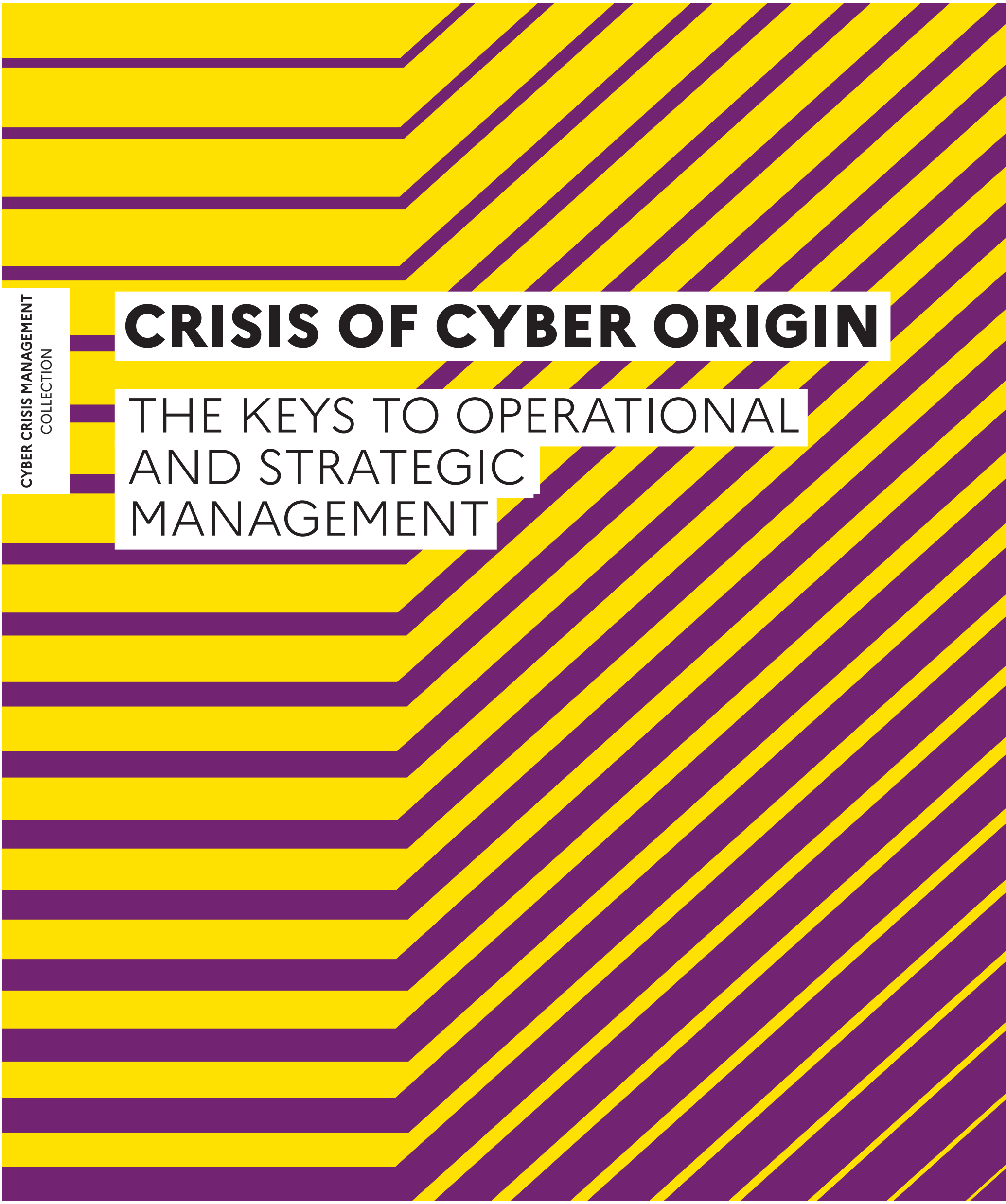
RÉPUBLIQUE
FRANÇAISE
Liberté
Égalité
Fraternité

AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION
ANSSI



CYBER CRISIS MANAGEMENT COLLECTION

CRISIS OF CYBER ORIGIN

THE KEYS TO OPERATIONAL AND STRATEGIC MANAGEMENT

CDSE
CLUB DES **DIRECTEURS**
DE **SÉCURITÉ**
DES ENTREPRISES

CYBER CRISIS MANAGEMENT
COLLECTION

GUIDE

CRISIS OF CYBER ORIGIN

THE KEYS TO OPERATIONAL AND STRATEGIC MANAGEMENT

CONTENTS

EDITORIAL

Let's start with a hint of controversy. I could say that there are two types of organisations: those that have already been the victims of a cyber attack and those that probably soon will be. In recent years, many organisations have invested heavily in protecting and defending their information systems and their digital services. Ever greater consideration is therefore given to cyber risks. This is excellent news for our collective security!

But to ensure their resilience, organisations must realise that these efforts are not always enough… And ensure they are fully prepared for the possibility of an attack. Nowadays, data theft and the partial or total paralysis of digital services have critical operational, legal, financial or reputational impacts. It is not possible to improvise a response in the middle of a disaster! Preparation, tooling and training are essential to maintain activity in the event of a cyber attack. And this applies not only to cyber experts but throughout the organisation, by involving business departments, directors and employees.

This guide, the result of the experience of officers from the French National Cyber Security Agency (ANSSI) and members of the Company safety and security directors' club (*Club des Directeurs de Sécurité et de Sûreté des Entreprises, CDSE*), will help you to make cyber crisis management the backbone of your resilience strategy.

I will end by giving my thanks to Bouygues Construction, the Nord-Ouest Hospital in Villefranche-sur-Saône and CMA CGM. Having suffered cyber attacks, these organisations have shared their experience with us to illustrate the recommendations of this publication and offer readers a more concrete understanding of cyber crisis management. Thank you for sharing these valuable testimonies with us!

Guillaume Poupard
Director-General of ANSSI

Prepare and respond effectively… This approach, presented in this guide, could be a leitmotif for the CDSE. It is true that the cyber threat has intensified, with an increasing number of more sophisticated, more formidable attacks. It is also true that cyber security is not always the priority for organisations, when in fact it is essential to always remain alert and to dedicate significant resources to it. Yet in this ocean of doubts and vulnerabilities, at least one certainty remains: with the dissemination of best practices, passed on by safety and security directors and experts in corporate information system security, a calmer, more relaxed approach can be adopted when anticipating the spread of a computer virus.

In terms of French and European digital sovereignty, service providers and digital solution providers are now realising that the time has come to take action. They now know that the price, functionality and ergonomics of their solutions must be in line with their foreign competitors. It is therefore cause for celebration that the national champions of the digital sector, French microenterprises, SMEs and start-ups, now represent a large "united cyber front", which will gain its market share only if it is efficient and competitive.

Faced with adversity and the exponential growth of the cyber threat, we need to arm ourselves with a protective shield and build robust digital security. The recommendations given in this guide are part of a more global anticipation strategy for the implementation of this protection.

To prepare and respond effectively, reading this guide is therefore a matter of public health!

Stéphane Volant
President of the CDSE

INTRODUCTION

Presentation

What is this guide for?

Given the destabilising nature of a crisis of cyber origin, the aim of this guide is to share best practices and recommendations useful to any organisation, firstly to ensure they are well prepared, and secondly to help manage the crisis step by step. These recommendations are based on feedback from public and private organisations that have been targeted by a cyber attack and that have shared with ANSSI the difficulties and successes of their crisis management.

By definition, cyber crisis management involves technical concerns, including the cyber and technological components required to return to optimal security conditions. However, it also involves more strategic concerns, including in particular maintaining the activity of the business lines affected by the crisis. To enable stakeholders to understand these different concerns and facilitate the decision-making process, this guide offers advice for each approach.

Who is it for?

These recommendations are intended for specific but complementary roles in the cyber crisis management decision-making process: executives, security officers, risk managers, business continuity or crisis management managers, digital managers, chief information security officers, business departments, civil servants in security and defence, and any other person whose involvement is required for the management of a cyber crisis.

What are the prerequisites?

This guide is based on the assumption that the organisation already has a global digital risk management scheme including components for governance, protection and the defence of its information systems, or IS (network segregation, cyber security solutions, offline backups, detection and protection tools, dedicated technical teams, etc.), providing it with a resistant security foundation adapted to the cyber risks involved in its activities. It also assumes that within the organisation there is a general crisis management scheme and tools dedicated to managing the impacts[1] (alerting mechanisms, crisis room, operational and decision-making scheme, management tools, business continuity and disaster recovery plan, etc.) contributing to the resilience of the organisation.

The ANSSI *Guideline for a healthy information system in 42 measures* and *Controlling the digital risk* guide are references on issues relating to the securing and resilience of the IS.[2]

How to use it?

This guide suggests adapting crisis management tools and schemes to a cyber scenario. The recommendations presented can be broken down according to the components involved ("strategic" and "cyber and IT operational" components) if they have different crisis management objectives. It focuses on elements considered essential to the crisis response and is not intended to be exhaustive.

[1] The family of AFNOR standards around societal resilience, and more specifically standard ISO 22301:2019 on business continuity management and standard ISO 22320:2018 on incident management are references for the definition of this crisis scheme.

[2] www.ssi.gouv.fr/en/guide/40-essential-measures-for-a-healthy-network/ and www.ssi.gouv.fr/en/guide/controlling-the-digital-risk-the-trust-advantage/

Challenges in preparing for the management of a crisis of cyber origin

What is a cyber crisis?

A "cyber" crisis is defined by the immediate and major destabilisation of the day-to-day operation of an organisation (halt to activities, inability to provide services, heavy financial losses, major loss of integrity, etc.) due to one or more malicious actions on its digital services and tools[3] (cyber attacks such as the use of ransomware, denial of service, etc.). Such events therefore have a considerable impact, which cannot be dealt with through usual processes and within the framework of the normal operation of the organisation. From this point on, we will refer to this as a "cyber crisis".

Accidental events, in other words those which are not the result of malicious activity on the IS, and malicious actions not resulting in immediate and major interruption to the organisation's essential services, are therefore excluded from the scope of the definition. However, the recommendations of the guide can be used as good practices for dealing with such situations.

Specific aspects of a cyber crisis

Compared to other crisis scenarios, cyber crises have their own specific characteristics which is it important to understand:

- Effects on two different levels, with immediate impacts and a longer-term remediation that can last for several weeks, or even months.
- Not limited to a single location, which implies a potential spread to other organisations due to interconnections between the IS.

[3] With which the organisation's information systems and those of its service providers are associated.

- A threat that is adapting to containment and remediation measures.
- Uncertainty with regard to the scope of the compromise.
- Complexity in understanding the attacker's objectives and in attributing the origin of the attack.

As decision-making teams get used to cyber issues, this should facilitate both a good understanding of the specific implications of the cyber crisis on the entity's activity and the integration of the operational component into the crisis scheme.

"The first alerts were raised by foreign countries very early in the morning. When we lost central supervision, we decided to shut down the IS worldwide! An *ad hoc* crisis unit was mobilised and several hundred people were directly involved in resolving the incident."

Bouygues Construction

"The alert was quickly raised by the on-call IT team, allowing us to go to the data centre to shut down the IS and stop the spread of the attack. Doctors subsequently had to return to a completely paper-based management method to follow up on patients."

The Nord-Ouest Hospital - Villefranche-sur-Saône

"As soon as our teams in Asia raised the first alerts, we launched our incident response plan and created a crisis unit. The decision to cut off the IS was taken quickly in order to stop the spread, determine the impact and start the investigations. The cyber, IT and business teams were mobilised in order to quickly restore access to the group's essential functions."

CMA CGM

PART 1

PREPARING TO FACE A CYBER CRISIS

The imbalances brought about by a cyber crisis force organisations to adapt and operate in unusual ways. These sudden upheavals, of uncertain duration, are a source of stress and complicate decision-making, when remedial actions must be decided and executed quickly to limit the impacts.

Crisis management therefore requires good preparation through the implementation of proven processes and tools. The objective is to ensure a smoother process and to adopt automatic reflexes making it possible to respond effectively in the long term and to restore trust to the teams and the ecosystem affected directly or indirectly by the consequences of the incident.

The aim of this first part is to help entities to build a resilient crisis organisation, limiting the impacts of the cyber crisis, maintaining the trust of the ecosystem, prioritising and keeping the affected critical activities in degraded mode. More specifically, it offers practical advice for adapting crisis management schemes and tools (crisis management unit, dedicated logistical resources, reaction and business continuity plans, etc.) to the specific impacts of a cyber crisis.

FACT SHEET 1
KNOWING AND CONTROLLING YOUR INFORMATION SYSTEMS

The first challenge for any crisis management team is to be able to assess the extent of the event's impact on the scope of the organisation.

In a cyber crisis, it is therefore essential to be able to identify and characterise the scope of the compromise, in other words the path taken by the attacker to enter and spread through the IS, as well as the impact of an attack on the entity's digital services and business continuity. As a minimum, it is recommended to have the following elements to allow the technical teams (cyber and IT) to conduct these investigations:[4]

- A list of critical applications and services provided by the organisation.
- A mapping of the systems on which critical business services rely and are interconnected.
- A mapping of IS peripheral devices.
- A list of IS interdependencies between the business lines and external partners (partners, subcontractors, outsourcers, etc.).
- A mapping of the stakeholders with the points of contact (in particular if the IS are partially subcontracted).[5]
- A list of supervision and detection resources and their scope.
- A conservation policy for application and network logs.
- An information flow matrix.
- The network and functional element architectures, linking the IS and the business processes.

[4] The use of the *Mapping the information system* guide is recommended for this action: www.ssi.gouv.fr/uploads/2019/04/mapping_the_information_system-anssi-pa-046.pdf
[5] The use of workshop 3 of the EBIOS Risk Manager method is recommended for this action: www.ssi.gouv.fr/uploads/2019/11/anssi-guide-ebios_risk_manager-en-v1.0.pdf

	STRATEGIC COMPONENT	CYBER AND IT OPERATIONAL COMPONENT
OBJECTIVE 1	**Mapping your critical business applications and resources**	**Mapping your IS**
RECOMMENDATIONS	A map of the critical services, applications and activities as well as essential data is kept updated and backed up offline in order to identify the **assets** to be protected and monitored as a priority and/or to be restarted in the event of a crisis. **The business impact assessment** can be used to help identify the organisation's critical resources. As a minimum, a list of critical services and associated applications is available offline.	A map of the main technological assets and their dependencies is kept updated and backed up offline to facilitate digital investigations. If all or some digital services are outsourced, a map with the interconnections is kept updated and available offline. Emergency contacts for service providers are available offline.

"It is essential to have an up-to-date view of digital assets, including those linked to critical activities or hosting sensitive or regulated data. This allows actions to be prioritised when not everything can be saved or isolated. It is also important to know which employees manage which systems, because they are often the only ones who can take the precise actions required. Finally, knowing your customers and partners means you can communicate with them in the event of a failure or security problem."

CMA CGM

FACT SHEET 2

CREATING AN OPERATIONAL CAPACITY FOUNDATION TO ENSURE AN APPROPRIATE LEVEL OF DIGITAL RESILIENCE

An organisation is considered resilient if, in the event of a cyber crisis, it is able to maintain its most critical activities (if necessary in degraded mode, or even without digital tools and services available) and restart them in a controlled manner so as to limit the impacts of the attack on the organisation, its activity sector and its customers, thus retaining the trust of the ecosystem.

For this reason, it is important for the organisation to have put in place operational methods and resources adapted to cyber crisis scenarios, which will be used to maintain or restore its critical activities. Significant educational work will have to be carried out by the cyber and IT teams with the business lines in order for them to take into account the cyber impacts and adapt their working practices and processes (in particular maintaining their activities without digital tools and services).

These practices and the crisis management scheme can be adapted by taking into account **reference cyber scenarios**, identified through an analysis of the strategic risks.[6]

[6] The use of workshop 3 of the EBIOS Risk Manager method is recommended for this action: www.ssi.gouv.fr/uploads/2019/11/anssi-guide-ebios_risk_manager-en-v1.0.pdf

	STRATEGIC COMPONENT	CYBER AND IT OPERATIONAL COMPONENT
OBJECTIVE 1	**Adapting the business continuity plan to the cyber crisis scenario** **The business continuity plan (BCP)** comes into play above all for unique scenarios in which key resources (human, IS, industrial systems, service providers or buildings) are unavailable. In a cyber crisis, the BCP must take into account the unavailability of multiple resources simultaneously, or even an activity without digital tools and services (encrypted servers, total shutdown of systems in order to avoid the spread of the attack, etc.).	
RECOMMENDATIONS	The BCP includes the analysis, evaluation and processing of digital and cyber risks, and takes into account in particular a total loss or highly-degraded operation of the organisation's critical services and processes. Business continuity solutions are envisaged in conjunction with the cyber and IT teams. BCP-related measures, such as the **maximum tolerable downtime** and the **work recovery time**, are defined taking cyber scenarios into account. It should be noted that the impacts of a cyber crisis can sometimes distort the measures defined upstream. Operational business systems are envisaged, maintaining the operation of the organisation's critical processes at a minimum threshold. The scope of the BCP also includes the loss of a cloud solution, a partner or a service provider of the entity. Cyber crisis management methods are included in outsourcing and externalisation contracts.	The cyber and IT teams support the business lines in the analysis, evaluation and processing of digital and cyber risks through educational work and an understanding of the impacts on business activity. A data backup and restoration plan is defined, with procedures for failover to a back-up network that can withstand cyber attacks. This relies on the existence of **healthy backups**. a catalogue of these backups is kept in protected storage. The risk of data inconsistency due to their synchronisation is taken into account. If digital tools and services are unavailable, business continuity solutions[7] are defined, tested and updated. The cyber threat assessment[8] is regularly reviewed and used as a basis for reflection on the resilience of the solutions and processes in place.

[7] Preferably qualified by ANSSI: www.ssi.gouv.fr/entreprise/qualifications/produits-recommandes-par-lanssi/les-produits/ (French only)

[8] CERT-FR alerts and reports are reliable and detailed sources on this subject: www.cert.ssi.gouv.fr/

OBJECTIVE 2

Producing a disaster recovery plan for the cyber scenario

Produced in addition to the BCP, **the disaster recovery plan (DRP)** ensures that the digital infrastructure is reconstructed and that an organisation's strategic applications are restarted in the event of a disaster. In a cyber crisis, the DRP must take into account the partial or total unavailability of digital infrastructures and the prioritisation of remediation actions.

RECOMMENDATIONS

The business lines define the **recovery time objective** for each service, incorporating a long downtime linked to the cyber scenario.

- A schedule of priority actions to restart digital services and restore business activity in the event of a crisis is formalised.
- In particular, the reconstruction of the **Active Directory**, servers, workstations, **domain name system** (DNS), **public key infrastructure** (PKI), **or any critical infrastructure,** is planned in order to restore services within an acceptable time frame.
- Failover procedures to a back-up network are formalised and tested.
- Data restoration and IS reinstallation processes are formalised and tested.

> "A formalised incident response plan, associated with threat scenarios, serves as a reference for the teams to align and coordinate their actions in order to save precious time throughout the crisis.
> It formalises schemes and processes so that actions are considered in the right order and relevant questions are raised early enough.
> It also includes tools and procedures, as well as the roles and responsibilities of each party."

CMA CGM

OBJECTIVE 3	**Putting in place resilient crisis management tools** The partial or total unavailability of digital tools and services makes any communication between the different entities of the organisation difficult. The crisis units must therefore have "back-up" tools to ensure, at the very least, the operation of the crisis scheme.	
RECOMMENDATIONS	• Cyber crisis management procedures are put in place and stored offline. • A crisis directory of internal and external stakeholders (including hierarchical and geographical contacts, outsourcers, suppliers, authorities) is stored offline. • Digital tools dedicated to the crisis unit are planned to be accessible offline. They are maintained in operational conditions. • Alternative means of communication,[9] both internal and external, are identified and tested.	• Crisis management procedures are put in place and stored offline. • A crisis directory of internal and external stakeholders is stored offline. • Offline digital tools dedicated to the crisis unit are put in place, in particular for carrying out digital investigations. • Alternative means of communication[10], both internal and external, are identified and tested.

"Alternative communication channels must be put in place when the nominal communication systems (telephone, email) are no longer operational. It is essential to have crisis directories disconnected from the IS in order to quickly add stakeholders to the information loop."

The Nord-Ouest Hospital - Villefranche-sur-Saône

[9] Preferably qualified by ANSSI: www.ssi.gouv.fr/entreprise/qualifications/produits-recommandes-par-lanssi/les-produits/ (French only)

[10] *Ibid.*

FACT SHEET 3
FORMALISING A CYBER CRISIS COMMUNICATION STRATEGY

Depending on its size, an organisation affected by a cyber crisis may quickly be confronted with internal and external pressures (media, customers, partners) likely to affect its reputation.

Firstly, it is therefore important for communication to be incorporated into the crisis management scheme to support the teams when they warn and advise the stakeholders (customers, suppliers, media, authorities, etc.) as soon as possible and to preserve the reputation (media, financial, legal, etc.) and trust in the organisation.

Secondly, tools and procedures must be prepared in advance of any crisis so as to anticipate the reactions, questions and perceptions of all the stakeholders, and provide the most appropriate communication on what is a technical matter.

	STRATEGIC COMPONENT	CYBER AND IT OPERATIONAL COMPONENT
OBJECTIVE 1	**Drawing up a list of stakeholders to be contacted**	
RECOMMENDATIONS	A list of the stakeholders to be warned[11] (partners, authorities, customers, etc.) is pre-identified, with the contacts and back-up communication channels to be used. An emergency contact is identified in contracts with the most critical customers and suppliers. A press file is available and stored offline.	A contribution on the mapping of stakeholders to be warned is envisaged.

[11] Depending on the legislation in force and the status of the organisation: www.ssi.gouv.fr/en-cas-dincident/ (French only)

	STRATEGIC COMPONENT	CYBER AND IT OPERATIONAL COMPONENT
OBJECTIVE 2	**Anticipating the crisis communication strategy**	
RECOMMENDATIONS	A communication strategy and a cyber communication plan are formalised and validated in order to maintain trust and to facilitate the definition of the communication stance and the organisation of teams during the crisis. Standard messages are formalised based on identified reference cyber scenarios, serving as turnkey responses in order to save time. Teams are familiarised with and trained in cyber crisis communication and provide regular training to officers and managers of the entity.	An initial media risk analysis is based on reference cyber scenarios. This analysis facilitates the construction of language elements relating to technical business lines. Several media subjects specific to cyber issues are to be anticipated (e.g. attribution for the attack). The content of the messages is reviewed with the communication teams in order to check the credibility of the formalised technical elements. Communication channels that can be used in the event of a crisis, including should conventional tools (emails) be unavailable, are identified in order to reach the various targets.

"We immediately integrated the communication department into the crisis unit. They were present from the very first hours, and able to get direct access to the information. They therefore saw and understood what was happening and were able to establish a communication strategy in response to all internal and external requests."

Bouygues Construction

FACT SHEET 4

ADAPTING YOUR CRISIS ORGANISATION TO THE CYBER SCENARIO

The specific nature of a cyber crisis scenario requires the mobilisation of business, cyber and IT profiles, as well as ensuring correct coordination between the different levels. A crisis organisation should therefore be planned prior to any event with the role of each party agreed, in order to facilitate mobilisation.

The crisis scheme to be established consists of a strategic component, supported as a minimum by a "strategic" or "decision-making" crisis unit. It brings together the representatives of the decision-makers within the entity, who take on the usual roles of a crisis unit: crisis director, people responsible for information management, crisis management support, communicators, etc.

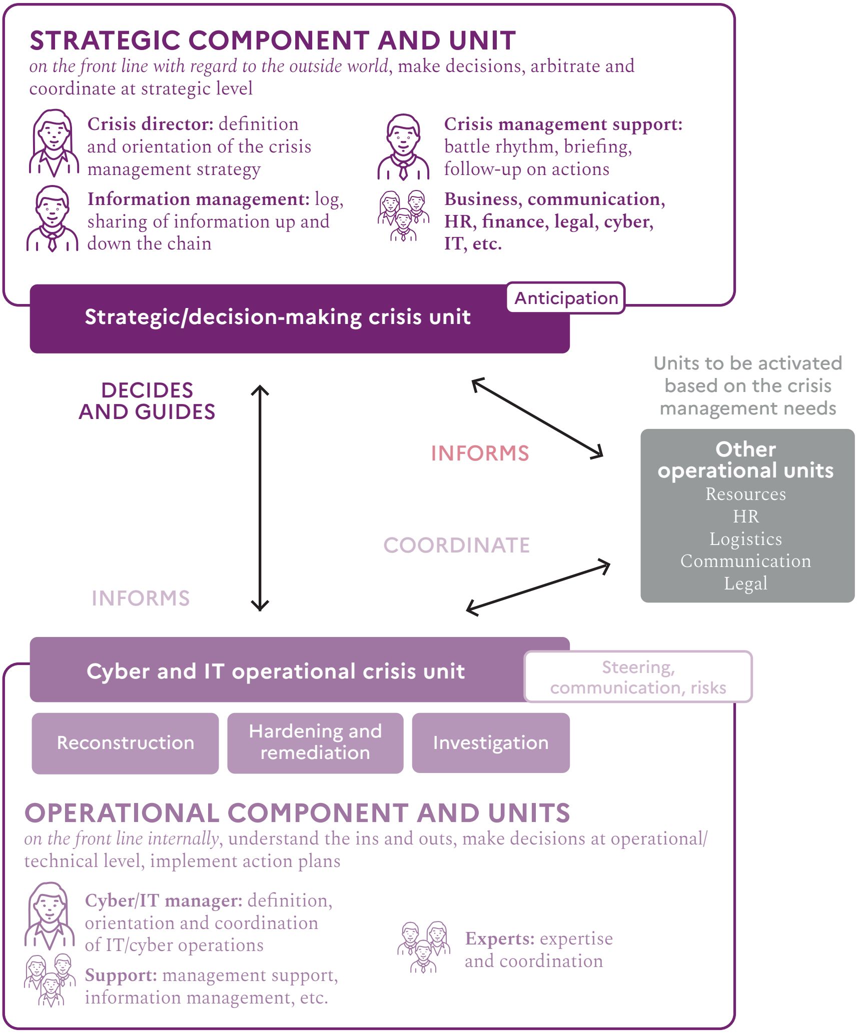
An operational component is also put in place. Within the organisation, the cyber and IT roles are responsible for managing one or more units, and for exchanges with the strategic unit.

Depending on the impact of the crisis to be managed, other units may also be put in place: business units, communication unit, HR unit, logistics unit, legal unit, cyber and IT operational crisis unit, etc.

"We implemented agile organisation around the partnership formed by our DGA and the CIO and "task forces", enabling us to respond quickly depending on the emergencies. A "resource unit" was responsible for bringing together service providers and reinforcements, helping our teams to focus on their core business."

Bouygues Construction

PROPOSAL FOR CYBER CRISIS MANAGEMENT ORGANISATION[12]



STRATEGIC COMPONENT AND UNIT

on the front line with regard to the outside world, make decisions, arbitrate and coordinate at strategic level

Crisis director: definition and orientation of the crisis management strategy

Information management: log, sharing of information up and down the chain

Crisis management support: battle rhythm, briefing, follow-up on actions

Business, communication, HR, finance, legal, cyber, IT, etc.

Strategic/decision-making crisis unit

Anticipation

Units to be activated based on the crisis management needs

Other operational units
Resources
HR
Logistics
Communication
Legal

Cyber and IT operational crisis unit

Steering, communication, risks

Reconstruction

Hardening and remediation

Investigation

OPERATIONAL COMPONENT AND UNITS

on the front line internally, understand the ins and outs, make decisions at operational/ technical level, implement action plans

Cyber/IT manager: definition, orientation and coordination of IT/cyber operations

Support: management support, information management, etc.

Experts: expertise and coordination

[12] Note that this organisation is particularly suited to large groups. However, it can also apply to smaller entities.

	STRATEGIC COMPONENT	CYBER AND IT OPERATIONAL COMPONENT
OBJECTIVE 1	**Implementing criteria and procedures for the activation of crisis units**	
RECOMMENDATIONS	The activation and deactivation criteria are established based on the defined reference cyber scenarios and are used to set the objectives for the mobilisation and demobilisation of a strategic unit. These criteria are known to the members of the scheme. A chain of alert is formalised. Several modes are anticipated, including an "alert" mode and a "crisis" mode. A cyber crisis management repository including a description of the entire crisis scheme (organisation, governance, resources, tools, directory) is formalised, promoted and kept updated. The organisation's decision-makers are made aware of cyber issues. Cyber and IT roles are systematically represented in crisis governance (cyber and non-cyber).	An incident alert, management and response process incorporating a "digital security" component is formalised and tested. It is based in particular on incident detection and management tools.[13] The criteria for activating and deactivating the operational scheme are defined based on the reference cyber scenarios. In particular, they can be activated due to a threshold effect (bottom-up) or on the decision of the strategic scheme (top-down). They are known to the members of the crisis scheme and the incident management teams. A chain of alert is formalised. Several modes are anticipated, including an "alert" mode and a "crisis" mode.

[13] The incident detection and management tools qualified by ANSSI certify compliance with regulatory, technical and security requirements: www.ssi.gouv.fr/entreprise/qualifications/produits-recommandes-par-lanssi/les-produits/ (French only)

OBJECTIVE 2	Organising your cyber crisis units	
RECOMMENDATIONS	Once the members of the crisis unit have been identified, they are informed of their appointment to the scheme, their role and their missions, and receive relevant training. The scope of action of each member (roles and responsibilities) is defined in advance. A single (dashboard-like) interface is put in place to standardise the flow of information. Achievable objectives and criteria for exiting the crisis are pre-identified. Depending on the organisation's level of maturity, an anticipation component can be put in place to identify scenarios for the deterioration or improvement of the situation. If required due to the geographical scope of the entity, international issues are taken into account (differences involving time zones, penal systems, cultures, etc.) and correspondents are identified.	A crisis organisation similar to the strategic crisis unit is defined. It incorporates key experts able to provide guidance, as well as a crisis communication correspondent. The crisis organisation in place must be as efficient as possible and does not necessarily rely on the usual internal organisation. The cyber and IT technical teams are organised in such a way as to carry out the investigation/containment, hardening/remediation and reconstruction actions. A register is put in place to monitor risks, exemptions and internal and external communication.

FACT SHEET 5
PREPARING YOUR INCIDENT RESPONSE CAPACITY

Ideally, each organisation should have an incident response unit (CERT or CSIRT).

Otherwise, it is recommended to at least put in place incident detection and response tools and to surround yourself with experts and service providers[14] to support business and cyber teams in building their capacity to detect, investigate and manage the impacts of the crisis.

Targeting or pre-contractualisation work can be carried out in advance (via framework contracts or referencing), taking into account the skills already represented within the organisation. Note that taking out a cyber insurance policy adapted to the needs of the organisation also ensures the availability of additional capacities and expertise in the event of a crisis.

It is important that the service providers identified are known to all players involved in crisis management, so that they can quickly call upon their expertise. This list must be updated regularly.

"You have to consider calling upon experts from other entities and accept that you can't do everything at once, to position the teams in the right place."

Bouygues Construction

[14] Preferably qualified by ANSSI: www.ssi.gouv.fr/entreprise/qualifications/produits-recommandes-par-lanssi/les-produits/ (French only)

	STRATEGIC COMPONENT	CYBER AND IT OPERATIONAL COMPONENT
OBJECTIVE 1	**Identifying the experts to call upon in a crisis**	
RECOMMENDATIONS	Expertise is identified and updated. It covers the following areas: ▸ Crisis management and conduct ▸ Cyber crisis communication ▸ Project management. Non-disclosure agreements are in place for all the experts called upon.	Expertise is identified and updated. It covers the following areas: ▸ Incident response[15] ▸ Security supervision[16] ▸ Technical remediation ▸ IT infrastructure ▸ Directories and privileged access (often Active Directory) ▸ Data restoration ▸ Data recovery ▸ Cloud solutions ▸ Networks ▸ Linux/Windows administration ▸ Firewall. Non-disclosure agreements are in place for all the experts called upon.
OBJECTIVE 2	**Putting in place the capacity for a strategic reaction to the various threats**	**Putting in place the capacity for a technical reaction to the various threats**
RECOMMENDATIONS	Technical memos are completed by the functional and strategic crisis management components. In particular, they include lists of actions to be carried out by the various business teams. These memos are tested during crisis management exercises. They are updated after each exercise or use in a crisis situation.	Incident detection and response tools are in place to facilitate detection and containment actions. Technical memos on containment and eradication procedures for an active cyber threat are formalised and tested.[17] In particular, ransomware attacks or denials of service are taken into consideration. Lists of actions to be carried out are formalised to help the technical teams carry out different actions.

[15] The selection of a qualified cyber security incident response service provider (PRIS) is encouraged.
[16] The selection of a qualified cyber security incident detection service provider is recommended.
[17] CERT-FR reports can enhance this approach: www.cert.ssi.gouv.fr/cti/

FACT SHEET 6

PUTTING IN PLACE APPROPRIATE INSURANCE POLICIES

The resurgence of cyber attacks and their effects on the viability of organisations is leading insurance professionals to develop a dedicated offer for cyber incidents. Just like a “traditional” insurance policy, cyber insurance is intended to top up the level of protection of an organisation’s assets.

Depending on the terms of the contract signed, the insurer can therefore support the risk management strategy put in place by the organisation. It can also assist victims of a cyber attack by giving them the benefit of expertise or providing them with financial support (reimbursement of operating losses, support for the costs of expert intervention, purchase and installation of new IS, any claims and damages suffered by third parties, etc.).

However, it should be kept in mind that a high level of digital security must be maintained at the same time, and that not all costs related to the incident can be covered. It is therefore recommended to discuss with your insurer prior to the crisis to check the damage covered by the contract in terms of reconstruction of the IS (reconstruction as is or reconstruction with strengthening), list your needs and compare the offers proposed to ensure the most suitable level of cover.

	STRATEGIC COMPONENT	CYBER AND IT OPERATIONAL COMPONENT
OBJECTIVE 1	**Adapting the insurance to the needs of the organisation**	
RECOMMENDATIONS	An inventory is carried out to identify the cover and existing policies within the organisation. An insurance policy activation threshold is defined. Its implementation is tested as part of a cyber crisis management exercise. Use of an insurance contract is subject to feedback after each activation.	Cyber risk mapping is used to facilitate the identification of exposure and the needs in terms of cover. The needs in the event of a cyber crisis are identified to complement existing operational schemes (expertise, coverage of costs, etc.). A good practice sheet is formalised to facilitate the use of the insurance policy in the event of a crisis: contacts for the insurer, storage of supporting documents, etc.

FACT SHEET 7
TRAINING AS PRACTICE AND TO IMPROVE

The organisation of cyber crisis management exercises is an effective way of making teams aware of cyber issues and learning how to deal with them. By training to deal with a series of incidents under realistic conditions, the crisis management teams involved develop the reflexes, methods and confidence to deal with them. They validate or improve their systems and practices, and also get used to interacting together, outside of the daily work environment.

The crisis management exercise[18] can take various forms (simulation, strategic exercise, technical exercise, tabletop exercise). These must be envisaged taking into account the desired objectives, the threats covered, the technical scope and the business lines involved.

A training strategy must be defined over several years to help create consistency in the different exercises while gradually ensuring greater complexity in the scenarios, the number of units involved and the scope tested. The mobilisation of partners on the tested scope must also be envisaged.

[18] The use of the *Organising a cyber crisis management exercise* guide is recommended: www.ssi.gouv.fr/en/guide/organising-a-cyber-crisis-management-exercise/

	STRATEGIC COMPONENT	CYBER AND IT OPERATIONAL COMPONENT
OBJECTIVE 1	**Defining a cyber crisis training plan**	
RECOMMENDATIONS	A crisis management training strategy is defined and exercises testing cyber scenarios are organised on a regular basis. The exercises involve different impact and threat scopes. The action plan, based on feedback from the exercise, is monitored to improve the cyber crisis scheme and the resilience of the organisation.	A cyber and IT operational training component is incorporated into the training strategy. Some exercises test the link between the operational and strategic components. The technical complexity of the exercises is adapted to the maturity of the organisation. They tend progressively towards greater realism in order to train investigation teams (Cyber Range training type).

> "Teams must be made aware of the crisis scheme through a variety of exercises and at all levels, because reflex sheets are useless if no one understands them."

CMA CGM

PART 2

RESPONDING EFFECTIVELY THROUGH THE ADOPTION OF BEST PRACTICES

In times of crisis, the teams act with the aim of limiting the impact of the cyber attack, restoring critical services within an acceptable time frame and maintaining the trust of stakeholders in the organisation. They then face multiple constraints (disorganised activity, media and political pressure, long and complex technical remediation, etc.), but can rely on the schemes, procedures and tools produced and tested before[19] the crisis to facilitate the management of the incident and deal with its impacts.

[19] The fact sheets in the first part of the guide provide the necessary insight into the tools to be put in place.

The actions of the teams are based around four main crisis phases:

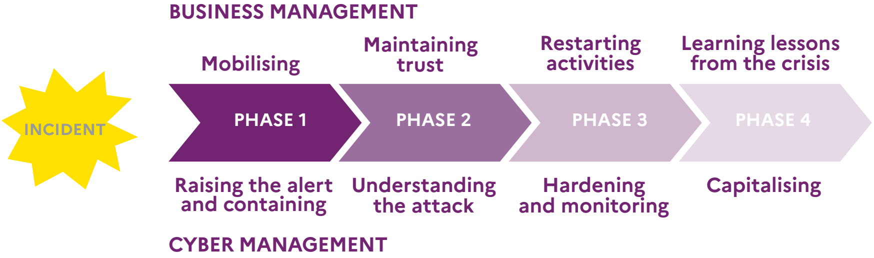
- Raising the alert, mobilising personnel and stopping the spread of the attack to protect the beneficiaries and the organisation.
- Understanding the attack pattern, ejecting the attacker, deploying measures to potentially work without digital tools and services, and communicating with their ecosystem to maintain trust.
- Hardening systems, restoring critical applications and data, and monitoring the attacker to resume core activities.
- Returning to normal and providing feedback.

The transition from one phase to another is based on criteria defined by the organisation and is accompanied by a communication plan for employees, customers, partners and if necessary the media in order to reassure them, restore trust and ensure business continuity. These phases may however overlap.

The teams involved will also have to prepare for a marathon rather than a sprint, since the crisis situation may last several weeks, with it potentially being several months before the incident is fully resolved.

Given these challenges, the aim of this second part is to introduce advice adapted to the different phases of a cyber crisis and to enable the organisation to gain trust in its management of the crisis.

CYBER CRISIS MANAGEMENT STAGES
(BUSINESS VERSUS CYBER)



BUSINESS MANAGEMENT

Mobilising

Maintaining trust

Restarting activities

Learning lessons from the crisis

INCIDENT

PHASE 1

PHASE 2

PHASE 3

PHASE 4

Raising the alert and containing

Understanding the attack

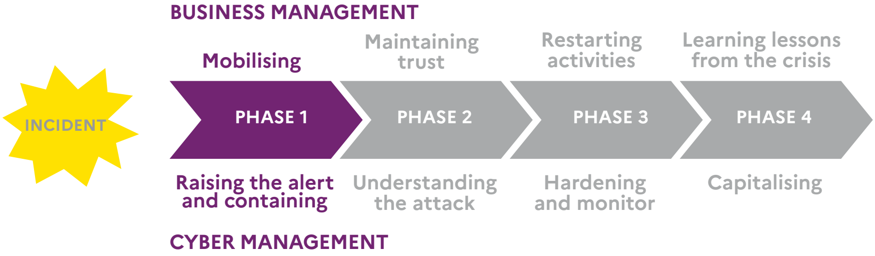
Hardening and monitoring

Capitalising

CYBER MANAGEMENT

PHASE 1

RAISING THE ALERT, MOBILISING AND CONTAINING



The detection of a major cyber incident requires the implementation of initial safeguard measures. Above all, though, it means mobilising the organisation's crisis management structure, which can bring together both a strategic unit and several operational units (HR, logistics, communication etc.).

During this first phase, three main objectives must be achieved:

- Mobilising and adapting the crisis system to the issues and the pace of the cyber crisis (fact sheets 8 and 10).
- Implementing the initial **containment** and business continuity measures (fact sheet 9).
- Warning the support networks (fact sheet 11).

FACT SHEET 8
ACTIVATING YOUR CYBER CRISIS SCHEME

The impacts following one or more cyber incidents may require the activation of the crisis scheme.

This activation is decided by the strategic component (top-down activation) based on pre-determined criteria. However, the operational scheme can be mobilised (bottom-up activation) without the strategic component if immediate actions are required to manage the incident.

At this moment, the main intention of the people mobilised must be to unite the personnel around a common objective: managing the impact of the crisis within the organisation. They must then work together to identify a response and defence plan, based on the technical and business requirements.

	STRATEGIC COMPONENT	CYBER AND IT OPERATIONAL COMPONENT
OBJECTIVE 1	**Deciding on the activation of a crisis unit**	**Warning the crisis management teams of the situation**
RECOMMENDATIONS	The organisation's decision-makers are made aware of the incident via the chain of alert and analyse the impact of the cyber attack on the organisation's business continuity. Based on pre-determined criteria, they decide to trigger a "state of crisis". They also define the criteria for an exit from the crisis in conjunction with the business, cyber and IT teams.	The teams in charge of incident management rely on the cyber crisis activation criteria to trigger the alert process and inform the organisation's decision-makers.

	STRATEGIC COMPONENT	CYBER AND IT OPERATIONAL COMPONENT
OBJECTIVE 2	**Mobilising the teams**	
RECOMMENDATIONS	Once the state of crisis is triggered, the strategic unit is set up. The members identified in accordance with the criteria and procedures defined in advance come together, and adopt the role they will perform during the crisis. Permanent contact with the cyber and IT operational teams is established. An initial inventory of the situation is produced on mobilisation of the unit. An initial "battle rhythm" is established with regular situation updates. A log is opened to inform the teams of the actions in progress.	The experts needed for the technical management of the incident are identified and brought together as required. Permanent contact is established with the decision-making and business teams. An initial inventory of the situation is produced on mobilisation of the unit. A log is opened to inform the teams of the actions in progress.

"In the first few hours, it can be difficult to distinguish an IT incident from a cyber incident. Both technical and business teams must therefore be familiar with cyber issues in order to raise the alert and mobilise the crisis scheme without delay. It is also essential for incident response teams to be able to detect weak signals in order to shut down the systems if necessary."

CMA CGM

FACT SHEET 9
MANAGING YOUR CRISIS SCHEME

As a cyber attack can have varied and significant effects on the organisation's activity (digital tools and services unavailable, impact of the attack extended to partners, etc.), cyber crisis management teams should seek to contain the incident and restart the operation of the organisation in a controlled manner. Each unit will therefore plan a certain number of actions. However, these actions can be counter-productive if poorly coordinated (stopping of essential systems, inappropriate communication strategy).

The strategic unit therefore adopts the role of crisis coordinator to guide the work of the teams and achieve the objectives set.

	STRATEGIC COMPONENT	CYBER AND IT OPERATIONAL COMPONENT
OBJECTIVE 1	**Focusing on understanding the attack and the extent of the impact**	**Containing the attack**
RECOMMENDATIONS	The decisions of the unit are made from a position of uncertainty, due to the changing situation. A balance is found in terms of frequency and formalisation in the escalation and passing down of crisis guidance/decisions, to allow time for the operational teams to perform the requested actions. Critical applications, systems and periods for the organisation are quickly identified thanks to the mapping produced during the preparatory work.	The cyber and IT teams mobilised seek to limit the effects of the attack through precautionary measures. The measures to be put in place to contain the attack are validated by the strategic unit if they have consequences for business continuity (isolation, disconnection of applications or servers, blocking of Internet access, etc.). The level of trust in the use of data and the IS is shared with the strategic unit. **Bypass measures** are taken if necessary.

	STRATEGIC COMPONENT	CYBER AND IT OPERATIONAL COMPONENT
RECOMMENDATIONS	The criticality of the compromised data and the level of trust for the use of this data, or the criticality of the systems themselves, is assessed. The issues facing the various stakeholders are identified, formalised and shared with the operational units. The cyber crisis communication scheme is activated (media and social network watch) and communication messages (internal and external) are formalised in anticipation based on the preparation carried out in advance. The payment of ransoms should be avoided as it maintains the fraudulent system and does not guarantee that the data will be recovered.	

“It is important that the technical or business teams are familiar with the concepts of cyber impact. Our management team's awareness of cyber security has therefore facilitated a good understanding of the issues and decision-making at a time of uncertainty.”

The Nord-Ouest Hospital - Villefranche-sur-Saône

FACT SHEET 10
SUPPORTING YOUR CRISIS MANAGEMENT TEAMS

As it can take several weeks to manage the impact of a cyber crisis, it is important to establish a solid crisis organisation from the start. Depending on the scale of the crisis, the teams may be overstretched by demands from numerous stakeholders, so they need to be protected and relieved in order to focus on priority actions. Many elements are therefore to be taken into account in order to facilitate their work (team organisation and management, working format - non-working hours, working hours - rotas, catering or hotel services, remuneration, meeting rooms, etc.).

	STRATEGIC COMPONENT	CYBER AND IT OPERATIONAL COMPONENT
OBJECTIVE 1	**Providing support for the communication and legal components**	**Creating cyber "teams"**
RECOMMENDATIONS	The actions carried out, in particular those relating to customers, partners and suppliers, are mapped. In the communication strategy, the language elements are adapted based on the elements formalised in the preparation phase. There is internal communication to provide information on the progress of actions, if necessary. A question/answer tool is put in place. The legal team is mobilised and the obligations to partners, customers and suppliers that cannot be respected are identified.	Employees with no activity can be mobilised to assist with the various actions to be carried out. The work can be organised in the form of project teams in order to meet several objectives in a short time.

	STRATEGIC COMPONENT	CYBER AND IT OPERATIONAL COMPONENT
	If necessary, the pre-defined channels are used to communicate with the partners within the time frames specified in the contracts.	
OBJECTIVE 2	**Putting in place appropriate HR support**	
RECOMMENDATIONS	Team turnover is anticipated and employee hours are monitored in order to preserve their ability to operate in the long term and to formalise their working time. The service providers mobilised also perform equivalent monitoring for the resources used. One person is dedicated to this monitoring.	
OBJECTIVE 3	**Organising the logistical components of crisis management**	
RECOMMENDATIONS	Catering, accommodation and means of transport are made available to the teams involved (particularly outside of the usual working days/hours). Part of the premises is temporarily rearranged if necessary. The family needs of the people mobilised are taken into account and solutions can be put in place (childcare, adapted hours, etc.). 24/7 access to buildings (badges, etc.) is implemented. If service providers are mobilised, a list of names is given to the logistics teams to provide badges and access to the premises. Meeting rooms allowing the various units to meet and work together are made available. Digital tools adapted to the context are provided. One person is dedicated to monitoring logistics.	

"The teams involved in managing the crisis needed support 24/7, both professionally, protecting them from excessive internal and external demands, and personally, making it easier for individuals to organise their time. The human support from caregivers and directors also helped them to stay motivated and keep up the pace."

The Nord-Ouest Hospital - Villefranche-sur-Saône

FACT SHEET 11
ACTIVATING YOUR SUPPORT NETWORKS

Managing the impact of a cyber crisis involves calling on a network of experts (insurers, CERTs, forensics teams, etc.) who will support the teams in their actions. To make it easier to mobilise the experts, it is in particular necessary to use the directories created in advance. Depending on the regulatory obligations to which the organisation is subject, it is also important to warn the competent authorities: they can in certain cases offer support to an organisation that has suffered a cyber attack.

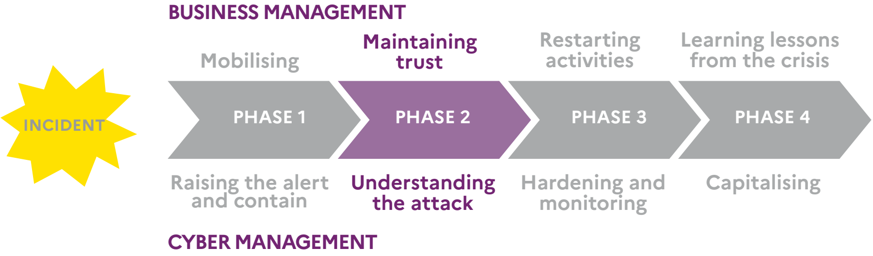
	STRATEGIC COMPONENT	CYBER AND IT OPERATIONAL COMPONENT
OBJECTIVE 1	**Activating your cyber insurance**	
RECOMMENDATIONS	Cyber insurance is activated on the decision of the strategic unit, based on pre-established criteria. The expertise to be called upon via the insurance is identified and the insurer notified. The log is used to track and centralise the actions and costs involved in managing the crisis.	The teams identify the necessary technical support, in particular for the investigation and reconstruction components. A summary of events and the current situation is formalised for sharing with the insurer.
OBJECTIVE 2	**Mobilising and centralising requests for reinforcement**	
RECOMMENDATIONS	The business and cyber teams centralise their needs in terms of resources. The people responsible for coordinating the network of experts are mobilised and carry out this task. They contact the experts identified in advance or undertake to identify them. Together with the logistics component, they are responsible for welcoming the experts.	The process to identify needs is carried out at regular intervals, in particular during the investigation and reconstruction phases. A unit (or person) is put in place to centralise resource requests. This unit or person is responsible for logistics and responds to requests. If a CERT/CSIRT is present, information can be shared with other CERTs/CSIRTs (e.g. sectoral network, circle of trust, etc.).

	STRATEGIC COMPONENT	CYBER AND IT OPERATIONAL COMPONENT
OBJECTIVE 3	**Reporting your incident to the competent authorities** Depending on the status of the organisation, several actions can be taken,[20] leading to recommendations from the authorities.	
RECOMMENDATIONS	Working together with the legal teams, the filing of a complaint is envisaged. Incident reporting (ANSSI, the French Data Protection Authority, judicial authorities) is centralised and coordinated by the strategic unit. In the event of a personal data breach (General Data Protection Regulation), the incident is reported by the Data Protection Officer. In the event of an international crisis, the legal teams take into account the applicable legislation and coordinate the reporting of the incident to the local authorities.	The cyber and IT teams share the information necessary for reporting the incident. Evidence of compromise (servers, data) is kept for the courts (in the case of legal action) and for the insurer (for activation of an insurance contract). In the event of legal proceedings, a specialised bailiff is called upon to establish the report. Depending on the legal obligations, an incident is declared and the details of the compromise are shared with ANSSI.

[20] www.ssi.gouv.fr/en-cas-dincident/ (French only)

PHASE 2

MAINTAINING TRUST AND UNDERSTANDING THE ATTACK



Once the crisis scheme has been activated and the teams mobilised, the aim is to limit as much as possible the immediate impact of the IS malfunction on the organisation's activity. To achieve this, the crisis management teams therefore aim to:

- Report on the situation to reassure trusted partners (fact sheet 12).
- Understand how the attack unfolded in order to define the scope of the cyber and business compromise (fact sheet 13).

FACT SHEET 12
COMMUNICATING EFFECTIVELY

Depending on its type and scale, the impact of a cyber attack can be immediately visible, requiring the organisation to quickly report the situation both in-house and externally. The number of stakeholders directly or indirectly involved in a cyber crisis sometimes makes it difficult to remain consistent across communication channels to control the overall message, as cyber issues are technical and change quickly.

A communication strategy should then be produced, combined with language elements with the help of the communication, cyber and IT teams, to inform, reassure, mobilise and protect the image of the organisation.

This strategy is based on an analysis of the situation and the elements already prepared,[21] but also on a media risk analysis incorporating elements relating to the operational situation (from the cyber and IT teams) and issues of reputation and trust defined with the strategic unit. It must therefore incorporate the impacts of the incident, the socio-political context (risks, topical issues) and the points of vigilance linked to the organisation (notoriety, sector news, takeover, financial communication, etc.).

[21] Refer to the first part of the guide, in particular fact sheet 3: formalising a cyber crisis communication strategy.

	STRATEGIC COMPONENT	CYBER AND IT OPERATIONAL COMPONENT
OBJECTIVE 1	**Adapting your communication plan to the situation**	**Informing the strategic unit of the situation**
RECOMMENDATIONS	Two plans are produced: an internal communication plan and an external communication plan. The frequency of communication is adapted to the strategic objectives. Communication correspondents (press, web, internal communication) are mobilised. Regional/international correspondents are identified and mobilised based on the size and activity of the organisation. One or more spokespersons (trained in cyber issues) are mobilised to allow the experts to focus on managing the crisis. Should the communication channels be unavailable, communications are broadcast on the alternative networks in place (physical communication, temporary site, temporary voicemail, etc.).	The actions carried out and those in progress are regularly reported to the strategic unit. Uncertainties and grey areas in particular are shared. The cyber and IT teams help the communication teams to adapt certain technical elements to make them easier for non-experts to understand.

OBJECTIVE 2	Reassuring your stakeholders and the media	Reassuring the stakeholders' technical teams
RECOMMENDATIONS	There is regular communication to keep stakeholders informed of the development of the situation, to control the information shared and to avoid the spread of rumours. The language elements are formalised and validated by the communication and legal teams. A single point of contact centralises press requests. A media monitoring unit is set up to make it easier to monitor the impact of the communication and to anticipate actions. Top-down communication is provided to ensure changes in the situation and major milestones are clear, in order to encourage support. a question/answer tool is put in place.	Requests from customers, partners and authorities for additional technical information on the attack are subject to centralised monitoring. A single outgoing channel is set up to respond to these requests.

“The communication department supported us in defining a communication strategy from the very first hours of the crisis. We worked on the messages based on the audience and were able to use the tools that remained at our disposal. The information correspondents in the company (CEO, sales reps, HR, financiers, legal experts, etc.) received the information necessary in order to answer questions from employees, customers and partners (suppliers, insurance, banks, etc.), and we also set up dedicated “hotlines”.

Bouygues Construction

“In the event of an attack, we can expect to receive numerous requests from the press. The involvement of the communication teams alongside the operational teams makes it possible to centralise press requests, produce language elements or answer questions in order to relieve them of a significant workload.”

The Nord-Ouest Hospital - Villefranche-sur-Saône

FACT SHEET 13
CONDUCTING THE DIGITAL INVESTIGATION

Understanding the actions of the attacker and what may have motivated them to target the organisation (sensitive data, greed, etc.) is an essential step in resolving the crisis since it allows remediation actions to be prioritised and a reconstruction strategy to be undertaken in order to recreate a trusted core. It also highlights the flaws exploited to break into the organisation's systems and *ultimately* obliges teams to raise the cyber security level.

Lastly, it helps to understand the extent of the compromise and the potential time for which services and tools will be unavailable, so that the business teams can implement the best business continuity strategy.

	STRATEGIC COMPONENT	CYBER AND IT OPERATIONAL COMPONENT
OBJECTIVE 1	**Supporting the investigation strategy**	**Establishing the investigation strategy**
RECOMMENDATIONS	A balance is found between the speed at which **business applications** are returned to production and the maintaining of an appropriate level of security. Arbitration is provided on the priority reactivation of business applications. This is based on the level of danger created by restarting the servers/workstations, the level of security of the **trusted core** and the ability to maintain this core over time. The level of complexity and the duration of the investigations are taken into consideration in the arbitration. The pace of the server and workstation reconstruction plan is defined, ensuring that there are no traces of the attack on the servers and workstations. Based on the mapping of sensitive assets, guidance is provided as to the systems and applications to investigate as priority.	Investigations initially focus on identifying the scope of the compromise, potential vectors of infection and malicious functions. Intermediate results are shared. These results are made easy to understand and put into context, and must be clear in order to avoid any misinterpretation. From the beginning, it is made clear within the entity that "patient 0" may never be identified and that certain questions will remain unanswered. The only priority must be to restart the services under acceptable security conditions. The attacker's actions are the subject of a summary document that can easily be addressed at strategic level. a service provider (PRIS) can be contracted for the analyses, concentrating on all the actions carried out by the attacker. Arbitration is requested on the direction of the investigations, based on the sensitivity of the assets.

OBJECTIVE 2	**Focusing attention on the attack rather than on those responsible**	**Organising investigations**
RECOMMENDATIONS	The investigative action carried out by the cyber teams is supported with the aim of understanding the extent of the compromise and prioritising remediation actions. The search for the perpetrator is not a priority for the strategic unit, which focuses its efforts on maintaining activity.	The investigations do not focus on all vulnerabilities, but on the **path of compromise** that enabled the attack to be carried out. The identification of the scope of compromise as an input for the **defence plan** is a priority. A dedicated organisation is put in place to manage all the log collections and the performance of actions related to the investigations. The various collections are centralised for distribution to stakeholders: cyber and IT teams, service providers, authorities, etc. The retention period for IS logs is adjusted, as investigations can potentially last for several weeks. All the service providers mobilised work together in a coordinated manner with clearly defined objectives and scopes.

"From the beginning of the crisis, our priority was very clear: to continue activity on the construction sites. To do this, we first restored the payment of our employees and suppliers. We had to show agility in mobilising employees from all regions to get them to work on a closed network. We also relied on employee initiatives to implement alternative measures. To restore activity as quickly as possible, we had to be flexible, but never without safeguards to prevent further compromise."

Bouygues Construction

FACT SHEET 14
IMPLEMENTING A DEGRADED OPERATING MODE FOR THE AFFECTED BUSINESS LINES

During a cyber crisis, ransomware can render all of the organisation's digital tools and services unavailable, forcing business lines to adapt their activities. In other cases, containment or remediation measures by IT and cyber teams may render certain tools partially unavailable as a result of isolation or disconnection.

The cyber crisis management strategy, backed by business continuity schemes, must therefore provide operational solutions to maintain the operation of the organisation without digital tools over what can sometimes be a very long period of time.

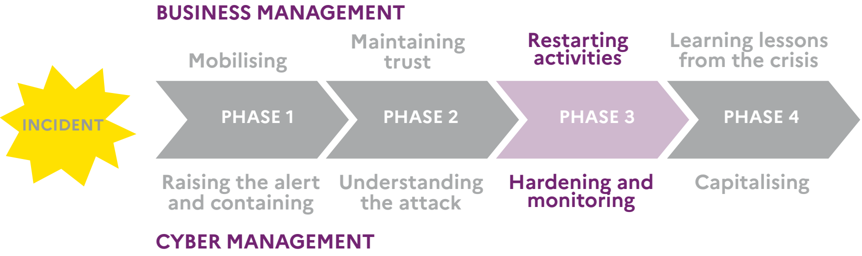
22. See the first part of the guide for the definition of systems adapted to the cyber threat.
23. See the website of the NoMoreRansom group which offers several file decryption tools: www.nomoreransom.org/

	STRATEGIC COMPONENT	CYBER AND IT OPERATIONAL COMPONENT
OBJECTIVE 1	**Defining methods for the use of bypass solutions**	**Supporting the deployment of bypass solutions**
RECOMMENDATIONS	The bypass solutions and the operational resilience capacity identified beforehand to maintain a degraded activity are implemented (cloud solution, service provider, paper, personal resources, etc.). There is internal communication on the chosen solutions to ensure that they are correctly understood and correctly used. If necessary, customers are informed of the rules for using the temporary tools and services.	The possibility of using healthy backups to restore the situation as quickly as possible is studied. The use of open-access decryption tools (with no ransom to pay) is also considered. The cyber and IT teams recommend digital bypass measures to be considered and facilitate their secure implementation. To carry out these actions, enhanced coordination is implemented in the local teams, in particular for IT. The planned dates for returning the applications into service are shared to allow the business teams to anticipate in particular the time for which degraded mode will be maintained.

"The progressive sharing of the investigation results was essential for the managers to understand the effects of the crisis on the business activity. Experts provide answers to many questions and you should not hesitate to use pictorial references to help understand the situation."

CMA CGM

RESTARTING BUSINESS ACTIVITIES AND HARDENING INFORMATION SYSTEMS



Once the scope of the compromise has been identified and the stakeholders informed, the crisis management teams must act to re-establish a normal situation. To achieve this, they must successfully:

- Implement security and hardening actions to allow the activity to resume (fact sheet 15).
- Adapt the organisation's activity to remaining constraints (fact sheet 16).

FACT SHEET 15
HARDENING AND REMEDIATING

Once the path and the scope of the compromise for the attack have been identified, the organisation's IS must be protected against new attacks. These new measures may lead to a significant change in practices, particularly in administration, and in business operating methods in the use of digital tools and services. An educational effort is therefore required to explain, at all levels, the sometimes profound changes that will be made to ensure the systems are not compromised again and to find a way out of the crisis.

The business, cyber and IT teams must therefore work together to adapt the pace of their actions and overcome this key cyber crisis management stage.

"Despite the urgent need for remediation, a certain degree of patience was required. The remediation of the incident affecting the digital environment requires a specific analysis of the impacts, the motives and the underlying causes. Short-term corrections are then carried out, but also more complex transformations. Third parties can then be mobilised on weekends and at night, and it must be ensured that their processes can stand the new pace of the crisis."

CMA-CGM

	STRATEGIC COMPONENT	CYBER AND IT OPERATIONAL COMPONENT
OBJECTIVE 1	**Setting objectives for orientations on hardening and remediation**	**Regaining control of the systems and harden them to prevent further compromises**
RECOMMENDATIONS	Hardening and remediation actions are scheduled to ensure optimum organisation of the work of the operational teams. These actions validate defined objectives. The risks of not carrying out certain hardening and remediation actions are assessed and taken into account. The objectives of the action plan and the associated schedule (in particular restarting the business application) are adjusted based on the technical constraints of the remediation. A change of **administration practices** and IS management may be needed to enhance security. This is then promoted by the decision-making teams. The DRP is adapted based on the progress of the current and forthcoming investigation and remediation actions. All decisions made are monitored and used to validate the criteria for emerging from the crisis.	A hardening and remediation plan is developed iteratively based on feedback from the digital investigations. It is used in particular to neutralise the vectors of infection and propagation. Global hardening measures are put in place to isolate the attacker if it manages to maintain its access to certain parts of the IS. In the case of structural measures, the impact on the IS and the business lines is identified and validated prior to deployment.

OBJECTIVE 2	Rebuilding a trusted core
RECOMMENDATIONS	A secure bubble is established and the services to be reintegrated are prioritised by the strategic unit. Systems are monitored, in particular those identified by the investigation as having been previously compromised. Support is provided on new security practices in the IT production teams, supported by the strategic unit. A strengthened coordination is implemented for the local teams, in particular IT. A validation process is also formalised to ensure the correct application of security measures before a system or application is put back into production.

FACT SHEET 16
PREPARING, AUTOMATING AND STANDARDISING THE RECONSTRUCTION

As the IS are compromised, consideration must be given to reconstructing them before returning to normal operation. The aim is to put more secure tools and systems back into production, respecting a higher standard of security in order to limit the risk of further compromise.

This cyber crisis management phase is particularly demanding in terms of human and financial resources. Priority must therefore be given to the most critical systems for the operation of the business lines or to respect critical periods of the organisation (payment of wages, deliveries, etc.).

As the application of new security measures may slow down the reconstruction, the strategic component must remain consistent and avoid favouring the application of more practical but less secure measures. Particular attention is therefore paid to the correct application of the rules and any exemption must be made known to the strategic unit with formal acceptance of the potential risks associated.

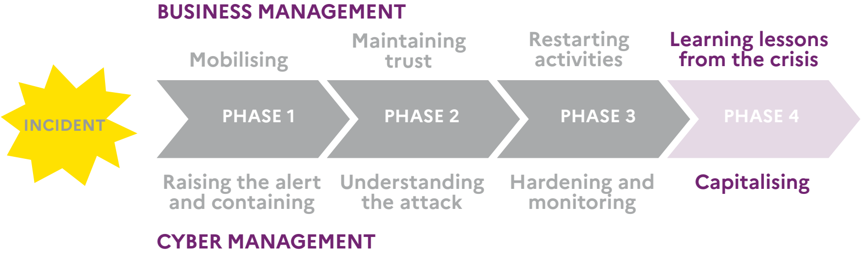
	STRATEGIC COMPONENT	CYBER AND IT OPERATIONAL COMPONENT
OBJECTIVE 1	**Organising and adapting user behaviour**	**Securing the automation and standardisation of the reconstruction**
RECOMMENDATIONS	The applications and systems to be reconstructed are given a priority level (P0 – P1 – P2 – P3, based on the criticality) which is then validated. Additional support resources are provided for the IT reconstruction, if necessary in shift work (24 hours a day). The decision-making teams request visibility and transparency from the cyber and IT technical teams on whether it is realistic to reopen business applications. The business lines are mobilised to carry out user tests before returning applications into production. External users and stakeholders are informed when the services reopen. Particular attention is paid to ensure that the measures taken do not imply an exit from the crisis until the criteria are met.	A reconstruction strategy is defined, based on healthy backups. This strategy includes a data restoration component. The risk of a partial restoration of data, due to desynchronised backups, is taken into account. The different stages in the process are monitored. This monitoring is regularly shared with the cyber and IT operational unit and the strategic unit. Provisional dates for returning the applications into service are also indicated to keep the teams mobilised. Coordination is strengthened between the teams responsible for hardening and remediation and those responsible for reconstruction in order to apply the cyber security measures. Should shift work be used for the reconstruction, the teams of the remediation component shall provide a counterpart to respond to validation requests.

"Many workstations had to be reinstalled, so the restarting of the most critical activities had to be prioritised. It was decided that the crisis would be closed only when all healthcare establishments were operational."

The Nord-Ouest Hospital – Villefranche-sur-Saône

PHASE 4

LEARNING LESSONS FROM THE CRISIS AND CAPITALISING ON THEM



With remediation and business recovery actions pointing to a return to greater stability, the crisis management teams must end by considering a way out of the crisis. To achieve this final objective, it is important that they successfully:

- Define and organise their crisis exit plan (fact sheet 17).
- Learn from the crisis experience to develop (fact sheet 18).

FACT SHEET 17
ORGANISING THE WAY OUT OF THE CRISIS

The end of a cyber crisis period does not mean that the organisation will return to normal operation from that moment, since the reconstruction and hardening of all systems can take several months. On the contrary, the end of the crisis is envisaged when the essential activities of the organisation can resume as usual. For this to happen, several conditions must be met, to be defined by the strategic unit.

> "We quickly formalised crisis exit criteria for a return to day-to-day business. Three main criteria were established: the priority applications are functional, the backups are in working order, and the international sites are reconnected."
>
> Bouygues Construction

	STRATEGIC COMPONENT	CYBER AND IT OPERATIONAL COMPONENT
OBJECTIVE 1	**Adapting crisis exit thresholds**	**Allowing the gradual recovery of digital tools**
RECOMMENDATIONS	The conditions necessary to exit the crisis, pre-defined at the beginning of the incident, are reassessed. In particular, they take into account knowledge of the attack, the restoration of services and the return to production of the affected systems. An action plan is formalised to capitalise on all the projects that will need to be carried out after the crisis. Communication is sent to all teams to report the end of the crisis. Regulatory post-crisis reporting obligations are identified and fulfilled. Human resources in particular are reviewed for potential adjustments (compensation, rest). The teams are thanked for their work and their mobilisation.	The bypass solutions are assessed to determine whether to maintain or remove them in consultation with the business teams. The **risk/exemption register** is made more reliable in order to use it as a key factor when exiting the crisis. The mobilisation of the teams gradually slows down. Monitoring of the IS is maintained, particularly on the attack path. The teams are thanked for their work and their mobilisation.

FACT SHEET 18
LEARNING LESSONS FROM THE CRISIS

Following a crisis, teams are tempted to quickly resume normal activity. However, this transition period is the best time to review the management of the crisis and capitalise on the experience and what could be improved. Feedback contributes in particular to improving the resilience of the organisation by highlighting the strengths and areas for improvement following the malfunctions observed. In particular, it ensures that certain crisis management schemes considered effective continue to be used.

The topics that can be addressed within the framework of the feedback concern:

- Governance and the crisis management process.
- Crisis communication.
- Decision-making and action follow-up process.
- Technical and operational capacities.
- Interactions between the teams mobilised in the crisis.
- Interactions with external stakeholders.

The feedback must be organised after closing the crisis and should not be considered as an audit, but as a means of capitalising on the experience. It is provided in two stages: "on the spot" feedback in the form of interviews or collection workshops; "delayed" feedback to present a summary of the observations, recommendations and the associated action plan.

	STRATEGIC COMPONENT	CYBER AND IT OPERATIONAL COMPONENT
OBJECTIVE 1	**Organising the feedback**	
RECOMMENDATIONS	The strategic unit identifies a team responsible for collecting feedback on the crisis management. This team identifies the parties to be interviewed and the interview grid, organises the practical aspects of the exercise (schedule, method, summary document, coordination). The feedback is organised for the strategic and operational component. A maximum period of 30 days is scheduled between the end of the crisis and the end of the feedback process. A digital investigation report and its summary (for the management teams) are requested from the service providers mobilised.	
OBJECTIVE 2	**Making use of the feedback**	
RECOMMENDATIONS	The team responsible for collecting the feedback uses the data collected to produce a report identifying the actions to be taken to improve the crisis management system. Feedback is organised on different levels, for example by distributing a summary to general management and a more comprehensive document to the crisis management teams. Areas for improvement are subject to specific follow-up via an action plan.	

> "Feedback was collected with all the teams to question and improve the practices and procedures of our business lines, both immediately and at a later date. Now the challenge is to be even more resilient in the event of a long-lasting crisis."

The Nord-Ouest Hospital – Villefranche-sur-Saône

APPENDIX 1

CYBER CRISIS MANAGEMENT TOOLKIT

This non-exhaustive list of tools and procedures that can be implemented prior to any incident can help you perfect your cyber crisis management scheme. It is essential to maintain them in operational conditions. Solutions and tools qualified by ANSSI may be used.

GENERAL TOOLS	SPECIFIC TOOLS
▸ Physical or virtual crisis room ▸ Crisis directory (internal and external people) accessible in the event of a blackout ▸ Action tracker ▸ Logging tool ▸ Resilient/off-network communication tools: generic email addresses, chat, videoconferencing, landline or mobile phones, etc. ▸ Role sheets ▸ Reflex action sheets ▸ Insurance contracts.	▸ Criteria for triggering a cyber crisis unit ▸ Cyber BCP and DRP ▸ Mapping of critical systems and services ▸ List of experts and service providers to be contacted ▸ Cyber crisis communication plan ▸ List of stakeholders to be informed (customers, suppliers, authorities) ▸ Register of risks and exemptions ▸ Off-network computer.

APPENDIX 2

OBJECTIVES OF THE CYBER CRISIS MANAGEMENT

FACT SHEET NAME
Fact sheet 1: Knowing and controlling your information systems
Fact sheet 2: Creating an operational capacity foundation to ensure an appropriate level of digital resilience
Fact sheet 3: Establishing a cyber crisis communication strategy
Fact sheet 4: Adapting your crisis organisation to the cyber scenario
Fact sheet 5: Preparing your incident response capacity
Fact sheet 6: Putting in place appropriate insurance policies
Fact sheet 7: Training as practice and to improve
Fact sheet 8: Activating your cyber crisis scheme
Fact sheet 9: Managing your crisis scheme
Fact sheet 10: Supporting your crisis management teams
Fact sheet 11: Activating your support networks

STRATEGIC OBJECTIVES	OPERATIONAL OBJECTIVES
Mapping your critical business applications and resources	Mapping your IS
Adapting the business continuity plan to the cyber crisis scenario Producing a disaster recovery plan for the cyber scenario Putting in place resilient crisis management tools	
Drawing up a list of stakeholders to be contacted Anticipating the crisis communication strategy	
Implementing criteria and procedures for the activation of crisis units Organising your cyber crisis units	
Identifying the experts to call upon in a crisis	
Putting in place the capacity for a strategic reaction to the various threats	Putting in place the capacity for a technical reaction to the various threats
Adapting the insurance to the needs of the organisation	
Defining a cyber crisis training plan	
Deciding on the activation of a crisis unit	Warning the crisis management teams of the situation
Mobilising the teams	
Focusing on understanding the attack and the extent of the impact	Containing the attack
Providing support for the communication and legal components Putting in place appropriate HR support Organising the logistical components of crisis management	Creating cyber “teams”
Activating your cyber insurance Mobilising and centralise requests for reinforcement Reporting your incident to the competent authorities	

Fact sheet 12: Communicating effectively

Fact sheet 13: Conducting the digital investigation

Fact sheet 14: Implementing a degraded operating mode for the affected business lines

Fact sheet 15: Hardening and remediating

Fact sheet 16: Preparing, automating and standardising the reconstruction

Fact sheet 17: Organising the way out of the crisis

Fact sheet 18: Learning lessons from the crisis

	Adapting your communication plan to the situation Reassuring your stakeholders and the media	Informing the strategic unit of the situation Reassure the stakeholders' technical teams
	Supporting the investigation strategy Focusing attention on the attack rather than on those responsible	Establishing the investigation strategy Organising investigations
	Defining methods for the use of bypass solutions	Supporting the deployment of bypass solutions
	Setting objectives for orientations on hardening and remediation	Regaining control of the systems and harden them to prevent further compromises Rebuilding a trusted core
	Organising and adapting user behaviour	Securing the automation and standardisation of the reconstruction
	Adapting crisis exit thresholds	Allowing the gradual recovery of digital tools
	Organising the feedback Making use of the feedback	

GLOSSARY

ACTIVE DIRECTORY: Windows directory service offering a centralised and standardised identity and access management system.

ADMINISTRATIVE PRACTICES: process of installation and configuration, updates, supervision, access constraints, making it possible to secure information systems.

BUSINESS CONTINUITY PLAN, BCP (ISO 22301): set of documented procedures serving as guides for entities to respond, restore, resume and return to a pre-defined level of operation following a disruption.

BUSINESS IMPACT ASSESSMENT: process identifying an organisation's critical and priority activities and determining the minimum resources needed to meet business continuity requirements.

BYPASS MEASURE: non-application of a nominal operating rule for an information system or technology involving its operation in degraded mode.

COMPUTER SECURITY INCIDENT RESPONSE TEAM (CSIRT) OR CERT: alert, processing and response centre for cyber attacks aimed at companies, administrations or authorities.

CONTAINMENT: protective action aimed at stopping the spread of an attacker on the IS.

DEFENCE PLAN: strategy implemented to protect information systems from a cyber attack.

DIGITAL SERVICES: services implemented by an organisation with which its information systems and those of its service providers or partners are associated.

DISASTER RECOVERY PLAN, DRP (ISO 22301): documented procedures allowing entities to restore and resume activity based on temporary measures adopted to meet usual business requirements following an incident.

DOMAIN NAME SYSTEM (DNS): service used to establish a correspondence between a domain name and an IP address.

EXPLOITED FLAW: weakness in an information system allowing an attacker to undermine the integrity of this system.

HARDENING: action of reinforcing IS security in order to prevent a new intrusion by the attacker.

HEALTHY BACKUP: process of saving data on offline servers conducted and tested regularly, ensuring the integrity and availability of the data.

INFORMATION SYSTEM: set of resources (hardware or software) and devices of an organisation used to collect, store and exchange the information necessary for its operation.

ISOLATION: procedure for partitioning or disconnecting information systems from the Internet or Intranet following a cyber attack to prevent it from spreading.

MAXIMUM TOLERABLE DOWNTIME: metric determining the total time for which a business process can be disrupted without resulting in unacceptable consequences.

PUBLIC KEY INFRASTRUCTURE: set of technical and organisational resources used to establish a strong guarantee of trust in the validity of a digital identity.

RECOVERY TIME OBJECTIVE: metric determining the maximum tolerable time required to bring critical systems back online.

REFERENCE CYBER SCENARIO: risk scenario for the organisation, assessed based on the severity and likelihood of the impact of the risk.

REMEDIATION: process for limiting the effects of the incident on the IS.

WORK RECOVERY TIME: metric determining the maximum tolerable time required to verify system and/or data integrity.

USEFUL RESOURCES

GENERAL

ANSSI

- *Ransomware attacks, all concerned - How to prevent them and respond to an incident*, 2020: www.ssi.gouv.fr/en/guide/ransomware-attacks-all-concerned/
- *État de la menace rançongiciel à l'encontre des entreprises et institutions (Assessment of the ransomware threat to companies and institutions)*, 2020 (French only): www.cert.ssi.gouv.fr/cti/CERTFR-2020-CTI-001
- Technical guides and collections of good practices (French only): www.ssi.gouv.fr/administration/bonnes-pratiques/
- Products and services qualified by ANSSI (French only): www.ssi.gouv.fr/entreprise/qualifications/produits-recommandes-par-lanssi/les-produits/
- "Ne soyez plus otage des rançongiciels" (Don't fall hostage to ransomware again - French only): www.ssi.gouv.fr/actualite/ne-soyez-plus-otage-des-rancongiciels/
- CERT-FR website www.cert.ssi.gouv.fr/cti

CYBERMALVEILLANCE.GOUV.FR

"Que faire en cas d'attaque par rançongiciel" (What to do in the event of a ransomware attack) reflex sheet (French only): www.cybermalveillance.gouv.fr/tous-nos-contenus/fiches-reflexes/rancongiciels-ransomwares

FACT SHEET 1

ANSSI

- *Mapping the information system, how-to guide in 5 steps*, 2018: www.ssi.gouv.fr/en/guide/mapping-the-information-system/
- *EBIOS Risk Manager method*, 2018: www.ssi.gouv.fr/en/guide/ebios-risk-manager-the-method/

FACT SHEET 2

ANSSI

- *Mapping the information system, how-to guide in 5 steps,* 2018: www.ssi.gouv.fr/en/guide/mapping-the-information-system/
- *Guideline for a healthy information system in 42 measures*, 2017: www.ssi.gouv.fr/en/guide/40-essential-measures-for-a-healthy-network/
- *Controlling the digital risk, the trust advantage*, 2019: www.ssi.gouv.fr/en/guide/controlling-the-digital-risk-the-trust-advantage/
- *EBIOS Risk Manager method,* 2018: www.ssi.gouv.fr/en/guide/ebios-risk-manager-the-method/
- Active Directory security assessment checklist, 2020: www.cert.ssi.gouv.fr/uploads/guide-ad.html
- *Recommandations de sécurité relatives à l'Active Directory (Security recommendations relating to Active Directory)*, 2014 (French only): www.ssi.gouv.fr/guide/recommandations-de-securite-relatives-a-active-directory/

AFNOR

- *ISO 22301:2019 Security and resilience, Business continuity management systems,* 2019: www.iso.org
- *ISO 22320:2018 Security and resilience, Emergency management, Guidelines for incident management,* 2018: www.iso.org
- *ISO/IEC 27035-1:2016 Information technology — Security techniques — Information security incident management — Part 1: Principles of incident management,* 2016: www.iso.org

SGDSN

- *Guide pour réaliser un plan de continuité d'activité (Guide on drawing up a business continuity plan)*, 2013 (French only): www.sgdsn.gouv.fr/uploads/2016/10/guide-pca-sgdsn-110613-normal.pdf

FACT SHEET 6

AMRAE

- *Controlling the digital risk,* "Step 6: Setting up suitable insurance policies", 2019:

  www.ssi.gouv.fr/en/guide/controlling-the-digital-risk-the-trust-advantage/ (p. 28)

FACT SHEET 7

ANSSI

- *Organising a cyber crisis management exercise, 2020:* www.ssi.gouv.fr/en/guide/organising-a-cyber-crisis-management-exercise/

FACT SHEET 11

ANSSI

- Reporting an incident on the ANSSI website (French only): www.ssi.gouv.fr/en-cas-dincident

FRENCH DATA PROTECTION AUTHORITY (CNIL)

- Notifier une violation de données personnelles (Reporting a breach of personal data - French only) www.cnil.fr/fr/notifier-une-violation-de-donnees-personnelles

CYBERMALVEILLANCE.GOUV.FR

- Incident support: www.cybermalveillance.gouv.fr/diagnostic

FACT SHEET 14

NOMORERANSOM GROUP

- www.nomoreransom.org/

CYBER CRISIS MANAGEMENT
COLLECTION

“To ensure their resilience, organisations must realise that their cyber security efforts are not always enough… And ensure they are fully prepared for the possibility of an attack! It is not possible to improvise a response in the middle of a disaster. The preparation, tools and training of cyber experts and business lines are essential to maintain activity in the event of a computer attack…”

Guillaume Poupard, Director-General of ANSSI

These days, preparing both in business and technical terms to manage the effects of a crisis of cyber origin is essential in order to gain resilience.

Produced in partnership with the Club des Directeurs de Sécurité et de Sûreté des Entreprises and the result of extensive experience in cyber crisis management, this guide will support you in implementing efficient and resilient crisis tools and procedures.

Version 1.0 – March 2022 – **ANSSI-PA-089-EN**
Licence ouverte/Open Licence (Etalab — V1)
ISBN: 978-2-11-167122-5 (papier)
ISBN: 978-2-11-167123-2 (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
www.ssi.gouv.fr — communication@ssi.gouv.fr