MEDIA CONTACT
The offshore company

CRISIS MANAGEMENT AROUND PERSONAL DATA (LEAKAGE, CYBERATTACK, ETC.)

Review History	
Last updated	January 2021

Summary

I.INTRODUCTION 33 3

II.THE SPECIFICITES OF CYBER CRISIS MANAGEMENT 34 3

III.CRISIS MANAGEMENT DEVICE 44 4

IV.The major stages of crisis management 56 5

V.The Means 89 8

VI.Our principles of communication in times of crisis 911 9

I. Introduction

Today's world is undergoing a digital revolution. New technologies (particularly those related to IT and telecommunications) are changing the business world. This digital revolution also has repercussions on business security. Their level of exposure to risks in general and cyber risks in particular has been on the rise in recent years and has become a subject of concern and concern for business leaders. Globalization and the digitization of the world of business and trade have brought new sources and new types of threats. The Information Systems (IS) of companies host a multitude of information that attracts covetousness, whether from competitors, cyber-offenders or even people inside society. These same information systems are increasingly interconnected and open (e.g. on the Internet), and therefore offer increasing exposure to intrusions and attacks that can be initiated from any part of the world.

First, the definition of a "crisis" should be recalled: "Sudden event causing significant loss and damage, resulting in an interruption of one or more critical activities or a shutdown of the organism, having long-term impacts and requiring the use of the Crisis Cell and, if necessary, an alternative site. A crisis can have consequences for the very survival of the company." Therefore, the crisis is a result of the materialization of risks with uncontrollable impacts that could jeopardize the reputation, operations, or even the very sustainability, of the company or the structure that suffers it. In general, the crisis is unpredictable, and when it materializes, it is generally a source of disorganization and the company that is the victim must be able to provide immediately appropriate and precisely calibrated responses according to the typology of it.

II. THE SPECIFICITES OF CYBER CRISIS MANAGEMENT

Cyber crisis management must be multidisciplinary: it is particularly at the crossroads of risk management and computer security (thus technical). Technical experts will be at the

service of the decision maker in this management. A peculiarity of cyber crises is that the attack, by altering the IS of the company, can directly decrease its ability to respond. It is therefore necessary to have a crisis management system to overcome this possibility and therefore:

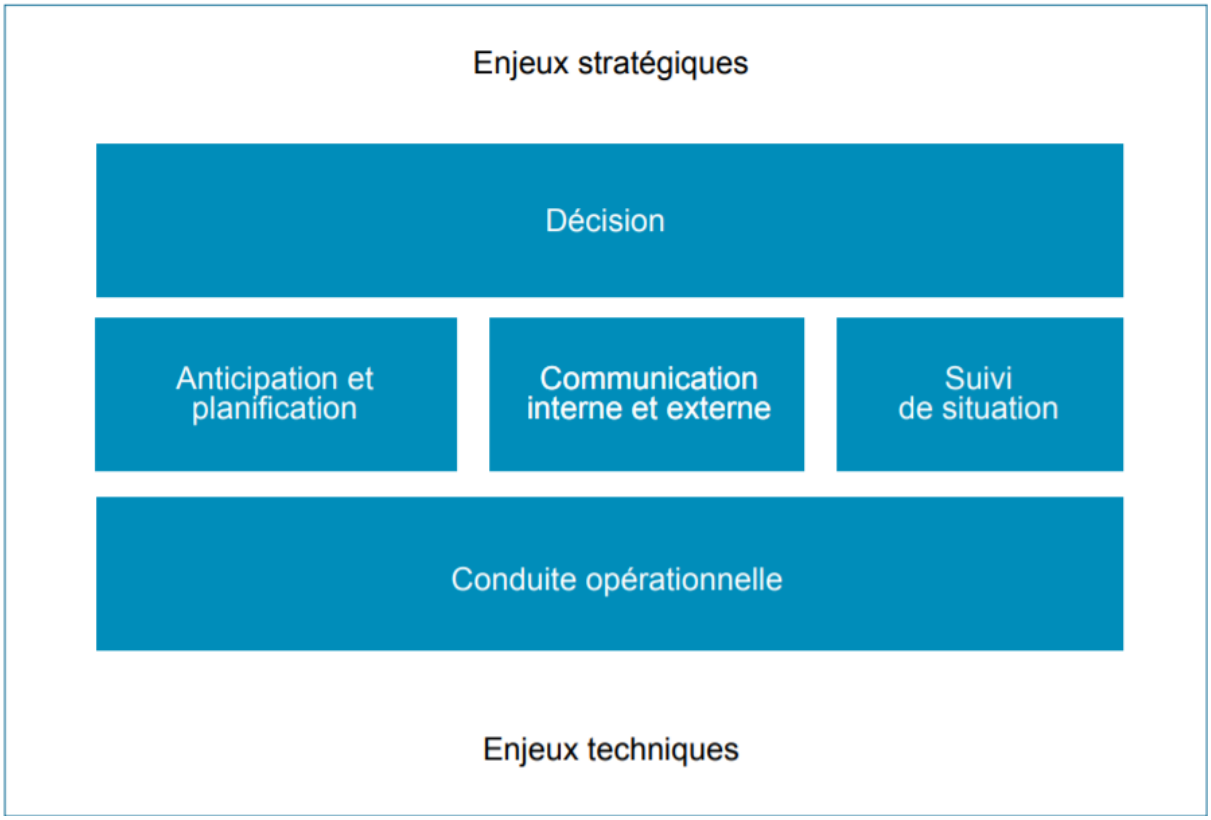
- Tore-manage crisis management means outside IS;
- To provide hardened workstations outside the administrative domains;
- Operate external exchange and communication services (e.g. cloud services).

III. CRISIS MANAGEMENT DEVICE A MEDIA CONTACT

The organization of crisis management within MEDIA CONTACT respects certain principles including:

1. Strategic piloting, provided by the head of the entity. The data leak is not only a computer crisis, the steering will be provided by the General Decision, DirectorSecurity and (Secretary General) ..., whichdistorts the synthesis between business vision and technical realities. The involvement of top management is thus one of the essential conditions for the effectiveness of the device;
2. Operational conduct provided by the trade or trades involved. ;
3. The mobilization of internal or external experts (if necessary) who will shed additional light and a certain step back on the situation. External experts will also be able to be valuable communication allies;
4. Constant monitoring and monitoring ofsituations.

Schéma : les fonctions d'un dispositif de gestion de crise



IV. THE BIG STEPS OF CRISIS MANAGEMENT A MEDIA CONTACT

Step 1: The alert.

- A whistleblower reports a data leak directly to the organization, which calls for a quick response so that information does not spread to the press;
- A hacker himself reports the leak to the company. Again, the information will have to be quickly taken into account with all the necessaryprecautions.
- The company's security team detects an incident and transmits the alert to its hierarchy after an initial assessment. In the case of blackmail, if it is necessary

to maintain a discussion channel to save time.

Step 2: escalation and mobilization.

Further assessment is being carried out to determine whether the crisis mechanism should be mobilised. Any incident is not necessarily a potential crisis. In the case of a data leak, the purpose of assessing the privacy and data integrity impact impact assessments that are normally performed for each processing of personal data will be assessed. If the incident is considered serious enough on the basis of different criteria (leak perimeter, nature of the "leaked" data, legal risk, financial risk, impact in terms of image, etc.), the crisis device is immediately activated.

Step 3: Containment

The aim is to take emergency measures to stop the data leakage, for example by putting the offending data processing on hold. This is a particularly delicate step, as it will often involve making trade-offs between the desire to isolate or even cut off a particular part of the information system and the need to maintain the same system in its current state to enable future investigations. Shutting down a server can destroy data stored in RAM, while a network disconnection will reduce the chances of going back to a potential attacker.

Step 4: Technical investigations.

This step is essential, both from an operational point of view in order to understand the causes of the data leak and to remedy it, as well as from a legal and insurance point of view. It results in the operation, by an internal or external team, of all logs of connection.

Step 5: Notification to the authorities.

Thenotification to the CNIL by the processing manager, which can be done in some lines, must take place no later than 72 hours after the organization has been aware of the leak. The CNIL may have been alerted simultaneously by the whistleblower, which reinforces the need for rapid action. Thenotification will have to be provided in parallel with ANSSI.

Step 6: Notification to customers.

As long as the leak entails a "high risk to the rights and freedoms of a natural person" the person in charge of the treatment must notify the customers concerned as soon as possible. Note that there are some derogations, especially in cases where leaked data is not usable, for example when it is encrypted.

Step 7: remediation and restoration.

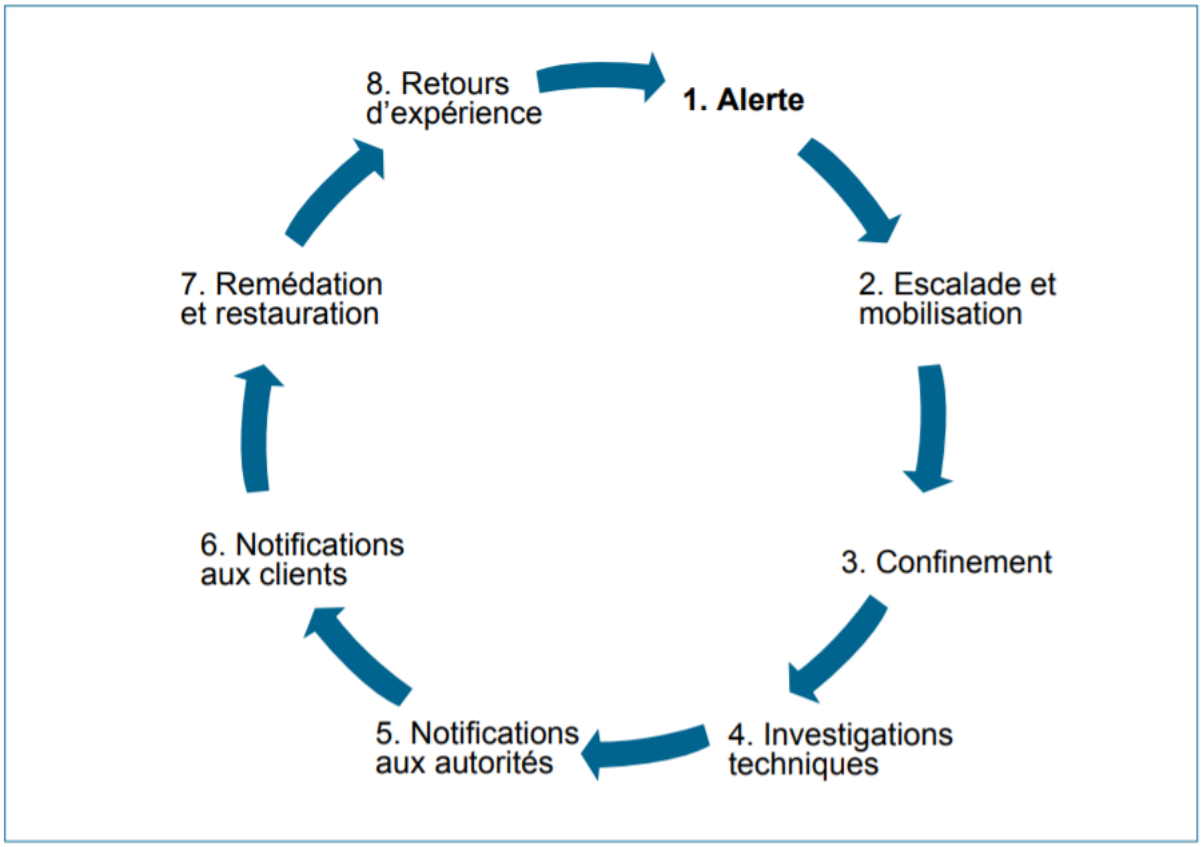
It is of course preferable that this step take place once the technical causes of the incident have been identified and analysed.

Step 8: feedback.

Any crisis must give rise to a feedback (RETEX) to improve the device. This RETEX involves both strengthening detection capabilities, for example by integrating new technical rules, creating a more or less automated "set" of incident responses, and seeking better application of information systems security policy, particularly in the area of updating critical servers. This process also aims to improve the overall operation of the device by optimising the procedures and means made available.

.

Schéma : les étapes de la gestion de crise



V. THE RESOURCES AVAILABLE TO THE CRISIS MANAGEMENT TEAM

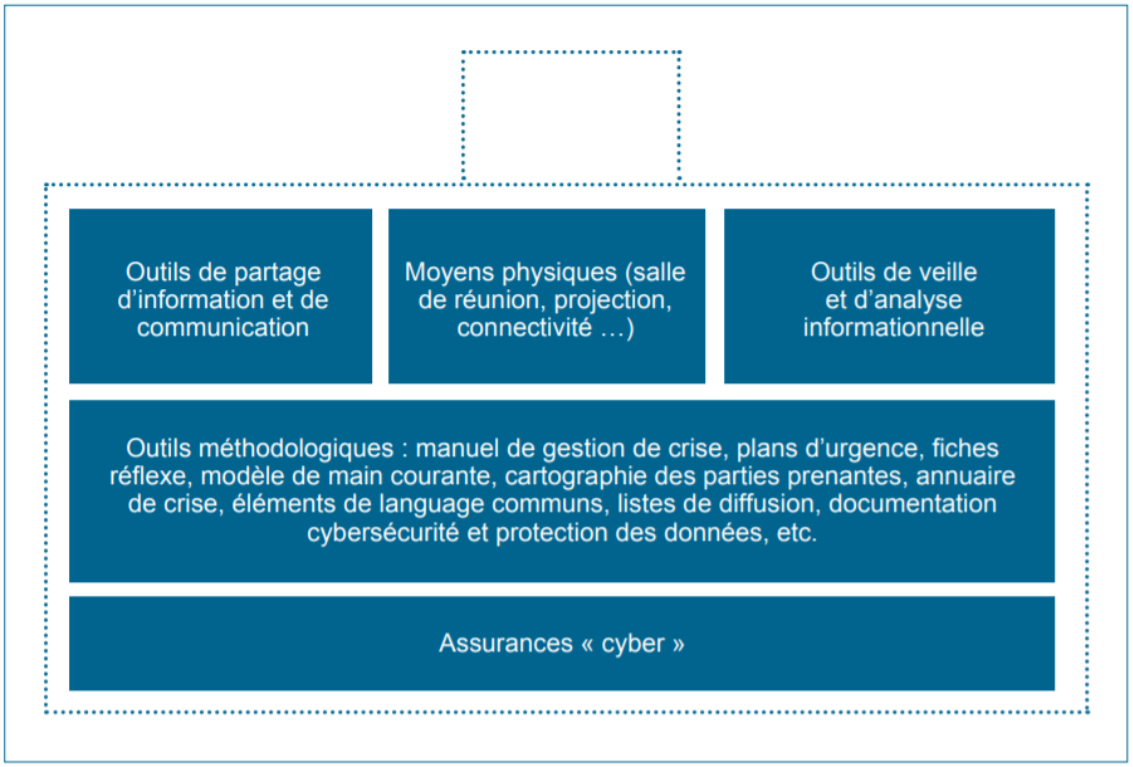
The compression of time in a crisis situation requires the rapid mobilization of a pre-tested toolbox. It is composed of:

- Tools for sharing information and communication: setting up a documentaryspace, instant messaging.
- Physical means: One or more meeting rooms are made available to the crisis device with all the necessary capabilities (connectivity, projection, etc.).
- Information monitoring capabilities: Regardless of the surveillance and detection capabilities used upstream to detect the occurrence of a data leak as soon as possible, a specific, real-time monitoring is conducted, especially on social networks,

to monitor the fallout of the crisis and fuel the holding of an "operational situation".

- Methodological tools: In addition to the crisis management manual and all the emergency plans (PCA/PRA, etc.), it is also a matter of having some generic tools: internal and external crisis directory, internal and external mailing lists.
- Specific insurance. While traditional insurance covers property damage on information networks and systems, specifically "cyber" insurance policies are used to assuring the consequences of data breaches.

Schéma : la boîte à outils de la gestion de crise



VI. Our principles of communication in times of crisis

- Prepare factual language elements about the cybersecurity and privacy device and company values. In the absence of specific information on the technical causes of the data leak in the first few days after the outbreak of the crisis, its perimeter or potentialvictims.
- Designate a spokesperson within the organization. This spokesperson may be

assisted by an IS or cybersecurity expert who will use more technical communication channels (including social networks).

- Take the initiative and communicate regularly throughout the crisis without systematically waiting for the information to reach the press and does not lead the organization to act in an exclusively reactive mode.
- Rely on a perfect identification of stakeholders (customers, suppliers, authorities, associations, media, elected officials...) in order to prepare targeted messages and identify the most appropriate channels of communication.
- Be transparent. Any information must not necessarily be disclosed, but the information that is disseminated must be authentic and verifiable.
- Avoid backpedaling by giving unverified information. Nothing is worse than going back on your own statements to "rectify the situation," for example on the number of potential victims.
- Keep it simple in its explanations based on concrete examples and cases.
- Do not seek to discard or blame a third party. This attribution is not only technically tricky, if not impossible, but strategically clumsy. The public questioning of a subcontractor should thus beavoided.
- Establish a direct communication channel with its customers (green number, forum...). Communication cannot be one-way.
- Manage internal communication in parallel and involve all employees during the exit from the crisis to make it an element of mobilization and avoid the frustration, quite frequent, of employees who learn from the outside information about their own organization.