



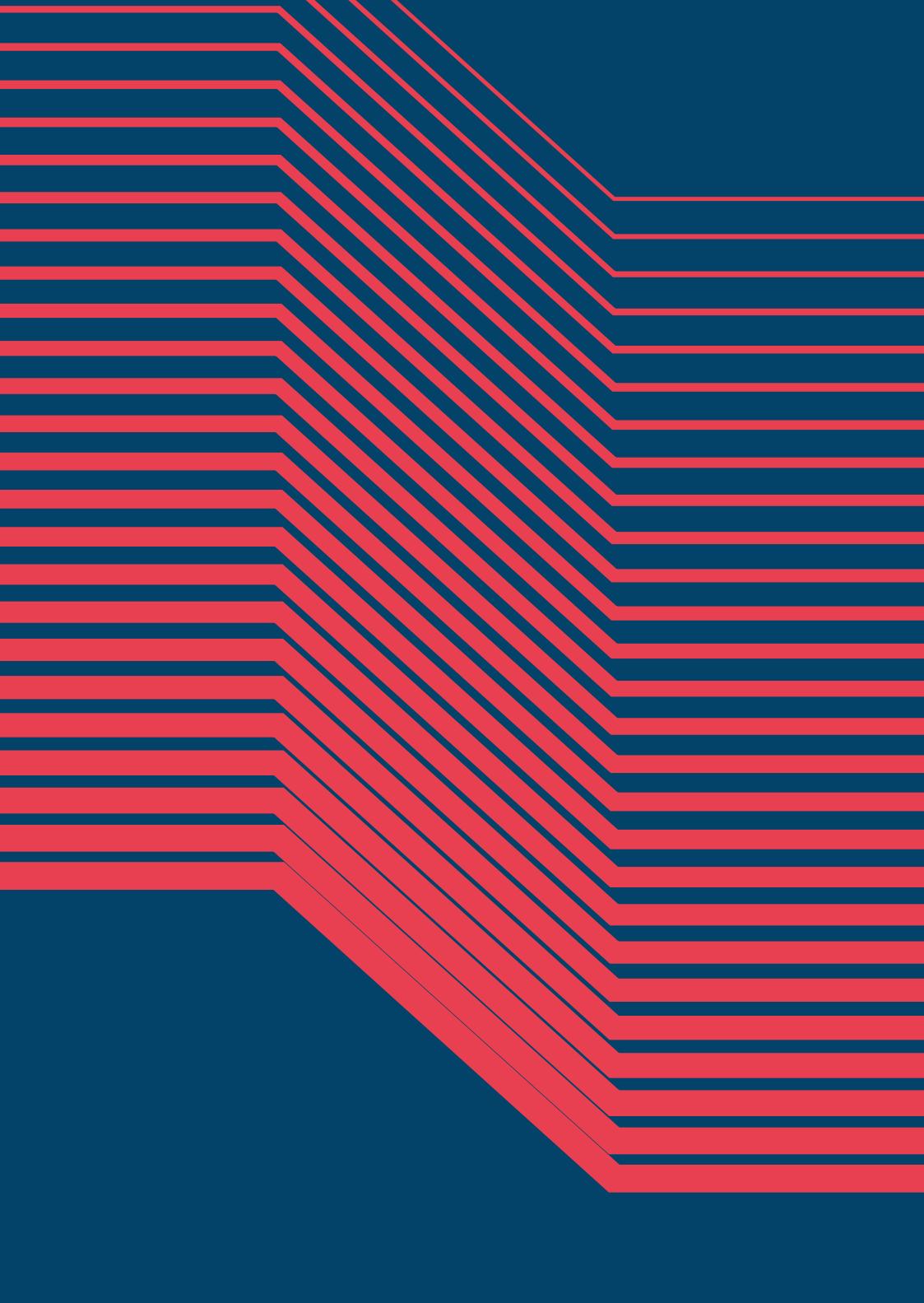
RÉPUBLIQUE
FRANÇAISE

Liberité
Égalité
Fraternité



COLLECTION
CYBER CRISIS MANAGEMENT

ORGANISING A CYBER CRISIS MANAGEMENT EXERCISE



COLLECTION
CYBER CRISIS MANAGEMENT

GUIDE

**ORGANISING
A CYBER CRISIS
MANAGEMENT EXERCISE**

CONTENTS

Editorial	6
Presentation	8
PRELIMINARY RECOMMENDATIONS: POSITIONING CYBER RESILIENCE AT THE HIGHEST LEVEL	10
Stage 1 Understanding cyber's specific features	12
What is a cyber crisis?	12
How do cyber crisis management exercises work?	15
Stage 2 Making the exercise part of a comprehensive reflection on resilience	17
Setting up a programme of exercises	18
Seizing the opportunities of the exercise	18
Coming together and communicating about the exercise	20
STEP 1: DESIGNING THE EXERCISE	22
Stage 1 Structuring the exercise	24
Establishing a project group	24
Defining the goals	25
<i>Fact sheet No. 1: Defining the goals of the exercise</i>	<i>26</i>
Deciding on the exercise format	28
Selecting the theme	28
<i>Fact sheet No. 2: Identifying events and incidents for your exercise</i>	<i>32</i>
Determining the duration	34
Naming the exercise	35
Planning logistical resources	35
Defining the timetable	36
Stage 2 Identifying stakeholders and players	38
<i>Fact sheet No. 3: Creating specifications - example guideline RANSOM20</i>	<i>44</i>
STEP 2: PREPARING THE EXERCISE	48
Stage 1 Defining the scenario	50
Interviewing experts	53
<i>Fact sheet No. 4: Drafting the scenario - example guideline RANSOM20</i>	<i>55</i>
Stage 2 Drawing up the timetable	61
Defining the rhythm and intensity of the exercise	61
Simulating communication challenges and media pressure	63
<i>Fact sheet No. 5: Simulating media pressure, roles to be taken and questions to be asked</i>	<i>66</i>

Drafting the injects.....	68
<i>Fact sheet No. 6: Drawing up a timetable: instructions example guideline RANSOM20</i>	70
Stage 3 Preparing the other documents.....	76
<i>Fact sheet No. 7: Producing a situation information - file example guideline RANSOM20</i>	78
<i>Fact sheet No. 8: Observing an exercise</i>	82
Stage 4 Briefing the participants and ensuring they are involved	86
Briefing moderators and observers.....	86
Briefing players.....	86
STEP 3: CONDUCTING THE EXERCISE	88
Stage 1 Applying what is planned.....	90
Setting the context for players.....	90
Following the timetable.....	90
Making the consequences real.....	91
Stage 2 Adapting to the players	92
Following their pace.....	92
Responding to unexpected reactions	93
<i>Fact sheet No. 9: Avoiding the most common pitfalls.....</i>	96
<i>Fact sheet No. 10: Overcoming simulation biases</i>	100
STEP 4: LEARNING FROM THE EXERCISE	104
Stage 1 Organising feedback collection immediately after the exercise	106
Stage 2 Collecting feedback collection some time after the exercise	109
Stage 3 Producing an after action report and providing for restitution.....	110
<i>Fact sheet No. 11: Collecting feedback - example guideline RANSOM20</i>	112
Conclusion	119
Annex 1 - List of deliverables to be produced for the exercise	121
Annex 2 - Glossary	122
Annex 3 - Useful resources	125

EDITORIAL

What is frustrating about cyber security is that the benefits of the efforts made in this area are scarcely noticed: no sound is made when an attack is blocked by good preparation! Let us not fool ourselves; the magnitude of the risk is real, and the lack of readiness is often devastating.

I would like to remind everyone as far as protecting information systems is concerned, that readiness is key. I understand that this represents an investment for organisations that also have other realities to consider. Therefore, the responsibility of the French National Cyber Security Agency (ANSSI) is to support their efforts in this regard and continuously remind them of the importance of cybersecurity issues.

In the face of the threat, organising exercises is crucial. I have seen this with my own eyes! Through training, and with each exercise, the teams involved in crisis management develop their reflexes and better ways of working together. They are then ready to cope when faced with an attack, especially considering the fact that cyber crises each have their specific features. We should not wait for disaster to strike to learn how to deal with it!

This guide will help you in setting up your own training courses. It results from a wealth of experience in organising cyber crisis management exercises developed over the years. I hope it will help you develop your teams' skills and thus strengthen your organisation's resilience.

Guillaume Poupard
Director-General of ANSSI

The Club de la Continuité d'Activité (Business Continuity Club, CCA) is an association comprised of more than 80 members, companies and consultancies. Its main purpose is to share best practices on crisis management and business continuity management among members. After more than ten years of existence, the CCA has become a key player in promoting corporate resilience.

Cyber risk, as the theme of one of our last inter-company annual exercises with more than 100 participants and a regular topic in our seminars, particularly crisis communication, is one of our major concerns. As a result of the manifold and severe consequences that cyber risk may have, the subject is regularly analysed and experience in this field shared within all our working groups.

“Talking” and “training” are the two words that drive us as practitioners of crises, business continuity and resilience in our organisations. This guide will allow many organisations to carry out cyber crisis exercises independently. It provides a very structured basis for understanding this risk, which affects all sectors and organisations of all sizes.

Vincent Vallée
President of the CCA

PRESENTATION

In the face of an ever growing and ever changing cyber threat, improving digital resilience through training in cyber crisis management is no longer just an opportunity but a necessity for all organisations.

The purpose of this guide is to provide step-by-step support to organisations in setting up a cyber¹ crisis management exercise that is credible and will serve as training, for both players and organisers.

It offers a methodology based on the recognised standard of the guidelines for exercises (ISO 22398:2013).

Who is this guide for?

Any private or public organisation, be it small or large, wishing to train in cyber crisis management can consult this guide.

More specifically, this guide is for anyone who wishes to organise exercises at the **decision-making level²** in order to train its organisation's crisis unit: the risk managers, those responsible for business continuity, exercises or crisis management, those responsible for the security of information systems (SIS) or equivalent, etc. This guide is not intended to construct exercises that are purely technical, for instance, by providing a complete simulation of an information system (IS) using virtual machines ("cyber range").

What does it contain?

- ▶ Four steps accompanied by fact sheets which supplement and illustrate these steps.
- ▶ Recommendations from the experience of ANSSI and the members of the CCA Crisis Management Work Group.

1: In the guide, "cyber crisis management" stands for "the management of a crisis of cyber origin", and "cyber crisis exercise" stands for "a crisis exercise of cyber origin".

2: The "decision-making level" refers to a crisis unit, made up of board members and professionals involved in crises, which will be responsible for monitoring and steering crisis management and decision-making.

- ▶ A complete exercise as the guide's main theme called RANSOM20 that is gradually developed to illustrate each step.
- ▶ Annexes, including a glossary defining all the terms used in this guide and that are specific to the exercises.

How can it be used?

The steps can be consulted independently depending on the organisation's experience and needs in crisis management exercises. This format also makes it possible to consider outsourcing all or part of these steps so that each organisation, regardless of its size and budget, can carry out this type of exercise.

The guideline: RANSOM20

An example exercise (RANSOM20) is developed throughout the guide. It serves to illustrate recommendations made at each step.

To make something that can be used by and adapted for as many people as possible, the example is a ransomware cyber attack. This type of operation is a growing trend affecting organisations of all sizes.

This example is developed in various practical fact sheets which, once compiled, form a complete exercise that can be reused by any organisation.

For more information on the RANSOM20 exercise, you can view the scenario (see fact sheet No. 4) or the timetable (see fact sheet No. 6).



PRELIMINARY RECOMMENDATIONS

POSITIONING CYBER RESILIENCE AT THE HIGHEST LEVEL

STAGE 1:

Understanding cyber's specific features 12

STAGE 2:

Making the exercise part of a comprehensive
reflection on resilience 17

These preliminary recommendations help to address the concepts of cyber exercises and crises by highlighting their specific features. They also stress the importance of including the exercise in a comprehensive reflection aimed at strengthening the organisation's resilience. Finally, the recommendations help to unite an organisation's team around the exercise.

The elements described in this section are to be developed alongside exercises and reflections on cyber crisis management.



DELIVERABLES TO BE PRODUCED:

- ▶ Exercise strategy (optional)
- ▶ Exercise programme (optional)
- ▶ Communication plan

STAGE 1

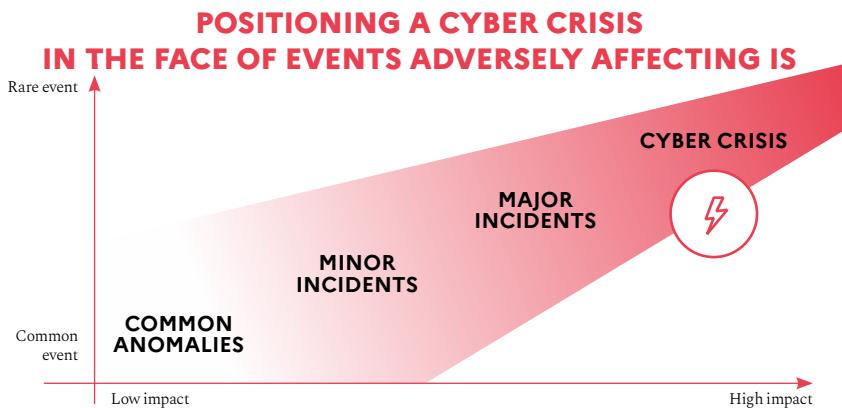
UNDERSTANDING CYBER'S SPECIFIC FEATURES

What is a cyber crisis?

Strictly speaking, there are no cyber crises, but there are crises that result from cyber attacks.

“Cyber crisis” refers to a situation when one or more malicious action(s) on an IS cause(s) a major disruption of the entity, having various and significant impacts, and sometimes causing irreversible damage.

A cyber crisis is a rare event that has a high impact. All organisations should perform a risk analysis and identify events that could pose a significant threat to their organisation and lead to a crisis.³ According to ENISA, the understanding of various key concept and terminology will differ not only between the general crisis management structure and cyber crisis structures or arrangements, but also within the structure depending on context.⁴



3: For more information on the risk analysis methodology, see the EBIOS Risk Manager method (ANSSI, 2018) – www.ssi.gouv.fr/en/guide/ebios-risk-manager-the-method/

4: Discussion on Terminology – Report on Cyber Crisis Cooperation and Management: www.enisa.europa.eu/publications/ccc-study

CHARACTERISTICS OF CYBER CRISES

Cyber crises have many specific features:

- ▶ **Intensity and ubiquity of impacts:** an organisation can be affected at multiple locations simultaneously.
- ▶ **Potential long-term uncertainty:** impacts are difficult to estimate, and the attacker's goal is not always easy to identify.
- ▶ **Scalability:** this type of crisis can rapidly change as attackers are likely to react to the actions undertaken by the targeted organisation, for example, by covering their tracks through destructive actions.
- ▶ **Technical nature of the subject:** due to the complexity of IS and the methods used by attackers, the key actors in crisis management are technical experts. The challenge is to ensure that these experts and the usual crisis management actors understand each other to work together efficiently.
- ▶ **Potential global spread:** given the interconnectedness of systems and the existence of systems with a global footprint, attacks can spread very quickly. The *WannaCry* ransomware attack reached more than 250,000 jobs in 150 countries in a single night and more than 900 million jobs in total.
- ▶ **Elasticity of crisis times:** it is easy for attackers to repeat their attacks with the same methods. In response to a cyber attack, it is, therefore, crucial not only to restore the proper functioning of IS but also to increase the level of protection in order to prevent attacks from occurring again. The *WannaCry* ransomware contaminated victims for more than a year after its appearance.
- ▶ **Exiting a long crisis (of several months):** the technical response, digital investigation and restoration of the normal functioning of the IS can take time. This means that immediate impacts must be managed while establishing a sustainable response. This is why organisations' business continuity plans (BCPs) are crucial in crises caused by cyber attacks.
- ▶ **Complexity of the source:** it is difficult to trace the origin of cyber attacks to a specific person or entity because it is easy to conceal their true identity in cyberspace.

HANDLING A CYBER CRISIS

The consequences of a cyber attack are manifold, as for any event that causes a crisis in your organisation. The effects can be judicial, regulatory, legal, professional, organisational, HR-related, financial, reputational, technical, etc. They can also generate strong media pressure.

Dealing with a cyber crisis, therefore, requires the **coordination of a variety of teams**, whose scope of actions and decisions are both technical (teams in charge of the security of IS, or SIS, IT services, etc.) and strategic (business continuity, communication, etc.) in order to **contain the effects of the crisis** on the one hand and to **restore the proper functioning of the systems** on the other.

At the decision-making level, this involves integrating the information system department (ISD) or the chief information security officer (CISO) into the usual crisis management system in order to provide decision-makers with an informed view of the **course of the attack**, which is essential to **adapt and direct remediation measures**.

At the same time, another unit is responsible for analysing the technical situation and suggesting measures to restore activity. This is the operational crisis unit, simulated as part of the exercises suggested here and which is, therefore, not covered by the methodology set out in this guide.

As regards technical solutions, several steps are to be implemented by the organisation alone, if it is able to, or with the help of service providers. These steps aim to end the effects of the attack and to throw the attacker out of the infected IS:

- **Investigation:** collecting and analysing the technical elements to understand the path of attack used by attackers and their actions on infected systems (measuring the extent of the damage, understanding the source of the damage, identifying actions that could help resolve the situation).
- **Remediation:** restoring systems to their original state by ejecting the attacker from the system and improving security to avoid a similar attack by applying remediation measures.

- **Stabilisation:** improving security in the longer term by defining and applying security measures and improving supervision (detection of attacks).

All of these cyber crisis management procedures must be documented and integrated into a dedicated plan.

The incident and the investigation and remediation stages can be simulated in an exercise. Only the incident and the investigation stage can be played in the RANSOM20 guideline exercise.

How do cyber crisis management exercises work?

A crisis management exercise consists of **simulating a scenario** (i.e. a chain of fictitious events simulating a realistic crisis), but not a real one. It takes place over a **limited period of time**, in a **context designed for the occasion** and is based on handling the management of a crisis that occurs at the time the scenario is played. In order to encourage players to participate and get involved, the simulated fictitious events must be based on **credible events**.

A crisis management exercise must **under no circumstances have a real impact on the organisation's activities**. For instance, in a scenario referring to a cyber attack that causes machines to shut down, the machines must under no circumstances really cease to function. This event is simulated by a call from an employee to their supervisors after noticing that the machines have shut down.

The specific features of the cyber issues described above demonstrate the need to prepare by organising exercises. These must be part of a comprehensive and high-level reflection so that they can provide resilience throughout the organisation and its ecosystem.



Recommendation

An exercise is not intended to surprise or trap participants but to guide them in a structured training session based on defined, communicated and shared goals.

The exercise is considered successful when it has engaged all the participants, enabled them to learn from the exercise and encouraged them to repeat the experience.

STAGE 2

MAKING THE EXERCISE PART OF A COMPREHENSIVE REFLECTION ON RESILIENCE

Making the exercise part of a more comprehensive reflection, which we will call here an exercise strategy, helps to **strengthen the organisation's resilience**.

The exercise strategy will take account of the organisation's crisis management procedures and business continuity, as well as SIS policies and must adapt to the organisation. If such procedures do not exist within your organisation, an exercise may also be an opportunity to consider such procedures.

This strategy must be applicable to the various branches of your organisation. For example, the communication department must be able to turn the overall strategy into a strategy of exercises on cyber crisis communication.

It must also strengthen skills through increasingly complex exercises until all the goals set out above have been achieved. It takes into account training at an organisation's decision-making levels as well as at operational levels.⁵

The exercise strategy particularly makes it possible to:

- ▶ **Raise awareness** about cyber issues among staff and train those who have a role to play.
- ▶ **Test and improve the efficiency of the procedures** implemented under this scheme.
- ▶ **Report on the efforts made** in terms of cyber resilience and therefore meet any legal requirements and societal expectations.

5: This guide only covers training at the decision-making level.

It consists of a concise document, the elements of which can be used to communicate about the approach to build resilience.

Setting up a programme of exercises

Setting the exercise in a dedicated programme makes it possible to **optimise the resources and means used**, as well as to improve the organisation's resilience to cyber attacks by ensuring that as many people as possible are prepared.

The exercise programme should be developed in relation to crisis management or resilience procedures. It is also part of a generally multi-annual step-by-step **learning approach** with goals and steps to be achieved over time. It makes it possible to:

- ▶ **Maintain consistency** with all the planned training.
- ▶ Ensure that the members of staff involved in crisis management can **master the fundamentals**.
- ▶ **Maintain the level of engagement** and awareness among crisis management actors, especially those with less experience in cyber issues.
- ▶ **Maintain knowledge and capitalise** on the acquired skills, particularly during the exercise, as some elements of project management or feedback collection contribute to the continuous improvement of crisis management and business continuity abilities.

Seizing the opportunities of the exercise

In addition to contributions related to preparing and training its participants, the value of the exercise can be seen as follows:⁶

- ▶ Demonstrating that the crisis management scheme makes it possible to **meet legal requirements and societal expectations**, particularly in the areas of SIS and business continuity. Several sectors are subject to specific regulations: Basel 3 (finance) and Solvency 2 (finance and

6: Learning from exercises - Report on Cyber Crisis Cooperation and Management: www.enisa.europa.eu/publications/ccc-study

insurance), Network and Information System Security Directive (NIS) for operators of essential services (OES) and digital service providers. Furthermore, all organisations must comply with the General Data Protection Regulation (GDPR). The organisation of an exercise may also be used to demonstrate to state or insurance bodies, or even customers, that training is being carried out.

- The scenario of the exercise should, therefore, include the necessary legal statements depending on the simulated situation and the applicable legislation. For example, if personal data is unavailable or exfiltrated, the simulation should involve sending a statement to the data protection authority.
- **Reassuring (and/or engaging) the organisation's ecosystem** on its capacity to test its crisis management mechanisms on a regular basis and thus seek resilience. Moreover, including one or more partners in an exercise may create dialogue.
 - Taking account of the organisation's risk analysis when choosing the exercise scenario helps to make the exercise more credible and to demonstrate the organisation's ability to face real threats.
- **Raising awareness internally** by using the exercise as an information vector.
 - Setting up or strengthening an organisation's data security policy can be a difficult project to defend, but it will be clearly illustrated in an exercise simulating a ransomware attack. The exercise may also focus on a critical network or business application to demonstrate the need to protect it.

Coming together and communicating about the exercise

Organising a crisis management exercise provides an opportunity to convey messages at different levels of the organisation by integrating them into a **communication plan**. It can focus on the exercise programme, highlighting the organisation's and directorate-general's ambitions in terms of resilience and the exercises organised in themselves in order to communicate about the specific challenges and goals of each event.

Depending on the scope of the exercise, the communication plan may be aimed at a wider audience than only the participants in the exercise, such as the directorate-general. In addition to communication campaigns to explain the exercise and how it is organised, the communication plan may also **promote and raise awareness about the exercise goals**.

The communication plan consists of the following elements:

- **Goals pursued**, both internally and externally if wider communication is planned.
- **Audiences targeted**, such as the list of persons, entities, internal and external professionals to whom elements about the upcoming exercise are to be sent.
- **Main messages**, both generally on the exercise strategy and then specific to individuals, entities and professionals.
- **Key project dates** (before, during and after the launch of a programme or exercise).
- **Useful resources for external communication** (communication tools on the approach and main lessons).

To draft this plan, you are strongly advised to **rely on your organisation's communicators**.

One of the goals of the communication plan is to calm certain concerns around cyber issues which may reduce participants' interest and/or involvement:

- ▶ Non-technical participants may be afraid that they will not understand the situation or may not feel concerned.
- ▶ Technical participants may be afraid that the exercise is not plausible enough (e.g. if the proposed scenario is too far from their real working environment), and that they will not be fully understood.
- ▶ If the scenario is based on the results of a risk analysis, some may fear being questioned if an uncorrected vulnerability is found (the correction may be complex).
- ▶ All participants may have a fear of failure, making mistakes and being “judged”; participants may view an exercise as a test or an exam, which is a feeling that should be avoided.

The communication plan can therefore be used as a reminder of the positive mindset in which the exercise must be built and conducted.

It may also be useful to identify project sponsors who will act as ambassadors to explain the aim and benefits of participating in the exercise to participants.

Finally, at the end of the exercise, the communication plan makes it possible to highlight the exercise and its conclusions.

In addition to internal actions, wider external communication also guarantees trust in its ecosystem in addressing cyber risks. It also demonstrates the organisation's willingness to prepare up to the highest level.

STEP 1

DESIGNING THE EXERCISE

STAGE 1:

Structuring the exercise 24

STAGE 2:

Identifying stakeholders and players 38

This stage makes it possible to structure the exercise and, therefore, to define the goals, type, scope, participants and date.



DELIVERABLES TO BE PRODUCED:

- ▶ Exercise specifications



FACT SHEETS TO BE CONSULTED:

- ▶ Fact sheet No. 1: Defining the goals of the exercise
- ▶ Fact sheet No. 2: Identifying events and incidents relevant to your exercise
- ▶ Fact sheet No. 3: Creating specifications – example guideline RANSOM20

STAGE 1

STRUCTURING THE EXERCISE

Structuring refers to the stage in which **the specifications are drawn up**. This project structuring document, produced by the planners forming the exercise project group, includes the following elements: goals, scope, theme, duration, participants and game conditions. In order to define this information, the project group may **rely on experts** on the subjects dealt with in the exercise.

Establishing a project group

The project group launches and monitors the development of the exercise. It is responsible for the following tasks:⁷

- ▶ structuring the exercise (see step 1)
- ▶ drafting the scenario and the timetable (see step 2)
- ▶ conducting the exercise (see step 3)
- ▶ collecting feedback from observers (see step 4).

Members of the project group are, therefore, the exercise planners.

The number of persons in this project group depends on the size of the organisation and the scope of the exercise. It usually consists of the following persons:

- ▶ **The director of the exercise (DIREX)**, who is responsible for steering the preparation of the exercise. For cyber exercises, these are usually the cyber decision-makers or the person in charge of SIS. It may also be the person usually in charge of crisis management exercises, risk management or business continuity within the organisation. On the day of the exercise, this person can join the moderating unit and take the role of moderating director (MODDIR).
- ▶ **Several planners**, including at least one SIS expert, one person in charge of business continuity, (potentially) one communicator and,

7: For these tasks, it can rely on experts, moderators and observers whose roles are defined in stage 2 of this step.

if need be, someone who is usually in charge of organising crisis management exercises. On the day of the exercise, the planners can also be moderators.

Defining the goals

Formulating the exercise goals clearly makes it easier to prepare and evaluate the exercise, and to create the action plan based on the feedback collected (see step 4).

To make an exercise as efficient as possible, it is important to define goals at **all levels of play and by area** (communication, decision-making level, SIS experts, etc.). All functions can present the main issues involved in the exercise in terms of professional goals, which will help to reduce passivity in players who may feel that they only have a small role to play in meeting very general goals.

Recommendation

Offer players to think about and prepare their own goals ahead of the exercise in order to strengthen their involvement.



One of the goals is to test the crisis communication strategy in the event of a cyber attack. The playing communicators can transform this general goal into business objectives:

- ▶ Testing how communication is organised in crisis situations (if several communicators are playing).
- ▶ Testing the exchange processes with the SIS expert and management.
- ▶ Communicating on a new topic.

EXERCISE
RANSOM20

Fact sheet No. 1 below provides examples of goals under the RANSOM20 scenario.

FACT SHEET 1:

DEFINING THE GOALS OF THE EXERCISE

The following typology suggests a non-exhaustive list of goals. It presents the elements that can be tested during a cyber crisis management exercise depending on the desired direction. It is illustrated from the RANSOM20 guideline scenario. Ideally, three to four goals should be selected from this list per exercise.

RAISING AWARENESS ABOUT CYBER ISSUES AMONG PARTICIPANTS

During the exercise, participants closely experience the crisis and its effects and will therefore be better equipped to measure the challenges posed by a cyber attack and how to deal with this type of situation. The exercise also increases their knowledge on this topic. The awareness-raising campaign may target:

- ▶ **A specific audience** (executive committee, management committee, board, decision-making/strategic unit, subsidiary, partners, stakeholders, etc.).
- ▶ **A specific problem** (spread of malicious software, exfiltration of data, phishing campaign, etc.).

EDUCATING OR TRAINING STAFF

The aim here is to ensure that those in charge of crisis management have taken on board the scheme, arrangements, procedures and tools developed as part of the cyber crisis management, and that they are able to handle situations where these issues are analysed or determined. Thus, the exercise may make it possible to:

- ▶ **Have the SIS teams work together with the staff** usually in charge of crisis management (as a first exercise).
- ▶ **Establish or develop procedures** specific to cyber issues.
- ▶ **Check that players take full account of all the issues** raised by the cyber attack.
- ▶ **Practise choosing** between different containment, bypass or remedial plans, where each plan will impact the organisation's activities in a specific way.
- ▶ **Develop the expertise** of the crisis unit and professionals in the field of cyber communication (towards customers, collaborators, service providers, subsidiaries, authorities, media, etc.).
- ▶ **Test coordination** with other stakeholders in the crisis (subsidiaries, providers, customers, users, other sites linked to the organisation, etc.).

TESTING THE CYBER CRISIS MANAGEMENT SCHEME

to update or improve it

Where procedures have been defined in advance, all or part of the cyber crisis management scheme may be tested, in particular, to:

- ▶ **Validate or adapt certain tools and documents:** cyber crisis management directory or directories (internal and external contacts (incident response providers, insurance, supervisory authority, etc.), role description of participants in cyber crisis management, etc.)
- ▶ **Test the proper functioning of alert and escalation chains** (have all those involved in crisis management been asked for help and if so, were they solicited at the right time?).
- ▶ **Test the crisis communication strategy** (have the communication tools been passed on to the right people, both internally and externally?).
- ▶ **Test back-up procedures** (other emails, other telephone networks, means of communication, etc.), or procedures for critical activities during a deteriorating crisis.
- ▶ **Test the BCP or the business recovery plan (BRP).**

A step-by-step approach can also be chosen to test the cyber crisis management system by trying to use a scheme with one crisis unit, then a scheme with several crisis units, and then testing the various aspects of the scheme (interactions, business, communication, etc.).

The goals set

- ▶ Ensuring that all the people needed to manage the crisis have been called upon.
- ▶ Testing the crisis communication strategy for cyber issues.
- ▶ Bringing about coordination between the organisation's main site and one of its secondary sites (sharing of information, transmission of instructions, etc.).
- ▶ Training players to manage a crisis that is deteriorating/testing deterioration procedures.

EXERCISE
RANSOM20

Deciding on the exercise format

The exercise format will be chosen based on:

- the goals set out in the previous step
- the allocated budget
- the resources available for preparation and participation
- the level of experience of the involved organisation(s).

You can organise tabletop exercises or simulations by announcing them in advance or not. Unannounced exercises are, however, to be limited to organisations that have already carried out a number of exercises and which, for example, have on-call professionals that can be asked for help at any time. Unannounced exercises should be avoided when inviting decision-makers. When organising a cyber crisis exercise for the first time, organising a planned tabletop exercise is recommended.

This guide suggests two⁸ exercise formats: a tabletop and a simulation exercise.

8: Reminder: the exercises in this guide are only at the decision-making level. However, other formats exist.

TABLETOP EXERCISE

MEANING	Participants gather around the same table. A moderator informs them of the situation. Players think together about what needs to be done to try to solve the crisis.
PLAYING LEVEL	A group is mobilised (or several sub-groups). This could involve the decision-making crisis unit alone or accompanied by technical experts on the discussed subject or a group of decision-makers whose awareness about cyber issues is to be raised.
DURATION	2-3 hours (including briefing and debriefing)
PREPARATION TIME	About 6 weeks
BENEFITS	Ideal for an organisation that is not used to running cyber crisis management exercises or that wishes to raise awareness on this topic. This type of exercise helps people who have little time to devote to an exercise to get familiar with the topic (management, executive committee, etc.). It allows ideas to be drawn up to establish or improve a cyber crisis management system. However, it is not possible to test your organisation's crisis schemes with this exercise.

If you choose this exercise format, the stages of step 2 can be followed less intensely. For instance, there is no moderating unit but only one or two moderators accompanied by an observer; only one player briefing is to be organised on the day of the exercise; feedback can only be collected once. However, it is advisable to draw up a short timetable to frame the exercise. To suggest a developing situation to the players, the RANSOM20 scenario may be used, and the different stages of the scenario may be presented to the players on slides (see fact sheet No. 4).

SIMULATION EXERCISE

MEANING	Exercise requiring at least one crisis unit, containing the players, and a moderating unit. The latter creates a crisis situation by simulating events and interactions between individuals and organisations asked by the players for help, but it does not take part in the exercise.
PLAYING LEVEL	SEVERAL POSSIBILITIES: <ul style="list-style-type: none">▶ If only one crisis unit is involved, the moderators must simulate all the interactions that this unit would have had in real situations.▶ If several crisis units are playing, moderators should simulate interactions with these units without interfering with the exchanges between players, and strengthen observation capacities. <p>Configuration examples:</p> <ul style="list-style-type: none">▶ decision-making unit alone▶ decision-making unit with one or more other entities (subsidiaries, other sites, etc.). <p>The greater the number of participants, the more time, resources and coordination between the different entities are required to prepare the exercise. For this type of exercise, at least one representative of each entity must be included in the project group as well as in the moderating unit.</p>
DURATION	Between half a day and two days (including briefing and debriefing).
PREPARATION TIME	Around two to six months.
BENEFITS	Deep immersion, increased awareness, makes it possible to test interactions between several crisis units, and shows the strengths and areas for improvement throughout the cyber crisis management scheme.

The RANSOM20 guideline exercise is developed in this format.

Selecting the theme

The choice of the cyber attack to be simulated during the exercise is guided by:

- ▶ the exercise goals defined above
- ▶ the analysis of the cyber threat to your organisation or industry
- ▶ scenarios based on risk analysis
- ▶ feedback from past crises and incidents, previous exercises and incidents that have affected other organisations.

Since those responsible for organising crisis management exercises do not necessarily master cyber issues, relevant expert advice, depending on the desired scenario, should be used. To this end, the first point of contact may be the person in charge of SIS within the organisation who can provide information about the state of the cyber threat. The information available from open sources or ANSSI publications⁹ can also be consulted to have an overview of recent cyber attacks.

Recommendation

It is important to be cautious about individuals or teams who are convinced that their systems are flawless. In order to avoid this pitfall and as a means of endangerment, you can create a fictitiously uncorrected loophole that has just been published, or you can plan an indirect attack (e.g. through one of your organisation's providers).

Fact sheet No. 2 below provides examples of cyber attacks that could constitute an exercise scenario.

9: Visit the CERT-FR website under “threats and incidents”: www.cert.ssi.gouv.fr/cti

FACT SHEET 2:

IDENTIFYING EVENTS AND RELEVANT FOR YOUR EXERCISE

Several types of events and incidents can be dealt with in the same exercise. A number of these are presented in the table below, which is not exhaustive.

TYPE OF ATTACK	REASON(S) FOR, OBJECTIVE(S) OF THE ATTACK
WEBSITE DEFACEMENT	Provocation, hacktivism
DENIAL OF SERVICE (DOS)	Provocation, profit-making attack, hacktivism
DATA EXFILTRATION	Personal data (employees and/or clients) with or without disclosure, profit-making attack, hacktivism, espionage, etc.
	Critical data (patent, strategic data, etc.) with or without disclosure, profit-making attack, hacktivism, espionage, etc.
DATA ENCRYPTION/ DESTRUCTION	Profit-making attack, sabotage
DESTRUCTION OF THE SERVICES	Sabotage via encryption/destruction of business applications. All or part of the servers hosting the applications are non-functional (email, SAP, etc.).
	Sabotage via encryption/destruction of infrastructure applications. All or part of the equipment supporting the infrastructure is destroyed (Active Directory, workstation, etc.).

INCIDENTS

POTENTIAL IMPACTS
Reputational impact
Reputational impact, unavailability of one or more application tools, partial or total triggering of a BRP or BCP
Reputational impact, triggering the GDPR/national authority scheme
Commercial impact, impact on trust and reputation
Offline backups that can be activated: operational impact, reputational impact, legal impact in the event of disclosure of confidential data
Encryption/destruction of backups: major operational impact, reputational impact, loss of data, unavailability of one or more applications, partial or total triggering of a BRP or BCP, legal impact in the event of disclosure of confidential data
Unavailability of all or part of the applications
Unavailability of all or part of the IS

To train players to manage a deteriorating crisis and to test coordination between two sites, one of the incidents selected for the scenario is data encryption via a ransomware attack that spreads to a second site of the organisation. As a result, activities are at a standstill, and the usual tools such as email are ineffective.

To test the communication strategy on cyber issues, blackmail with data exfiltration has been selected. The publication of exfiltrated data makes the attack visible and requires the preparation of communication elements.

EXERCISE
RANSOM20

Determining the duration

To give the players time to become familiar with the scenario and adapt to the pace of the exercise, the recommended **minimum duration** for a cyber crisis exercise is **around three hours**. However, tabletop exercises may be shorter (one-two hours).

The ideal duration for a simulation is a day (about six hours), as it allows for a more comprehensive scenario from the onset of the crisis to the beginning of the resolution.

Most of the time, **the pace of cyber crisis management exercises is accelerated compared to the real pace**. The constraints of players' work schedules make it harder to mobilise participants for more than one or two days. For example, in real life, investigations to better understand the origin of an attack take several days or even weeks. The same applies to the return to normal operation of the affected IS. These differences in timing are worth reminding people of before and after the exercise.

A **short exercise** reduces realism but can increase intensity. It also makes it possible to involve **players with a busy work schedule** for whom it is complicated to devote a whole day to an exercise.

A **long exercise** helps to **increase realism**, to really train to work in a **deteriorating crisis mode** and to add more injects without overwhelming the players. However, it may be more complicated to implement when working with a decision-making unit and particularly the members of the management. In such cases, it is possible to only mobilise players at certain key times with a playing rate that is representative of real conditions.

Consider a night stage exercise to test on-call procedures. It is possible to relay the teams involved. However, it should be borne in mind that a multi-day exercise consumes time and resources and can lead to disengagement. Decision-making level exercises rarely exceed two days.

Naming the exercise

Giving the exercise a name (e.g. RANSOM20) encourages **interactions between participants** and helps to prevent alarming non-playing employees by explicitly referring to interactions related to the exercise. However, the name should not be too explicit to keep a certain amount of surprise for players as to the chosen topic.

Planning logistical resources

The logistical aspect is essential. It depends on the facilities that are already in place in the organisation and on the existing incident management and crisis management procedures.

To ensure that the exercise runs smoothly, the following elements are required:

- ▶ **Tools** for participants to exchange with each other (computers, telephones, organisational applications, discussion groups, etc.). This equipment must have been sufficiently tested before.
- ▶ If the exercise is carried out in-person, **one room per crisis unit** equipped with means of communication.
- ▶ A **moderating room** that is also equipped with means of communication and that is large enough for moderators not to disturb each other when they are on the phone. It should be noted that the moderation room may be located in a different location from the rooms dedicated to crisis units.
- ▶ **Catering** for participants if the exercise lasts one or more days.
- ▶ **Displays** showing the unavailability of IT equipment if this corresponds to the chosen scenario.

Taking stock of the state of preparedness helps to **see how well your organisation is prepared for a cyber attack**, particularly through ransomware. Additional tools (emergency means of communication)

or operating procedures for a deteriorating crisis can thus be implemented in advance of the exercise.

Defining the timetable

The timetable is drawn up in parallel with the structure for the exercise and must take account of the calendar year (public holidays, holidays) and, if need be, the constraints caused by the participation of organisations located abroad (holidays and local public holidays, time difference).

A timetable generally includes the following steps:

- A **kick-off meeting** to present the project to planners and sponsors, to identify key objectives and to define the timetable.
- An **initial planning meeting** bringing together only the planners and allocating roles and tasks for the design of the exercise.
- **Interviewing of experts stage.**
- **Defining the timetable stage.**
- **Progress points** to coordinate the project team and ensure that its developments are consistent.
- A **final planning meeting** to agree and conclude the drafting of the scenario and the timetable.
- **One to two player briefings** to present the project, the goals and the playing conditions; the first one will take place a few weeks before the exercise; the second is essential and takes place on the day of the exercise.
- **Two briefings for moderators and observers**, before the exercise and on the day of the exercise, to ensure that everyone is familiar with the scenario, roles and goals.
- **A date for the exercise**, to be communicated to the participants as soon as possible (a few months ahead) to ensure that they are available throughout the whole exercise in advance.

- ▶ **A second date in case the exercise is postponed**, for example in case an incident occurs.
- ▶ **A collection of feedback meeting** (ideally immediately after the exercise) to collect participants' opinions.
- ▶ **A collection of feedback meeting later on** (ideally between two weeks and a month after the exercise) to complete the after action report and present initial conclusions.

Between the project kick-off meeting and the date of the exercise, preparation may take between two to six months. The preparation time depends on the complexity of the exercise.

Recommendation

Postponing the exercise should be avoided as far as possible, since it may discourage participants.



STAGE 2

IDENTIFYING STAKEHOLDERS AND PLAYERS

An exercise can involve both a limited number of people as well as your organisation as a whole.

It is important to identify stakeholders from the start of the project, i.e. those who will be involved in the preparation of the exercise (planners, experts) and in the exercise itself (moderators, players, observers).

The number of stakeholders and players determines the required preparation time and the organisation of any training and information sessions.

As the project group has been presented in Step 1, its role is not detailed here.

EXPERTS

DEFINITION

In support of the project group, experts contribute to the construction and realism of the scenario by providing input on the chosen theme. Experts may also include people who, beyond their area of expertise, are familiar with the history of the organisation both in terms of how it operates and past exercises, incidents and crises.

DESIRABLE PROFILES/SCOPE

In a cyber exercise, the following experts can be relied upon:

- ▶ **“Professional” experts:** one to three people who are (ideally) part of or who know of the occupations affected by the shutdown of office stations and of a department or production chain;
- ▶ **“Technical/SIS” experts:** a person with knowledge of the IT environment in its architecture and major security features, and, if possible, one or two persons in charge of SIS activities such as security incident detection, network security or incident response.

APPLICABLE STEP(S)

STEP 1 

STEP 2 

OTHER POSSIBLE ADDITIONAL ROLE(S)

- ▶ Moderators or observers (recommended).
- ▶ Players if they do not know the scenario.

PLANNERS/MODERATORS

	On the day of the exercise, planners can become moderators and their task is to implement the timetable in order to suggest a cyber crisis situation to players and thus meet the goals set in advance. Some moderators may not have been involved in planning the exercise. However, it is essential that they have a good knowledge (and understanding) of the scenario, the timetable and the goals.
DEFINITION	The moderators run the scenario by sending the injects that can be in the form of emails, calls or real interactions. They answer questions and adapt to the players' reactions. A standard FAQ document may be prepared to assist them in this task.
	In order to train a crisis unit in the conditions closest to reality, it is essential to have moderators who are able to answer questions and who are familiar with the problems that players will face.
DESIRABLE PROFILES/SCOPE	<p>A cyber crisis exercise requires at least:</p> <ul style="list-style-type: none">▶ A leading moderator responsible for coordinating the moderating unit and, if need be, for adapting the scenario to the players' reactions. This could be the DIREX who steered the planning of the exercise and who then becomes the MODDIR.▶ A secretary responsible for monitoring the timetable to ensure that the exercise is consistent (a register may be used in a moderating unit).▶ Depending on the number of simulated players, one to four moderators to respond to players' calls and emails. To be more effective, moderators can allocate roles to each other depending on their expertise. <p>Together, they form the moderating unit.</p>
APPLICABLE STEP(S)	<p>STEP 3 ✓</p>
	<p>STEP 4 ✓</p>
	<ul style="list-style-type: none">▶ They are often members of the project group.

OBSERVERS

The role of an observer is, as the name indicates, to check that the crisis management scheme is operational. In order to do so, observers must rely on the exercise goals, the expected reactions specified in the timetables as well as the players' actual reactions.

DEFINITION

Unlike moderators, observers do not intervene during the exercise itself. They provide an external view to identify strengths and areas for improvement. Their role is also to alert the moderating unit if an exercise is blocked, particularly when the moderating unit is physically far from the players' crisis unit.

In order to carry out an active observation, it is strongly recommended that observers have knowledge of crisis management and/or cybersecurity as well as the organisation's overall functioning. They may also be persons who were involved in setting up the scenario or the injects. Project group members or experts who are not moderators can also be observers.

DESIRABLE PROFILES/SCOPE

Depending on the scope of the exercise, observers are divided across different sites or different crisis units. They may also be tasked with observing specific players (head of the crisis unit, communication officer, etc.). However, in order not to disrupt players' views, it is recommended to limit the number of observers (no more than two per room).

Observers may have observation grids identifying the key areas required for collecting feedback immediately after and some time after the exercise. Observation elements are suggested in fact sheet No. 8.

APPLICABLE STEP(S)

STEP 3 ✓

STEP 4 ✓

OTHER POSSIBLE ADDITIONAL ROLE(S)

- ▶ Experts

PLAYERS

DEFINITION

The players are those who will face the fictitious crisis presented by the moderators. They are not familiar with the scenario and are preferably playing at their place of work, using the usual means of communication and operational procedures. The aim is for them to be immersed in the most plausible way possible, even if all the events and incidents are simulated.

DESIRABLE PROFILES/SCOPE

The profile of players depends on the type of exercise, its goals and its theme. For a cyber exercise at the decision-making level, high-level profiles should be involved, as well as a cyber decision-maker or someone in charge of SIS. More generally speaking, the exercise should involve all those who would be mobilised if the exercise's simulated event were to happen in real life.

On the day of the exercise, these players must be able to:

- ▶ **Evaluate:** provide an assessment of the impact of the situation and of the residual risks from which part of the decisions would be taken.
- ▶ **Plan:** in particular, make decision-makers (whether they are players or simulated) aware of the deadlines for implementing the intended measures and of regulatory constraints.
- ▶ **Anticipate:** suggest various developments in the crisis, particularly based on the adopted corrective decisions, and the necessary trade-offs between continuity issues (to remedy and restore certain IS as soon as possible) and security issues (isolating and interrupting certain IS).
- ▶ **Explain:** to explain, in a nutshell, the concepts of IT security and the issues at stake to all employees, especially those with no technical skills.

APPLICABLE STEP(S)

STEP 3 



Recommendation

When a player has never participated in an exercise and appears to refuse to participate, a solution is to involve this person as an observer first. This helps to downplay the challenges of the exercise and to show that it is possible to make mistakes. Furthermore, assigning the players' direct superiors as observers should be avoided. This may mislead them into believing that they are being monitored or evaluated during the exercise. To avoid distorting the players' reactions during the exercise, the scenario developers should avoid participating as players. However, certain experts who were interviewed to create the scenario may participate as players if they are not aware of the whole scenario.

Once all these elements have been identified, a specification is obtained as the starting point for the next steps (see fact sheet No. 3 below).

The scenario still needs to be defined in detail. This is the goal of the next step.

FACT SHEET 3:

CREATING SPECIFICATIONS

EXAMPLE GUIDELINE RANSOM20

TYPE OF EXERCISE	<input checked="" type="checkbox"/> Partial <input type="checkbox"/> General	<input type="checkbox"/> Tabletop <input checked="" type="checkbox"/> Simulation	<input checked="" type="checkbox"/> Expected <input type="checkbox"/> Unexpected
ADDRESS OF EXERCISE SITES	[address of organisation] [address of second site]		
SCHEDULED DATE	DD/MM/YYYY		
TIME SLOT	<input checked="" type="checkbox"/> Day <input type="checkbox"/> Night	<input checked="" type="checkbox"/> Morning <input checked="" type="checkbox"/> Afternoon	START EX 09:30 END EX 17:00
PLAYER LEVEL	Headquarters decision-making crisis unit + crisis unit of the second site		
NAME OF DIREX	Cyber or safety director		
NAME OF MODDIR	CISO		
GOALS	<ul style="list-style-type: none">▶ Ensuring that all the people needed to manage the crisis have been called upon.▶ Testing the crisis communication strategy for cyber issues.▶ Bringing about coordination between the organisation's main site and one of its secondary sites (sharing of information, transmission of instructions, etc.).▶ Training players to manage a crisis that is deteriorating/testing deterioration procedures.		
THEMES	Ransomware attack on the organisation's headquarters and that spreads to a second site + data exfiltration and threat of public disclosure with ransom request.		

PARTICIPANTS			
PLAYERS	<p><i>[fill in the players' names]</i></p> <p>At each site: decision-making people, people involved if the event played during the exercise were to occur in real life (professional impacts, SIS experts, communicators).</p>		
PLANNERS/ MODERATORS	<p><i>[fill in the planners' names]</i></p> <p>The CISO or a member of that team, "professional" experts (one to three people who know of the occupations affected by the shutdown of office stations and of such departments or production chains) and "technical/SIS" experts (persons with knowledge of the IT environment in its architecture and major security features, and, if possible, one or two persons in charge of SIS activities such as security incident detection, network security or incident response).</p>		
OBSERVERS	<p><i>[fill in the observers' names]</i></p> <p>At least one per unit: one of the members of the project group who is not a player, planner or moderator and one or two experts.</p>		
ROLES TO BE SIMULATED BY THE MODERATING UNIT	Type of actor		
	Internal	Public	Private
The organisation's technical team and any actor relevant to the exercise who is unable to take part.	Ministry or supervisory authority.		Subsidiaries, suppliers, providers, insurers, customers, etc.
	Other	Any body which can provide assistance or to whom the incident must be reported.	
PACE	<input checked="" type="checkbox"/> Fast	<input type="checkbox"/> Slow	<input checked="" type="checkbox"/> Reduced time
EXERCISE COMMUNICATION	<input checked="" type="checkbox"/> Yes Conclusions of the feedback collected internally at the end of the exercise.		<input type="checkbox"/> No

FACT SHEET 3: CREATING SPECIFICATIONS FOR EXAMPLE GUIDELINE RANSOM20

	Outline and organisation over time
SCENARIO	<p>Stage 0: before the start of the exercise (context and situation information file).</p> <p>Stage 1: START EX, several of the organisation's members of staff report the appearance of a ransom note on their computers.</p> <p>Stage 2: the malware has been deployed throughout the office space and is now also affecting a second site of the organisation.</p> <p>Stage 3: the attackers have published the data that they have exfiltrated from the organisation and the second site. They request ransom payment to prevent other documents from being published. At the same time, the press contact the organisation.</p> <p>Stage 4: information on the ransomware and the source of the attack is obtained after analysis, and potential approaches have been agreed upon for a (non-immediate) recovery of activities.</p> <p>END EX and start of feedback collection.</p>
RULES OF THE EXERCISE	The investigation stage is fully simulated. Technical information will be sent to the crisis unit by a member of the moderating unit who will act as a member of the technical/SIS team. The stage of return to normalcy is not played in this exercise.
LOGISTICS	Ransomware affecting the entire office space, computers and some of the staff's usual tools (including those in a crisis unit) are no longer usable. Remember to show this by, for example, displaying a false ransom demand on the screens of the crisis room and preventing players from using the tools involved.
IMMEDIATE COLLECTION OF FEEDBACK	DD/MM/YYYY – 17:00
LATER COLLECTION OF FEEDBACK	Day of the exercise + 15/MM/YYYY – 10:00

STEP 2

PREPARING THE EXERCISE

STAGE 1:

Defining the scenario 50

STAGE 2 :

Drawing up the timetable 61

STAGE 3 :

Preparing the other documents 76

STAGE 4 :

Briefing the participants and ensuring they are involved 86

Preparing an exercise is as important as running it. It is important to define a plausible scenario, to draw up a timetable with the right degree of probability and intensity, i.e. it does not make participants feel bored or overwhelmed, and it is essential to prepare injects adapted to the players.

At the end of this stage, you will have a finished scenario and timetable. You will also have written out all the injects that are ready to be sent.

The moderators and observers have been briefed. You are now ready to start the exercise.



DELIVERABLES TO BE PRODUCED:

- ▶ Scenario
- ▶ Moderator and observer briefings
- ▶ Timetable
- ▶ Observation sheet
- ▶ Directories
- ▶ Player briefings
- ▶ Situation information file



FACT SHEETS TO BE CONSULTED:

- ▶ Fact sheet No. 4: Drafting the scenario
- ▶ Fact sheet No. 5: Simulating media pressure, roles to be taken and questions to be asked
- ▶ Fact sheet No. 6: Drawing up the timetable
- ▶ Fact sheet No. 7: Producing a situation information file
- ▶ Fact sheet No. 8: Observing an exercise

STAGE 1

DEFINING THE SCENARIO

The scenario is based on the general outline of the exercise (see step 1). It describes the entire crisis situation and its repercussions, sometimes going up to its resolution (only with long exercises).

This document may change over the course of the creation of the exercise. It must constantly be kept up to date, along with the timetable.

The scenario should include an **event leading to the activation of a crisis unit** around a cyber issue. Most of the time, a cyber crisis starts with an SIS incident. It is the scope and impact or uncertainty of the severity of this incident on the organisation that causes the situation to turn into a crisis. In order to determine this event, you must **ask your SIS expert** what could have a significant or major impact on your organisation (endangering the activity of several departments, major damage to the organisation's image, etc.). The business continuity officer and/or the risk manager may also provide you with information on the risks that have been identified in this area.¹⁰

Whether it is made-up or based on real facts, a scenario must, above all, be credible and reflect the **state of the cyber threat** that may affect your organisation at the time of the exercise.

The “**technical**” part of the exercise, simulated as part of a decision-making exercise, consists of gradually making players discover the **course of the attack and its developing impact** (for example, by communicating the results of technical analyses to players). The information used to simulate the technical part will be obtained in advance by interviewing experts.

The RANSOM20 scenario, described in fact sheet No. 4, focuses on the **immediate reaction and investigation stages**. It ends with the communication of elements to start the **remediation stage** which is not detailed in the given play time. A cyber crisis management sce-

¹⁰: Ideally, the scenario is based on an upstream risk analysis, particularly with the help of the EBIOS Risk Manager, ANSSI, 2018: www.ssi.gouv.fr/en/guide/ebios-risk-manager-the-method/

nario may, however, cover the **remediation stage**, in preparation for a return to normalcy.

It is also possible to play a scenario involving a **ramped up crisis scheme**, where the crisis director convenes the various participants. This may make it possible to test the organisation's ability to identify the right participants for this type of crisis, having previously identified and alerted all potential players.

The diagram below illustrates the different stages of a cyber crisis that can be played during an exercise:



Recommendation

When an exercise is conducted for the first time, it is not appropriate to suggest an exit from the crisis immediately at the end of the scenario, as this may give the impression that a cyber crisis does not take long to resolve. Moreover, this prevents participants from thinking about the medium/long term consequences.

In any case, irrespective of the stage played, scenarios will include the following elements:

- ▶ **A cyber attack**, the consequences of which mark the start of the exercise (for example, a ransom note is displayed on screens).
- ▶ The occupational **consequences** and impacts on the organisation's activities, which may change over the course of the year (increase of the scope affected).
- ▶ **Technical details of the attack** which may be more or less detailed depending on the type of players (a publisher's paper on a vulnerability, information on the tools used by the attacker, information on the impacted IS, etc.).
- ▶ **Elements relating to the organisation's ecosystem, socio-political elements and media pressure** (reactions from partners, customers, regulatory authority, press, general public, etc.).
- ▶ **Technical resolution of the situation**, the drafting of which is recommended when the exercise lasts at least one day (distribution of a day zero vulnerability correction used when the situation has not yet been corrected, restoration of the impacted systems in the presence of healthy safeguards or reconstruction of these systems if need be). This helps to avoid frustration from players who will want to continue playing until the situation is resolved. For shorter exercises, the conclusion of the exercise or debriefing stage may be used to address the technical resolution strategy.

Recommendation

To examine real examples, visit the CERT-FR website¹¹ which identifies the most recent and serious vulnerabilities. You can also consult the ransomware memo¹² to choose one or to simulate a fictitious malicious code.



11: CERT-FR website: www.cert.ssi.gouv.fr

12: Ransomware threat to companies and institutions: www.cert.ssi.gouv.fr/cti/CERTFR-2020-CTI-001

To maintain an **educational** dimension and encourage players to participate in other exercises, **an overly catastrophic scenario should be avoided**. Such a scenario would risk overwhelming players by causing excessive stress due to the exercise containing too many serious events, which may **discourage participants**, especially if it is their first exercise of the sort. One solution may be to **limit the perimeter of the attack** to a specific part of the IS (only the office IS, critical business application, etc.).

A strong **lack of realism** can also be an obstacle making it hard for participants to imagine the scenario, to make decisions, causing them to question the scenario, etc. This is another aspect that can **discourage participants**.

Interviewing experts

Interviewing experts allows you to obtain the information needed to draft a realistic scenario and timetable.

It also helps to **know the cyber risks** that the organisation is exposed to, to determine **which event(s) will trigger the crisis** and to identify the various consequences of the event. **Expert interviews provide technical insights into the IS affected** and provide a **better understanding of the procedures** and functioning of the organisation in the event of a cyber attack.

- In the case of a scenario involving the exploitation of a vulnerability, it is essential to look into the likelihood of the existence of such a vulnerability in relation to the organisation's IS.

In order to establish the framework of the scenario and the elements for drawing up the timetable, at least one **collegial meeting with all the experts** should be organised. Then, bilateral meetings, with one or two experts, on specific aspects of the scenario or the drafting of certain injects can be considered.

In order to have a clear view of the series of incidents and to structure the collected ideas and opinions, a first version of the scenario should be **drafted quickly after the interviews with the experts**. This will prevent the scenario from involving a scope that is too large or too far from the predefined structure. This format, which is more literary and concise than the timetable, can be sent to anyone who needs to quickly read the scenario (with the exception of players) or validate it. It can also be **used during the collection of feedback** immediately after and some time after the exercise.

FACT SHEET 4:

DRAFTING THE SCENARIO

EXAMPLE GUIDELINE RANSOM20

The suggested scenario is based on four main events: an attack on the office network; its spread to at least one other site; media coverage of the attack; publication of the exfiltrated data by a group of attackers to pressure the organisation to pay a ransom.¹³

Disclaimer: the scenario imagined here involves French entities. It simulates the intervention of ANSSI, the French National Cyber Security Agency (national authority for cyber security) and CERT-FR (national CERT, part of ANSSI). It is recommended to adapt the scenario and injects to your national cyber organisation and legislation.

PROPOSED ORGANISATION OF THE EXERCISE DEPENDING ON ITS DURATION:

	PLAYER BRIEFING	EXERCISE	IMMEDIATE COLLECTION OF FEEDBACK	COMMENTS
HALF A DAY	09:00 to 09:30	09:30 to 12:30	12:30 to 13:30	Start the exercise by immediately announcing the attack and its consequences: the entire IT environment is affected by a cyber attack, it is impossible to use the organisation's computers. Then, an hour later, simulate a call from a second site that is also affected by the attack. The team will focus on understanding the situation and business continuity. It is also possible to announce requests from the press and social media to train the communication departments. ¹⁴
ONE DAY	09:00 to 09:30	09:30 to 17:00	17:00 to 18:00	Follow the exercise as presented below.
ONE AND A HALF DAYS	09:00 to 09:30	09:30 to 17:00 (D1) 09:30 to 14:00 (D2)	14:00 to 15:00	It is possible to slow down the pace of the exercise to add realism and to train players to use investigative time to anticipate. It is also possible to add data exfiltration on the second day to test crisis communication. On the morning of the second day of the exercise, it is possible to inform the players of the events that fictitiously took place in the night (e.g. results of technical analyses).

13: The exfiltration and possible disclosure the victim entity's internal data is neither characteristic nor systematic of a ransomware attack. The latter may be accompanied by a separate attack with a different malicious code designed to exfiltrate data which may potentially be disclosed by the attackers.

14: For more information, see the recommendations for conducting a tabletop exercise, p. 29.

FACT SHEET 4: DRAFTING THE SCENARIO

EXAMPLE GUIDELINE RANSOM20

1. INFECTION OF THE IS OF THE ORGANISATION'S MAIN SITE

At 09:30, the technical teams receive a call from an employee of the organisation: their workstation has restarted by itself and is displaying a static message asking for a ransom to be paid within 24 hours to retrieve the data that has been encrypted and that is, therefore, no longer accessible. The employee can no longer use their workstation. In the following hour, several employees report similar problems and send photos of their screens displaying the same ransom message.

It appears that the office network of the organisation's main site has been targeted by a ransomware attack. **At 10:15**, following the attack, a large part of the network is affected and made unavailable. Many employees of the organisation's main site can no longer work.

- Note: list all the functions interrupted by the infection: to be chosen by the planner of each organisation depending on the internal organisation.

2. START OF MEDIA PRESSURE

At 10:45, one of the employees publishes a picture of one of the infected workstations on Twitter. Press contacts the organisation about the ongoing incident. The organisation is also contacted on social media.

At 11:00, the ransomware has infected the entire IT environment, counting the workstations and servers, including back-up servers connected to the network.

- Depending on the desired level of difficulty for the exercise, the attack may or may not affect the entire IS and all means of communication (emailing, telephony). The development of the exercise must reflect the scope of the consequences of the attack: if emailing services are no longer available, communication is no longer possible by email, and injects must be communicated using other means.

At 12:00, a claim for the attack appears on a website, stating that in addition to the IS encryption, data has been exfiltrated and will be published if a ransom is not paid within 24 hours.

"NATIONAL AUTHORITY SIMULATION" OPTION, IF APPLICABLE

At around 13:00, the national authority is informed of the incident and initially sends good practice documents on ransomware attacks.

If your organisation does not fall within the national authority's scope, you can simulate a service provider who carries out the analyses and provides recommendations (see fact sheet No. 6).

French case: most injects simulating ANSSI in the timetable can also be issued by a cyber security provider.

→ Whether it is the national authority or a provider, the transfer of technical elements is simulated. The national authority or the provider, after fictitiously carrying out analyses, will provide information on the ransomware and recommend the actions to be taken to resolve the situation.

3. SPREAD OF THE ATTACK

OPTION TO "PLAY WITH ONLY ONE CRISIS UNIT INVOLVED"

At 13:10, the head of a second site of the organisation informs the technical teams that the workstations (or industrial control systems) on their site are no longer available. The workstation screens display a note demanding a ransom payment.

At 13:10, employees at the second playing site inform their superiors that their screens are displaying a note demanding a ransom payment.

→ The aim is, particularly, to work on coordination and communication between these two entities.

For both options, the attack gradually spreads throughout the second site. Orders or services can no longer be fulfilled.

→ All orders or services which cannot be fulfilled due to the infection should be listed here.

OPTION TO "PLAY WITH SEVERAL CRISIS UNITS INVOLVED"

FACT SHEET 4: DRAFTING THE SCENARIO

EXAMPLE GUIDELINE RANSOM20

4. OVERVIEW OF THE ATTACK

At 15:20, the IS interconnections of the other sites of the organisation as well as the systems of the main site are cut off, stopping the spread of the malicious code. Only the main site and a second site are affected by the attack.

- If the organisation takes this decision earlier on, this must be taken into account by the moderating unit.

5. INCREASED MEDIA PRESSURE

**OPTION TO
"PUBLISH
EXFILTRATED
DATA"**

At 15:35, an employee announces that the organisation's data (headquarters and second site) has been published on the Internet. After several employees have looked into it, they confirm that the documents come from the organisation and the second site.

- The moderating team must decide which documents have been published and draw up a list to be forwarded to the players. No real documents need to be gathered to simulate the publication.

The press, which has heard about this publication, contacts the organisation to obtain confirmation of the incident. Internally, several employees are worried about the publication of personal data.

6. FIRST RESULTS OF THE TECHNICAL ANALYSES OF THE ORIGIN OF THE ATTACK

From 15:45 onwards, elements from the investigation conducted by the technical teams (with the support of a provider or the national authority if choice was made to simulate one or both) are gradually shared with the crisis unit. The attackers appear to have entered the IS either by exploiting a vulnerability affecting the Remote Desktop Protocol (RDP) (already identified vulnerability but the patch had not been deployed yet on certain servers of the organisation connected to the Internet) or via a phishing campaign (an employee opened a malicious attachment/clicked on a malicious link exploiting a vulnerability affecting the already known or unknown Windows operating system, day zero). Moreover, the malicious programme uses multiple means of lateralisation (e.g.

exploitation of legitimate Microsoft Windows services based on the NotPetya code model, and codes published on the Internet to exploit known vulnerabilities such as Eternal Blue).

The ransomware used by attackers appears to be Evil Ransomware, which has been active since 2019 (more information below).

→ Important: in order to allow players to experiment with several stages of the crisis, the exercise is voluntarily accelerated and is not representative of what would have happened in real life. Investigations can last between several days to several weeks.

7. REMEDIATION

At around 16:50, the technical teams have established a remediation strategy. Depending on the state of the backups, two options are to be suggested by the technical teams simulated by the moderating unit:

- It should be determined beforehand whether or not the organisation has offline backups as the management of consequences will be different.
- ▶ **A. Off-line backups are protected** (on an isolated server and completely disconnected from the infected network) **and functional:** the aim is to deploy these backups once the attack has been contained (after a few days). However, this data may be old or even obsolete if it is not frequently updated. The nominal resumption of activities will be possible within around a week.
- ▶ **B. The backups are impacted** (partial or complete loss of data), in which case all or part of the system needs to be restructured. This may take time and means that activities can gradually resume in a few weeks' time.

Media pressure continues throughout the day with calls and emails from journalists looking for more information on the situation, the origin of the attack and the organisation's resumption of activity.

END OF THE EXERCISE

Since exercises have a limited duration, it is difficult to go up to the resolution of the situation, which, in the event of a cyber crisis, can take several days or even weeks. The resolution may, however, be announced at the end of the game or

FACT SHEET 4: DRAFTING THE SCENARIO

EXAMPLE GUIDELINE RANSOM20

when organising the collection of feedback for immediately after the exercise. A member of the moderating unit then explains how the situation would have developed in real life and what the steps and deadlines would have been for resuming normal activity.

Example: after containing the attack and expelling the attacker from its IS, the organisation deployed the backups or reconstructed its IS and partially resumed its activities after 6 days of interruption. A week later, all activity has resumed even if some databases will not be reconstructed in the same way for several months; the complaint is ongoing. In the event that backups cannot be used, the reconstruction of the IT environment forces the organisation to maintain deteriorated working methods for at least a month.

FOR MORE INFORMATION ON FEEDBACK COLLECTION, SEE STEP 4.

MORE INFORMATION ON RANSOMWARE FOR PLANNERS AND MODERATORS¹⁵

The ransomware Evil Ransomware has been active since 2019. The very large amount of versions of the Evil Ransomware code with various configurations suggests that this ransomware is shared, probably under the "ransomware-as-a-service" model.

Evil Ransomware is responsible for 20% of the infections detected in 2019 and is probably offered at low prices. The ransom amount and the chances of retrieving files vary greatly depending on the attacks. Some attackers have also demonstrated poor control of the code, preventing victims from recovering their files even though the ransom was paid.

Evil Ransomware is distributed by phishing with a malicious link or a trapped email attachment. The latter sometimes uses the false identity of an antivirus. Like many other ransomware, it also endangers its victims by exploiting an already known vulnerability affecting the Remote Desktop Protocol for which a patch is available but not yet implemented. The multiplicity of infection methods is typical of the "ransomware-as-a-service" model. Evil Ransomware then encrypts the files on the equipment and on the accessible network shares. It also deletes hidden copies.

15: To use information linked to an existing ransomware, read ANSSI's CTI reports : www.cert.ssi.gouv.fr/cti/

STAGE 2

DRAWING UP THE TIMETABLE

The timetable takes the form of a table which, line by line, describes **the chronological course of the exercise** from the START EX to the END EX. It is drafted on the basis of interviews with the experts carried out in step 1.

It describes all the interactions that can be anticipated between players and the moderating unit. However, the latter must be able to adapt to the players' reactions, which may sometimes differ from the expected reactions (*see step 3, stage 2*).

Fact sheet No. 6 suggests a timetable for the RANSOM20 guideline scenario. The technical elements suggested in this fact sheet must be completed depending on the internal organisation of the IS.

Defining the rhythm and intensity of the exercise

The pace of a cyber exercise is not regular. It depends on the number of injects sent. The pace is fast to start with in order to immerse the players, and it is then slowed down to help them become familiar with the events and think about how to handle the crisis. Over two exercise days, a rebound may be considered to restore momentum.

In a cyber crisis, if the impact is dramatic, understanding the attack may take longer (several days or even weeks). Translating this into an exercise is then equivalent to finding a compromise between **simulating the investigation time needed by the technical teams** and sufficiently developing the scenario so that players have an overall view of how a crisis unfolds. To this end, an “accelerated pace” should be prioritised when drawing up the timetable.

Within a few minutes, it becomes impossible for staff to work. By sending injects at a fast pace (e.g. every three minutes), the scale (multiplicity of injects) and the severity (the different entities impacted) of such an event can be demonstrated. On the other hand, for the investigation stage (search for patient zero or isolation of the strain giving rise to the malicious software), the crisis unit can experience waiting times that can be felt by spacing out the inject rate (10 or even 15 minutes of silence).

Uncertainty about the objectives and perimeter of the attack is one of the **major characteristics of a cyber crisis**. It is important to make players feel that there are still unknown elements by delaying the sending of certain injects (particularly those responding to requests for technical investigations) or by indicating this in certain injects. The pace at which injects are sent should maintain the players' interest while showing that a cyber crisis has lasting consequences that are difficult to assess.

For organisations that are used to conducting cyber crisis management exercises, it is possible to propose a scenario that involves different points in time to allow players to experience the various stages of a cyber crisis. On the other hand, for organisations that are not familiar with cyber issues, it is best if the duration of the **exercise corresponds, as far as possible, to the duration of the event if it happened in real life**.

In both cases, it is crucial, at the end of the exercise, to give a reminder of the real deadlines required for a cyber investigation (analysis of logs of different equipment, code analysis, etc.) and the implementation of certain technical measures (applying a patch to a whole IT environment, etc.). Moreover, the first and/or second briefing also provides an opportunity to tell the players that the pace of the exercise is voluntarily faster than in real life.



Recommendation

Software to automate certain tasks can help you to implement this step, step 3 (conducting the exercise) and step 4 (learning from the exercise).

Simulating communication challenges and media pressure

Cyber crises do not escape media coverage and can, therefore, have an **impact on your organisation's image and reputation**. Including a media and/or communication component helps the communicators of a crisis unit to manage this type of event.

The challenge for players will be to reassure and control the communication of their entity in a stressful environment (novelty of this type of attack) and sometimes without any means of communication (e.g. if office equipment is affected).

This step consists of two parts to be simulated: media pressure and the challenges of internal and communication and communication with stakeholders. For these elements, the project group must **surround itself with communicators** from the organisation (not participating in the exercise) and/or specialised service providers.

Elements relating to external communication and simulated media pressure should be included in the timetable.

SIMULATING MEDIA PRESSURE

To simulate media pressure, **emails or phone calls from fake journalists** and **press articles** on the incident (which may include interactions between journalists with players) are required. **Social media** should not be neglected either when it comes to likely media pressure. Fake tweets or publications by Internet users, experts and journalists can

also be sent to the players, as well as video extracts from news channels with false banners. The elements provided to the players during the exercise must be identified as part of the exercise to prevent it from being confused with real information. For instance, calls from simulated journalists can start with “Exercise–Exercise–Exercise”.

Several methods can be used to simulate media pressure:

- ▶ Using a platform simulating social media via a provider.
- ▶ Regularly making press articles, tweets, etc. mentioning the attack accessible to players (for example, by simulating a person responsible for carrying out media monitoring for the organisation who regularly reports information); you can draw inspiration from newspaper articles that have been written about real cyber attacks.

The actors that can be simulated to generate media pressure are: journalists, influencers, digital security community, etc.

When simulating media pressure, you can write fake press articles on the attack, as well as fake tweets, that will be sent to players. Following interactions between players, elements may also be written live. These articles may be voluntarily dependent, exaggerated or they may reproduce exactly what the communicators say.

INTERNAL COMMUNICATION AND COMMUNICATION WITH STAKEHOLDERS

As in the case of media pressure, the elements linked to internal communication and communication with stakeholders are **emails or phone calls using the usual or backup means of communication**.

For this component, different types of actors can be simulated: internal teams affected by the crisis, collaborators, shareholders, social partners, customers, providers, competitors, associations, sectoral authorities, etc.

FREQUENTLY ASKED QUESTIONS

Whether questions are asked by the organisation’s employees or by journalists or external stakeholders, the most frequently asked ques-

tions include the nature of the attack, its impact on the organisation's activities and the measures taken to ensure a return to normalcy.

Members of the moderating unit who simulate media pressure and internal communication issues should bear in mind that the time span of a cyber crisis is always difficult to explain: the consequences sometimes appear immediately, while technical analyses take time, as do thorough remediation measures. Therefore, most questions (who, what, how) are likely to remain unanswered during the exercise.

The role of the SIS expert will be to provide a simple explanation of the technical elements to make sure that the communicators understand them well.

Fact sheet No. 5 lists all the actors who can be simulated as well as the questions they may ask.

FACT SHEET 5:

SIMULATING MEDIA PRESSURE AND QUESTIONS TO BE ASKED

ACTOR	DESCRIPTION
INTERNAL Relevant teams, collaborators, shareholders, social partners	
CUSTOMERS Potentially sensitive customers (OVI, OES, administrations)	If the consequences of the cyber attack are visible, various questions are to be expected from employees, customers and, more generally speaking, your organisation's ecosystem.
ECOSYSTEM Competitors, associations, providers, sectoral authorities, etc.	
JOURNALISTS Those specialised in cyber security and experts of the sector affected	In the event of a computer attack, you may be approached by your traditional media contacts (sectoral press, national and/or regional generalist) but also by specialist IT press, and more particularly those specialised in IT security.
INFLUENCERS AND COMMUNITY OF THE SIS AND THE SECTOR AFFECTED	The community is composed of demanding, active and curious people who want to understand the attackers' methods. They make extensive use of social media to discuss technical elements, debate, and comment on official communications. All of this can be simulated in the exercise.

ROLES TO BE TAKEN

STANDARD QUESTIONS

Is it still possible to work? Should we pay the ransom? How can we do this? What actions are recommended? What measures have been put in place? What are the instructions? What should be done? How can I continue working? This task cannot be postponed, I need functional IT resources. Publication of screenshots of the computers on social media, etc.

What is happening? What are the consequences on our usual interactions? Do we risk being infected/targeted as well? When can we resume our usual interactions? Can you keep me informed of developments?

What is happening? What are the effects for you? For the sector? Can you keep us informed of developments?

NON-SPECIALISED JOURNALISTS:

What is the scope of the incident, its extent and what are its consequences? When did it occur? How long will it last? Is the attack still ongoing?

SPECIALISED JOURNALISTS:

What is the type of attack? What is the method of attack? What are the direct consequences (technical, financial)? Indirect consequences? Spread? Are any customers victims of the attack? What about sensitive customers? What are you doing today to restore the IS? Has a complaint been lodged? Has a GDPR statement been made to the authority? Is the national cyber authority supporting you? What about service providers? What measures will you take in future? Who is the attacker? What are their motives?

The questions may be identical to those of specialised journalists. However, they will not be put directly to the organisation but will be debated on various social networks. This can help to boost media monitoring or a simulated media pressure platform.

Drafting the injects

Injects must be written before the exercise and be included in the timetable. They may take the form of emails (often with attachments), scripts in the case of a telephone call or false extracts from newspapers, tweets or publications on a social network platform. Nothing should be drafted on the day of the exercise, with the exception of additions or changes to the margin, if the situation so requires. The way in which they are communicated must be adapted to the situation simulated in the exercise.

For instance, if the simulated attack paralyses emailing and telephony, other means of communication will have to be identified and used during the exercise.

Recommendation

Software to automate certain tasks can help you to implement this step, step 3 (conducting the exercise) and step 4 (learning from the exercise).



It may be useful to provide optional injects that will be sent to help or disturb players, if need be. For example, if the crisis manager does not plan a situation update, an inject coming from an authority asking what is happening can be planned in advance.

Fact sheet No. 7 suggests a timetable model based on the RANSOM20 guideline exercise scenario.

FACT SHEET 6:

DRAWING UP A TIMETABLE: INSTRUCTIONS

EXAMPLE GUIDELINE RANSOM20

The drawn-up timetable is based on the interviews with the experts carried out during stage 1 of this step.

This timetable is filled in from right to left, starting with the expected reaction that corresponds to one or more of the goals. Then the player(s) to whom the information is sent should be selected. Then, fill in the sender, who will be simulated by the moderator to send the information. The event that will be transmitted to the player by the moderator in order to get the expected reaction is only drafted afterwards. Finally, the means to communicate the information and the time at which it will be sent is filled in.

The technical elements suggested in the timetable below should be completed depending on your internal organisation.

Disclaimer: the scenario imagined here involves French entities. It simulates the intervention of ANSSI, the French National Cyber Security Agency (national authority for cybersecurity) and CERT-FR (national CERT, part of ANSSI). It is recommended to adapt the scenario and the injects to your national cyber organisation and legislation.

Inject: It corresponds to the information transferred to one or more players. Each row of the timetable corresponds to an inject. You should write your script ahead of the day of the exercise. Depending on their speciality, the moderators and experts write down the events using their business terminology to make the exercise realistic.

No.	TIME	STAGE	INJECTS CONTENT (content of email or telephone call to be adapted to your organisation)	SENDER (non-player – simulated by the moderating unit)
Situation information file (SIF)	YYMMDD 08:30	SIF	Sending the SIF as an attachment to an email addressed to all players.	MODDIR

GAME OPTION SIMULATING NATIONAL AUTHORITY (HEREBY FRENCH AUTHORITY, ANSSI)

GAME OPTION WITH SEVERAL AFFECTED SITES AND SEVERAL CRISIS UNITS INVOLVED AS PLAYERS

GAME OPTION WITH SEVERAL AFFECTED SITES AND ONE CRISIS UNIT INVOLVED AS A PLAYER

GAME OPTION AS TRAINING FOR EXFILTRATED DATA ISSUES



Recommendation

When drafting the timetable, it is quite usual not to address all players as some interactions will naturally occur between them. For example, the head of the crisis unit will ask their teams to carry out a situation update at a specific time, or the CISO will ask their technical teams to carry out analyses. Therefore, these interactions do not need to be simulated. Moreover, players will ask the moderating unit to respond to requests or questions in the most realistic way possible, hence the importance of having experts on the discussed topics in the moderating unit.

Sender: the simulated professionals from which the moderating unit will send the message to one or more recipients (players). The moderating team may be required to simulate persons internal to the organisation who are not taking part in the exercise (e.g. journalist). It is possible to add a column immediately after "sender", titled "played by", to specify which moderator will be responsible for sending the inject.

Recipient: The player(s) who will receive the message. You must be vigilant and not send all the messages to the same person. It is particularly important to check that information is flowing smoothly within the crisis unit(s). One person cannot be both the sender and the recipient in the same exercise (moderators are not players and vice versa).

Expected reactions: For each line written in the timetable, the players' expected reactions need to be written down, and they must correspond to the goals described above. This also helps the moderating team to anticipate the adaptation of the scenario on the day of the exercise if the players' reactions differ too much from what was planned.

RECIPIENT (= players for action)	MEANS OF COMMUNICATION	EXPECTED REACTIONS	COMMENTS FOR THE PLANNER
All players	Email	Getting familiar with the information. No specific action expected.	This inject can also be sent the day before the start of the exercise.

Means of communication: This column is used to decide which means will be used to communicate information to the player(s). These are mainly emails or phone calls or tools such as a platform simulating media pressure. It is important to use the means of communication that players would have to use in a real crisis while taking into account the consequences of the cyber attack (e.g. unavailable Internet messaging).

EXTRACTS

No.	TIME	STAGE	INJECTS CONTENT (content of email or phone call to be adapted to your organisation)	SENDER (non-player – simulated by the moderating unit)
1	YYMMDD 09:30	Start of the exercise (START EX)	"Hello, the exercise is starting now. Please feel free to contact us if you have any questions or if there is anything you don't understand."	MODDIR
2	YYMMDD 09:32	First messages about the incident	"Hello, I am calling you because my team members can no longer use their computers. The computers are all displaying the same message demanding a ransom to retrieve the data. We have to deliver a very important project at the end of the week, we must be able to work. What do we need to do? What is more, I believe that the problem extends to at least our entire floor..."	Manager of a team of the organisation (service/ department of your choice)
3	YYMMDD 09:35	First messages about the incident	"Hello, I am calling you because since this morning we have received several calls from employees who can no longer use their computers. According to the photos received, the data seems to be encrypted and could be retrieved if a ransom is paid. Are you aware of this situation? The number of phone calls is starting to become overwhelming, and we have no information to report on the situation..."	Relevant IT contact point
19	YYMMDD 13:00	[Option "ANSSI Simulation" #1] If the organisation is part of the ANSSI's scope of intervention and one of the players has reported the incident	"Hello, We are calling you back following your incident report to the CERT-FR. What are the effects on your activities? Do you have a provider to help you? Do you need support from the national authority? [if support from the national authority is requested] An ANSSI official will contact you very shortly to help you qualify the incident and possibly to remotely provide support in the investigation and remedial procedures. Here are some good practice documents on the measures to be implemented when faced with a ransomware (see the ANSSI website for information)."	ANSSI
19 bis	YYMMDD 13:00	[Option "ANSSI Simulation" #2] If the organisation is part of the ANSSI's scope but has not reported the incident	"Hello, We have identified a publication on social media that may indicate that a security incident is affecting your IS. Could you confirm this information? Do you need support from the national authority? I recommend that you consult the 'What to do in the event of an incident' section on our website to implement the first measures. [if support from the national authority is requested] If you wish to be supported by ANSSI, a staff member will contact you very shortly to help you qualify the incident and possibly to remotely provide support in the investigation and remediation procedures. Here are some good practice documents on the measures to be implemented when faced with a ransomware (see ANSSI website for information)."	ANSSI
21	YYMMDD 13:10	[Option "Game with multiple sites and a single crisis unit involved as a player"] Lateralisation of ransomware	"Hello, All of the site's workstations are disabled. They are all displaying the same message asking us to pay a ransom. Working is impossible, and the whole site is at a standstill! Orders/services/projects will not be ready in time, it's a disaster. Can you send a team to resolve the situation? Does the rest of the organisation have the same problem? We do not understand what is happening at all."	Second site manager (service/ department of your choice)

RECIPIENT (= action players)	MEANS OF COMMUNICATION	EXPECTED REACTIONS	COMMENTS FOR THE PLANNER
All players	Email	No specific action expected.	
Manager of the business line/activity concerned	Phone call	Alerting/exchanging with the CISO.	<p>Inject to be multiplied (at intervals of 5 to 10 minutes) as much as deemed useful (depending on the number of activities involved or the desired pressure on players).</p> <p>The aim of these injects is to show that all of the organisation's services are gradually becoming affected. Specific business consequences to each service can be added in the script of telephone calls and emails.</p>
CISO or equivalent	Phone call	Transmission of the alert and triggering of the crisis unit.	<p>It may be interesting to mobilise the crisis unit. The crisis unit can be activated between this inject and inject 12. After inject 12, the moderating unit should insist that a crisis unit meet as soon as possible.</p>
CISO (or person generally responsible for reporting incidents)	Phone call	Transmission of the available information to ANSSI.	<p>If you are a regulated beneficiary (NIS), you can simulate reporting your incident to the established authority.</p> <p>Injects 19 and 19b should only be used when an incident report has been simulated by the players to the moderating unit. Their timeslot is to be adapted according to the time at which players make their report (contact is taken about an hour after the incident report).</p>
CISO or equivalent	Phone call	Transmission of the available information to ANSSI.	<p>To help players, it is possible to add a national authority or service provider contact in the directory that is redirected to the moderating unit.</p> <p>In this inject, the national authority or provider tries to obtain as much information as possible to understand the situation and make recommendations.</p>
Safety/security officer, commercial manager, or any player in the organisation's crisis unit deemed relevant and who would be the contact point for the second site	Phone call	Transmission of information to and within the crisis unit and dissemination of initial instructions.	<p>This could be any second site (located in France or abroad): subsidiary, production site, second building, etc.</p> <p>To continue the simulation with a single crisis unit, reuse the injects with two crisis units (pink injects) and replace the sender by the site manager and the recipient by any player in the organisation's crisis unit deemed relevant and who would be the contact point for the second site.</p>

EXTRACTS

No.	TIME YYMMDD 15:15	STAGE [Option "Game with multiple sites and several crisis units involved as players"] Press contact	INJECTS CONTENT (content of email or phone call to be adapted to your organisation)	SENDER (non-player – simulated by the moderating unit)
29			<p>"Hello, We have heard that your site has just suffered a cyber attack. Do you confirm this information? Is this attack linked to the attack at headquarters this morning? Are you able to continue your activity?"</p>	Journalist
32	YYMMDD 15:35	[Option "Publication of exfiltrated data"]	<p>"Hello, I have just found a publication on the Pastebin website which includes a large number of documents that potentially come from our organisation (pastebin.com/xxxx). At first glance, these documents seem authentic, but I have not looked at everything. With a group of colleagues, we are in the process of rereading them and checking this."</p>	Person in charge of media monitoring (employee or provider)
48	YYMMDD 16:50	<p>[Option "ANSSI simulation"]</p> <p>Conclusive inject for the end of the exercise through a simulated member of the organisation's technical team or a provider</p>	<p>"Hello, I would like to inform you about the first results of the investigative stage [option: led by national authority teams/provider]. We can confirm the following information in relation to the incident: malicious software has been deposited on your IS after a successful phishing campaign exploiting the vulnerability CVE-20xx-xxx affecting the Windows xxx operating system. The malicious programme uses multiple means of lateralisation (exploitation of legitimate Microsoft Windows services and of codes published on the Internet to exploit known vulnerabilities such as Eternal Blue), [option: which explains why the second site has also been affected]. In order to complete these initial analyses and to secure your IS, the attacker needs to be ejected from the system, and they must be prevented from returning. [option: To this end, a national authority team/service provider should be able to intervene as soon as possible in order to support you in this remediation stage.] Lastly, the editor has just published a patch for the vulnerability mentioned above (see CERT-FR alert in attachment). It should be applied as soon as possible. [A: protected offline backups] Backups can be deployed once we are sure that the IS are healthy and secure. Tests will be carried out in advance. If successful, we will continue operating on the whole IT environment. This should take at least a few days. [B: backups affected] The back-up servers are disabled. We will need to completely reconstruct the IT environment, which is expected to take between a week to ten days."</p>	ANSSI or technical team member or service provider
49	YYMMDD 17:00	End of the exercise (END EX)	<p>"Hello everyone, The exercise has come to an end. Thank you for your participation. You are invited to take part in the immediate feedback collection that will take place in five minutes."</p>	MODDIR

RECIPIENT (= action players)	MEANS OF COMMUNICATION	EXPECTED REACTIONS	COMMENTS FOR THE PLANNER
Second site communication team	Phone call	Use (if transmitted) HQ.LTT (lines to take) or request them before responding. Referral to a joint press release if existing.	
CISO or equivalent + communication manager + security officer	Email if accessible, otherwise phone call or emergency messaging	Preparation of a communication strategy.	During the exercise, distributing all the documents that will be published to the players is not useful. However, it is useful to have certain documents on hand to send as illustrations (which may, for example, be mentioned by the press). It is up to the planners to determine their number and degree of sensitivity.
CISO or equivalent	Email if accessible, otherwise phone call or emergency messaging	Transmission of information to the second site. Reflection on business continuity and recovery.	To allow players to experiment with several stages of the crisis, the pace of the exercise is voluntarily accelerated and is not representative of what would have happened in real life. By way of illustration, it is not uncommon for the IS to be completely unavailable for one-two weeks in the face of such attacks. Moreover, the restoration of the IS often takes time, sometimes several months. This inject can also be issued by a provider or simulated member of the organisation's technical team.
All players	Email	Participation in the collection of feedback.	Well done, you have put in place a cyber crisis management exercise!



To support you in drawing up your timetable, download the full excel file of our example at:

www.ssi.gouv.fr/en/guide/organising-a-cyber-crisis-management-exercise/

STAGE 3

PREPARING THE OTHER DOCUMENTS

DOCUMENT	DESCRIPTION
MODERATORS	
DIRECTORIES	Detail the updated contact details of all participants
REGISTER	Record the significant events of the exercise in writing to prepare the collection of feedback (see
PLAYERS	
DIRECTORIES	Include all the contact details of the moderators and players involved in the exercise and clearly explain the roles simulated by the moderating team (the same number may allow several simulated persons to be reached). This information must correspond to the means of communication that would be used in the context of a real crisis. Producing and keeping this directory up to date is important to prevent players
SITUATION INFORMATION FILE (SIF) [OPTIONAL]	Present the state of the world at the start of the exercise. The SIF can particularly be seen as the first element to raise the players' awareness about the state of the cyber threat affecting the organisation. It may be supplemented by recent press articles
RULES OF THE EXERCISE	Present the rules of the game, such as mentioning "Exercise-Exercise-Exercise" by email and telephone to avoid confusion between simulated events that are part of the exercise and real events taking place during the exercise, or the prohibition to use these
RELEVANT DOCUMENTATION	Add documents and procedures to be tested as
OBSERVERS	
FICHE D'OBSERVATION	Give a reminder of the goals and detail the points
ACCESS TO THE MODERATOR'S REGISTER [OPTIONAL]	Monitoring the crisis as a whole (particularly when

To ensure that the exercise is running smoothly, various documents must be produced for the participants.

	COMMENTS
(players, facilitators, observers). stage 2 of step 4).	
from contacting persons who are not taking part in the exercise. The directory should also include a number to call the moderating unit, to reach anyone who is not taking part in the exercise as a player and who is not mentioned in the directory' to avoid forgetting anyone.	
that help to illustrate what is being said with real examples. Fact sheet No. 7 provides an example of a SIF corresponding to the scenario put forward in fact sheet No. 4.	These documents may be sent by email before the exercise and/or during the player briefing(s).
means of communication if these become unavailable due to the cyber attack.	
part of the exercise.	
that the observers have to pay attention to. playing on more than one site).	Fact sheet No. 8 provides a list of the elements to be observed during a cyber crisis management exercise.

FACT SHEET 7:

PRODUCING A SITUATION INFORMATION FILE

EXAMPLE GUIDELINE RANSOM20

This fact sheet is a situation information file in the format in which it could be sent to players ahead of the RANSOM20 exercise. It contains general information on the state of the cyber threat and related to the organisation.

1. GENERAL CONTEXT: STATE OF THE CYBER THREAT

Today, organisations can be targeted by cyber attacks for a variety of reasons:

- ▶ **Computer espionage operations** through the exfiltration of strategic information, trade secrets, or R&D information from a variety of sectors.
- ▶ **Claim attacks**, through defacement, the disclosure of data (via exfiltration), denial of service, aimed at mobilising opinion leaders and damaging the image or reputation of individuals or organisations.
- ▶ **Sabotage attacks** through the logical or physical destruction of equipment.
- ▶ **Attacks to make money**, which may take the form of ransomware, data exfiltration for resale or blackmail.

Different methods can be used during cyber attacks to weaken the IS of the targeted entities and achieve the desired goals:

- ▶ **To exploit vulnerabilities:**¹⁶ this involves using a code that exploits a vulnerability, that has been corrected or not, affecting a software or hardware product, in order to invade an organisation's IS. The exploitation of a vulnerability can be automated and allow the rapid and large-scale spread of a malicious code. For example, in May 2017, the malicious code WannaCry quickly spread worldwide through the automated exploitation of a known vulnerability during a global wave of attacks.
- ▶ **Indirect methods of attack:** some attackers exploit the interconnections between digital service providers and its customers to discreetly weaken the customers' IS, sometimes with high added value; other attackers trap software before spreading these to infect a large number of entities. For example, the

16: Find the most critical vulnerabilities on the CERT-FR website: www.cert.ssi.gouv.fr

Cloud Hopper attack campaign, conducted in 2017, allowed its authors to compromise many organisations around the world after infiltrating the IS of digital service providers. In 2017, the compromise of two CCleaner updates before they were spread allowed attackers to compromise more than 2 million jobs worldwide.

- ▶ **Ransomware attacks:** ransomware attacks are increasing since 2018 and have been carried out in a more targeted manner in 2020. On 19 March 2019, following an infection caused by the ransomware LockerGoga, Norwegian aluminium company Norsk Hydro was forced to shut down a large part of its network and to perform its production "manually". Because it had data backups, the company chose not to pay the ransom. The drop in productivity due to the attack cost the company around USD 40 million. Since the end of 2019, some attackers exfiltrate data before encrypting it, using the threat of the publication of this data as blackmail. However, this involves two separate attacks using different malicious codes. This emerging trend poses a new risk to victim entities faced with the threat of the disclosure of their data.
 - Players should be given insight into the situation they will experience without revealing the scenario. The risk of a ransomware attack is therefore inserted in the middle of other threats.

2. SPECIFIC CONTEXT OF THE ORGANISATION

- ▶ **Examples related to the threat status:** the organisation operates in a sector that is already particularly targeted by ransomware cyber attacks. Last week, the French company XYZ suffered a ransomware attack and still has not resumed normal activity. The media estimates the cost of the attack to be several million euros. At the beginning of the month, the company ABC was the subject of a cyber attack. Many internal documents have been published by the attackers. Operating in the same sector, the organisation is also likely to be targeted by the same type of attack.
- ▶ **Examples related to the organisation and its business sector:** release of a new offer before the critical sales period or a few days later; drawing up the balance sheets; stock exchange listing; acquisition of a competitor.
- ▶ **Examples related to the external context:** a major political or sporting event which could, indirectly, explain a potential increase in attacks.
 - Depending on the pressure you want to put on players, it is possible to place the crisis in a particular context (important event for the organisation, critical period, orders to fulfil, milestone that cannot be postponed, etc.).

FACT SHEET 7: PRODUCING A SITUATION INFORMATION FILE EXAMPLE GUIDELINE RANSOM20

Recommendation

To illustrate the situation information file with examples related to your organisation, see CERT-FR CTI reports on its website in the media.¹⁷



¹⁷: www.cert.ssi.gouv.fr/cti/

FACT SHEET 8:

OBSERVING AN EXERCISE

The observation sheet is an essential tool for the observer. It includes indications to help them to focus on specific points and questions to be answered in the light of the exercise goals. Observers do not need to have the answers to all the selected questions. They may also note other points deemed useful. The register filled in by the players may also provide some elements which could not be directly observed.

This sheet contains a non-exhaustive list of questions that are useful to observers, which the planners can use to create an observation sheet. They can be adapted to each crisis unit.

ALERT

- ▶ Who forwards the alert? How?
- ▶ Who decides to activate the crisis unit and to call employees?
- ▶ At what time is the unit summoned?
- ▶ Have all the services needed for crisis management been alerted?
- ▶ If not, which services are missing?
- ▶ At what time will the crisis unit be functional?

LOGISTICS AND TOOLS OF THE UNIT

- ▶ Does the size of the premises seem appropriate (ergonomics, ease of movement, etc.)?
- ▶ Do the procedures and tools allow the situation to be managed effectively, or are they problematic? Are they operational?
- ▶ Are emergency tools provided? Are they being used?
- ▶ Do any tools seem to be missing? If so, which ones?

INFORMATION FLOW

- ▶ Is the register regularly filled in and accessible to all? If not, why?
- ▶ How do messages flow between members of the crisis unit? And between the various crisis units?
- ▶ Are messages being understood by the recipients?
- ▶ Are the competent bodies/services consulted?

- ▶ Have stakeholders (authorities, customers, providers, etc.) been informed of the situation?
- ▶ What is the frequency of situation updates? How are these organised?
- ▶ Are they precise, concise and understandable to everyone? Do they demonstrate a proactive approach?
- ▶ Is the information received and are the decisions taken regularly forwarded to the services and other crisis units?
- ▶ Is the information from the operational unit, simulated by the moderating unit, actually transferred to the decision-making unit? Is this information explained by the CISO and understood by non-specialist players?

THE PLAYERS' REACTIONS

- ▶ Is everyone well aware of their role in organising a crisis?
- ▶ Is the scope of each person's tasks respected?
- ▶ Are the roles that have been defined for crisis management correctly applied?
- ▶ Do the crisis units know of and use the crisis documentation as well as the already defined procedures (reflex action sheets, plans, etc.)?
- ▶ Is the situation understood well?
- ▶ Has the scope of the attack been determined?
- ▶ Do the actions and decisions taken seem appropriate and coherent?
- ▶ Can people quickly analyse the situation and its developments?
- ▶ In how much time are the first decisions taken?
- ▶ In how much time are these decisions implemented?

COMMUNICATION

- ▶ Have the communicators been integrated into the crisis unit?
- ▶ Are they exchanging with technical experts?
- ▶ Have any communication tools been defined?
- ▶ Has the information given to the media been coordinated with the decision-making unit?
- ▶ Is media monitoring (rumours, media announcements, etc.) carried out and is it adjusted in the communication strategy?
- ▶ Have the organisation's employees been informed of the situation and of what they should do?

FACT SHEET 8: OBSERVING AN EXERCISE

CLARIFICATION OF THE IMPACT OF THE ATTACK AND REMEDIATION

- ▶ Have the effects, such as the impossibility of using all or part of their tools and the loss of all or part of their data for X amount of time, been clearly explained to the affected sectors?
- ▶ Have the real deadlines of events that have been voluntarily accelerated in the exercise (investigation, mitigation/remediation) been clearly explained to all players?
- ▶ Does the dialogue between actors in the SIS chain and those involved in crisis management/business continuity/lawyers, etc. seem sufficient? Does coordination seem effective?
- ▶ In a real situation, would internal technical resources be sufficient and would technical support be sought or planned?

Recommendation

The observer may take note of compliance with the rules in a crisis unit, laid down beforehand, such as the distribution of roles, each person's position in the room, compliance with set times and speaking turns, etc.

The purely "behavioural" aspect of a crisis unit can be analysed. If this choice is made when structuring the exercise, only a professional (psychosociologist, coach) can provide an informed and useful opinion when setting out the situation. This analysis is interesting to carry out, particularly in crisis units that are already professionalised, by integrating individual debriefings, possibly leading to a team-building session during the later collection of feedback. The results may enrich the participants' personal and professional experience.





EXERCISE
RANSOM20

In the context of the RANSOM20 exercise, two different locations can be observed:

- ▶ the organisation's decision-making crisis unit
- ▶ the crisis unit at the organisation's second site.

Based on the goals set out in advance, observers may focus specifically on the following points:

- ▶ mobilising the people needed to manage the crisis
- ▶ strategy for crisis communication on cyber issues
- ▶ coordination between the organisation's main site and its second site (sharing of information, transmitting instructions, etc.)
- ▶ decision-making, implementation of deteriorated crisis management and functioning procedures.

STAGE 4

BRIEFING THE PARTICIPANTS AND ENSURING THEY ARE INVOLVED

Briefing moderators and observers

A week before the exercise, a meeting should be organised with the moderators and observers to ensure that the scenario and objectives are understood and that everyone knows their role. For observers, this is an opportunity to specify the elements of the exercise that need to be observed (e.g. the application of a procedure to be tested). A brief reminder may also be made on the day of the exercise.

Briefing players

Briefing the players is recommended one to two weeks before the beginning of the exercise. A briefing on the day of the exercise, right before starting the exercise, is also required.

The following points can be addressed:

- ▶ Goals of the exercise.
- ▶ Success factors (remind the participants that being involved is the key to success and that the exercise is training them).
- ▶ Exercise rules (rules of the game).

- **The concept of a moderating unit**, i.e. the fact that a group of “moderators” simulates people who exist in real life (internal and external IT teams, CERT/CSIRT, but also partners, HR, service providers, etc.); players often find it difficult to understand this concept, which can lead to certain questions (Can I contact my teams during this exercise? How?, etc.); it should be made very clear which people are simulated by the moderating unit and which people are taking part in the exercise as players.

Annex 1 presents all the deliverables to be produced to organise a cyber exercise.

STEP 3

CONDUCTING THE EXERCISE

STAGE 1:

Applying what is planned.....90

STAGE 2:

Adapting to the players.....92

Conducting the exercise involves following the timetable that has been prepared beforehand step-by-step and adapting to the players' reactions. At the end of this step, you will have all the tools you need to run a cyber crisis management exercise and you will be able to respond to players' reactions, which may sometimes be unexpected.



FACT SHEETS TO BE CONSULTED:

- ▶ Fact sheet No. 9: Avoiding the most common pitfalls
- ▶ Fact sheet No. 10: Overcoming simulation biases

STAGE 1

APPLYING WHAT IS PLANNED

On the day of the exercise, it will be time to conduct the exercise by following the scenario and the timetable, while being able to adapt to the players' reactions.

Setting the context for players

For simulated exercises, the START EX may be preceded by a contextualising message which informs participants, in particular, of the rules of the exercise. It may also be accompanied by a situation information file which helps to place the exercise in a more precise context. This generally translates into a message sent a few days before the exercise, and again 10 to 15 minutes before the START EX, allowing the means of communication to be tested at the same time. The briefing carried out on the day of the exercise also provides a reminder of the rules and the context.

With regard to the tabletop exercise format, the various stages of the scenario should be presented on slides to offer an evolutionary situation to players.

Following the timetable

All the information needed to organise the exercise has been prepared ahead of the day of the exercise (see steps 1 and 2). The moderating team must follow the timetable with the predefined maximum pace.

However, in most cases, the exercise does not happen exactly as planned and it needs to be adapted to the players' reactions (see step 3 stage 2).



Recommendation

If the moderating unit is far from the players, the first injects need to be completed with a telephone call to ensure that the players are in place and ready to play. The observer may also contact the moderating unit to inform them of the players' initial reactions.

Making the consequences real

A number of specific features are involved with the logistics of a cyber crisis exercise which sometimes require someone to intervene with players during the game (this role may be given to a moderator):

- ▶ **Isolate players' equipment** that is considered to be affected by the scenario; for example, if the financial director's laptop is compromised, that player will not be able to use it for all or part of the exercise.
- ▶ **Making the consequences seem realistic** in terms of alternative and/or remediation solutions for all of the participants' equipment; for example, if a temporary shutdown of emailing is agreed upon, no player will be able to send or receive emails.

EXERCISE
RANSOM20

Players no longer have access to computers connected to the network as the organisation has suffered a ransomware attack across the entire IS. The organisation's email addresses and potentially the fixed phone lines no longer work. Therefore, they should be removed, or a message stating that they are unusable should be displayed.

STAGE 2

ADAPTING TO THE PLAYERS

Following their pace

The timetable defines the pace of the crisis simulated as part of the exercise, but the moderating team must adapt to the players' reactions, for instance, by changing the time at which an inject is sent. Therefore, the possibility of delaying the sending of certain injects must be foreseen.

In order to avoid any misunderstandings and the loss of the scenario's overall consistency, any major modifying decision must be taken within the moderating unit in a **collegiate** fashion. Observers should also be informed of such changes to the pace of the exercise.

If the decision to isolate the workstations from the network is taken earlier than expected, the related injects should be implemented. If this decision is not taken fast enough, other injects insisting on the need to do so may be added.

EXERCISE
RANSOM20

If elements of simulated media pressure are prepared for your exercise in response to actions that have to be carried out by players, then you must wait until the players have carried out these actions before sending the injects (e.g. dissatisfied customers due to the unavailability of a service that has been interrupted to prevent the spread of the attack).

If the exercise is not carried out as planned or the players' misunderstanding is too great, it may be appropriate to **intervene to address certain issues again** or to explain the situation and expectations to the players. Support can also be given to a player who is really struggling. For example, if the head of the crisis unit is struggling, remind them to organise a situation update with their team. **The failure of the exercise should be avoided to protect its educational benefits.** However, this does not mean that negative points or areas for improvement cannot be highlighted. Feedback collection gives an opportunity to discuss these topics and helps to draw up an action plan to address them.

Recommendation

Players should not be removed from the game during the exercise. Nevertheless, it is useful to prepare for the unforeseen potential departure of a member of the directorate-general in the event of an emergency: in such cases, the exercise should continue with a designated substitute player.



Responding to unexpected reactions

In a cyber crisis scenario, around 70% of the injects in the timetable are followed, while 30% are redesigned or even completely improvised. This is an indicative average ratio which shows that, despite all the attention paid to preparation, being prepared is necessary to be able to adapt. Indeed, the players' reactions may sometimes differ from the expected reactions (see step 2 for more information on drawing up the timetable).

However, **it is impossible to anticipate everything**. If you have not anticipated a certain reaction from players that will influence the game, you must intervene. Otherwise, the rest of your moderating actions risk no longer being coherent.

Ensuring that players understand the injects on a regular basis helps to limit unexpected reactions. This is, particularly, the role of the MODDIR, who can regularly exchange with the observers or go to the crisis management room in person.

It is also possible to **complete an inject sent by email, a telephone call and vice versa**, particularly for the first inject and for the most important ones in order to ensure the smooth start of the exercise and the understanding of the triggering element. However, make sure not to do so systematically, as this could risk interrupting the pace of the game.

Moreover, depending on the players' concerns, it may be necessary to put a stronger emphasis on a certain point of the crisis that they would otherwise dismiss. For example, players may focus on the implementation of the BCP without analysing the implications for the SIS.

It may also be that certain elements have been forgotten when drawing up the timetable or that unexpected questions are asked by the players. In this case, a response must be prepared with the moderating unit and particularly the appropriate experts, where possible.

Recommendation

A player's request does not require an immediate response. It is best for moderators to meet to discuss and determine what would be the best response and the right time to respond. As in real life, it is perfectly possible not to know the answer.



It may be appropriate for the MODDIR to intervene to remind players of certain rules of the exercise or to inform them that, in reality, the resources requested (technical, human and financial resources) would not arrive as quickly as during the exercise. Special attention should also be paid to players who tend to minimise the consequences of an attack, thus making the scenario irrelevant. Attention should be paid to this issue, which often occurs during cyber exercises.

Fact sheets No. 9 and No. 10 offer tips that moderators can follow to handle unforeseen situations.

FACT SHEET 9:

AVOIDING THE MOST COMMON

The pitfalls mentioned below do not cover everything and are specific to cyber crisis management exercises. These can be avoided by focusing on these points when briefing players on the day of the exercise. However, if some or all of the exercise goals risk not being met due to the occurrence of one or more of the pitfalls described below, the MODDIR must then intervene, e.g. on the basis of the suggested solutions, to realign decision-making and players' choices.

PITFALL 1: THE DECISION-MAKING CRISIS UNIT BECOMES AN OPERATIONAL CRISIS UNIT

It often happens that players discuss technical issues that require a high level of IT expertise and an inappropriate level of granularity in the decision-making crisis unit. A high-level crisis unit is not the place to discuss technical details. This leads to tunnel vision, which is detrimental to decision-making. Discussions should focus on possible remediation solutions and consequences that are financial, professional, reputational, etc. The way in which the chosen remediation solutions are implemented technically is decided within operational teams, in particular, IT teams.

- | | |
|---------------------|--|
| SOLUTION 1.1 | The moderating unit may contact the decision-making crisis unit and ask for a situation update particularly focused on the professional point of view (e.g. must certain employees be temporarily laid-off?) to push players to refocus on strategic aspects. |
| SOLUTION 1.2 | The moderating unit can exfiltrate one of the people feeding this debate via an email or a phone call, asking them to go to another room and, thus, limit this type of discussion. The moderating unit will explain the reasons for doing so to this person before sending them back to the crisis unit. |
| SOLUTION 1.3 | The moderating unit can create injects for the person fuelling these debates to better occupy them on the one hand and, on the other hand, if possible, to steer them towards strategic questions, in order to give them the capacity to redirect their approach in a decision-making crisis unit. |

PITFALLS

PITFALL 2: MISUNDERSTANDINGS BETWEEN DECISION-MAKING AND OPERATIONAL LEVELS IN THE IMPLEMENTATION OF THE GUIDELINES

A discrepancy is likely to increase between the guidelines and the decisions taken by the decision-making level and the implementation constraints (technical, time, etc.), particularly in exercises where the technical level is simulated by the moderating unit.

SOLUTION

If the technical actions are entirely simulated by the moderating unit, it is possible to add injects to set out certain difficulties in implementing the decisions taken by the crisis unit either due to a lack of precision given by the decision-making level or because this measure is not realistic. The idea is to send these "alerts" to the decision-making unit in the form of questions and requests for clarification to prevent rejection from the players forming the unit.

PITFALL 3: CONTRADICTIONS BETWEEN DECISIONS TAKEN BY THE CRISIS UNIT AND THE EXERCISE GOALS

The analysis of the effects of the remediation areas is sometimes incomplete and some measures may contradict the exercise's guidelines and goals. For instance, a crisis manager may decide to close its entire organisation and to send all employees home, except for the crisis unit and a few people from the IT teams, while one of the exercise goals is to find a middle ground between remediation constraints and a certain continuity of business.

SOLUTION

It is up to the moderating unit to refuse such measures, either by having someone intervene (simulated or not) or by means of an exercise agreement.

FACT SHEET 9: AVOIDING THE MOST COMMON PITFALLS

PITFALL 4: TOO MANY DEMANDS ON TECHNICAL TEAMS (SIMULATED BY THE MODERATING UNIT) TO THE DETERIMENT OF THE PLAYERS INVOLVED IN THE EXERCISE

It is often the case that too many demands are made on technical teams by the decision-making crisis unit, which wishes to have a permanent and instant view of the situation, thus giving it a sense of control, to the detriment of other members of the crisis unit, particularly those in charge of business issues and of those managing incident consequences.

SOLUTION

If there are too many demands, this can be corrected in two ways: by banning certain bridges of communication or by grouping these calls towards a person who will act as a proxy. In both cases, the decision-making crisis unit should be made aware that investigations take time and that technical information must be communicated with a high level of certainty.

PITFALL 5: LACK OF UNDERSTANDING AND EXPLANATION OF CYBER ISSUES

The lack of a clear explanation of cyber issues occurs frequently and may lead to confusion within the decision-making crisis unit. This is even more the case in organisations where there is a lack of a shared culture and vocabulary between technical and decision-making teams.

SOLUTION

The moderating unit creates ad hoc situation updates, together with the CISO and the crisis director, in order to strengthen vertical communication.

FACT SHEET 10:

OVERCOMING SIMULATION BIASES

The conduct of an exercise can generate a number of behavioural and organisational biases, which are all even harder to master during the moderating stage. Some of these are described and illustrated in the table below. It should be noted that these biases are inherent in crisis management and may, however, be highlighted during exercises.

UNDER-REACTION		
TYPE	ILLUSTRATION	SOLUTION
Detachment	<p>Passive attitude, disinterest</p> <p><i>"This is not real life. All we need to do is say is that we carried out this action and that it worked."</i></p>	<p>ENCOURAGE COMMITMENT / IMMERSE IN EXERCISE</p> <p>Encourage people to immerse themselves in the exercise by creating injects for them that require action.</p>
Distancing	<p>Attitude with a form of distancing (e.g. standing in the corner of the room), does not want to make decisions or take responsibility.</p> <p><i>"I should not be the one performing this action, this is not my responsibility."</i></p>	<p>REPUTATIONAL IMPACT / UNAVAILABILITY OF TOOLS</p> <p>Reputational impact, unavailability of one or more application tools, partial or total triggering of a BRP or BCP.</p>

Ideally, it is up to the moderating unit to identify these behaviours, particularly with the help of the observers, and to act in order to prevent such people from negatively impacting the game.

This (non-exhaustive) table is based on the experience obtained by observing many cyber crisis management exercises.

OVER-REACTION

Type	Illustration	Solution
INVOLVEMENT		
Over-investment	<p>A person takes a central position in the room, is visible to everyone, looks at neighbours' actions and behaviour, moves a lot.</p> <p><i>"I will take charge of this or that, I will deal with these actions, I will check that, I am responsible for..."</i></p>	Explicitly ask for a situation update from another player whose scope of work is not being respected by the person in question and only speak to that other player.
Excessive need for control	<p>A lot of unrest, excessive requests for feedback on the ongoing actions.</p> <p><i>"How is this action, measure, discussion developing?"</i></p>	Interrupt or do not respond to certain requests that are considered to be excessive, for example by requesting a phone call at a later point in time.

FACT SHEET 10: OVERCOMING SIMULATION BIASES

UNDER-REACTION

Type	Illustration	Solution
MANAGING TIME		
Delay	<p>Form of inertia and lack of dynamism.</p> <p><i>"We have all the time in the world because this is not real life."</i></p>	<p>Give a reminder of the time frame of the exercise, frequently give deadlines, request an interview by the Executive Committee, etc.</p>

LEADERSHIP OF THE DIRECTOR(S)/

Withdrawal	<p>Little or no arbitration, lack of guidance.</p> <p><i>"We will see later, we cannot decide now."</i></p>	<p>Send a request for an item invoking the strategy implemented (solicitation of media, investors, executive committee).</p>
------------	--	--

OVER-REACTION

Type	Illustration	Solution
AND STRESS		
Hyper-activity	Moving around the room and gesturing a lot, asking many questions and struggling to manage the stress caused by the exercise.	Reassuring the person in question by reminding them of the goals and the fact that exercises are not intended to evaluate anyone. On the contrary, the exercise helps to train stress management.

CRISIS MANAGER(S)

Tyranny	Central but fixed posture, interrupting, makes decisions without waiting for the options, does not listen much.	Removing the crisis director from the unit for a given amount of time (e.g. simulation of a press conference).
---------	---	--

STEP 4

LEARNING FROM THE EXERCISE

STAGE 1:

Organising feedback collection immediately
after the exercise.....106

STAGE 2:

Collecting feedback some time after the exercise...109

STAGE 3:

Producing an after action report and
providing for restitution.....110

Organising an immediate collection of feedback is essential to improve the organisation's crisis management scheme. It helps to draw lessons from the exercise, i.e. to highlight what worked well and what needs to be improved.

At the end of this step, you will have:

- ▶ Identified the strengths of your organisation for cyber crisis management as well as areas for improvement.
- ▶ Established a specific action plan to overcome shortcomings and strengthen what already exists.

Well done! You have put in place a cyber crisis management exercise!



DELIVERABLES TO BE PRODUCED:

- ▶ Report on immediate collection of feedback
- ▶ Report on later collection of feedback
- ▶ After action report



FACT SHEET TO BE CONSULTED:

- ▶ Fact sheet No. 11: Collecting feedback – example guideline RANSOM20

STAGE 1

ORGANISING FEEDBACK COLLECTION IMMEDIATELY AFTER THE EXERCISE

Organising immediate feedback collection, at the END EX is strongly recommended as participants will still be preoccupied with the exercise. Immediate feedback collection allows observers to collect the main elements and to make note of any frustrations caused by the exercise. It also provides an opportunity to present the observed strengths as well as the areas for improvement.

Recommendation

Feedback collection is a sensitive moment that requires a tactful approach. During immediate feedback collection, and especially with a first exercise, particular emphasis should be placed on the positive points observed. Negative points can be presented as improvement areas.



Feedback collection usually happens by going around the table to hear each player's opinion. There should be one person to moderate the collection of feedback and one or two people to take notes during the discussion. The duration of an immediate collection of feedback is around an hour for an exercise lasting half a day to a whole day. All participants should have a chance to speak.

During this meeting, the following topics are often discussed:

- ▶ Preparing the participants and organisations for the exercise.
- ▶ Likelihood of the scenario.
- ▶ Quality of the exchange of information between the teams.

- ▶ Quality of internal and external communication.
- ▶ Operation of equipment and materials.
- ▶ Logistics (crisis room, tools, etc.).
- ▶ Human resources (team creation, relay, use of skills, etc.).
- ▶ Etc.



Recommendation

Players should be given the opportunity to speak first in order to prevent observers from influencing their feedback. It is important for everyone to express their opinion. Free speech (that is respectful of others) should be encouraged and the meeting should not be too formal to allow all parties to express their views.

If more than one crisis unit is involved, it is possible to:

- ▶ **Simultaneously collect feedback**; this option will be chosen if the time allocated to the collection of feedback is too short, or if the crisis units need to express their views independently.
- ▶ Set up a **shared collection of feedback** (even if the crisis units are remote), so that the members of each unit can share their experiences; this option is preferable to capitalise on the exercise and it allows different professionals of the same organisation to gather around cyber issues.

For immediate feedback collection, it can be interesting, in order to trace and structure players' thoughts, to ask them to provide a self-assessment questionnaire covering the main items of the observation sheet. This questionnaire does not intend to gather the subjective elements of the participants' behaviour.

Organising feedback collection is also an opportunity to **explain the situation** that players have just experienced. Indeed, the decision-making crisis unit often sees a cyber crisis scenario through its impact.

It is, therefore, interesting to trace the recent attack on the organisation in a simplified way to give all participants a complete and realistic view (e.g. by indicating whether the vulnerabilities exploited during the attack actually exist).

Recommendation

If elements of the exercise differ from what would happen in real life, it is important to clarify these during the collection of feedback (for example, a shortened investigative action to allow the exercise to move forward more quickly).



STAGE 2

COLLECTING FEEDBACK SOME TIME AFTER THE EXERCISE

Organising feedback collection some time after the exercise, a few days to a month afterwards, helps to **round off the immediate collection of feedback and to conclude the collection of opinions** on the course of the exercise. This second stage of feedback provides an opportunity to gather a number of suggestions or findings after participants have been able to think about their experience of the exercise. Later feedback collection particularly makes it possible to identify and suggest any forgotten areas for improvement and proposals for action. In practical terms, later feedback collection must gather all the participants and also last around an hour.

In order to prepare later feedback collection, players are invited to use the evaluation questionnaire if they wish to do so. Additionally, individual interviews may also be organised. These help participants to feel more confident and to more sincerely share how they feel about the exercise.

STAGE 3

PRODUCING AN AFTER ACTION REPORT AND PROVIDING FOR RESTITUTION

The final stage of organising a crisis exercise is to write down the collected feedback in the form of an after action report (drawn up by the project group members and observers) and to send it to all participants. This report **identifies the actions to be taken to improve the crisis management scheme**.

The report can have several levels, for example a summary can be sent to the directorate-general, and a more comprehensive document can be sent to the participants. This document may also be important for inspection purposes (carried out by insurances, external audits, etc.).

To draw up this report, the following elements must be collected and analysed:

- ▶ The register(s) of the exercise (at least one register will have been held by one of the players in a crisis unit).
- ▶ The emails exchanged during the exercise.
- ▶ The notes taken by the observers during the exercise and when asking for the players' opinions.
- ▶ The immediate feedback collection.
- ▶ The completed questionnaires and interviews carried out for the later collection of feedback.

A cyber crisis management exercise must be used as an opportunity for an **organisation to gain more experience** to deal with a cyber crisis. Therefore, the report must:

- ▶ Present the **strengths** to build on and the **areas for improvement**.
- ▶ Suggest a **specific action plan** to resolve gaps or weaknesses and/or strengthen existing action plans (this plan must identify the persons responsible for carrying out each action).
- ▶ Provide factual elements supported by objective evidence or arguments.
- ▶ Be **concise** in order to be read and understood by as many people as possible.
- ▶ Be published within a short amount of time following the exercise (maximum two months);
- ▶ Potentially **involve an oral report** in order to maintain a dialogue between all participants and to resolve any conflicts, if need be. The main lines of this report can be presented (and validated) during a later collection of feedback.

Communicating all or part of this collected feedback is a way of, both internally and externally, showing the work that has been carried out to improve cyber resilience within its organisation. Distributing the collected feedback and the action plan derived from it also helps to **continue involving participants** in accordance with the exercise goals.

Fact sheet No. 11 at the end of this stage provides an example of feedback collection for the RANSOM20 exercise.

FACT SHEET 11:

COLLECTING FEEDBACK

EXAMPLE GUIDELINE RANSOM20

This fact sheet consists of the fictitious collection of feedback for exercise RANSOM20 as it could be led by an organisation that has decided to test two crisis units (headquarters and the organisation's second site).

This is a summary for decision-makers who are in charge of validating the proposed action plan. It highlights the main lessons learned with regard to the goals that have been set in advance.

0. REMINDER OF THE ACCELERATIONS IN PACE COMPARED TO REALITY

This exercise mainly focused on the incident and the investigation and business continuity stages. Several actions have been accelerated to allow players to think about how to resolve and maintain or resume activity in a deteriorating crisis.

In real life, the scope impacted, the information on the type of ransomware and the path of attack would not have been obtained on the first day. These investigations can take several days or even weeks of work, especially if the ransomware was hitherto unknown. The analysis of the backups and their re-installation would also have been carried out later, once the attack had been interrupted, the attackers ejected and the IS secured. Depending on the status of the IS, these actions can last several days or weeks.

1. REACHING THE GOALS (SEE FACT SHEETS 1 AND 4)

The RANSOM20 exercise involved 27 participants (20 players, 5 moderators and 2 observers). It was an opportunity to ensure that **all the people needed to manage the crisis were called upon** [*goal 1*]. It also **tested the crisis communication strategy** for ransomware issues and highlighted the need for emergency internal communication tools to effectively contact all employees [*goal 2*]. The involvement of the teams on the second site demonstrates **good coordination between the central crisis management system and the local system**. On the other hand, it was noted during the preparation of the exercise and in view of the direct (simulated) impact on the organisation's activities that the ability to isolate the IS directly linked to production presents an issue and needs to be thoroughly analysed [*goal 3*]. The simulation of the interruption of activities was the opportunity to **review the back-up needs** and revealed the need to increase the rotation of key staff, as some of them do not have a substitute [*goal 4*].

2. GOOD PRACTICES

This exercise made it possible to **include cyber experts in the organisation's crisis management system** for the first time. The interactions between the "crisis management experts", the representatives of the affected sectors and the SIS experts were successful and have led to constructive decisions. The information also flowed well between the headquarters of the organisation and the production site.

The consequences of the malfunction of the organisation's activities were quickly identified, making it easier to implement **adequate response scenarios** which are planned in the BCP and BRP. The existence of a recently updated BCP also helped to quickly identify the organisation's vital functions and to prioritise remediation.

The teams quickly decided to (fictitiously) **isolate the contaminated equipment** (by disconnecting network cables, cutting off the Wi-Fi). Communications to and from the Internet have been cut off in agreement with the business managers, and the encrypted machines have been put on extended standby.

Doing media monitoring helped to **draft the communication tools** which were defined by the communication team, together with the technical teams and were distributed via a press release. The national authority was notified of the data exfiltration.

Finally, **not paying the ransom** made it possible to comply with the posture defined in advance and in line with national authority's recommendations in this area.

3. AREAS FOR IMPROVEMENT

The organisation's deteriorating crisis procedures do not cover all crisis management activities (no emergency emailing, no back-ups of paper directories, etc.). This makes it difficult to contact all the employees and to provide them with information and instructions on the situation.

(Simulated) providers/customers/subsidiaries were not informed of the situation and wondered about the impact of the attack on their services.

While the presence of **off-line backups** made it possible to restore part of the system, they were dated: some data was lost and some IS had to be rebuilt. In reality, this would have led to a longer period for the resumption of activities (around 10 days).

The decision to rebuild a large part of the IS was not problematic on the second site's production chain; on the other hand, the **complete loss of customer databases and associated (simulated) applications** constitutes major damage, and the decision-making crisis unit was not given a significant warning for it,

FACT SHEET 11: COLLECTING FEEDBACK

which would have made it possible to communicate with the affected sectors at the highest level.

Finally, **notifying the attack to the insurer** was not one of the objectives but was mentioned by the players in the crisis unit, particularly to cover for operating losses and **legal assistance**, which would have been highly appreciated. An information session for members of the crisis units (both at the main and secondary sites) on this **specific insurance policy** should be prepared and the associated procedure tested in a future exercise.

4. SUMMARY OF THE ACTION PLAN

THEME/ACTION	WHO'S RESPONSIBLE	PRIORITY
CREATING/CORRECTING/IMPROVING "REFLEX" PROCEDURES		
Launching a campaign to create/update "reflex" sheets in the event of a ransomware attack: saving backups offline, analysing logs, introducing new firewall rules, banning the use of removable media, etc.	CISO	P2
CORRECTING/IMPROVING CRISIS MANAGEMENT AND BUSINESS CONTINUITY PROCEDURES (MANAGING ACTIVITIES IN A DETERIORATING CRISIS)		
Acquiring tools to communicate with all employees in a deteriorated mode.	BCP officer	P2

THEME/ACTION	WHO'S RESPONSIBLE	PRIORITY
--------------	-------------------	----------

CORRECTING/IMPROVING THE REFLEXES OF THE DECISION-MAKING CRISIS UNIT

Reviewing the cyber insurance policy in the event of a claim (legal assistance and financial cover for material, non-material loss, penalties, etc.); anticipating a training session for members of the crisis unit and including the procedures associated with the next exercise.	Legal officer	P1
Improving the flow of information to the decision-making crisis unit by highlighting the areas where urgent and high-level arbitration is needed.	Head of BCP + CISO	P2

CORRECTING/IMPROVING CRISIS COMMUNICATION PROCEDURES

Mapping audiences and the associated communication goals: employees, customers, partners, authorities, general public/media.	COM	P1
Mapping the stakeholders in communication and coordinating with them: providers, subsidiaries, authorities, etc.	COM	P2

CORRECTING/IMPROVING PREVENTIVE SIS MEASURES

Backups Increasing the frequency of off-line backups; improving the back-up system architecture.	CISO	P1
--	------	----

FACT SHEET 11: COLLECTING FEEDBACK

THEME/ACTION	WHO'S RESPONSIBLE	PRIORITY
CORRECTION/AMÉLIORATION DES MESURES PRÉVENTIVES DE SSI		
Audit campaign Audit at the main site: <ul style="list-style-type: none">▶ Specific partitioning of equipment for administrators or administrative roles.▶ Rights management. Audit at the second site: <ul style="list-style-type: none">▶ Filtering scheme to separate different network areas (internal servers/servers displayed on the Internet, user/administrator workstations).▶ Rights management.▶ Control of Internet access (analysis of application links, gateways).	CISO	P1
Raising awareness among staff Training/awareness raising: reinforcing certain reflexes among staff by asking them to inform the organisation's IT department of anything suspicious (suspicious email or attachment, a USB stick that was given to them, unusual questions, etc.); ¹⁸ including IT teams and particularly highly targeted administrators.	COM + CISO	P1

Recommendation

A deadline should be indicated for each part of the action plan and all traceability elements should be attached to the collected feedback.



¹⁸: To create educational resources, visit the ANSSI website (www.ssi.gouv.fr/en/) and cyber-related harm websites.



CONCLUSION

A first cyber crisis exercise helps to raise the awareness of a large number of actors about SIS issues and increase their experience of cyber crisis management situations.

Preparing such an exercise is educational, and the exercise itself is an opportunity to start or continue the implementation of SIS-related measures and projects within your organisation.

A cyber crisis management exercise is built as a project and opens a large number of opportunities for the people preparing it, those taking part and those who are then involved in implementing the areas identified for improvement.

Regularly organising cyber crisis management exercises (once a year or once every two years), accompanied by more theoretical training, raises skills and increases efficiency when managing real cases, particularly when actors master essential reflexes such as characterising a situation, sharing information with the right people and quickly establishing a state of the knowledge of the event.

Training in crisis management also involves a crucial human, and therefore behavioural, aspect, namely stress management, as well as individual and then collective decision-making in complex situations, which can be learned and improved.

Preparing for and communicating about how to deal with a cyber crisis leads to internal and external trust.

You now have the information to convince as many people as possible that the exercises are not intended to “punish” or “monitor” anyone but to raise the level of skills of those who are being trained.

ANNEX 1:

LIST OF DELIVERABLES TO BE PRODUCED FOR THE EXERCISE

PRELIMINARY RECOMMENDATIONS:

ENSURING THE HIGHEST LEVEL OF CYBER RESILIENCE

- ▶ Exercise strategy (optional)
- ▶ Exercise programme (optional)
- ▶ Communication plan

STEP 1:

DESIGNING THE EXERCISE

- ▶ Specifications
- ▶ Project timetable

STEP 2:

PREPARING THE EXERCISE

- ▶ Scenario
- ▶ Timetable
- ▶ Directories
- ▶ Situation information file
- ▶ Observation sheet
- ▶ Briefing moderators and players

STEP 3:

CONDUCTING THE EXERCISE

- ▶ No deliverables

STEP 4:

LEARNING FROM THE EXERCISE

- ▶ Report on immediate collection of feedback
- ▶ Report on later collection of feedback
- ▶ After action report

ANNEX 2:

GLOSSARY

MODERATOR: moderates the exercise, interacting with players by simulating actions to train and test their reactions in crisis situations. A moderator can play several roles.

MODERATING UNIT: group of “moderators” simulating people in real life who do not take part in the exercise and with whom players interact in the context of the crisis management.

TIMETABLE: table which, line by line, describes the entire chronological course of the exercise from the START EX to the END EX. It also specifies the means to communicate injects (email, telephone calls, SMS, etc.) and the reactions expected from players in order to define and frame the actions played directly by the players and those simulated by the moderating team.

RULES OF THE EXERCISE: rules of the game structuring the exercise (for example, prohibiting players from using any means of communication that have

become unavailable or informing players, without providing any evidence, that the exfiltrated data does indeed belong to their organisation).

MODERATING DIRECTOR (MODDIR): head of the moderating unit who ensures that each moderator is playing their role and that the players understand the received information. To this end, the MODDIR interacts with the observers who can provide information on any of the players’ unexpected reactions or misunderstandings.

DIRECTOR OF THE EXERCISE (DIREX): validates the exercise guidelines and each stage of progress. The DIREX can lead the exercise.

SITUATION INFORMATION FILE (SIF): concise document that presents the state of the world to the players at the beginning of the exercise. It helps to set the situation that players will experience in a more precise context.

EXPERT: contributes to the construction and realism of the scenario by providing expertise on a particular topic or on the history of its organisation.

PROJECT GROUP: group of people responsible for drawing up the exercise.

PLAYER: takes part in the exercise by reacting to the various simulated events. The players come from one of the various sectors of the organisation that would be involved in the crisis management scheme if a crisis were to occur in real life.

OBSERVER: responsible for observing how the exercise is run and for taking note of the strengths and areas for improvement. An observer does not intervene during the exercise. Ideally trained (even briefly) in cyber crisis management before the exercise, they have a good understanding of how the organisation works.

BUSINESS CONTINUITY PLAN (BCP):¹⁹ its goal is to apply the strategy and all the provisions laid down to ensure that

an organisation resumes and continues its activities following a disaster or event that seriously disrupts its normal functioning. It must allow the organisation to meet its external (legislative or regulatory, contractual) or internal obligations (risk of loss of business, survival of the firm, image, etc.) and to meet its goals.

BUSINESS RECOVERY PLAN (BRP):²⁰ an organisation's documented procedures for restoring and resuming its activities based on temporary measures adopted to meet usual business requirements after an incident.

PLANNER: member of the project group involved in constructing the exercise. On the day of the exercise, the planner is either a moderator or an observer.

SITUATION UPDATE: usually consists of a written summary to inform stakeholders and decision-makers of what is understood about an incident, its effects and the progress of remediation actions.

19: Guide pour réaliser un plan de continuité d'activité (Guide on drawing up a Business Continuity Plan), SGDSN, 2013.

20: ISO 22301, Societal Safety – Business Continuity Management Systems, clause 8.4.5 Recovery

ANNEX 2:

GLOSSARY

EXERCISE PROGRAMME: multiannual plan containing several crisis management exercises on various topics to educate and gradually train as many people within its organisation as possible, in line with the exercise strategy.

RANSOMWARE: contraction of “ransom” and “software”, a ransomware is, by definition, a malicious program that aims to obtain a ransom payment from the victim. To achieve this, ransomware prevents users from accessing their data by encrypting it, and then gives them instructions to pay the ransom in exchange for recovering their data.

COLLECTION OF FEEDBACK: group time (around a table) and/or individual time (interview) during which all participants speak about their experience during the exercise.

SCENARIO: tells the “story” of the exercise, consists of a description of the overall crisis situation affecting the organisation.

INJECT: information sent by the moderating unit and received by the players. An inject is a part of the scenario that is used to guide the players’ actions. Injects generally consist of emails or phone calls. Together, the injects form the timetable.

EXERCISE STRATEGY: tool that helps to highlight the exercises organised among the organisation’s stakeholders and to structure the training session so as to contribute to improving its resilience.

INCIDENT: (cyber) incident is a disruption of IT services where the expected availability of the service disappears completely or in part. It can also be the unlawful publication, obtaining and/or modification of information stored on IT services.

ANNEX 3:

USEFUL RESOURCES

SGDSN

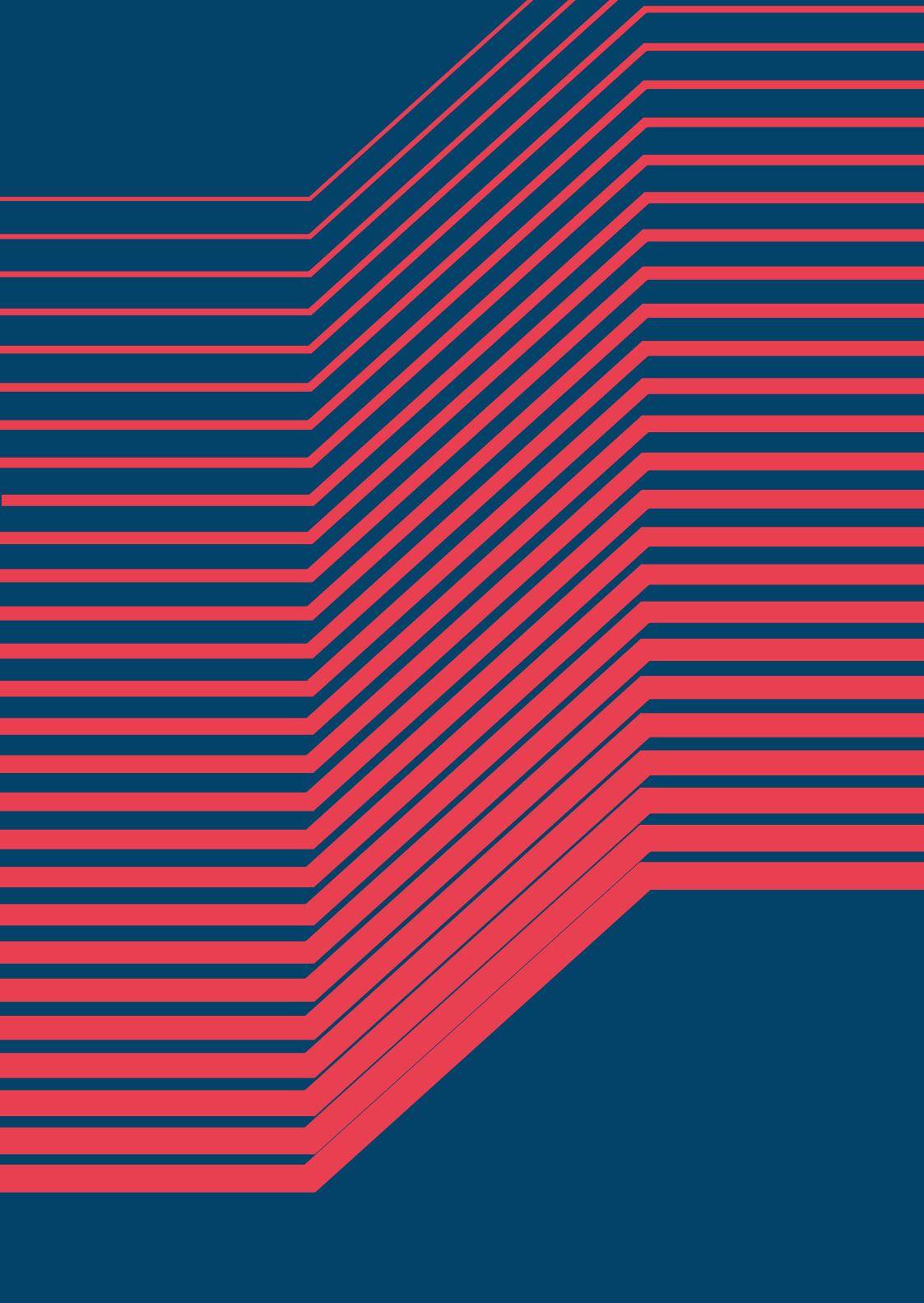
- ▶ *Guide pour réaliser un plan de continuité d'activité (Guide on drawing up a Business Continuity Plan)*, 2013.

ANSSI

- ▶ www.ssi.gouv.fr/en/
- ▶ *Ransomware attacks, all concerned, how to anticipate them and react in the event of an incident*, 2021:
www.ssi.gouv.fr/en/guide/ransomware-attacks-all-concerned/
- ▶ CERT-FR website, "Menaces et incidents" (Threats and incidents) section: www.cert.ssi.gouv.fr/cti
- ▶ *E BIOS Risk Manager*, 2018: www.ssi.gouv.fr/en/guide/ebios-risk-manager-the-method/

ENISA

- ▶ *Cyber Europe exercises*
www.enisa.europa.eu/topics/cyber-exercises/cyber-europe-programme?tab=publications
- ▶ *Good Practice Guide on National Exercises*
www.enisa.europa.eu/publications/national-exercise-good-practice-guide
- ▶ *Report on Cyber Crisis Cooperation and Management*
www.enisa.europa.eu/publications/ccc-study



"Anticipation is the key to protecting information systems. Through training, and with each exercise, the teams involved in crisis management develop their reflexes and better ways of working together. Then they are ready to cope when faced with an attack."

Guillaume Poupart, Director-General of ANSSI

Cyber crises can be devastating: we should not wait for disaster to strike to learn how to deal with it!

Carried out in partnership with the Club de la Continuité d'Activité and resulting from a wealth of experience in organising cyber crisis management exercises, this guide will support you in setting up your own training.

Version 1.0 – September 2021 – **ANSSI-PA-081-EN**
Licence Ouverte/Open Licence (Etalab — V1)
ISBN : 978-2-11-167103-4
Dépôt légal : septembre 2021

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

