election periods,

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

against the IT system generate(s) major destabilisation of the entity, having various and significant impacts, sometimes causing irreversible

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



in terms of media, political, financial, commercial, internal and

STEP 3

DEVISING YOUR COMMUNICATION STRATEGY IN RESPONSE TO A CYBER CRISIS

It is more beneficial to devise your crisis communication strategy

pressure and speed. Several steps can be identified:

1. **context**

2. Defining **communication objectives**

crisis is being managed effectively and protecting the entity's image

3. **targets**

influencers, etc.).

4. stakeholders

5. spokesperson(s)
representing

6. communication stances
messages

7. Defining the organisation of crisis communication
communication tools

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

situations identified, simply repeating the same steps, this time to include the codes and specific characteristics of the cyber field:

1. Context:

recent news (publication of results, major events, etc.)? The context

2. Goals:

3. Audience:

4. Stakeholders: integrate service providers, often called upon to assist

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

5. Spokesperson

6. Stances and messages

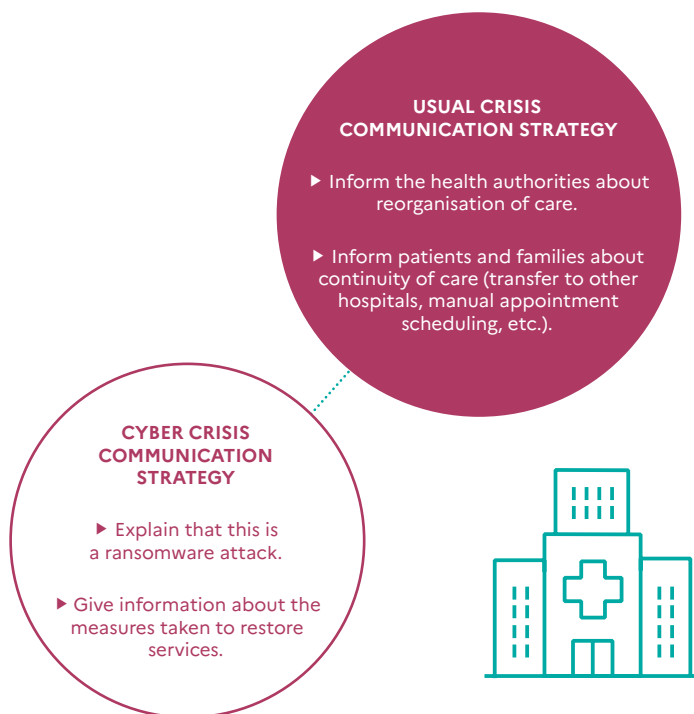
7. Tools and organisation



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.).

its office automation system:



STEP 4

INTEGRATING THE COMMUNICATION FUNCTION WHEN ORGANISING CYBER CRISIS MANAGEMENT

within the first few hours. As a communicator, you have several roles

To alert:

To react quickly:

different audiences, both internal and external, must be constructed

To analyse and adapt:

This means a detailed analysis of the way different audiences perceive

► **Strategy unit**

be included here, as decisions affecting the image and reputation of an

► **Operational and technical units**

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
DoS website
defacement

services, sometimes with significant financial cost. As they are

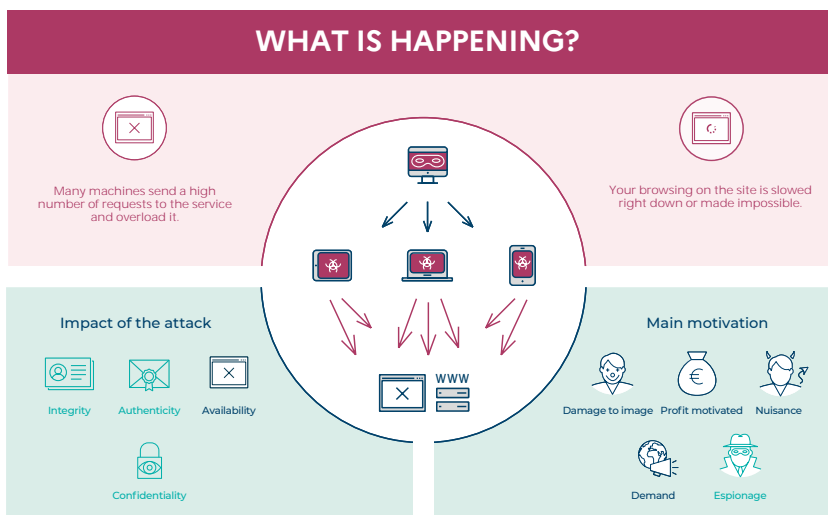
symbolic and emotional impact

**the perception of the incident
and the technical complexity**

destabilisation by stirring up a media and social frenzy.

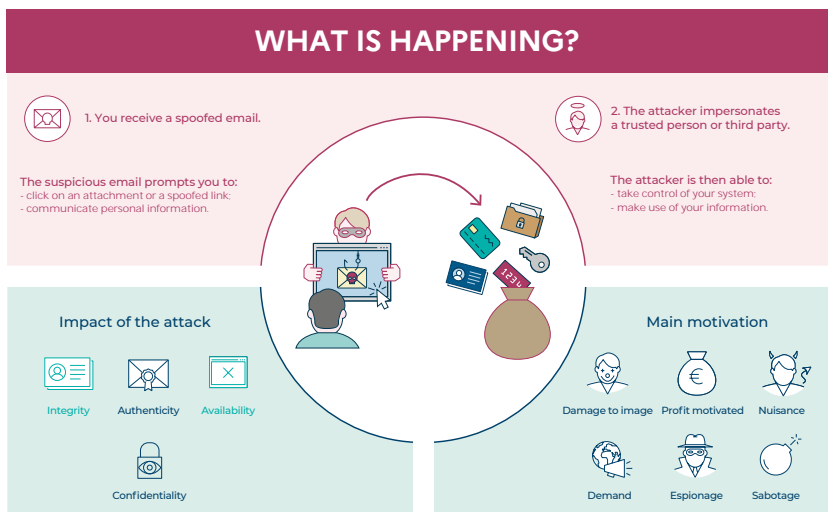
DDOS: DISTRIBUTED DENIAL OF SERVICE ATTACK

Access to the site you are viewing is disrupted



PHISHING

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



STEP 5

ORGANISING CRISIS COMMUNICATION

Depending on the size (communications team or single contact communication), you should pre-determine a specific crisis

- ▶ **Coordination:** a communication representative attends the briefings

- ▶ **Monitoring and perception:**

- ▶ **Reaction:**

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.

"REFERENT"
COMMUNICATOR
(CRISIS COMMUNICATION
SM0165 (IALISC)5 T
COMMUNICATIOS()/C2121



STEP 6

CREATING A DEDICATED TOOLBOX FOR CYBER CRISIS MANAGEMENT

- ▶ **The crisis communication strategy**
- ▶ **crisis management system**
- ▶ **Steering tools:** a press file, account login credentials (social
- ▶ **A glossary**

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

- ▶ **A clear and instructive definition of the most commonly occurring computer attacks:** DoS, ransomware, defacement. This definition (unavailability, potential data exfiltration and publication, loss of
- ▶ **A list of questions to anticipate:** has a complaint been filed? Do we

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

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

of your organisation and your tools in the face of a major attack that

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

- ▶ **A general exercise:**

adequacy and effectiveness of the processes for dialogue between different units.

- ▶ **An exercise solely dedicated to communication:**

- ▶ **An exercise with external participants:**

(sector-specific regulator, customers, etc.).

Exercises are effective when they go hand in hand with training

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

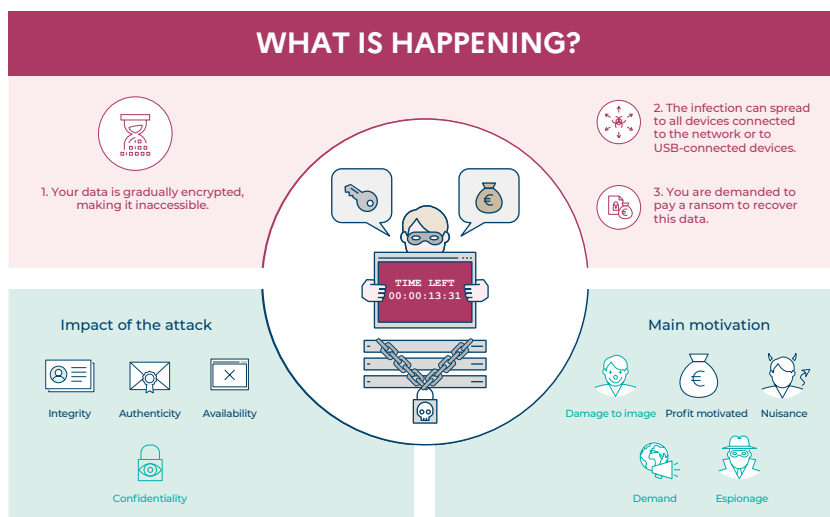
DEALING WITH A RANSOMWARE ATTACK

Ransomware attacks⁹

affect any entity, regardless of its activity, nature or size. In terms of attack is visible, with immediate effects (unavailability) and sometimes

RANSOMWARE

Your data is held hostage



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

► **Tempo:**

technical and managerial teams, especially since the attackers often opt for periods with reduced staff numbers (weekends, public holidays,

In contrast, the remediation time remains long, with an often

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 can affect staff. Some cyber criminal groups are quick to establish



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:

(press file, access to social network accounts or website, emails, etc.) makes it more difficult to implement communication actions swiftly,



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)



STEP 1

INTEGRATING THE CRISIS MANAGEMENT UNIT

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:**
effects on the business lines and services/tools of your organisation.
- ▶ **Sharing your reflection process within the area of expertise that is communication:**

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).

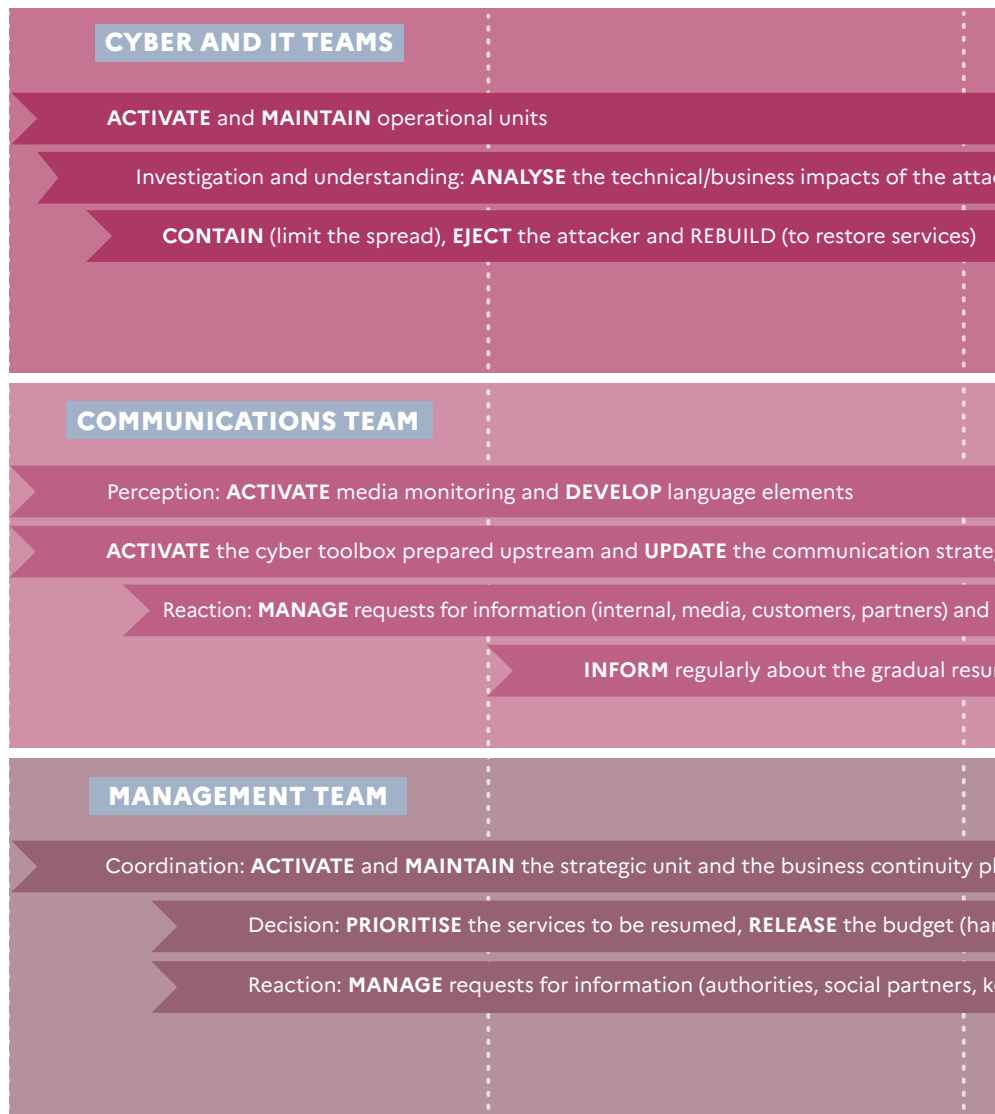


THE TIMELINE OF A RANSOMWARE ATTACK

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

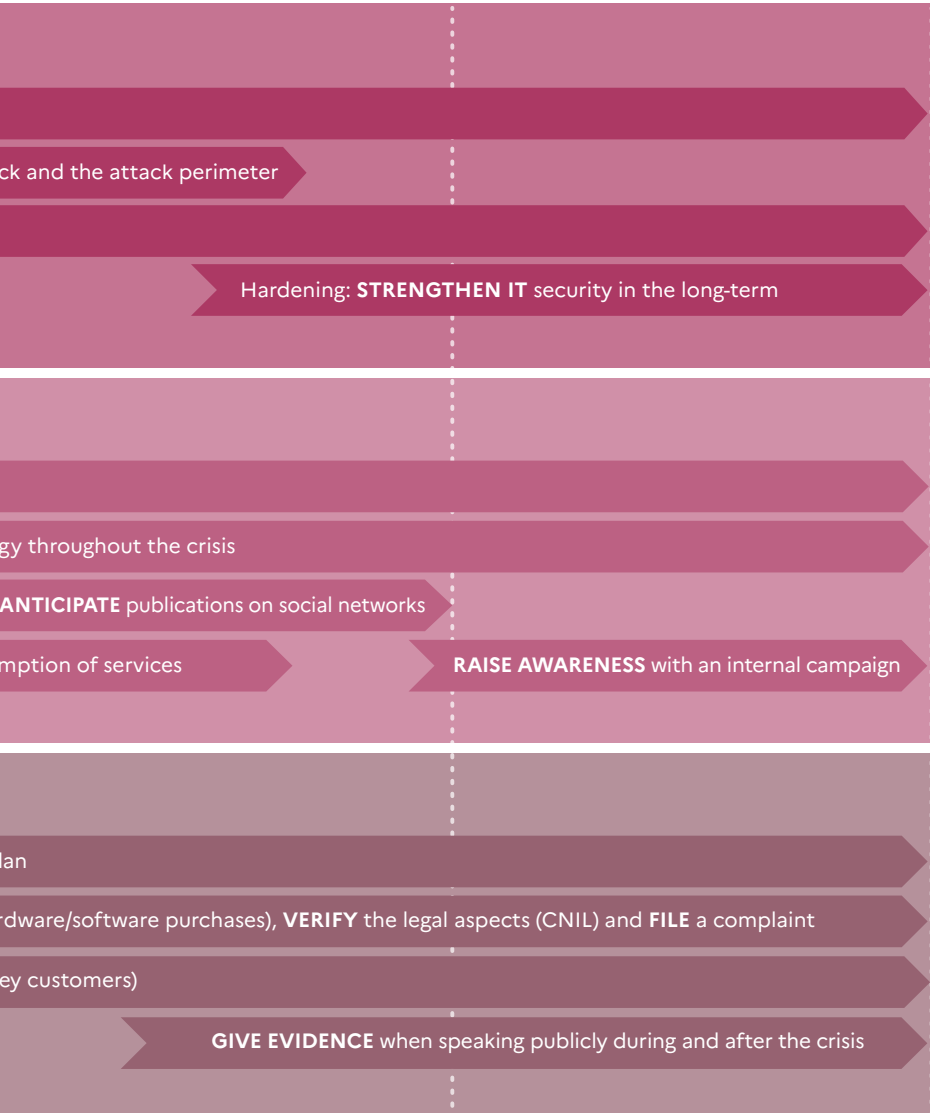
ONE ATTACK, THREE TEMPOS

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



CARRYING OUT YOUR RISK ANALYSIS REGARDING COMMUNICATION

- ▶ **Facts established:**

of exposure to the crisis suffered by your company in the short and

- ▶ **Context:**

First and foremost, this task is a cost/benefit analysis which requires,

EXAMPLE OF AN ESPIONAGE TYPE COMPUTER ATTACK

A cyber attack is not necessarily visible. Ransomware is just one

approached differently, especially if the attack was detected by chance



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

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**

- ▶ **The technicality of the information may also vary depending on the audience.**

and show more of an instructive approach. Even when simplified, the

- ▶ **The pace of information transmission.**

visibility at each key stage, following the “battle rhythm” defined for

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



this means for the customers or users affected and the actions they



to give too firm a resolution date: the complexity of computer attacks



filing a complaint with specialist gendarmerie or police services.

The tone of your communications can also change with the crisis:

Note that if the incident involves legal jurisdiction, certain specific competent investigating authority. In the event of a significant

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

- ▶
- ▶
- ▶

- ▶ **technical teams;**
- ▶ **general management;**
- ▶ **professional roles in contact with external interlocutors**
- ▶ **stakeholders**

WHO ULTIMATELY HAS A COMMUNICATION ROLE?

Overview of the different lines of communication: objectives,

Communication

- ▶ Message:
- ▶ Audience:
- ▶ Medium:

Technical teams

- ▶ Message:
- ▶ Audience:

- ▶ Medium:

General management

- ▶ Message:
- ▶ Audience:
- ▶ Medium:

Other professionals

- ▶ Message:
- ▶ Audience:
- ▶ Medium:

Other stakeholders

- ▶

- ▶ Sector-specific authorities, customers, partners and service providers:

STEP 5

SUPPORTING INSTITUTIONAL 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

Internal communications

► **Goal:** to reassure and explain the situation. In the event of major work

► **Tools:**

► **Your messages:**

-

-

External communications

► **Goal:**

► **Tools:**

► **Your messages:**

-

-

TYPICAL QUESTIONS TO ANTICIPATE FROM JOURNALISTS

more specifically in computer security.

Overview of typical questions asked by specialist journalists:

- ▶
- ▶ What are the direct consequences (technical, financial)? What are
- ▶
- ▶
- ▶
- ▶ Has a complaint been filed? Has a GDPR declaration to the
- ▶
- ▶
- ▶

STEP 6

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

go to the ANSSI and [Cybermalveillance.gouv.fr](https://cybermalveillance.gouv.fr) websites to find

RECOMMENDATIONS FOR DEALING WITH RANSOMWARE

Recommendations

- ▶
- ▶ keep software and systems up to date;
- ▶ use anti-virus software and keep it updated;
- ▶
- ▶
- ▶
- ▶
- ▶

Existing resources

- ▶ 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?
- ▶
- ▶

CHECKLIST

☐ **Start preparing**

☐ **Contact**

☐ **Integrate**
global crisis management system to support staff teams and

☐ **Take an interest**
influencers, news, vocabulary.

☐ **Practise**

☐ **Approach**

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

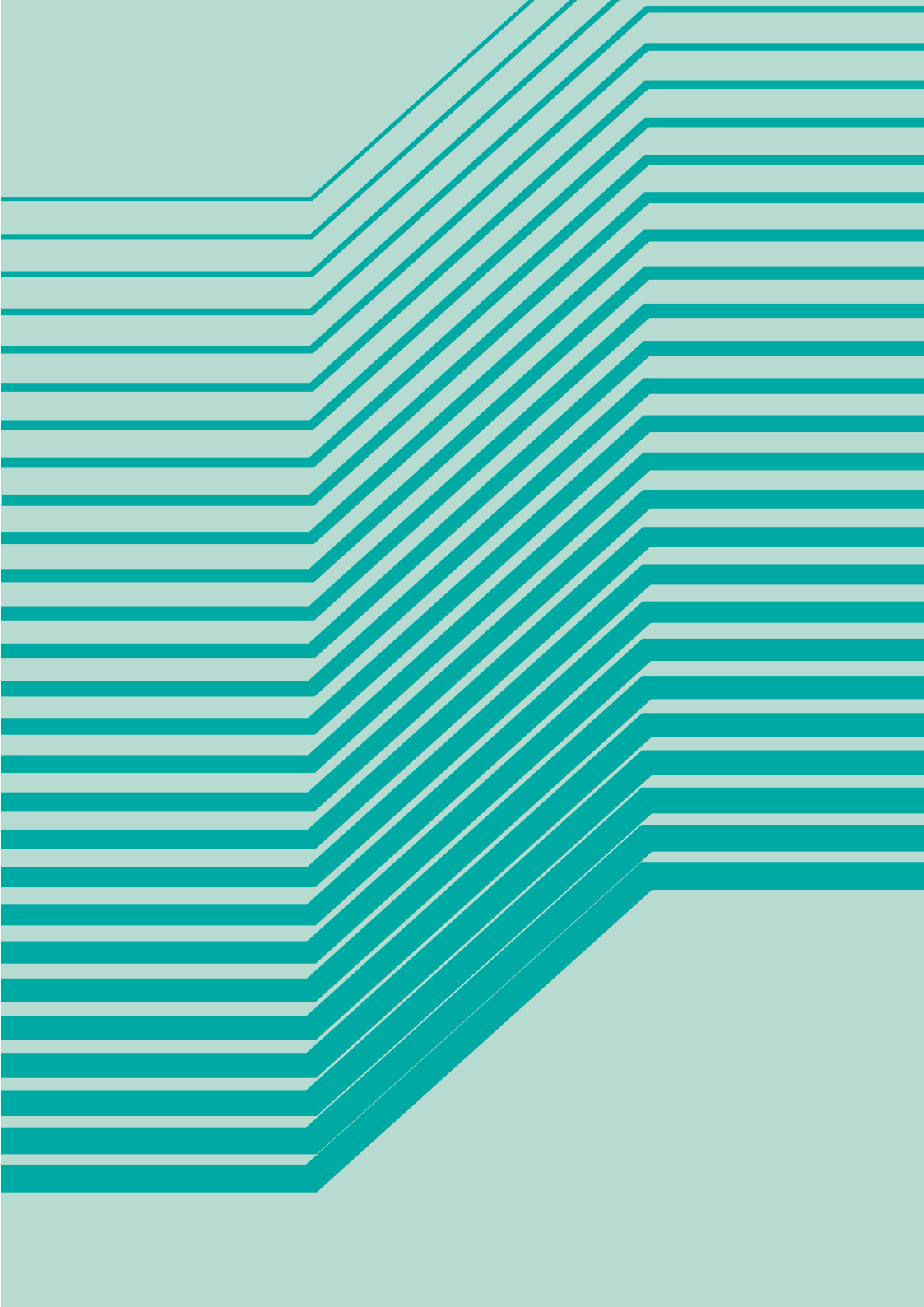
ATTACKERS: equates to the attacker's signature, the method of operation they use to target and attack their victims.

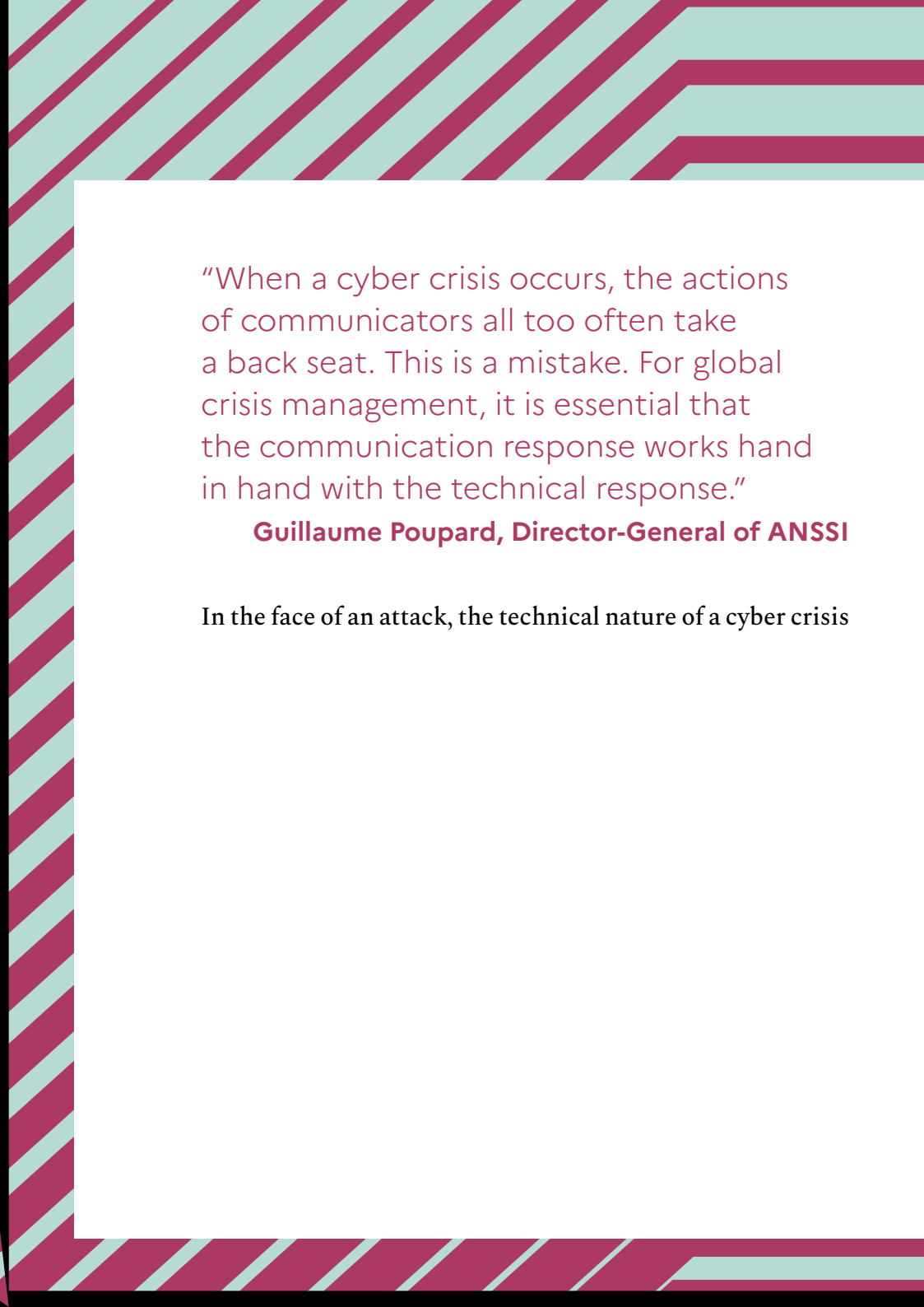
GENERAL DATA PROTECTION

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.





“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