How do our solutions contribute to a Business Continuity Plan?

Cyber-Resilience by Nuabee · https://nuabee.com/documents/nuabee-continuity-plan-solution/

Definitions: what is a Business Continuity Plan?

In the vocabulary of Business Continuity, a BCP (Business Continuity Plan) represents all the elements making up a plan that should enable a company to function even in a disaster situation, and at the very least in degraded mode.

This Business Continuity Plan has several dimensions:

- a **logistical dimension**: the offices have burned down, how are we going to relocate employees and which ones can be sent to telework?
- a **business dimension**: which business processes must continue to function (and which are less or not critical and will be mothballed)?
- an **IT and network dimension**: which applications support the most important business activities. This is often referred to as a DRP (Disaster Recovery Plan)?
- Finally, a **crisis management dimension** which, depending on the disaster scenario, must address the articulation of business vision, internal and external communication, and relations with customers and the authorities.

How Nuabee solutions contribute to a Business Continuity Plan

As a Business Continuity Plan solution, Nuabee focuses primarily on IT and network recovery, but also participates in IT crisis management.

So, in addition to the highly technical dimension of restarting servers in the right order and to respect restart deadlines (normally based on business needs), Nuabee supports customers in their IT crisis management.

This is all the more important in a crisis context linked to a cyber attack, where in the first few hours it can be difficult to distinguish an IT incident from a cyber incident.

The particular context of a cyber attack

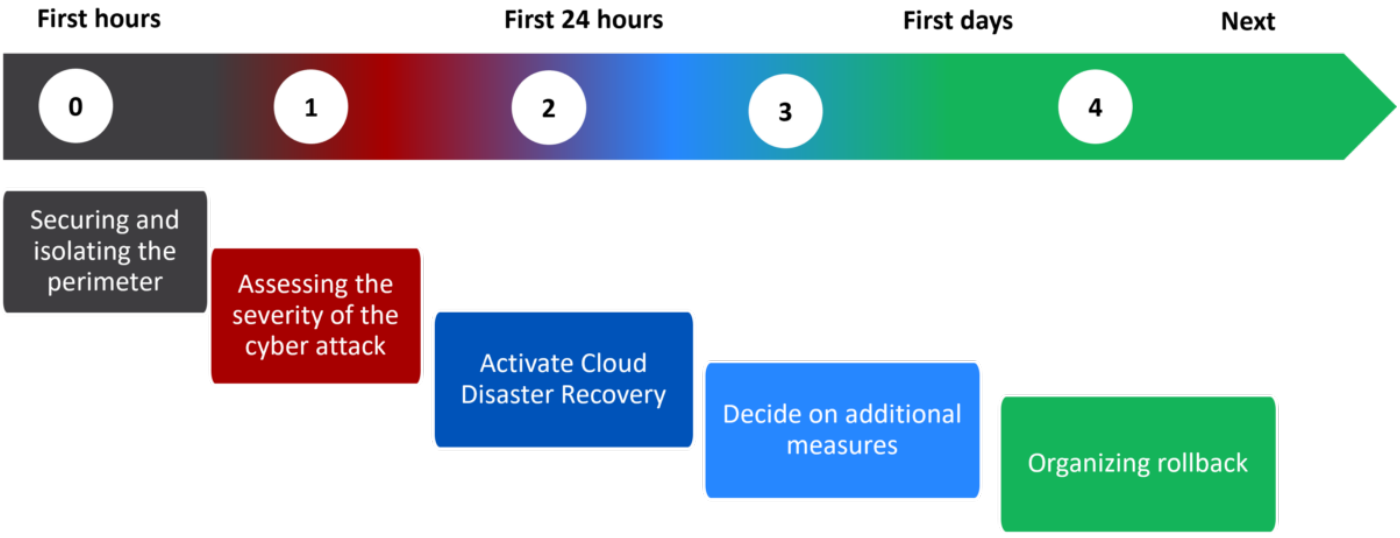
Compared to other crisis scenarios, cyber crises have specific characteristics that are important to understand:

- Uncertainty about 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 dual temporality, with immediate impacts and a long remediation process that can extend over several weeks or even months.

This crisis implies a certain complexity in understanding the attacker's objectives and attributing the origin of the attack.

Nuabee's involvement in the chronology of a cyber crisis

The main stages of a cyber crisis are as follows:



Nuabee can support you in these 4 stages and can propose additional actions before reopening applications to users, such as :

- Running anti-virus scans on disks and VMs
- Run forensic tools on disks and VMs

- Provision of an isolated environment for the customer's security provider to run digital forensic tools.

