Cigref

Reacting to a massive cyberattack

Managing the consequences of a cyber-crisis

February 2023

EDITORIAL

Most organisations and businesses now consider cybercrime to be the greatest risk. Cigref is actively engaged on this issue and has devised a doctrine based on four pillars:

- Reinforcing organisations' protective capabilities,
- Increasing policing and judicial resources to fight cybercrime,
- Intensifying government cyberdefence to capture criminals, even when they are outside the country,
- Enforcing security standards and requirements for digital products,

The collective intelligence work in this report contributes to the first pillar by providing concrete details to readers so they know how to react to cyber crises. Whilst companies are generally well-equipped with crisis management procedures specific to their activities, cybercrime is a special case due to its speed, its impact and the difficulty of grasping and remedying it.

Feedback from proven cyberattacks is always useful but can be tricky to share. However, everyone is aware that an organisation cannot, on its own, reach the level of maturity needed to face this challenge. On the other hand, the literature is full of relevant, high-quality background works, reports and benchmarks. These are particularly useful for preparation. A bibliography is available in the appendix to this report.

However, being prepared is not enough; you also need to have the right reflexes when a wide-scale crisis occurs. The stress that IT teams, business units and executives experience can impede enlightened decision-making and hinder taking essential, decisive action at the start. The cure can sometimes be worse than the disease. This study seeks to offer the tools and methods needed to mount an effective response to a wide-scale attack as the major phases of the crisis unfold.

The topics explored are not only technical, but also organisational, legal, and insurance-related and deal with internal and external communication. The details are drawn from the experience of Cigref members who participated in the work, representing a wide range of sectors. In addition, specialist experts also made contributions.

This report offers feedback, recommendations, a timeline, checklists and action plans as well as indicators for IT departments, CISOs, risk and communication departments and, more generally, for all members of corporate or administrative crisis units. Due to this topic's special nature, we decided to keep the contributions anonymous. Thank you to all the participants who agreed to share their experiences and challenges with transparency and humility so that we can all benefit and strengthen our organisations' resilience.

The coordinator of the working group

OVERVIEW

This report covers how to manage a massive cyber crisis that can have significant consequences for the organisation's activity, and it can serve as a practical guide to responding to a cyberattack. These consequences can impact a variety of domains, including operations, finance and brand image.

Cyber crisis management is made up of different stages that need to be clearly identified to avoid getting bogged down in the crisis. Initially, the organisation must limit the attack's impact as best it can to prevent the crisis from spreading. It can then repair and stabilise its information system. Meanwhile, investigations can be conducted to identify the reasons for the attack and ensure that the IT environment is safe once again. In parallel to all this, it is important to consider the legal process from the start of cyberattack since it will last long after the crisis is over.

Two crisis units are established to manage the cyber crisis: the operational unit, which for cyber crises is comprised mainly of members from IT, and the decision-making unit, which ensures the organisation's business continuity. All stakeholders in how the crisis's technical and strategic aspects are managed should be identified. The moment when the crisis unit is activated is also key to reacting quickly: this moment is usually set out in the business continuity plan (BCP) and depends largely on the consequences for all the business units that use IT.

Beyond the technical aspects – diagnosing the attack and repairing the IT – communication is important to avoid a crisis within a crisis. A communication process that foregoes the organisation's IT system needs to be set up to maintain internal communications. Secondly, all stakeholders within the organisation, the ecosystem and potentially the media need to be considered in the messaging.

A cyber crisis often leads to a legal process as well, which requires the IT department to coordinate with the legal department. If there is a personal data leak, the CNIL must be notified immediately. It is also important to notify your cyber insurance company as soon as possible. Evidence of the attack should also be preserved to provide significant proof for the proceedings.

External service providers are often needed to reinforce in-house teams so they can benefit from expertise that is lacking internally. ANSSI can be an ally on several fronts when managing a cyber crisis.

The longer the crisis lasts, the more overworked the IT teams will be. It is important to make life easier for the teams by managing the logistical aspects as best as possible, without forgetting to allow time for rest, even for the most essential and motivated employees.

When the crisis ends, the legal process must be followed carefully, because it can still last several months. This is often a chance for the IT department to improve its security.

ACKNOWLEDGEMENTS

We would like to thank the coordinator of this work as well as all those who participated and contributed to this group. There were 54 participants coming from IT-related functions within organisations from a wide range of sectors:

- Various fields of industry such as aeronautics, pharmaceuticals, and automobiles,
- The banking and insurance sector,
- The food processing sector,
- The building and public works sector,
- The energy sector,
- The service sector.

We would also like to thank all the experts whose input significantly contributed to our work (in alphabetical order):

- Damien Arcuset, Head of the Analysis Coordination Office, ANSSI
- Hélène Chauveau, Head of Public Affairs, AXA
- Christophe Fleury, Head of Cyberdefence Operations, ANSSI
- Georges Laederich, Senior Consultant in crisis management and communication, Cabinet Arjuna
- Thibault Richard, Senior Consultant in crisis management and communication, Cabinet Arjuna
- Corinne Thiérache, Lawyer at the Paris Bar, IP/IT/Privacy Partner at Alerion law firm
- Stéphane Vauterin, Underwriting Manager Professional & Specialty Lines, AXA XL
- Cécile Wendling, Group Head of Security Strategy and Awareness, AXA

This document was developed and drafted by Aurélie Chotard, Mission Officer at Cigref.

TABLE OF CONTENTS

TABLE OF ILLUSTRATIONS

1 INTRODUCTION: COMPANIES FACE LARGE-SCALE CYBERATTACKS

First, we will define the term "wide-scale cyberattack", and then we will briefly discuss the cyber environment that confront companies today. This introduction will explain how this report is organised, following a typical timeline to serve as a practical guide for organisations that want to prepare for a cyber crisis.

In addition to working group participants' feedback and experts' contributions, we have innovated in our working methodology by slipping into the shoes of a company that wants to improve its crisis management. We were inspired in particular by the ANSSI report on how to hold a crisis management drill. We thus produced a timeline (see appendix) to identify the relevant stakeholders and tasks for each event, and the ANSSI's practical sheet was of great help to us during this workshop.

This report focuses on cyberattacks that can have significant consequences for a company's business or even the public at large. We concentrated on the period ranging from the crisis's onset to its resolution, i.e. the general resumption of the company's activity. Thus, the subject mainly deals with crisis management, not prevention or anticipation, although we are aware that anticipation is the key to effective management. However, every crisis is different, and following a pre-set protocol is not always enough. Flexibility is needed to fully tackle it. This report provides recommendations and practical advice for managing a cyber crisis and dealing with the unexpected.

1.1 WHAT IS A WIDE-SCALE CYBERATTACK?

1.1.1 DEFINING A CYBERATTACK

According to ANSSI, a cyberattack is a malicious action that seeks to undermine an information system's integrity. A cyberattack is the realisation of a threat and requires exploiting a weakness within the IT system. IT divisions of large organisations are subjected to computer attacks on a daily basis, but few of these succeed. We therefore only really use the term "cyberattack" – and not "IT incident" – when the hackers' damage to the information system has consequences for the organisation's activity. There are various terms for cyberattacks that occur at different levels; here is a glossary of the best-known terms that will appear in this report:

- *Ransomware* is the type of attack with the most significant consequences today. It consists in infiltrating an organisation's servers to make a copy of and then encrypt its data; making a copy is not systematic but is becoming increasingly common to increase the chances of the ransom being paid. The organisation can no longer access its data, and the cybercriminals demand a ransom in exchange for the decryption key and non-disclosure of the data.
- Malware (or virus) refers to any computer program developed to harm the targeted organisation by altering a particular technical component (software or hardware).
- *Spyware* is software whose purpose is to collect information to be forwarded to third parties. It aims to spy on a targeted organisation, either to discover new vulnerabilities in the computer system to carry out another attack at a later date, or to engage in state or economic intelligence. Since this software does not alter the system's operations, it may only be discovered after a long time.

- A distributed denial of service (DDoS) attack overloads a digital system's capabilities to hamper its service capabilities or even make it wholly unusable. There are many ways to prevent this type of attack, but it is still a common way to strike at smaller structures.
- *Phishing* is the practice of impersonating a person or organisation to obtain information and/or infiltrate a computer system. This is often the first step to a larger attack.

These are just a few of the types of attack in use. The ANSSI glossary can provide you with the exact definitions.

1.1.2 THE VARIOUS CONSEQUENCES OF A CYBERATTACK

Whether a cyberattack is considered "wide-scale" does not depend on its type, but on the consequences it can have on the target organisation and on its close or distant ecosystem. The more numerous and widespread the consequences, the more likely it is that the cyberattack falls into this category. The effectiveness and type of the attack have little bearing on its impact potential. Rather, its impact depends more on how the organisation secured its IT system before the attack and planned for alternatives to cope during a crisis. Small and medium businesses and certain government departments remain the most affected by cyberattacks because the cyber resources in place are often insufficient to deal with increasingly organised and efficient cybercrime.

Cyberattacks can have devastating consequences when they impact critical operators[1] and services[2], such as hospitals, transport and energy. These organisations must be able to resume their activities quickly without burdening the society at large with the consequences. That cybercriminals target these infrastructures is a major concern. During the health crisis, both hospitals and municipalities were widely targeted. The attacks were unsophisticated, but the impact on the ability of hospitals to care for their patients and on the ability of municipalities to meet the needs of their citizens was significant.

In its 2021 activity report, ANSSI mentioned that 75% of its interventions were related to espionage attacks. These sorts of attacks have little to no direct impact on a company's business and its ecosystem. Although organisations should take them seriously, we have not included them in the report since the resulting crisis management practices are too specific. Therefore, this report deals mainly with ransomware attacks.

Cyberattacks can have many types of consequences and can reach critical proportions for the affected organisation:

1. **The impact on the organisation's business**: One of the first visible consequences concerns the total or partial stoppage of the target organisation's activity. For example, following a cyberattack in 2020, shipping company CMA CGM had to partially cease trading for two weeks due to major malfunctions in its IT system.
2. **Financial consequences**: A prolonged stoppage of activity can have a significant impact on a company's turnover. For example, in 2017 Saint-Gobain Group announced a loss of €200 million after a cyberattack shut down its business – completely for 4 days and partially for 10 days – before it could return to normal. Similarly, Eurofins announced losses of €70 million in 2019 and Sopra Steria €50 million in 2020.

[1] *La sécurité des activités d'importance vitale, Secrétariat Général de la Défense et de la Sécurité Nationale* (SGDSN), 18 March 2016.

[2] List of critical service operators as defined in the NIS Directive: Decree No. 2018-384 of 23 May 2018 on the security of networks and information systems of critical service operators and digital service providers

3. **Reputational consequences**: Business customers and the general public can lose trust in organisations that suffer a cyberattack, especially if the attack results in a significant data leak. For example, the attack on APHP in 2021 received widespread media coverage due to a major data leak of its patients' Covid test results. More recently, La Poste Mobile suffered a ransomware attack that left its website offline for a week, severely impacting the service offered to its customers.

1.1.3 THE SPECIFICITIES OF CYBERATTACK CRISES

The potential consequences posed by cyberattacks can compel target organisations to put in place **a crisis management system**. Whilst this sort of system uses the same principles that can be found in general crisis management, it must be adapted to a digital crisis that can have multiple, cross-cutting consequences.

Based on the ANSSI report, Crisis of cyber origin, the keys to operational and strategic management, we can identify aspects specific to cyber crises:

- **Latency**: A cyber crisis can start long before it is detected. Before the consequences emerge, the organisation is already in a crisis: it just doesn't know it yet. This latency is also reflected in crisis management since the organisation does not know whether the hacker is still in its IT system or not. The fact that they may still be present during a cyber crisis can be particularly hard for crisis managers to accept.
- **Multiple forms**: Cyberattacks can take many forms and target many places at once. Depending on the type of target infrastructure, a multipronged attack can make the target organisation – even the wider public if the organisation provides an essential service – progressively worried. For example, in Ukraine in 2015, a simultaneous attack on several energy operators led to a major power outage in the country. After breaking into and taking control of the systems, the malware rendered the equipment inoperable. Meanwhile, a DDoS attack was unleashed on the operators' call centres. This simultaneous, multipronged act not only prevented operators from reacting quickly but also worried the public.[3] Attacking multiple points at once forces organisations to review its entire ecosystem to assess the crisis' full extent and impact.
- **Speed**: An organisation targeted by a cyberattack is immediately confronted with its extent and effects. This renders it unable to measure how severe or how long the crisis will last. A cyber crisis is not just a single IT incident that needs to be addressed. During a cyber crisis, attacks come one after the other.

1.2 A FAVOURABLE ENVIRONMENT FOR HACKERS

The adoption of new digital tools and practices has made IT systems more vulnerable. This has resulted in a sharp increase in the number of cyberattacks in recent years, hamstringing companies' and administrations' activities. These organisations worry that cybercriminals' skills are increasing faster than their ability to defend themselves. While cybercriminals are becoming better organised thanks to

[3] Read more about this cyberattack *Les détails de la cyberattaque qui a mis des centrales ukrainiennes hors service*, L'Usine Digitale, 04/03/2016

a better structured dark web, some companies – especially SMEs – and administrations are still ill-prepared to deal with this growing threat.

In response to the increase in cyberattacks, the European Union has proposed a revision of the NIS Directive with the aim of ensuring a high common level of cybersecurity in the Union (the "NIS 2 Directive"). Europe also offers tools to help Member States improve their digital security.

1.2.1 THE EXPONENTIAL GROWTH OF THE CYBER THREAT

According to *Le panorama de la menace informatique* published by ANSSI, 1,082 proven intrusions were detected in IT systems in 2021, compared with 786 in 2020. This represents an increase of 37% in one year.

This exponential increase in the cyber threat is linked to three main phenomena. Firstly, cybercriminal groups are becoming more professional and specialising in certain attack techniques, as illustrated by Ransomware as a Service (RaaS) sales, a subscription that includes everything a hacker needs to launch a ransomware attack. A typical RaaS subscription costs around $50 and includes the ransomware's code and decryption key. This illegal business activity simplifies the development and execution of ransomware and is aimed at less experienced cybercriminals. Moreover, this sale of malicious code makes it more difficult to identify who is behind a cyberattack. The code of a hacking group can be used by a multitude of hackers of different nationalities.

Furthermore, this organisation of cybercrime has been made possible by dark web's greater structure. According to a company specialising in blockchain technology, dark web markets are believed to have set a new record in revenue in 2021, bringing in a total of $2.1 billion in cryptocurrencies. Approximately $300 million of this amount was generated by fraud shops, which acted as intermediaries for the sale of stolen logins, credit cards and exploit kits, among other things.

This increase in attacks has also been facilitated by the considerable increase in IT systems' vulnerability. US cybersecurity firm Mandiant identified 80 exploited zero-day vulnerabilities in 2021, more than double the previous record of 2019. Hackers look for the easiest entry points to access. Therefore, they target the IT component supply chain. This method helps the attack to spread quickly by targeting a software company or a digital services company that can result in a cascade of compromised systems. The best known example to date is a cyberattack that infiltrated large private companies and government institutions, particularly in the United States, via the Orion software from SolarWinds. This attack was revealed in December 2020 by the private cybersecurity agency, FireEye.

1.2.2 USE OF CYBERSPACE AS A MEANS OF POLITICAL PRESSURE

The increasing porosity between cybercriminal groups and state actors is transforming cyberspace into a zone of conflict between states where political pressure can be exerted. A few recent examples illustrate this point:

- **An increase in espionage cases**: The increase in the number of private companies specialising in online espionage is a sign of the industrialisation of the practice, similar to ransomware attacks. The Israeli company NSO, which was behind the Pegasus affair that broke out in the summer of 2021, sold smartphone hacking software to several states for several years, including Morocco, Mexico and Saudi Arabia, allowing these states to spy on political leaders,

political opponents and journalists. These kinds of tools, sold by private companies, are then used by cybercriminal groups.

- **The militarisation of cyberspace in the conflict in Ukraine**: Since the beginning of the conflict, Russia has been behind disinformation campaigns in all the countries that have supported Ukraine and has launched cyberattacks on its neighbouring countries, especially the Baltic States, which block its operations. Lithuania, for example, is an important target because, by implementing EU sanctions, the country has barred Russia's access to Kaliningrad, preventing the flow of certain Russian goods. Meanwhile, Russia is experiencing a wave of "retaliatory" cyberattacks, mainly from North America and Europe, launched not only by "hacktivist" groups supporting Ukraine but also by state actors.

In this context, companies are prime targets, whether for economic intelligence purposes or to destabilise the activities of governments and impact the population of a country.

1.2.3 TALENT SHORTAGES WEIGHING ON COMPANIES

Companies are currently experiencing a shortage of digital technology talent, even more so in the cybersecurity sector. 45% of French companies say they are struggling to recruit in this field, with around 5,000 vacancies currently in France.

According to PwC, there are several reasons for this:

- The image of cybersecurity professions is out of step with reality and attracts few people.
- Training courses in this field are often long and complex, and only recruit a minority of candidates.
- The low gender mix in these occupations also halves recruitment opportunities.
- Despite attractive salaries, these jobs are not well recognised and valued in society.

In addition to the lack of cybersecurity experts and specialists in companies, not all employees are aware of the basic principles of cybersecurity. This knowledge is nevertheless crucial to protect against cyberattacks.

1.3 THE DIFFERENT STAGES OF CYBER CRISIS MANAGEMENT

Managing a cyberattack crisis involves several stages incorporating aspects of classic crisis management, including technical remediation, communication, team management, and establishing a legal process. We have identified three simultaneous processes that cover the spectrum of cyber crisis management:

1. First, **managing a crisis's consequences** follows a sequence comprised of four main stages:
   - Emergency measures to be taken in the early moments of the crisis (1-3 days),
   - Corrective measures to get the business back on track and in a pre-crisis state. This step entails offering reduced service and then taking the time to repair it. (1-3 weeks),
   - Stabilization of the situation to avoid an escalation of crises and improve the security of its IT (several months),
   - Feedback, to learn from the predicament by improving the organisation's crisis management system, for example, and to avoid a similar disaster in the future (several months).

2. At the same time, **investigations** are launched. These investigations initially serve to ensure that the affected organisation's IT environment is sound so that the corrective stage can be undertaken without risk. Failure to carry out this stage of investigation exposes the organisation to additional hacking attacks. To avoid further incidents, it must ensure that the hacker is no longer present in the system and has no way of accessing it. Investigations then continue to find out how the cyberattack started. This second stage is separate from crisis management because knowing the origin of a cyber crisis is not essential to taking corrective action. However, it is necessary and important to carry out these investigations to address potential IT vulnerabilities. Investigations can take several months.

3. Finally, these investigations also allow for evidence to be collected for the **legal process**. In addition to crisis management, the organisation must also fulfil its legal obligations. This legal period is much longer than the crisis period and can last for months, even years.

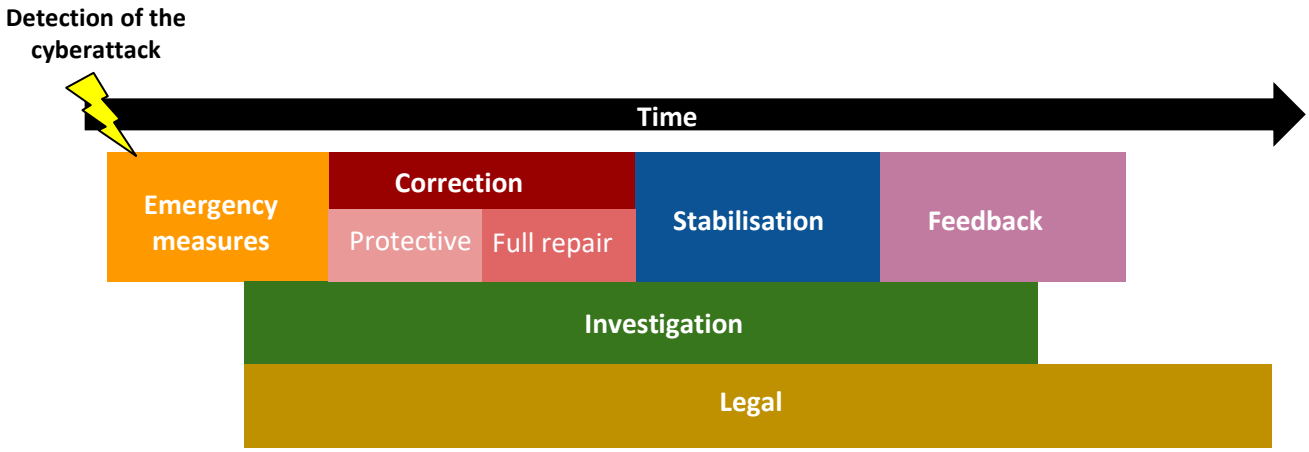

Figure 1: Steps in cyber crisis management

This report's structure reflects this timeline and breakdown of the different stages in crisis management. These different sections aim to provide operational tools and recommendations to deal with each of these phases in the most efficient way.

2 COPING WITH THE CRISIS: TAKING THE FIRST DECISIVE STEPS

When a cyber crisis arises, the initial measures are decisive in determining how the rest of the crisis management process will unfold. Several questions need to be answered in these first stages:

- Who is part of the crisis unit? When should it be activated?
- What actions should the IT department take to stop the spread of the attack, if it is not already too late?
- What relationships should the IT department have with other departments in the company during the crisis?
- Does the organisation have all the necessary resources in-house to deal with the crisis?

The answers to these questions are usually determined ahead of the crisis as part of a business continuity and crisis management plan. However, each crisis is unique, and an organisation's ability to adapt to the unexpected is a key factor in dealing with them.

2.1 ORGANISING THE CRISIS UNIT

To manage a cyber crisis, a variety of teams must coordinate their technical (IT security, digital services, etc.) and strategic (business continuity, communication, etc.) decisions and actions to handle the crisis's effects while working to re-establish systems operations. At the **decision-making** level, it is important to involve the IT Department or the Chief Information Security Officer (CISO) in a regular crisis management system to inform decision-makers about progress on the attack. This information is needed to adjust and coordinate corrective actions. At the same time, another unit is responsible for analysing the technical situation and suggesting actions to restore activity. This is the **operational crisis unit**.

The crisis unit's organisation must be prepared before the crisis. This allows you to work within pre-existing frameworks and avoid making things up as you go. Foresight is essential here and must incorporate the various ways in which a crisis can manifest itself since this will entail different forms of organisation.

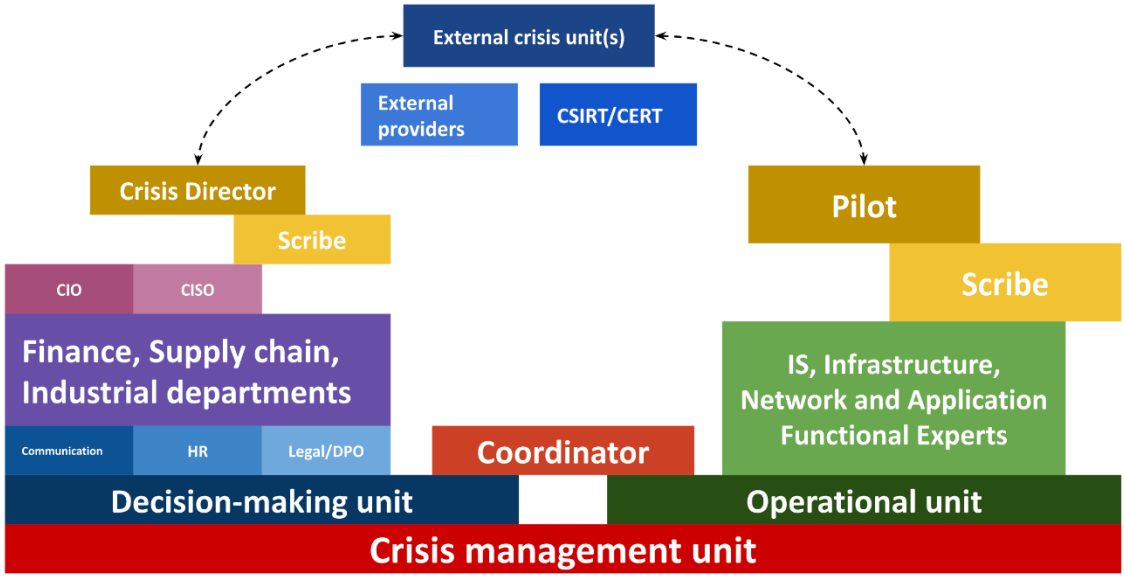

Figure 2: Crisis unit organisation

2.1.1 THE DECISION-MAKING UNIT, RESPONSIBLE FOR THE COMPANY'S BUSINESS CONTINUITY

The role of the decision-making unit is to guide crisis management by taking strategic decisions. How it is composed is therefore important to quickly resolving crises while avoiding significant damage. Although executive committee members often form the core of this unit, the issue of other people's presence may arise. However, the composition of the decision-making crisis unit depends greatly on the organisation's size and activity.

It is essential to include **a person from the legal department as well as a Data Protection Officer (DPO)** in the decision-making unit. Depending on the type of attack, the DPO may act as an observer, or they may play a real role in the crisis unit, for example if the cyberattack has led to a leak of personal data. Depending on the company's business, it may also be important to involve certain business departments in the decision-making unit, either because they are essential to the continuity of the group's activity in contractual terms or because they are the most heavily impacted.

When several branches are affected by the crisis, **decision-making units can be established in each of the affected business units**. The IT department is also part of this organisation. Within the IT department, two units are set up: a decision-making unit that includes all the IT directors, and an operational unit that itself brings together several operational sub-units that are activated according to the systems affected: industry, finance, and others. The challenge lies in coordinating these various units. This division of labour is adapted to the size of the IT department and the organisation.

The CISO can play different roles depending on how the group is organised. In general, each organisation should have a strategic IT security component and an operational IT security component, which can be covered by the same person. **The CISO is more of a decision maker** because, provided they have the mandate to do so, they can take important decisions during the crisis, such as cutting off and isolating sites, with significant impacts on the business. A distinction must be made between those who are part of the operational unit and those who participate in the unit's regular orientation meetings. In this case, the CISO participates in the meetings, but they are not really part of the operational unit, and if they have a foot in each of the units, they can also partly serve as a coordinator. Whether these roles are combined in this way depends on the structure's size and the CISO's position in the company, whether they are the head of a department independent of IT, whether they depend on the IT department, etc. However, the CISO cannot be the only one to perform all these functions. **Roles and contacts** should be **rotated** if the crisis lasts.

In addition to the composition of the decision-making unit, another problem in cyber crisis management can sometimes be the **lack of awareness of cybersecurity issues on the part of the employees dedicated to crisis management**. Crisis management "experts" are indeed more used to managing other types of crises than cyber crises. They sometimes have difficulty in grasping the elements affected by the cyberattack and in making the right decisions. It may therefore be useful to include a "cyber interpreter" in the decision-making unit so that everyone understands each other between the decision-making unit and the operational unit. For example, a cyber crisis often requires isolating the components affected by the cyberattack, which can lead to problems of understanding the consequences of such action. It is therefore necessary to explain the impacts and solutions of a cyber crisis to the crisis manager beforehand. In the investigation phase, the data must also be transcribed into a language that the business units can understand.

2.1.2 THE IT OPERATIONAL UNIT

In the context of cyber crisis management, the unit that manages the bulk of the operations to resolve the origin of the crisis is the operational unit from IT. Its role is to **help managers take decisions** by informing them of the situation and providing an initial action plan. Then, the guidelines established at the decision-making level help define the strategy that the operational unit pursues on the ground through action plans.

To ensure its effectiveness, the operational crisis unit works independently. It is up to the **coordinator**, who has one foot in the operational unit and one in the decision-making unit, to translate decisions

and operations on both sides. When a crisis lasts more than 24 hours, the coordinator's function is even more important, translating what is happening in each of the units.

2.1.3 WHEN SHOULD THE CRISIS UNITS BE ACTIVATED?

Because of their rapid and multipronged nature, cyber crises must be addressed by all stakeholders in the company as quickly as possible. Activating crisis units is thus one of the first decisions the CIO is to take. We have identified two main considerations in this:

- **The provisions of the BCP** (Business Continuity Plan): The BCP stipulates when and how the crisis unit will be activated. The CIO must use this plan when deciding this; activation may be gradual (pre-activation, gradual activation of the different levels of the crisis unit).
- **The consequences for the business** that determine whether to activate the crisis unit at all.

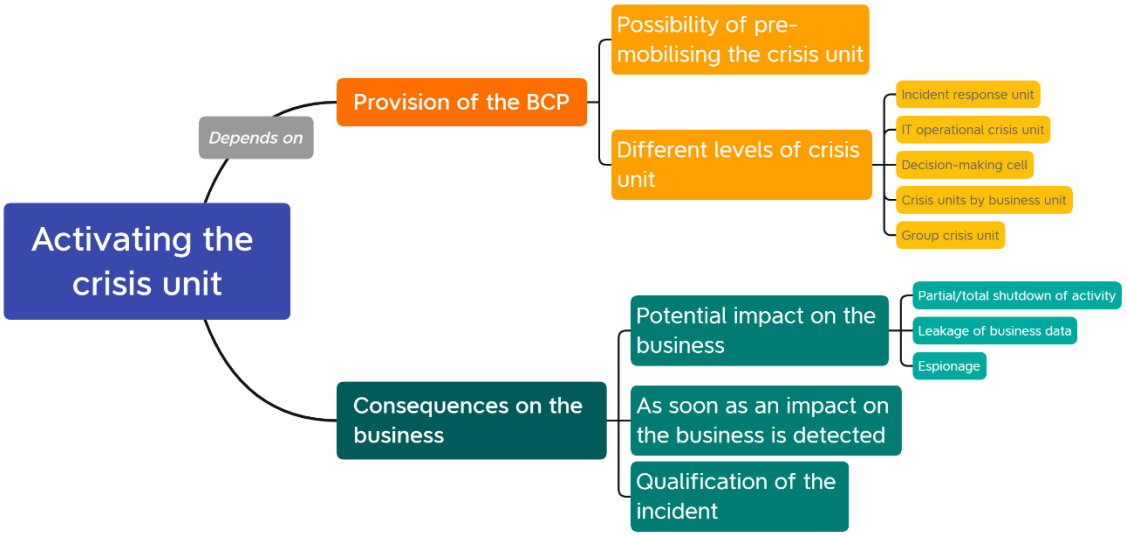

Figure 3: Decision tree 1 - Activating the crisis unit

When a crisis begins, the incident's origin may not always be known. For example, a production incident may or may not be a cybersecurity incident. To deal with all types of crisis, **the entire crisis unit is activated at the beginning of the crisis**, and the crisis director stands down members who are not needed as and when required. The crisis's cybersecurity aspect may thus come into play at a later stage.

Secondly, **activating the crisis unit depends on the impact on the business**. The operational IT crisis unit is sometimes set up without activating the entire crisis unit. As soon as there is an impact on the business, the decision-making unit is activated. When an incident alert is raised, a pre-analysis is performed on it. If the incident is real, a response unit is set up. If the impact of the incident is visible on the business, the crisis unit is activated.

However, an incident alert does not always come from inside the organisation; it can also come from outside, from suppliers for example. An attack on a supplier can have repercussions for the organisation. This is called a **supply chain attack**. It is therefore necessary to be able to coordinate with external crisis units.

Example organisation of a crisis unit in a food processing company

The business continuity plan included a business aspect and technical remediation elements. Three separate but inter-communicating crisis units were set up:

- A crisis unit at the executive level to take strategic decisions,
- An operational crisis unit consisting mainly of the communication department,
- A crisis unit on the IT department side to manage the technical aspects.

The CIO was mainly involved in communication issues with customers and partners. They established daily internal communications with employees and also managed relations with the executive committee, whose objective was to restart the IT system as quickly as possible. The CIO's role with the executive committee was therefore crucial during the crisis to protect their teams. The CISO's scope, meanwhile, expanded, and they managed the crisis's impact on international subsidiaries.

Within the IT crisis unit, an ad hoc organisation consisting of three people was set up to manage each line of work, including:

- An application person,
- A contact in the business unit,
- A technical person.

This organisation was maintained for two to three weeks after the resumption.

2.2 MANAGING THE FIRST CONSEQUENCES ON THE INFORMATION SYSTEM

In order to take the first appropriate operational measures on the information system that has been the victim of a cyberattack, it is necessary to **diagnose the IT security incident**. The aim here is not to discover the origin of the incident but to identify the initial consequences in order to respond as quickly and effectively as possible.

In order to diagnose an IT incident, the IT department can take a variety of actions, such as

- Consulting the EDR (Endpoint Detection and Response), an advanced threat detection tool installed alongside the antivirus. This tool detects the threat and acts immediately to stop it,
- Record and identify the nature of the incident itself with the help of staff in the department,
- Analyse the logs in the SIEM (the security information management system), a tool that manages security events in the information system,
- Consult the number of incident/alert tickets reported either by the SOC (Security Operations Centre) or by the team responsible for IT security,
- Contact the IT operations team to troubleshoot the servers,
- Analyse the volume and recipients of traffic to/from the Internet.

This initial diagnosis is based mainly on the **use of supervision tools and the work of the IT department's employees**. The first objective is to qualify the scope of the incident. In this context, logging,[4] which allows all movements in a system to be recorded, is an excellent way of defining the scope affected by the attack and of tracking the stages of the diagnosis.

The incident's scope and nature determine the first actions to be taken on the IT system. At this stage, the goal is to stop the incident from spreading to all the company's IT systems, limiting it to its initial scope. These are called containment measures and are not permanent actions. These measures, if not carried out correctly and at the right time, can have an impact on the corrective stage, which takes place at a later time. Containment incorporates a number of measures, including:

- Isolating the affected systems (servers, file servers, workstations (a geographical set)) and the most vulnerable systems (usually those using Windows). It is best to do this in the EDR console,
- Involving a security incident response team,
- Disabling most administrator accounts because the hackers' objective is to have administrator access to reach and modify all systems,
- Identifying and securing the last sound backup.

If the scope of the cyberattack is too broad or not clearly identified, a complete shutdown or containment of systems is often triggered to allow time for further investigation.

2.3 MANAGING THE INITIAL CONSEQUENCES ON THE ORGANISATION'S ACTIVITY: COLLABORATING OUTSIDE THE IT DEPARTMENT

In the event of a cyberattack, the IT department is the first department in the company to deal with the consequences of the crisis. However, it should not neglect other aspects of crisis management, such as communication or meeting legal obligations. In order to deal with all these aspects, the IT department must actively collaborate with the other departments of the company. Successful collaboration helps the company to better respond to the problems encountered by a partial or total shutdown of the company's activity.

2.3.1 REGULAR CONTACT WITH THE EXECUTIVE COMMITTEE

The executive committee forms the main contingent of the decision-making crisis unit. It needs to be regularly informed of how the crisis is progressing and what is being done. **Regular meetings** are held with the coordinator, the CIO and perhaps the CISO to keep them informed. At the beginning of the crisis, these meetings or communication reviews take place very regularly, several times a day. They are then spaced out over time depending on the operational teams' ability to resolve the crisis.

Maintaining and updating **a dashboard** is the best way to keep executives informed of how the action plans are progressing. Without seeking to be exhaustive, the working group's contributors have listed the key information that the executive committee wants at the beginning, middle and end of a crisis.

[4] The sequential recording in a file or database of all events affecting a particular process, such as an application or computer network activity. - Logging (computing), Wikipedia

Topics to be addressed	Main indicators
DATA	Date of last secure backups
	Time scale for providing the latest backups
	Estimated data loss (possible restoration date)
FINANCIAL IMPACTS	IT investments needed to restore and improve the information system (hardware, software, etc.)
	Deductible amount for cyber insurance
	Lost turnover due to the cyberattack
	IT reinforcements needed (expert consultants)
REPUTATIONAL IMPACTS	Media monitoring - Number of announcements or notifications in the press and on social networks
HR IMPACTS	Number of employees unable to work
	Ability to manage payroll due to complete or partial shutdown of IT systems
IMPACTS ON THE IT SYSTEM	Volume of PCs/Applications/Systems unavailable
IMPACT ON BUSINESS UNITS *(depending on the sector of activity)*	Number of users/customers impacted
	Number of business processes impacted
	Volume of lost orders
	Volume of production stoppages
NATURE AND SCOPE OF THE CRISIS	Ransomware, data leakage?
ACTION PLAN	Percent of progress on approved action plans
	Number of people involved in the action plan
	Percent of servers and PCs repaired
SPONSOR RELATIONS	Monitoring of information and alerts, mandatory or recommended

Figure 4: Dashboard for the executive committee

2.3.2 PREPARING YOUR CRISIS COMMUNICATION WITH THE COMMUNICATION DEPARTMENT

The cooperation of all stakeholders is essential and plays a crucial role in communication. Communication is needed in all situations. Partners will never blame the company for falling victim to a cyberattack, but it will be blamed for failing to communicate. Even if it turns out that the organisation did not sufficiently protect its IT information before the attack, it is advisable to be forthcoming with any information. It is important to ensure that all points of contact have all the information they need to cope. It is also essential to make all teams in the company aware of any new communication channels. You should **establish a contingency for communication that does not rely on the company's IT system** before or at the start of a crisis. This will allow communication to continue if the usual tools are no longer accessible. Additionally, even if they are accessible, it is also recommended that another, more secure means be used to ensure that cybercriminals do not have access to it.

Communication is crucial during a crisis, but doing so is difficult because all stakeholders must be informed:

- **Within the company**: employees, business units, subsidiaries and the executive committee, which must have dashboards providing visibility on the entire crisis management process.
- **With the ecosystem** (customers, suppliers, partners, etc.): they expect guarantees concerning any leaked data. You should give them as much information as you can about what you know.
- **With the media**: The media can adopt various stances. Some stick to the facts, and others may be biased (some may even get in direct contact with the hackers).

Coordinate with the communication department

During a cyber crisis, the company's technical and operational capabilities can be severely hamstrung and potentially impact its customers, partners, employees and all its stakeholders more generally.
Restoring, maintaining or strengthening their trust in the company's ability to manage the situation and safeguard their interests requires coordinated analysis and action.
The communication department is in charge of mounting this response strategy and must therefore be informed of events quickly.
Once the stakes are known, its role is to devise and gain approval for a communication strategy and the key messages to convey to stakeholders. These elements can be translated into various formats and sent to those internally who are likely to be contacted. These messages will be regularly updated throughout the event.

There are four main categories of stakeholders:

- The authorities: depending on the company and the impact of the event, the crisis unit may be in contact with various public authorities such as ANSSI, DRIEETS, ANSM, ARS, AMF or CNIL.
- Internal contacts: employees, unions, business units, subsidiaries, shareholders, executives, etc.
- Professional partners: customers, suppliers, service providers, competitors, interprofessional organisations, insurance companies, lawyers, bailiffs, etc.

- Sensitive contacts and the media: victims of the cyberattack, associations, local elected officials, influencers and opinion leaders, social networks, local and national media, specialised media, etc.

Stakeholders are all potential allies or obstacles. You should coordinate with them in line with their constraints and challenges, with an aim where possible to:

- Maintain good relations
- Be transparent
- Obtain additional information
- Relay key messages

When things are calm, note all the stakeholders and identify their internal points of contact to react quickly.
Example: Contacts of CISOs within partner organisations, such as customers, suppliers, and service providers.

Checklist of actions to be taken with the communication department

Preventive actions:

- Open discussions between IT and the communication team outside of a crisis period: These conversations are crucial to making the company's priorities, stakes and cybersecurity resources clear to the communications team.
- Draft a cyber crisis response strategy: make a checklist of the first actions, map stakeholders, identify targets, etc.
- Anticipate crisis scenarios and draft messages: press releases, arguments, internal communication, messages for social networks, customer messages, messages published on the website and customer applications, etc.
- Include the communications team in the cyber crisis organisation,
- Hold regular training sessions and build shared reflexes between IT, communication and other members of the crisis unit during simulation drills.

In a crisis situation:

- Ensure that the communications team is notified and integrated into the crisis plan,
- Brief communications staff on the current situation (technical aspects and impacts on business units, services and tools) and the initial actions taken,
- Work with communications staff to assess the factors that may attract the media and in what situations, and the risks that information on the cyberattack may be known,
- Help draft the communication plan and identify all targets: internal, clients, media, authorities, partners, etc.,
- Help devise key messages before sending them to target stakeholders. If possible, second a cybersecurity expert to the communication unit.
- List the questions that journalists, especially those from the expert media, might ask.

Preparing your key messages for the press

Three families of key messages are to be prepared:

- Factual messages: state the verified facts and the action plan that has been implemented in coordination with the authorities and partners,
- Conceptual messages: educate on the subject, especially the existing procedures, the systems in place, and the teams' preparedness,
- Messages of empathy: take into account the concerns and present all the measures implemented for the benefit of those affected.

Several pieces of information need to be conveyed in an educational way to the communication department so that it can work out key messages:

- The nature of the attack and especially the impact on the organisation and its products and services.
- In the event of a data breach, the implications for the customers or users and the actions they can take to protect themselves.
- The actions taken to restore the organisation's services and tools as quickly as possible.
- The time needed for investigation and correction.
- Action taken with the authorities, if any:
  - the report to the data protection authority CNIL in case of a data breach,
  - the complaint filed with specialised police forces.

2.3.3 COORDINATE WITH THE LEGAL DEPARTMENT TO MEET LEGAL OBLIGATIONS

When a cyberattack occurs, the legal and compliance departments support the IT department **with the legal tools** it needs to respond to the crisis and fulfil its legal requirements:

- Notify the data authority CNIL of any personal data breaches if the incident constitutes a risk to the data subjects' privacy (Article 33 of the GDPR).
- Preserve evidence or entrust it to a professional.
- File a complaint and follow the legal procedure.

If there are no legal experts within the IT department, the legal department plays a crucial role in a cybersecurity crisis. The CISO may have legal skills; if so then they may be this department's main contact.

However, the legal department does not always have a full grasp of cybersecurity issues. It is important to establish a dialogue before a crisis occurs to create complementarity between the two departments by designating dedicated, trained points of contacts who know each other well.

2.4 WORKING WITH EXTERNAL SERVICE PROVIDERS

By definition, a crisis is an extraordinary event, and organisations may not be well prepared for it. It can require exceptional resources to resolve, and crisis management specialists may need to be involved.

2.4.1 WHY USE SERVICE PROVIDERS?

There are three main reasons why an organisation might call on an external service provider:

- It does not have sufficient resources within its workforce. Involving external service providers helps to **reinforce internal teams**.
- It requires **specific expertise** in a field for which it lacks the skills in-house.
- **Other players in the ecosystem are involved**, and working with an external service provider allows them to be involved in resolving the crisis (suppliers, software publishers, authorities, partners, etc.).
- **External management costs can be reimbursed by cybersecurity insurance**, which is not the case when paying overtime to in-house employees.

There may be other reasons, depending on the specifics of the crisis and the organisation.

To support the teams, some organisations can help the IT department effectively during a cyber crisis:

- A law firm specialising in cybersecurity law,
- A firm specialising in cyber crisis communication,
- A company specialising in crisis management,
- A specialist cybersecurity organisation,
- ANSSI, depending on the sector of the organisation,
- Its cybersecurity insurance, which itself has partners to support its policyholders,
- A coach for the CIO to help them gain perspective on the situation,
- A rapid response force combined with a CSIRT service: taking out one of these contracts ensures that IT experts' skills will be available with on-site presence,
- Staff representative bodies and works councils to provide reassurance in the face of legitimate worries of staff's personal data leaking during an attack and/or averting conflicts resulting from overwork during the crisis or non-compliance with laws on work, such as working at night,
- An organisation to manage logistics and support for teams, such as food, laundry, and rest areas.

2.4.2 NOTIFY YOUR INSURER

If the organisation suffering a cyberattack has taken out cyber insurance, they must inform their insurer as soon as the crisis begins. The CIO must have access to the policy number even if the organisation's IT system is unavailable. Access to IT files is not guaranteed during a cybersecurity crisis.

Cybersecurity insurance generally has three components:

- **Civil liability coverage**: the policy covers the financial consequences, the costs of notification, particularly with regard to the data authority CNIL, and regulatory sanctions when they are insurable (this is not the case in France but abroad),
- **Coverage for damages**: the policy covers the cost of data recovery, the cost of restoring systems (as they were before the cyberattack, but it does not usually cover the cost of system upgrades), business interruption (blocking systems and operations),[5]

[5] The operating loss is calculated based on the gross margin. An expert is dedicated to making this calculation, which is based on the company's invoices and on discussions between the company and the insurance company. The figures can quickly reach very high amounts. Depending on the sector of activity, the calculation can be more or less complex.

- **Assistance**: the policyholder has access to a 24/7 assistance service with help from a panel of service providers and specialised experts as soon as a claim is made.

The assistance aspect allows the organisation to meet its needs for external service providers at rates negotiated in advance by the insurance company, with the guarantee of a rapid response.

A few notions about cyber insurance

A cybersecurity insurance policy is an effective tool for companies when a cyberattack occurs.

The key steps in managing a cyberattack can be summarised as follows:

- Intrusion,
- Discovery of the intrusion,
- Information first given to top management as well as the risk manager or the insurance manager,
- The IT department reflects on which strategy to adopt - cut off, isolate, control, etc.,
- Report the facts to the cybersecurity insurer as soon as there is an overview of the problem (normally within 48 hours after the intrusion is discovered),
- ANSSI is also contacted, as they might provide assistance depending on the assessment of the situation,
- The insurer sends its service provider to the site, as provided for in the assistance policy,
- An initial exchange is held with the provider and the IT department (general questions) to assess the state of the threat,
- A second, more in-depth discussion is held with the service provider to devise a response strategy.

The insurer's service provider serves as a "conductor" for the company to coordinate the actions to take, but in no way replaces the company's IT teams. It goes through a number of preliminary questions to determine the best response strategy. It also ensures that the company takes all necessary measures for this kind of event. The sooner the right decisions are made, the better off the company will be in resolving the claim.

The insurer can provide its client with the assistance of a panel of specialised service providers, whatever the nature of the threat. This panel allows specialists to be brought in at pre-negotiated rates to avoid companies being faced with costs that run out of control given the situation's urgency. It should be noted that the more a company is aware and prepared in advance, the less it is confronted with problems of pure extortion. Ransomware is inherent to this type of criminal activity, but companies with a sufficiently mature level of prevention generally refuse to pay the ransom, thanks mainly to their back-up systems and their ability to restore corrupted systems.

Finally, follow-up meetings to continue to optimise the company's IT security after the incident's resolution are usually held, but this can take place without the insurer.

The end of 2022 saw significant progress on insurers' coverage of cybersecurity risks after the passage of two laws:

Article 5 of the Ministry of the Interior's orientation and programming law (LOPMI), passed on 14 December 2022, **makes insurance coverage** for loss and damages caused by a cyberattack **conditional to the victim filing a police report within 72 hours**. This obligation to file a police report raises questions: it allows public authorities to obtain almost certain feedback to help fight cybercrime, but it can also be perceived as an incentive for ransomware-type attacks since the insurance company could then pay the ransom the hackers demand.

The Finance Act for 2023, enacted on 30 December 2022, provides for a **tax-free scheme for the provisions of certain reinsurance captives**. The aim of this favourable tax system is to allow companies to improve the insurance coverage for their risks, particularly cybersecurity risks.

Finally, this new tax measure refers to a decree of 13 December 2022, which adds two categories dedicated to cybersecurity risks to the French Insurance Code so that insurers can offer better coverage for them.

2.4.3 CONTACT ANSSI

ANSSI reports to the French General Secretariat for Defence and National Security (SGDSN). It is the authority responsible for supporting and securing the development of digital technology. As a major player in cybersecurity, ANSSI offers expertise and technical assistance to administrations and companies, with a special responsibility toward regulated operators. It offers a service to monitor IT systems and detect, warn of and respond to computer attacks.

ANSSI comprises teams dedicated to both monitoring cyber threats and managing cyber crises. There are teams dedicated to crisis communication and the various aspects of crisis management, including forensic analysis.[6] There are also cross-cutting teams responsible for coordination.

ANSSI does not have set criteria for determining the extent of its involvement with a company in managing a cyberattack. Generally, the Agency assesses the impact on the company, on the ecosystem, and on the political and public stage in deciding what it will do. The ANSSI director decides whether to send teams and what role they will play, such as steering, providing technical support, or communicating. ANSSI covers an increasing number of fields, and its support reassures organisations that are victims of an attack.

[6] **Forensic analysis** is the **investigation of an information system after a cyberattack**. Analysts will collect all the raw data (deleted files, hard disks, backups, system logs, etc.), study it to understand what happened and draw conclusions. This task can be arduous, but it gathers the evidence needed for internal action or legal proceedings, for example. (Source: Tehtris)

3 WHEN THE CRISIS LASTS

After dealing with the initial consequences of a cybersecurity crisis, the victim organisation tries to maintain its activity while containing the attack's effects. Initially, the IT department works to limit the damage caused by the cyberattack on the information system and to repair this damage as best as possible.

When the crisis lasts, the company must overhaul how it functions normally. This reorganisation is particularly demanding for IT teams, who have to manage an additional workload, and for the business teams, who have to work with reduced service or are unable to work at all.

This second phase of crisis management is also the period when the organisation must manage its legal obligations and when it enters a long-term regulatory process. It must also regularly communicate its progress internally and externally. Communication is often missing from crisis management processes, even though it can avoid exacerbating them by preventing crises among employees or in the media, for example, and it facilitates the resolution process by offering stakeholders the correct information.

3.1 MANAGING THE TECHNICAL CONSEQUENCES OF A CYBERATTACK: BETWEEN PROTECTIVE MEASURES AND IT REPAIR

The IT department is the core of the process that manages a cyberattack's technical consequences. This process has two main objectives, which must be clearly defined. The first is to repair or even rebuild the information system; the second is to investigate the origin of the cyberattack. However, it is important to bear in mind that knowledge of how the crisis started is not necessary to repair the consequences. Most resources should be spent on crisis management rather than on tracing the origin. Investigating the hacker and knowing how they operate are not priorities, even if this can be necessary to rebuild the IT system.

The decisions taken during crisis management are mainly based on concrete technical elements. How long has the attack been going on? Was the attack detected as soon as the hackers entered the organisation's information system? Some technical details, such as the geographical origin of the attacker, are of little importance.

To properly manage the crisis management process, you must define technical and operational criteria for exiting the crisis. Care should be taken to avoid extending the investigation indefinitely to satisfy some technical curiosity.

ANSSI's feedback on the key stages of technical crisis management

Managing a cyberattack's consequences on an information system entails four separate processes:

- Information gathering,
- The investigation phase,
- Containment measures,

- Reconstruction or “hardening”.

Information gathering

The information gathering process must be well targeted during the investigation, because nothing else can be done whilst it is going on. This is very costly in terms of human resources.
There are two types of information to be gathered:

- Systems collections, if the attack is not too old: vtx, dd, ORC (or equivalent), AD logs, DNS logs, proxy logs, etc.
- Network data collection: WAF logs, firewalls, configurations, etc.

Information must be gathered discreetly since attackers can spot small movements. Moreover, the information collected will be useful for law enforcement, even if judicial time is quite different from technical time. An unanalysed copy of the information should therefore be kept.

The investigation phase

The investigation phase is used to understand the impact of the attack on the IT system, identify the hackers’ permissions and their critical persistence resources.
In a large-scale breach, the search for “patient 0”, or the entire chain of the breach, should not be a priority. This research is costly and provides little help in overcoming the crisis.
Hackers are focused on gaining permissions within the IT system, including access to an administrator account. Reconstruction should therefore focus on removing these privileges from the hackers. However, doctrines are changing rapidly, so these investigative techniques must be adapted to cybercriminals’ evolving techniques.

Containment measures

Containment measures:

- Limit the attack’s consequences on the IT system,
- Allow the IT system to provide reduced service, for example by isolating a part of the system or by disabling a compromised account,
- Create a “bottleneck” for hackers.

These measures can impact the investigation that is carried out in parallel. Care should also be taken not to fall into a form of guerrilla warfare against the hacker. Typically, these measurements are carried out by system administrators.

Reconstruction

Before you begin to rebuild the IT system, you should ensure that you have identified the critical means of persistence and that you know the system’s security level in relation to the type of attack that was carried out.
These actions have two main objectives: to regain control of the IT system and to improve its security.
Training and coaching administrators is key in this process. To ensure that the incident is indeed over, you generally must supervise the systems. At this stage, continuing to observe intrusion attempts confirms that the security systems in place are working properly. It is difficult to establish an exhaustive list of specific measures to take at this stage, since these depend on the type of attack and the given priorities.

Pitfalls to avoid

In the event of a massively compromised IT system, here are things NOT to do:

- Be vague with service providers about your needs and instructions (dividing tasks and objectives),
- Focus only on the point of entry,
- Begin corrective actions before investigations end (or have even begun),
- Confusing correction with containment (risk of "guerrilla warfare"),
- Not preserving logs,
- Interacting with the opposing infrastructure,
- Discuss incident response on the compromised network: generally, you should remain discrete or have an alternative network,
- Fix only the symptoms, not the cause.

3.2 MANAGING TEAMS DURING A CRISIS

Should the crisis drag on, IT teams will work long hours for a long, indefinite period of time. CIOs must take care of their teams so they can continue to work well. **Team overtime entails logistic accommodations**, such as opening premises at unusual times and providing meals in the morning and evening when company cafeterias may be closed. This aspect is rarely considered when preparing crisis plans, yet it is a major factor in successful cyber crisis management.

In addition to the IT teams, the business units' teams must also be considered, either because they are unable to work or because they must work longer hours as their working conditions have deteriorated. Keeping these teams informed of how the crisis management process is progressing also helps to avoid internal dissent and brings them onboard the effort. The human resources department must be involved in team management.

From a managerial point of view, the consideration of **stress and how it is managed within the teams is essential throughout the crisis**. It is important to identify people who are unable to cope with stress at the outset of a crisis so that they are not overworked. In general, any behaviour that is detrimental to crisis management must be dealt with quickly and effectively, regardless of hierarchical position.

Operationally, here is a list of tips on how to best manage your teams during a crisis:

- Protect the IT teams so that they are not distracted by information or requests other than those from the crisis unit coordinator,
- Conversely, have these operational teams refrain from sharing information without going through those responsible for communicating with business units and the decision-making unit,
- Show gratitude often: for example, you can organise a party after the crisis, and make sure to invite members' partners to recognise their contributions to the effort,
- Despite the many proposals of outside support, prioritise working with in-house teams that have deep knowledge the IT system – there isn't time to train new people,

- Keep to a small crisis unit with key people only,
- Separate teams by objective: one team for correction and construction work and another for investigations. However, this segmentation should not prevent people from meeting each other when necessary,
- Manage the logistical aspects: food, opening buildings, etc.,
- Involve occupational health services.

However, there are things that should be avoided to best manage teams during a crisis:

- When resolving the crisis, don't look for who to blame. This will be done once the crisis is over, during the feedback process which aims to improve the crisis management and cybersecurity processes. If you look for a culprit during the crisis, teams may hide the evidence needed to resolve it. Full transparency and the right to make mistakes must be accepted.
- When users see the difficulties in using the IT system after an attack, do not hide the situation from them; instead, share the information you have, because otherwise they could look for details outside the organisation and cause a leak.
- Communication should not be restricted to those impacted within the group, but should be extended to all branches and subsidiaries to limit other risks, such as using shadow IT during the crisis.

Managing teams in a crisis, according to a pharmaceutical company

The CIO of one pharmaceutical company looked back on the key lessons they learned on crisis team management:

- A speedy decision-making process is crucial to protect teams and get back on track quickly. In this company's case, major decisions like rebuilding the AD and rolling out an EDR were taken within 24 hours of the cyberattack's detection.
- Experts needed to be brought in to relieve the teams.
- Obsessive questions need to be managed as best as possible, for example: "Are the hackers still there?" or "are we doing too much?" or "is this the right level of security?".
- The strategy and organisation had to evolve as the crisis progressed.
- Involving business units on an ongoing basis is fundamental to maintaining trust.
- Promote and harmonise internal and external communication: communicate a lot, and align external and internal communications. Partners, particularly in logistics and R&D, must be reassured, and all the relevant authorities must be notified.
- Manage fatigue: some key people do not want to stop working despite accumulating fatigue. However, it is important for teams to rotate: no one should be indispensable.

Communicating with teams in times of crisis, according to a food company

When computer systems are unusable, so are the usual means of communication (e-mail, company chat, etc.). This leads to difficulties in communicating with teams at the start of a crisis and as it progresses. To address this difficulty, Signal accounts were created to share new mailbox passwords. Without prior preparation, a list of all employees' telephone numbers had to be collected, and not employees had business numbers.

3.3 COMPANIES' LEGAL OBLIGATIONS IN A CYBER CRISIS

As discussed earlier in this report, there are certain legal obligations that need to be taken into account in the early days of a crisis. However, once the complaint has been filed, the legal procedure must still be followed throughout the crisis. The investigations into the IT system and the information collected both serve the future case. Even though IT teams must keep these regulatory requirements in mind, the legal department and/or a specialised law firm will help to see they are fulfilled.

Companies' legal obligations in a cyber crisis, according to Corinne Thiérache

Organisations must fulfil certain obligations in a cyber crisis, including launching legal proceedings against the offenders:

- **Notify ANSSI** without delay of any incident affecting networks and information systems according to extent to which affected users are impacted, the geographical area concerned or the duration of the incident. ANSSI may decide to inform the public.
- **Notify the data authority CNIL of any personal data breaches** if the incident constitutes a risk to the data subjects' privacy (Article 33 of the GDPR).

  Information on the incident should be documented, including:

  - The nature of the breach,
  - If possible, the categories and approximate number of people affected by the breach,
  - The categories and approximate number of personal data records involved: some data is particularly sensitive, such as credit card numbers. Data should be hosted according to their sensitivity, and not all data should be put in one place,
  - The likely consequences of the data breach,
  - The measures taken or under consideration to prevent such an incident happening again or to mitigate any potential negative consequences.

  In case of high risk, data subjects must also be notified (Article 34 of the GDPR), either by email or by notifications on the site (especially for banks).

This notification must be sent to data authority CNIL via a dedicated service as soon as possible and, if possible, no later than 72 hours after becoming aware of a breach presenting a risk to the rights and freedoms of individuals.
However, if all the required information cannot be provided quickly because further investigations are needed, it is possible to proceed with the notification in two stages:

- Initial notification within 72 hours, and, if the deadline has passed, the reasons for the delay,
- Additional notification as soon as more information is available.

Note: companies have been fined up to €10 million for failing to notify of a breach.

The procedure may be closed if CNIL finds that:

- The breach does not adversely affect personal data or pose a risk to individuals' rights and freedoms,
- The persons concerned have been properly informed,
- Appropriate technical protection measures were put in place prior to the breach.

- **Preserve evidence or have it preserved by a professional**, for example a copy of a hoax message, firewall logs, physical copies of affected workstations or servers (failing that, preserve their hard disks), and a few encrypted files which could help the company report the attack to the authorities and which will be useful for the investigation.

- **File a complaint** alongside the technical resolution of the incident and before the affected devices are reinstalled, so that the technical evidence of the incident can be preserved and provided to investigators.

  - Where? Any company can lodge a complaint directly with the police.
    If the company has computer equipment located in Paris or its three neighbouring departments (92, 93 and 94), or if the act affects an essential operator not within a restricted zone, it is advisable to contact France's information technology fraud investigation brigade at the BL2C. At the Paris Public Prosecutor's Office, a specialised section has been created to deal with complaints about cybercrime (Section J3).
    Finally, you can file a complaint by sending a letter to the relevant public prosecutor.
    If the computer attack is particularly serious or if it concerns sensitive information or a strategic sector, the DGSI should be contacted: cyber.dgsi@interieur.gouv.fr

  - Who? The complaint must be filed on behalf of an organisation. If the process is entrusted to an employee, they will need a delegation of authority signed by a legal representative of the organisation.

  - How? For ransomware, for example, the following elements should be provided to the authorities as part of the complaint, depending on the organisation:
    - The details and sequence of events relating to the incident (the official record of the incident will provide a record of the related actions and events), including the date of the ransom demand and the facts of the incident,

- Locations of potentially infected devices,
- Security logs related to the incident,
- The technical analysis of the attack,
- Samples of encrypted files,
- The media or machines on which the ransomware has run (system disk) – hence the need to preserve them well when possible,
- Email addresses and cryptocurrency addresses provided by cybercriminals,
- The text of the ransom note,
- Contact details of witnesses to the incident.

3.4 EXTERNAL COMMUNICATION, OFTEN NEGLECTED IN CYBER CRISIS MANAGEMENT

As we have already noted on several occasions, communication is key to successfully managing a crisis. The communications should be appropriate to the type of organisation and take place both internally and externally with the press and the organisation's ecosystem. In this section, we will look at the fundamentals of successful media communication. Above all, this communication aims to maintain or restore trust. Before speaking publicly, it is important to set a clear objective.

3.4.1 CHOOSING TO COMMUNICATE TO THE PRESS

Deciding whether to communicate with the press should first involve the communications department. Generally, it is wise to communicate externally to avoid shadow communication without the organisation's knowledge. However, sometimes it may be appropriate to keep quiet if the crisis remains internal and is unlikely to escalate, or depending on the context.

To determine whether communicating to the media is necessary, it is important to ask these questions beforehand:

- **Scope of the information**: impacts on the daily life of citizens (e.g. in the event of a data breach), the stakes of the crisis, potential political involvement.
- **Visibility of the information**: a spectacular quantity of data stolen, reputational stakes if the group is well-known, conflictual crisis (the issue of data security), mysterious character (if it is not known where the attack comes from),
- **Symbolism of the information**: ability to arouse emotions and concerns, especially when the victims are innocent (personal data such as health, bank, etc.).
- **Journalistic opportunities**: cyberattacks interest the media.
- The potential impact of uncontrolled shadow communication done without the organisation's knowledge.

The first objective of this assessment is to establish whether the company should communicate about the cyberattack. The global context should also be taken into account. During important national events, such as presidential elections, large-scale communication is unlikely to be relayed.

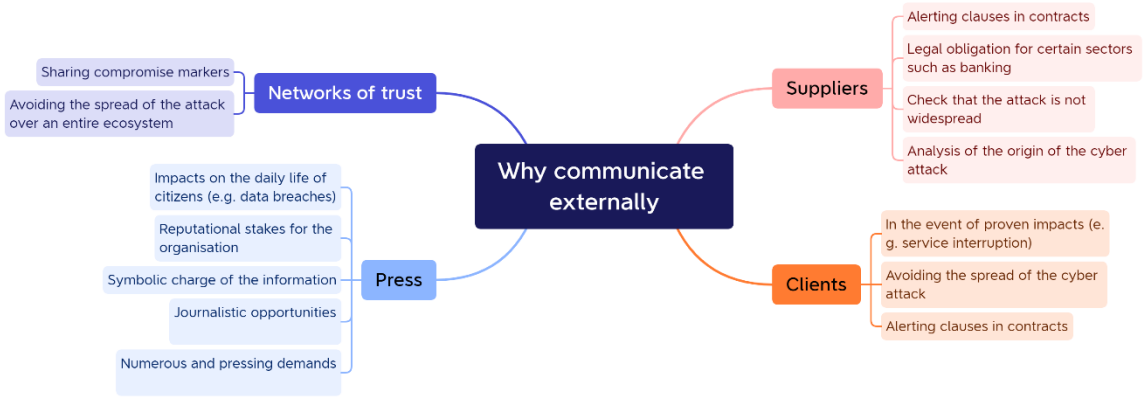

Figure 5: Decision tree 2 - Why communicate externally?

It is also important to note that the decision to communicate to the media does not always come from the company. News travels fast, and often before the company is even aware of it. It generally comes from one of these four channels:

- News agencies, such as AFP,
- Government services,
- The regional daily press and local investigative media,
- Social networks.

Maintaining a news watch on these four channels is also essential during a cyber crisis.

3.4.2 HOW TO COMMUNICATE WITH THE MEDIA

If you decide to communicate, you must show that the organisation is taking action to deal with the crisis. At the start of a crisis, you will need to immediately demonstrate that you have acted to protect customers and data. You will also need to be able to explain and detail the procedures you have in place: be educational and show your professionalism. The subject is difficult to popularise and foresee. You should use appropriate vocabulary that everyone can understand. You must also show empathy and, if the crisis has an impact beyond your organisation, you have to demonstrate that you are aware of this fact.

Good communication management entails identifying stakeholders and choosing the right messages and timing. A few questions to ask yourself are:

- What context surrounds the crisis: its nature, impacts, risks, legal/insurance, etc.,
- Who has power over what? The company, the competent authorities, partners, etc.,
- How is the process progressing? In terms of technical resolution, operations, link with entities/subsidiaries,
- Do I have all the information? Exchange regularly with other stakeholders to develop the full range of messages,
- Who are the players: identify the relationships between the players: the authorities, professional partners, internal employees, sensitive contacts (media, associations, victims and relatives, opinion leaders, etc.).

The IT department's role here is to provide the communication department with concrete information on the consequences of the crisis without trying to minimise the impact. More than any other department during a cyber crisis, the IT department educates on the risks and potential impacts.

The crisis should not be downplayed in the media: the media tend to reveal and highlight instances where an organisation has evaded or sought to hide certain elements. To avoid dissonance, it is important that messages are shared internally to ensure everyone stays on topic.

Both internally and externally, you should avoid stressing any search for blame. It is important to show solidarity with all parties involved in the crisis and not to point the finger at one provider or employee.

If the messaging entails a press conference or television appearance, it is crucial to work with the organisation's spokesperson to thoroughly rehearse their key messages. Even if the organisation is in the middle of a crisis, this preparation should not be neglected. This spokesperson must have in mind the major strategic decisions that were taken during the crisis and speak with the CIO to understand the action plan put in place and the accompanying impacts.

4 PREPARING TO EXIT THE CRISIS

When you exit a cyber crisis depends on the criteria defined at the beginning. These criteria generally include an end to the consequences on the company's activity and the total or partial repair of the IT system. Exiting the crisis can be a process that lasts months, even years. Once the impacts of the cyberattack have been repaired, the objective is then to improve IT security. Exiting the crisis often means considerable investments in cybersecurity for companies. The IT department must also support the legal department in the legal process that was set in motion during the crisis.

4.1 SUPPORTING THE LEGAL PROCESS[7]

Once the organisation has filed its complaint, legal proceedings begin based on the information collected by the IT department to identify and judge the cyberattack's perpetrators. Unfortunately, these procedures rarely come to a successful conclusion.

4.1.1 CYBERATTACKS IN THE FRENCH CRIMINAL CODE

Categorising the offence is the first step in the procedure. Depending on the type of attack and its consequences, several criminal charges may be brought against hackers, such as:

- **Extortion**: Article 312-1 of the French Criminal Code states: "Extortion is the act of obtaining by violence, threat of violence or coercion, either a signature, a commitment or a renunciation, the revelation of a secret, or the handing over of funds, securities or any other asset. Extortion is punishable by seven years' imprisonment and a fine of €100,000."

Indeed, cyberattacks are characterised by tangible coercion - the freezing of the computer or its files - requiring an involuntary handover of funds.

- **Violation of an automated data processing system**, according to Article 323-1 of the Criminal Code:
  - "Fraudulently accessing or remaining in all or part of an automated data processing system is punishable by two years' imprisonment and a fine of 60,000 euros.
  - Where this results in either the deletion or modification of data contained in the system, or an alteration of the functioning of the system, the penalty is three years' imprisonment and a fine of €100,000.
  - When the offences provided for in the first two paragraphs have been committed against an automated personal data processing system implemented by the State, the penalty shall be increased to five years' imprisonment and a fine of €150,000."

Since 2013, the possession or transfer of ransomware without legitimate reason has been punishable by the same penalties (Article 323-3-1 of the Criminal Code).

- In breaches of automated data processing systems, the **aggravating circumstance of organised crime is very often accepted** (Article 323-4-1 of the Criminal Code).

[7] This section summarises the contribution from lawyer Corinne Thiérache.

Indeed, committing these offences usually involves a variety of skills, requiring several people to design and inject the malicious code, send an infected e-mail and collect the ransom.

How criminal offences are categorised is especially important for stakeholders, including those assisting victims.

4.1.2 CLAIMING COMPENSATION FOR DAMAGES

In the case of a cyberattack, the victim can generally claim several types of damages. Depending on the case, the **financial losses** can include:

- Lost income that affects the company's operations, such as lost cashflow, a lack of funds, supply chain breakdowns, etc.
- Loss of opportunity to make a profit: this is particularly relevant when business activity is stopped or when the company has lost a contract,
- Extra costs: this can be claimed in the event of a malfunction in the company.

Compensation for **moral prejudice** requires a legal entity to "demonstrate concrete damage to its reputation or image among its customers" (Versailles Court of Appeal, 9th ch., 30 June 2021).

The proof the victim provides is subjected to strict inspection. It is therefore essential for the victim of a cyberattack to gather material evidence of the various losses associated with this type of incident.

However, whilst authorities often issue heavy fines against companies who fail to correct flaws in their systems – one example being British Airways, which was fined a record £20 million by the Information Commissioner's Office in July 2019 following an investigation after a massive cyberattack involving the data of nearly 400,000 that revealed the airline's lack of sufficient security for its customers' data – **convictions of hackers are less frequent and less consequential**:

- Court of Cassation, Criminal Division, 7 November 2017, 16-84. 918: Dismissal of the appeal brought by Mr Pierrick Y. against the judgment of the Paris Court of Appeal, Chamber 4-11, dated 30 June 2016, which sentenced him to a two months' suspended sentence with probation and included civil damages for participating in an arrangement to prepare to interfere with the proper functioning of an automated data system.

In this case, the web portal of essential operator EDF suffered a "distributed denial of service" attack in April 2011 as part of a widespread offensive mounted by the organisation "Anonymous" and appearing under the title "Opération Greenrights", which was charged with participating in arrangements to interfere with the proper functioning of an automated data system.

- Nîmes tribunal, 28 June 2013, no. 13/1677: A computer science student was convicted of fraudulently accessing and remaining in an automated data processing system after they designed and disseminated on the Internet the "TUBEMASTER ++" software, which was used to record files streamed by the website Deezer in violation of copyright. The software analysed streams coming from Deezer and retrieved the decryption key installed on the user's computer to listen to these streams.

The defendant was fined €15,000 and ordered to pay damages to Blogmusik amounting to €7,285.02 as well as €5,000 for moral damages and €5,000 in damages for each of the other civil parties (SACEM, SDRM, SCPP).

Finally, even if the perpetrator is convicted, the decision must still be enforced, and any damages paid to the party who suffered the cyberattack.

4.2 REBUILDING THE INFORMATION SYSTEM

Whilst the crisis is still ongoing, a recovery strategy must be devised. Priorities must be set (if they were not done so prior to the crisis); some will be self-evident, such as paying employees and suppliers and resuming the core business. This should only be done once it has been ascertained that the systems are secure again.

Once the recovery is complete, the IT department will aim to improve the IT system's cybersecurity for the long term. Some such projects include:

- Improving the security of the Active Directory and limiting privileged accounts (work that can be carried out in collaboration with ANSSI),
- Redesigning administration practices and using multi-factor authentication technologies,
- Deploying EDR technology on all servers and PCs. Whilst some old systems will not support EDR, they still need to be protected by other solutions,
- Partitioning of central and local infrastructure,
- Setting up controls of data flows,
- Cleaning up global networks and restoring servers.

5 BEST PRACTICES IN CYBER CRISIS MANAGEMENT

***On the technical side*:**

- Set criteria for exiting the crisis.
- Do not dwell on investigations just to satisfy your technical curiosity, but seek to prevent the attack from happening again.
- Do not look for who should be blamed internally for the cyberattack during the crisis; this happens during the feedback period.
- First, contain the attack, then remedy it. The two stages should not be confused.
- See the crisis as an opportunity to improve IT security.

On team management:

- Do not underestimate the fatigue of employees involved in crisis management.
- Manage team stress and act quickly and effectively on behaviour that hinders crisis management.
- Establish a rota so that no one is indispensable.
- Make employees' lives easier by managing logistical aspects (24-hour opening of the premises, opening the company restaurant from morning to evening, etc.)
- Take quick decisions to facilitate operational teams' work.
- Be flexible: do not hesitate to change your strategy if it is not working.
- Involve business unit teams in the process and communicate as much information as possible internally.
- Keep technical teams out of crisis unit communications, so that they do not get distracted by them.
- Use service providers to relieve teams and provide expertise.

On crisis communication:

- Set up an alternative communication system to the main network.
- Internal communication is essential to avoid external leakage of information.
- Communicate with the ecosystem (suppliers, customers, etc.) as soon as the consequences of the crisis are known.
- Communication to the media should be considered, but it must have a specific objective and be carefully prepared.

In terms of the legal aspects

- Fulfil your legal obligations as soon as the crisis is known: inform ANSSI, notify CNIL, file a complaint.
- Collect and preserve evidence needed for legal proceedings.
- Fulfil contractual obligations to give notice of suspected or actual crimes.

6 CONCLUSION

Businesses and public administrations are increasingly subjected to cyberattacks. This has a range of consequences, not just for the company's business and employees, but for its finances and reputation as well. Large-scale cyberattacks are not characterised by the method used but by the impact it can have on the organisation and its ecosystem.

The early stages of a crisis are crucial to limiting the spread of a cyberattack since this is the time when the internal organisation is being put in place and the first strategic decisions are being taken. Whilst the crisis originates in computing, the IT department is not the only department involved in the crisis management process. It must work with other departments and relay as much information as possible to them. Establishing cross-cutting communication from the start of the crisis is essential for successful crisis management.

The height of the crisis may last a few days or a few weeks. Although the heart of operations is in the IT department, the business units should not be neglected. If the crisis lasts some time, the teams will be under stress and tire quickly. Managing the essential logistics for teams avoids adding a crisis on top of the cyber crisis. Similarly, a crisis that lasts increases the risk of media reporting on the issue. Implementing accurate crisis communication can prevent a reputational crisis.

Emerging from a cyber crisis can take months or even years. Once the crisis is over, it is time to strengthen the security of the information system and to accompany the legal process.

Managing a cyber crisis cannot be improvised; anticipation and preparation are crucial for success, but organisations are never sufficiently prepared. Cyberattacks can happen at the wrong time with unforeseen consequences, and when they do, there is no longer time to hold crisis drills or review business continuity plans. Reflecting on how to react in a crisis, as we did in the working group, is essential.

At the least, the increase in the number of cyberattack victims has made it easier to talk about the subject. Organisations' feedback help to spread operational best practices and advice to increase the overall level of cybersecurity.

7 APPENDICES

7.1 CREATING A TIMELINE

As part of this working group, we underwent a crisis management drill. Participants were put in the shoes of a large company facing a ransomware attack and were asked to react to the changing situation. We focused on the first moments of the crisis. In the table below, you will find the results of this exercise, which you can adapt to your organisation to simulate crisis management. If you wish to hold a crisis management drill, you can use ANSSI's practical sheet.

Time	Event	Actions/Decisions	Actors involved
17:00	Some staff are unable to use their computers.	1. Qualify the incident 2. Use the EDR to isolate all the workstations in the affected department	1. Pre-activate the crisis unit 2. Risk management department 3. Crisis management department 4. Several participants from IT: ● the IT helpdesk ● the operational security team ● the production manager ● the network manager ● the Windows and workstation manager
17:15	Ransomware attack: data encryption and ransom demand.	1. Isolate all systems and cut off the means of propagation 2. Activate the cyber crisis unit 3. Investigate the affected scope	1. Competent authorities of the countries concerned 2. Cyber insurance (according to contract) 3. The members of the crisis unit (see composition above)
17:45	The virus spreads to all departments of the group.	1. Share this information with suppliers and customers 2. Complete isolation of the system 3. Stop and isolate backups 4. File a complaint	1. Deploy the group crisis unit, if this is not already the case
17:50	The cyberattack is announced on a social network.		1. Communication Department
18:00	The business units and executive committee demand information.	1. Share and regularly update a dashboard with all members of the crisis unit 2. Regular updates within the crisis unit	CRISIS UNIT
18:12	The executive committee realises that a critical operation has to be carried out in two days. (e.g. payroll)	1. Activate the business continuity plan 2. Propose a workaround solution	
18:30	Attack claimed by a group of cybercriminals and data published on the dark web.	1. Analysis of the type of data stolen	

Figure 6: Summary timeline produced during a workshop on crisis management

7.2 A SHORT MEMO OF THE TOOLS SUGGESTED BY PARTICIPANTS

7.2.1 WHAT TO DO AS SOON AS THE CRISIS HITS

Here is a checklist of things to do or think about when a cyberattack has been detected:

- Identify the scope of the crisis and stop the spread as quickly as possible,
- Use a communication tool separate from the IT system,
- Depending on the scope of the crisis, share as much information as you have (at least internally, then to suppliers and customers, and possibly to the press),
- Activate the decisional and operational crisis units,
- Trigger the business continuity plan,
- Propose an initial action plan and provide a summary dashboard to describe the initial situation, to be updated according to progress,
- Notify your cybersecurity insurer,
- Notify ANSSI,
- Organise how you will manage the crisis (regular updates) and the logistical aspects (accommodation, food, opening of premises for the teams).

7.2.2 ANTICIPATION: WHAT TO DO BEFORE A CYBER CRISIS

Although anticipation is not the focus of this report, we have nonetheless drawn up a list of “must-dos” in advance of a cyber crisis (not in order of importance):

- Have a directory of contact details for the competent authorities in the country where the organisation is located (ANSSI, CNIL, FBI, etc.), the cybersecurity insurer, external service providers, etc,
- Ensure you have access to the BCP,
- Set up a communication tool separate from the IT system,
- Have a directory of crisis unit members’ contact details,
- Organise crisis management training,
- Plan the organisation of the crisis unit and identify several people for each position,
- Raise awareness of cybersecurity among employees,
- Plan a reporting format (dashboard, weather report, etc.),
- Have offline backups on independent systems, including in the contracts of SaaS services,
- Know the key elements of the IT system: architecture diagrams, flow maps, network addressing plan, inventory of assets (owner, sensitivity, business concerned, etc.),
- Identify service providers that provide forensic services,
- Design and display a sheet with the first actions to take,
- Plan logistical aspects (taxis, food, hotels, 24/7 access to sites, etc.),
- All documents and lists must be printed and accessible even when the IT system is unavailable.

7.3 BIBLIOGRAPHY: RESOURCES TO IMPROVE YOUR CRISIS MANAGEMENT

ANSSI's main guides on cyber crisis management:

- TOP 10 vulnerabilities in 2021.
- Landscape of threats to IT 2021.
- APT31 attack campaign: description, countermeasures and code.
- State of the ransomware threat to businesses and institutions.
- Active Directory inspection points.
- Security recommendations for building a logging system.
- Security recommendations for logging on Microsoft Windows systems in an Active Directory environment.
- An overview of cybersecurity professions.
- Hold a cyber crisis drill.
- Cyber crisis, the keys to operational and strategic management.
- Anticipate and manage your cyber crisis communication.

On cyber crisis management:

- Les fondamentaux de la gestion de crise cyber, Laurane Raimondo, Ellipses, 2022.
- Plan de continuité des activités et gestion de crise, Cécile Weber, Afnor, 2021.
- Cyber-crise, bonnes pratiques dans la gestion de crises de cybersécurité, CCN-CERT, 2020.
- Fuite de données: gestion de crise, mode d'emploi, Guillaume Tissiers, CEIS, 2018.
- Common practices of EU-level crisis management and applicability to the cyber crises, ENISA, 2016.

On cyber insurance and legal aspects:

- LUCY study:LUmière sur la CYberassurance by AMRAE, May 2021.
- Report on the insurability of cyber risks, *Haut Comité Juridique de la Place Financière de Paris*, 28 January 2022.
- General Data Protection Regulation, 27 April 2016.
- Guidelines on the notification of personal data breaches under Regulation (EU) 2016/679, revised and adopted on 6 February 2018.
- Reporting safety incidents to regulatory authorities: how to organise and who to contact CNIL, 18 May 2020.
- Information report on behalf of the enterprise delegation on businesses' cybersecurity, Sébastien Meurant and Rémi Cardon, Sénat, 10 June 2021.
- Le droit pénal à l'épreuve des cyberattaques, Le clubs des juristes, April 2021.
- La Cyber-assurance, Valéria Faure-Muntian, Assemblée Nationale, 2021.
- Code de la cybersécurité, Dalloz, 2022.

Achieving digital success to help promote the economic growth and competitiveness of its members, who are major French corporations and public administrations, and users of digital solutions and services
Cigref is a network of major French corporations and public administrations set up with a view to developing its members' capability to acquire and master digital technology. It is a unifying player in the digital society, thanks to its high-quality thinking and the extent to which it represents its members. Cigref is a not-for-profit body in accordance with the French law of 1901, created in 1970.
To achieve its mission, Cigref counts on three business units, which make it unique.

Belonging
Cigref speaks with one voice on behalf of major French corporations and public administrations on the subject of digital technology. Its members share their experiences of the use of technology in working groups in order to elicit best practices.

Intelligence
Cigref takes part in group discussions of the economic and societal issues raised by information technologies. Founded nearly 50 years ago, making it one of the oldest digital associations in France, it draws its legitimacy from both its history and its understanding of technical topics, giving it a solid platform of skills and know-how, the foundation stones of digital technology.

Influence
Cigref ensures that its member companies' legitimate interests are known and respected. As an independent forum in which practitioners and actors can discuss and create, it is a benchmark recognised by its whole ecosystem.

www.cigref.fr
21 av. de Messine, 75008 Paris
+33 1 56 59 70 00
cigref@cigref.fr