# Cyberattack and resilience with Nuabee

Cyber-Resilience by Nuabee · https://nuabee.com/documents/cyberattack-and-resilience-with-nuabee/

## The specific nature of cyber attacks

Compared to other crisis scenarios, cyber crises have specific characteristics that are important to understand:

- A dual temporality, with immediate impacts and a long remediation process that can extend over several weeks or even months;
- Uncertainty regarding the scope of the compromise;
- A lack of uniqueness of location, which implies a potential propagation to other organizations/companies due to the interconnection of IS;
- A threat that can adapt to containment and remediation measures;
- A complexity to understand the attacker's objectives and attribute the origin of the attack.

(extracts from ANSSI documents)

## The different stages

1. secure the perimeter
2. assess the severity of the cyber disaster
3. activate DRP measures
4. decide on complementary measures

Compared to other crisis scenarios that may require the activation of a DRP, cyber crises have specific characteristics:

- Immediate impacts (shutdown of certain activities, inability to deliver services, etc.).
- Uncertainties concerning the scope of the compromise.
- The complexity of deciding what can or cannot be restarted in DRP mode, and in what order, as this is linked to :
  - The vector of the attack: is it a worm, externally controlled ransomware, etc.

- Potential propagation to other organizations due to the interconnection of IS.

In the first few hours, it can be difficult to distinguish an IT incident from a cyber incident.Technical teams must try to detect weak signals to shut down systems if necessary.

## Step 0: Secure the perimeter

| List of actions to be taken | Action details | Persons responsible for implementation | Available tools and documents |
|---|---|---|---|
| Isolate affected perimeters and secure perimeters not yet impacted | This involves activating environment / VM / network isolation mechanisms. | CISO + IT Manager | Technical procedures + reflex cards |
| Decide to cut WAN & LAN networks | Decide to cut the following networks:<br>• Internet access<br>• VPN IPsec / SSL<br>• Wifi / Bluetooth Endpoint ... | Customer IT team+ Telecom service providers | Customer technical procedures |
| Mobilize the usual external technical service providers | This involves mobilizing the external players who may be needed to diagnose incidents, signals, .... | IT manager + IT team | Outsourced list of service provider contact details |
| Putting Nuabee teams on call | Even before deciding whether to switch to standby mode, you need to put the Nuabee **teams on standby.** It may be decided to activate the restart of certain servers as a priority. | Person authorized to activate DRP Nuabee | PRA activation procedure in the PRA console |
| Mobilize external cyber experts for advice/support on the scale of the cyber crisis | • If subscribed to CSIRT or OCD **Incident** Response<br>• Without subscription: "best effort | CISO + IT Manager + Finance Manager | Outsourced list of experts |

## Step 1: Assess the severity of the cyber loss

- Which businesses (services) are affected
  - Which businesses (services) are able to work or not?
  - Which IS applications are affected?
  - Which IS applications can continue to be used?
- Are employee and/or customer data affected?

| List of actions to be taken | Action details | Persons responsible for implementation | Available tools and documents |
|---|---|---|---|
| Designate and convene the first meeting of the Cyber Crisis Unit | In a cyber crisis, the buildings remain available.<br>We need to define a location and convene the first CC meeting. | CISO + IT Manager | - Contact details CC actors- CC logistics |
| Organize Cyber Crisis Unit logistics (premises, communication tools) | In the event of a cyber attack, we need to define :<br>• The means of communication to be used<br>• The communication tools to use<br>And how to communicate them to internal and external experts. | CISO+ IT Manager | - Fallback communication tools- Note-taking tools |
| Receive situation reports | Receive situation reports from business units/external contributors via agreed communication channels. | CISO + IT Manager | External backup messaging solution |
| Mobilize external Cyber experts | Mobilize external experts to advise on the scale and scope of the cyber crisis. | CISO + IT Manager | |
| Understand the type of attack and how to contain and clean it up. | Find out if the attack is known and if action can be taken to remediate it. | CISO+ External experts | |

| | | | |
|---|---|---|---|
| Assessing the severity of the incident | This involves estimating the potential impact of the crisis, and producing a Report that gives an initial idea of the scope of the crisis. | All CC Cyber players | |

## Step 2: Activate DRP measures

This stage involves restoring critical applications and data so that core activities can be resumed:

1. The scope of the DRP to be activated, in particularThe
    1. choice of sites (if the DRP concerns several sites)
    2. The list of VSThe
    3. restoration date (last backup or specific date)
2. Additional actions to be carried out before opening access to usersExecution of
    1. security testsLaunch of
    2. additional security appliances in the recovery space

| List of actions to be carried out | Action details | Persons responsible for implementation | Tools and documents available and comments |
|---|---|---|---|
| Define the scope of the DRP to be activated | This involves defining :<br>• Site selection (if the DRP involves several sites)<br>• List of VMs (functional scope)<br>• Restoration date (last backup or specific date) | Customer IT team | PRA console containing list of servers |

| | | | |
|---|---|---|---|
| Decide on additional actions before opening the rescue space | This section identifies optional actions to be taken before opening the rescue space to users:<br>• Run anti-virus scans<br>• Perform forensics<br>• Isolate certain VMs on reboot<br>• ... | IT Manager + External Cyber Experts | |
| Run antivirus scans on restarted servers | This involves running antivirus scans on restored and restarted servers to check that restarted servers do not contain any known malware. | Customer IT team | • Windows Defender scan by default.<br>• Other solutions available. |
| Performing forensics | Provision of a dedicated Cloud space for the Cyber consulting firm:<br>• Opening of access rights<br>• Copying disks from the project perimeter<br>• Support in using Cloud space. | External Cyber Experts with **Flexible Recovery** team support | |

| | | | |
|---|---|---|---|
| Isolating certain VMs on reboot | For certain VMs, it may be necessary to isolate them on a specific VLAN without any communication with other servers, pending advice from Cyber Security experts. | **Flexible Recovery** + Customer teams | |
| Decision to open networks | We need to decide:<br>• Which networks can be opened.<br>• What security and monitoring measures are implemented on open networks? | IT Manager | The IT manager's decision is passed on to the **Flexible Recovery** teams. |

## Step 3: Decide on additional measures

It's important to bear in mind that remediation in the wake of a cyber crisis can be a potentially lengthy process, lasting several days, weeks or even months.

You need to draw up a list of additional urgent actions to be carried out, and identify those responsible for implementing them.

This stage involves adapting the scope of the disaster recovery plan, hardening the systems and monitoring the attacker, so that core activities can be resumed.

In the event of a cyber-attack, it is possible (or even probable) that modifications will have to be made to infrastructures (security architecture, OS versions, server hardening, telecom architecture modifications, etc.) before a return to the nominal situation can be envisaged.

## Stage 4: organizing the return

This involves organizing the return to the nominal situation, after the activation of the DRP and its use in real-life by a Customer.

The aim is to present the general process and, depending on the context of the cyber crisis, the implementation mechanisms will be adjusted.

All these phases are explained in a specific document: **Return to nominal situation after use of the DRP.**