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 cyber security) 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.

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.

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.

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.

No.	TIME	PHASE	STIMULATION CONTENT (content of the eemail or phone call to be adapted to your organisation)	SENDER (non-player - simulated by the moderation team)	RECIPIENT (players to take action)	INJECT DELIVERY MEANS	EXPECTED REACTIONS	COMMENTS FOR THE PLANNER
Situation information file (SIF)	YYMMDD **08:30**	**SIF**	Sending the SIF as an attachment of an email to all players.	MODDIR	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).

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

No.	TIME	PHASE	STIMULATION CONTENT (content of the eemail or phone call to be adapted to your organisation)	SENDER (non-player - simulated by the moderation team)	RECIPIENT (players to take action)	INJECT DELIVERY MEANS	EXPECTED REACTIONS	COMMENTS FOR THE PLANNER
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	All players	Email	No specific action expected.	
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)	Manager of the business line/ activity concerned	Phone call	Alerting/exchanging with the CISO.	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). 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.
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	CISO or equivalent	Phone call	Transmission of the alert and triggering of the crisis unit.	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.
4	YYMMDD **09:40**	**First messages about the incident**	*"Hello,* *Following our telephone conversation, you will find attached a photo of one of the posts. Please do not hesitate to send me any instructions that will allow me to answer future calls from employees. I will call you again if other services inform us that they are affected. We are really saturated with the volume of calls and have no information on the situation."*	Relevant IT contact point	CISO or equivalent	Email	Estimation of the first impacts, launching of investigations, preparation of the first measures to manage the incident and defining instructions for employees. Possibly, contacting a service provider or with ANSSI (simulated by the moderation team).	Depending on the malware chosen when designing the scenario, it is possible to use ransomware screenshots found on the Internet. For more information on the best practices to put in place in the context of a ransomware attack, consult the ANSSI guide *Ransomware attacks, all concerned, how to anticipate them and respond to an incident.*
5	YYMMDD **09:45**	**First messages about the incident**	*"Hello,* *I would like to inform you that the workstations of my entire team are unusable and all display the same message. Its impossible to work. Have we been hacked? Do you have an opportunity to resolve this fairly quickly because we have to deliver our project at the end of the week? We tried to restart the PCs without success."*	Manager of a team of the organisation (service/department of your choice)	CISO or equivalent	Phone call	Information taken into account and transmission of the first instructions if defined.	
6	YYMMDD **09:50**	**First messages about the incident**	*"Hello,* *Following our call, I confirm that my entire team's workstations are unusable and are all showing the same message. I'm texting you a picture of one of the stations. What is going on ?"*	Manager of a team of the organisation (service/department of your choice)	CISO or equivalent	Phone call	Information taken into account and forwarded to the crisis unit.	
7	YYMMDD **09:55**	**First messages about the incident**	*"Hello again,* *In light of the calls received so far, services/departments X and Y are affected as well as project team Z which must report its conclusions at the end of the week [indicate a critical deadline]. Can you give me instructions so that my team can answer users' questions? We are saturated and nothing seems to be working anymore."*	Relevant IT contact point	CISO or equivalent	Phone call	Transmission of the first instructions if defined, probing the scope of the attack and the start of discussions on business continuity.	
8	YYMMDD **10:00**	**Lateralisation of ransomware**	*"Hello,* *All of the Service X teams no longer have access to the data on their computers following the display of a message demanding a ransom. We were in the process of finalising project Y which we absolutely had to deliver today. What can we do in order to continue working? What is going on? I'm texting you a photo of a screen from one of the unusable computers."*	Manager of a team of the organisation (service/department of your choice)	Manager of the business line/ activity concerned	Phone call	Transmission of information to the CISO and distribution of instructions if defined.	
9	YYMMDD **10:05**	**Lateralisation of ransomware**	*"Hello,* *All of the Service X teams no longer have access to the data on their computers following the display of a message demanding a ransom. What is going on ? When can we get back to work?"*	Manager of a team of the organisation (service/department of your choice)	Manager of the business line/ activity concerned	Phone call	Transmission of information to the CISO and distribution of instructions if defined.	

No.	TIME	PHASE	STIMULATION CONTENT (content of the eemail or phone call to be adapted to your organisation)	SENDER (non-player - simulated by the moderation team)	RECIPIENT (players to take action)	INJECT DELIVERY MEANS	EXPECTED REACTIONS	COMMENTS FOR THE PLANNER
10	YYMMDD **10:15**	**Lateralisation of ransomware**	*"I am getting more and more calls from multiple parts of the organisation telling me that I cannot work because of a message displayed on their screen asking for a ransom. Our service is now completely saturated. Here is the list of services that contacted me:* *- service/department 1* *- service/department 2* *-...*	Relevant IT contact point	CISO or equivalent	Phone call	Taking information into account and further investigation. If not previously carried out and if deemed necessary, contact a service provider or national authority (simulated by the moderation team).	
11	YYMMDD **10:45**	**Publication of a photo of one of the workstations on social media**	*"Hello,* *I would like to inform you that a photo of one of the organisation's workstations appears to have been posted on social media (either it is one of our posts or an extremely similar photo). The organisation is not named, but if the link is made we should receive calls from the press soon. I will come back to you to inform you of the reactions observed on social networks."*	Person in charge of media monitoring (employee or service provider)	Communication manager + CISO	Email if accessible, otherwise phone call or emergency messaging	Start thinking about the communication strategy and the definition of lines to take (LTT).	
12	YYMMDD **11:00**	**Lateralisation of ransomware and start of investigation**	*"Hello,* *We confirm that the entire IT park has been impacted by the incident that is ongoing since this morning. The analysis of the network captures taken this morning confirms the lateralisation of the malicious code within the internal network, by a vector that we are trying to identify. We have no further information and investigations are difficult."*	Incident response team/ network administrator	CISO or equivalent	Email if accessible, otherwise phone call or emergency messaging	Implementation of degraded procedures, activation of the BCP or any procedure contributing to the management of the crisis. Verification of the application of best practices in the event of a ransomware attack.	Exercise planners will need to decide beforehand whether the organisation still has access to its email. If so, exchanges can continue as before. Otherwise, the crisis unit will have to put in place other tools to communicate. More generally, from this inject it is necessary to materialise the loss of access to the network: computers, crisis unit tools, directories, messaging, etc. will no longer be usable if they are managed on the impacted network. The players will thus have to think of back-up solutions to manage the crisis and maintain certain critical activities. This option, while realistic and likely, however increases the level of difficulty of the exercise. It is possible here to multiply the injects of this type, coming from different technical teams (administrators, security teams, network teams, etc.) in order to emphasize that the situation is very serious and that the organisation has very little information on what is going on.
13	YYMMDD **11:10**	**Social media posts**	*"Hello,* *Here are some examples of social media posts: @organisation, you confirm to have been attacked? #cyberthreat* *Looks like @organisation got pwnd. Info? #insecure"*	Person in charge of media monitoring (employee or service provider)	Communication manager	Tweet	Taking information into account, preparing a communication strategy.	
14	YYMMDD **11:15**	**Request for transparency and status update from the business units**	*"Hello,* *Could you send us the information you have on the current incident, in particular what concerns its nature and extent in order to allow our services to continue despite the situation, in degraded mode if necessary. Besides, we are told that everything is backed up, I hope this is really the case because we absolutely need our files back."*	Different heads of departments contact their managers to find out what they are going to say to their teams and whether they need to initiate degraded procedures	Manager of the business unit/ activity affected	Email if accessible, otherwise phone call or emergency messaging	Prepare and transmit instructions adapted to the situation.	Inject to push as many times as desired to increase the pressure on the players.
15	YYMMDD **11:30**	**Media pressure**	*"Hello,* *Reports circulating on social media seem to indicate that your organisation is the target of a computer attack. Can you confirm? How deeply impacted is your organisation? Can you continue your activities?"*	Journalist	Communication manager	Phone call	Transmit the previously defined LTT (if these are not ready, offer to call the journalist back later). It is also possible to not comment and issue a press release later.	

No.	TIME	PHASE	STIMULATION CONTENT (content of the eemail or phone call to be adapted to your organisation)	SENDER (non-player - simulated by the moderation team)	RECIPIENT (players to take action)	INJECT DELIVERY MEANS	EXPECTED REACTIONS	COMMENTS FOR THE PLANNER
16	YYMMDD **12:00**	**Taking responsibility for the attack and threat of publishing the exfiltrated data**	*"Hello,* *Below is a copy of the attack claim message posted on an Internet forum: ""All of [organisation] 's data are belong to us !!! We will the data give back, when You to us XXXX BTC before 24H give. After 24H will we the data on the Internet for all to see publish !!! "" [optional] In attachment, a screenshot of the message."*	Person in charge of media monitoring (employee or service provider)	Communication manager + CISO	Email if accessible, otherwise phone call or emergency messaging	Taking into account the information and investigating a potential exfiltration of data.	The screenshot can be created based on ransomware images found on the Internet. If this option is chosen, the publication of the attackers can be spotted by Internet users who then challenge the organisation on social networks.
17	YYMMDD **12:30**	**Remediation strategy**	*"Hello,* *We have seen in the press that your organisation has suffered a cyberattack. Are your activities completely at a standstill? When do you think you can get them back? Can you give us an update on the situation as quickly as possible and tell us about your strategy to remedy this event?"*	High ranking non-playing authority (example: supervisory authority, controlling authority, shareholders, etc.)	Crisis manager	Email if accessible, otherwise phone call or emergency messaging	Development of the remediation strategy and presentation to the upper hierarchy.	
18	YYMMDD **12:45**	**Clients/Users requests**	*"Hello,* *I have been contacted by several clients/users who have noticed that our website is inaccessible. They can therefore no longer access our services [specify which ones here]. They also say they saw in the press that we had suffered a cyber attack and ask us if this is the cause of the unavailability of the service. They are finally wondering about the resumption of the latter. What information can be shared with them?"*	Customer relationship manager	Service manager	Email if accessible, otherwise phone call or emergency messaging	Dissemination of LTT aimed at reassuring about the handling of the incident.	
19	YYMMDD **13:00**	***[Option "ANSSI Simulation" #1]*** **If the organisation is part of ANSSI's scope of intervention and one of the player 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	CISO (or person generally responsible for reporting incidents)	Phone call	Transmission of the available information to ANSSI.	If you are a regulated beneficiary (NIS), you can simulate reporting your incident to the established authority. 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). 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. In this inject, the national authority or provider tries to obtain as much information as possible to understand the situation and make recommendations.
19bis	YYMMDD **13:00**	***[Option "ANSSI Simulation" #2]*** **If the organisation is part of 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	CISO or equivalent	Phone call	Transmission of the available information to ANSSI.	
19ter	YYMMDD **13:00**	***[Option "Service provider Simulation"]*** **If one of the players has reported the incident**	*"Hello,* *We get back to you following your incident report. What are the impacts on your activities? Someone from our team will contact you very soon to support you remotely in the investigation and remediation process."*	Service provider	CISO (or person generally responsible for reporting incidents)	Phone call	Transmission of the available information to the service provider.	
20	YYMMDD **13:10**	***[Option "Game with multiple sites and several crisis units invloved as a players"]*** **Lateralisation of ransomware**	*"Hello,* *I'm calling because my team members can no longer use their machines. The screens show a message asking for a ransom to recover the data. We have a very important order/project to return at the end of the week, we absolutely have to be able to work. What do we have to do ? Also, I think the problem is at least spreading across our entire floor ... What's going on?"*	Seconde site manager (service/department of your choice)	Second site CISO or equivalent	Phone call	Transmission of the alert, triggering of the second site's crisis unit and sharing of information with the organisation.	This can be any second site (located in France or abroad): subsidiary, production site, second building. To simulate the gradual impact and the increasing magnitude of the crisis, this inject is to be repeated (in 5-minute intervals) according to the number of services/activities of the second site / subsidiary that you wish to immobilise following the lateralisation of the ransomware . To simulate aspects of lateralisation within the organisation, it is possible to add business consequences specific to each department in the scripts of phone calls and eemails.

No.	TIME	PHASE	STIMULATION CONTENT (content of the eemail or phone call to be adapted to your organisation)	SENDER (non-player - simulated by the moderation team)	RECIPIENT (players to take action)	INJECT DELIVERY MEANS	EXPECTED REACTIONS	COMMENTS FOR THE PLANNER
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)	Safety/security manager, commercial director, or any player within the crisis unit of the organisation deemed relevant and who would be the point of contact of the second site	Phone call	Transmission of information to and within the crisis unit and dissemination of initial instructions.	This could be any second site (located in France or abroad): subsidiary, production site, second building, etc. 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.
22	YYMMDD **13:30**	***[Option "ANSSI simulation"]*** **Request for further information**	*"Hello,* *We have taken into account your report, recorded under the reference [RM # XXXXXX]. As part of our incident handling process, we would like more information. You will find below the elements requested as well as the first recommendations.* ▸ *Last name and first name/email address/telephone number of the CISO and / or the person in charge of this incident* ▸ *Which machines are affected by the infection? What type of files were encrypted? Is the compromised IS linked to other ISs?* ▸ *What is the impact of this incident on the continuation of your activities?* ▸ *Date and time of infection?* ▸ *What is the vector of the compromise (malicious eemail, exploitation of vulnerability, compromise of IS, etc.)?* ▸ *Do you know the ransomware? Its version?* ▸ *What is the extension of the encrypted files?* ▸ *Do you have digital fingerprints (MD5, SHA1, SHA256 ...), a ransomware sample or screenshots to send to us?* ▸ *Can you communicate the ransom note, the email addresses involved, the Bitcoin wallets?* ▸ *Do you have healthy backups that would restore the infected system?* ▸ *Did you hire a provider to help you? If yes: which one?* ▸ *What were the reactive measures taken following this incident?* ▸ *In the event that personal data has been affected, have you reported the incident to the DPO?* ▸ *Have you thought about making X or Y declaration (e.g. if listed on the stock market, declaration to the stock market watchdog) [to be adapted to the context]?* ▸ *Are you considering or have you already filed an official complaint?* ▸ *It is very unlikely that the data can be decrypted. However, do you seek assistance from ANSSI in your remediation actions? If so, for which field (s) of intervention?* **Note that at this stage, the level of ANSSI's commitment cannot be defined.** *You can also find the first remedial measures in the event of a ransomware infection by following these links:* ▸ *www.cert.ssi.gouv.fr/information/CERTFR-2017-INF-001* ▸ *www.cybermalveillance.gouv.fr/tous-nos-contenus/fiches-reflexes/rancongiciels-ransomwares* *Then, and with a view to a criminal proceeding (recommended), we remind you that you are invited to keep without making any changes, any document or information establishing the facts and which could potentially constitute evidence:* ▸ *physical copies of the hard disks (or VM) of the compromised workstations.* ▸ *copies of event logs available on any network equipment that could have allowed the transmission of malicious code.* *Finally, depending on the type and version of the ransomware, there may be a dedicated decryption tool or keys. A repository of these solutions is available on the No More Ransom website (www.nomoreransom.org/fr/index.html). We invite you to consult the preliminary advice and user guides before any decryption operation.* *A person in charge of communication at ANSSI will contact your communicators. Can you send me their contact details? I suggest to quickly plan a planning meeting.*	ANSSI	CISO or equivalent	Phone call	Transmission of the available information to ANSSI	It is possible to simulate instead of this inject a call from a provider, if contacted by the players (via the moderation team), who will ask similar questions.

No.	TIME	PHASE	STIMULATION CONTENT (content of the eemail or phone call to be adapted to your organisation)	SENDER (non-player - simulated by the moderation team)	RECIPIENT (players to take action)	INJECT DELIVERY MEANS	EXPECTED REACTIONS	COMMENTS FOR THE PLANNER
23	YYMMDD **13:40**	**Social media requests**	*"Hello,* *Here are some examples of social media posts:* *@organisation you confirm to have been hacked? Apparently data has been exfiltrated #ransomware #cyberthreat* *@organisation you plan to pay the ransom? #hostage #ransomware* *@organisation is already unable to avoid being hacked, and now they can't even manage the consequences and secure the data #insecure #ransomware* *@organisation the attackers would be in possession of your customers' data. Do you confirm? #organisation_leak #ransomware"*	Person carrying out media monitoring (employee or service provider)	Communication manager	Tweet	Taking all available information into account in the communication strategy.	
24	YYMMDD **13:50**	***[Option "Game with multiple sites and several crisis units invloved as a players"]*** **Lateralisation of ransomware**	*"Hello,* *All the workstations on the site are disabled, they all display the same screen asking us to pay a ransom. Unable to continue working, the site is down! Orders/services will not be ready on time, it's a disaster. Can you send a team to fix it? Does the main seat have the same problem? We do not have more information as it stands, we are completely in the dark about the origin of the problem."*	Second site technical team	Second site CISO or equivalent	Email if accessible, otherwise phone call or emergency messaging	If not completed previously, transmission of the alert, triggering of the second site's crisis unit and sharing of information with the organisation. Estimation of the first impacts, launching of investigations, preparation of the first measures to manage the incident and definition of instructions for employees.	As with the organisation's main site, exercise planners will need to decide beforehand whether the second site still has access to their emailbox. If so, the exchanges can continue as before. Otherwise, the second site's crisis unit will have to set up other tools to communicate. It is also necessary to materialise the loss of access to the network: computers, crisis unit tools, directories, messaging, etc. will no longer be usable if they are managed on the network. The players will thus have to think of back-up solutions to manage the crisis and maintain certain critical activities.
25	YYMMDD **14:00**	***[Option "ANSSI simulation"]*** **Contacting COM**	*"Hello,* *I work in the communication division of ANSSI and I am contacting you following the discussions you have with the agency about your incident. We offer to support you in anticipating and/or preparing your elements of external and internal communication in the event of visibility of the attack.* *Have the first elements of internal or external communication already been transmitted? Have you been solicited by the media? To build your communication strategy, several actions to take as a first step: definition of stakeholders (internal, customers, authorities, etc.), targets and objectives of your communication as well as any points of vigilance specific to your entity (reputation/brand image, media exposure), your business sector (market news, etc.), your schedule (financial communication obligation, buyout, etc.), etc. We can assist you in drafting your communication elements (press release, internal communication). If you wish to mention ANSSI, we will ask to validate the mention."*	ANSSI COM	Communication manager	Phone call	Development of the communication strategy and transmission of information to the second site.	ANSSI's general posture is to support the organisation but not to communicate for it.
26	YYMMDD **14:20**	***[Option "Game with multiple sites and several crisis units invloved as a players"]*** **Details on the suspension of the activities of the second site**	*"Hello,* *Following the incident that has been ongoing since this morning, here is an update on the impact identified:* *Examples:* *- impossible to take orders (or to follow them);* *- impossible to mark products and therefore to issue them;* *- activities in degraded mode/shutdown;* *- etc."*	Manager of a team at a second site [service/department of your choice]	Head crisis unit of the second site or business unit representative in the crisis unit	Email if accessible, otherwise phone call or emergency messaging	Reflection on business continuity.	Impacts to be defined according to the specifics of your organisation and your second site and has to be broken down into as many injects as there are desired impacts.
27	YYMMDD **14:35**	**Press contact**	*"Hello,* *We learned that your organisation has just been the target of a cyber attack and that the attackers issued an ultimatum: pay the ransom or have your data posted online. Do you confirm this information? Does this attack have a significant impact on your organisation? Who do you think is causing it?"*	Journalist (specialised press)	Communication manager	Phone call	Transmission of previously defined LTT or referral to a press release if published.	
28	YYMMDD **15:00**	**Press contact**	*"Hello,* *For your information, we have just identified an article in the press relating to the ongoing incident. The article particularly calls into question our ability to respond to and remedy the incident."*	Person in charge of media monitoring (employee or service provider)	Communication manager + CISO or equivalent	Email if accessible, otherwise phone call or emergency messaging	Transmission of previously defined LTT or referral to a press release if published.	These press contacts can also be sent to the second site.
29	YYMMDD **15:15**	***[Option "Game with multiple sites and several crisis units invloved as a players"]*** **Press contact**	*"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?"*	Journalist	Second site communication manager	Phone call	Use (if transmitted) HQ LTT or request them before responding. Referral to a joint press release if existing.	

No.	TIME	PHASE	STIMULATION CONTENT (content of the eemail or phone call to be adapted to your organisation)	SENDER (non-player - simulated by the moderation team)	RECIPIENT (players to take action)	INJECT DELIVERY MEANS	EXPECTED REACTIONS	COMMENTS FOR THE PLANNER
30	YYMMDD **15:20**	**Assessment of the attack**	*"Hello,* *I would like to inform you that in order to stop the spread of malicious code, the interconnections of the information systems of the other sites of the organisation with the systems at headquarters have been cut. To our knowledge, only the main site and a second site were impacted by the attack."*	Technical team member or service provider	CISO	Email if accessible, otherwise phone call or emergency messaging	Include/take into account in the situation update and transmission of information to the crisis unit.	If the organisation makes this decision earlier, it must be taken into account by the moderation team (send this stimulus earlier). More generally, any preventive measure taken (such as network cuts) must then be integrated into the scenario at the right time so that the players think about warning the stakeholders for whom they deem it necessary to do so and can anticipate the related communication actions.
31	YYMMDD **15:30**	**Press contact**	*"Hello,* *Your organisation appears to be the target of a sophisticated computer attack. The attackers ask you to pay a ransom within 24 hours. Do you plan to pay the ransom? How has your organisation been impacted? How long has this situation been going on?"*	Journalist	Communication manager	Phone call	Transmission of previously defined LTT or referral to a press release if published.	
32	YYMMDD **15:35**	***[Option "Publication of exfiltrated data"]***	*"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."*	Person in charge of media monitoring (employee or provider)	CISO or equivalent + communication manager + security officer	Email if accessible, otherwise phone call or emergency messaging	Preparation of a communication strategy.	As part of the exercise, it is not useful to distribute to players all of the materials that would be released. However, it is interesting to have some documents on hand to send as illustrations (and which may for example be mentioned by the press). It is up to planners to determine the number and their sensitivity.
33	YYMMDD **15:40**	**Internal pressure (organisation headquarters)**	*"Hello,* *The workstations of the service are still unusable. Can you let me know when this situation will be resolved? My agents can no longer work and orders are behind schedule, the situation is becoming untenable and we are still lacking information on the situation."*	Manager	CISO	Phone call	Dissemination of instructions.	Injects to multiply as much as desired to increase the pressure on the players. Requests can also be addressed to the business managers present in the crisis unit.
34	YYMMDD **15:45**	**Technical analysis via** ***[Option "ANSSI simulation"]*** **or a service provider**	*"Hello,* *Here are some findings from our analysis. We have been able to identify the malicious code behind the attack, believed to be EvilRansomware ransomware. However, we have not yet identified the initial infection vector. This malicious code encrypts files on the machine as well as on accessible network shares. It also removes shadow copies. Your IS will not return to normal operation for at least a week. It will therefore be necessary to plan to work almost without IT and therefore in degraded mode during this period. What are the priorities for restoring services? Have you planned measures to manage this situation over time (deployment of the BCP, shifting of teams/night work/refueling, use of one or more service providers, etc.)?"*	ANSSI or service provider	CISO	Email if accessible, otherwise phone call or emergency messaging	Preparation of a remediation strategy, update of the current situation. Reflection on the continuity of activity and the operation in degraded mode.	Important: to allow players to experience several phases of the crisis, the game is intentionally accelerated and is not representative of what would have happened in a real case. Indeed, by way of illustration, it is not uncommon for the IS to be completely unavailable for 1 to 2 weeks in the face of this type of attack. In addition, the return to nominal operation of the IS often takes a long time, sometimes even taking several months. This inject can also be emitted by a provider.
35	YYMMDD **15:50**	***[Option "Publication of exfiltrated data"]*** **Analysis of data published by attackers on a website**	*"Hello,* *The few people who have started to read the leaked documents confirm their authenticity. For example, we found a list of names which corresponded well to the staff of the organisation, a meeting report and a report (see attachment). We are continuing to read the documents and will get back to you as soon as possible."*	Head of department (free choice, department impacted by simulated disclosures)	Crisis manager	Email if accessible, otherwise phone call or emergency messaging	Adaptation of the communication strategy.	This inject can also be adapted to the second site with different documents.
36	YYMMDD **15:55**	***[Option "Game with multiple sites and several crisis units invloved as a players"]*** **Social media requests**	*"Hello,* *Here are some examples of social media requests:* *@secondsite you confirm to have been hacked? #ransomware #cyberthreat* *Looks like @ secondsite got pwnd. Info? #insecure #ransomware* *@organisation @secondsite you plan to pay the ransom? #hostage #ransomware"*	Person in charge of media monitoring (employee or service provider) within the second site	Communication manager of second site	Tweet	Take these messages into account for the communication strategy and exchange with the organisation for LTT.	

No.	TIME	PHASE	STIMULATION CONTENT (content of the eemail or phone call to be adapted to your organisation)	SENDER (non-player - simulated by the moderation team)	RECIPIENT (players to take action)	INJECT DELIVERY MEANS	EXPECTED REACTIONS	COMMENTS FOR THE PLANNER
37	YYMMDD **16:00**	***[Option "Game with multiple sites and several crisis units invloved as a players"]*** **Customer/user requests**	*"Hello, I have been contacted by several clients/users who have noticed that our website is inaccessible. They can therefore no longer access our services [specify which ones here]. They also say they saw in the press that we had suffered a cyber attack and ask us if this is the cause of the unavailability of the service. They are finally wondering about the resumption of the latter. What information can be given to them?"*	Customer relationship manager of the second site	Service director of second site	Email if accessible, otherwise phone call or emergency messaging	Dissemination of LTT to reassure on the treatment of the incident.	
38	YYMMDD **16:05**	**Infection vector info via *[Option "ANSSI simulation"]*, a simulated member of the organisation's technical team or a service provider**	*"Hello, We have identified the phishing eemail that led to the initial intrusion of your IS. Our analysis is continuing to identify the lateral movement. The workstation which is the origin of the compromise belongs to a member of the executive committee. We have located the malicious attachment that caused the attack. It appears to be EvilRansomware ransomware. To our knowledge, there is no decryption key. However, we can use backups that are not very recent. Some data will be irretrievably lost. As a result, some activities will not be able to resume immediately. The return to normal operation of the IS will take a long time, you have to prepare for it."*	ANSSI or technical team member or service provider	CISO or equivalent	Email if accessible, otherwise phone call or emergency messaging	Transmission of information to the second site and sharing of the technical elements.	Important: to allow players to experience several phases of the crisis, the game is intentionally accelerated and is not representative of what would have happened in a real case. Indeed, by way of illustration, it is not uncommon for the IS to be completely unavailable for one to two weeks in the face of this type of attack. In addition, the return to nominal operation of the IS often takes a long time, sometimes even taking several months. This inject can also be sent by a provider or a simulated member of the organisation's technical team.
39	YYMMDD **16:07**	***[Option "Publication of exfiltrated data"]*** **Internal questions**	*"Hello, I learned that belonging to us has been published. Do you know where to find these documents and if any from my department are included? We are dealing with very sensitive data that should not be known to the outside world."*	Head of department [free choice, department impacted by simulated disclosures]	CISO or equivalent	Email if accessible, otherwise phone call or emergency messaging	Communication on data verification efforts.	These concerns can relate to different services which can be simulated using this same format.
40	YYMMDD **16:15**	**Social media posts and requests**	*"Hello, For information, elements of the attack are circulating on social networks. Users share the article and question the organisation's ability to cope with it and directly challenge our management on Twitter."*	Person in charge of media monitoring (employee or service provider)	Communication teams, CIO/CISO	Email if accessible, otherwise phone call or emergency messaging	Preparation of LTT for the response to these messages.	Injects to multiply as much as desired to increase the pressure on the players. Requests can also be addressed to the business managers present in the crisis unit.
41	YYMMDD **16:20**	***[Option "Publication of exfiltrated data"]*** **Press contact**	*"Hello, For information, a press article has just been published and mentions the publication of data from the organisation. Journalists only mention a few titles of documents and do not seem to have analysed them. It appears that reports and notes exist. [optional: write the press article to attach to the message]"*	Person in charge of media monitoring (employee or provider)	Communication manager + security officer + CIO/CISO	Email if accessible, otherwise phone call or emergency messaging	Adaptation of the communication strategy.	
42	YYMMDD **16:25**	***[Option "Game with multiple sites and several crisis units invloved as a players"]*** **Publication of data exfiltrated by attackers on a website**	*"Hello, For information, a press article has just been published and mentions the publication of data from the organisation. Journalists only mention a few titles of documents and do not seem to have analysed them. It appears that reports and notes exist. [optional: write the press article to attach to the message]"*	Person in charge of media monitoring (employee or service provider) within the second site	Communication manager + security officer + CIO/CISO of second site	Email if accessible, otherwise phone call or emergency messaging	Adaptation of the communication strategy.	
43	YYMMDD **16:30**	***[Option "Publication of exfiltrated data"]*** **Internal questions**	*"Hello, As a result of the disclosure of data from our organisation over the Internet, my staff are concerned that their personal data may have also been published. Can you tell me what will be put in place to address these concerns?"*	Manager	CIO/CISO	Email if accessible, otherwise phone call or emergency messaging	Transmission of the instructions defined by the crisis unit and taking into account the remark for internal communication.	

No.	TIME	PHASE	STIMULATION CONTENT (content of the eemail or phone call to be adapted to your organisation)	SENDER (non-player - simulated by the moderation team)	RECIPIENT (players to take action)	INJECT DELIVERY MEANS	EXPECTED REACTIONS	COMMENTS FOR THE PLANNER
44	YYMMDD **16:35**	***[Option "Publication of exfiltrated data"]*** **Clients/users requests**	*"Hello,* *Following the disclosure of data from our organisation on the Internet, we have been contacted by several clients/users concerned that their data may have been published."*	Customer service or in contact with users	Communication manager + security manager + CIO/ CISO	Email if accessible, otherwise phone call or emergency messaging	Adaptation and dissemination of LTT or referral to a press release or statement if it was created.	
45	YYMMDD **16:37**	***[Option "Game with multiple sites and several crisis units invloved as a players"]*** **Clients/users requests**	*"Hello,* *Following the disclosure on the Internet of data from our second site, we were contacted by several clients/users concerned that their data might have been exposed."*	Customer service or in contact with users of the second site	Communication manager + security manager + CIO/ CISO of second site	Email if accessible, otherwise phone call or emergency messaging	Adaptation and diffusion of LTT.	
46	YYMMDD **16:42**	***[Option "Publication of exfiltrated data"]*** **Social media request**	*"Hello,* *For information, many tweets commenting on the disclosure of our organisation's data. The messages published question the authenticity of the data and the security of the data of our customers, who continue to contact us."*	Person in charge of media monitoring (employee or provider)	Communication manager + security manager + CIO/ CISO	Email if accessible, otherwise phone call or emergency messaging	Verification of the entire data set, preparation of LTT.	
47	YYMMDD **16:45**	***[Option "ANSSI simulation"]***	*"What was the feedback following the publication of your press release? Would you like to post something again?"*	ANSSI COM	Communication manager	Email if accessible, otherwise phone call or emergency messaging	Prepare a status update on the communication strategy.	
48	YYMMDD **16:50**	***[Option "ANSSI simulation"]*** **Conclusive inject for the end of the exercise through a simulated member of the organisation's technical team or a provider**	*"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."*	ANSSI or technical team member or provider	CISO or equivalent	Email if accessible, otherwise phone call or emergency messaging	Transmission of information to the second site. Reflection on the 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.
49	YYMMDD **17:00**	**End of the exercise (END EX)**	*"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."*	MODDIR	All players	Email	Participation in the collection of feedback.	Well done, you have put in place a cyber crisis management exercise!