CYBER CRISIS MANAGEMENT

GOOD PRACTICES IN THE MANAGEMENT OF CYBERSECURITY CRISIS

CCN-CERT BP/20

BEST PRACTICES REPORT

OCTOBER2020

CCN centro criptológico nacional

CCN-CERT centro criptológico nacional

Edit:

GOBIERNO DE ESPAÑA
MINISTERIO DE DEFENSA

CCN
centro criptológico nacional

2.5.4.13=Qualified Certificate: AAPP-SEP-M-SW-KPSC, ou=sello electrónico, serialNumber=S2800155J, o=CENTRO CRIPTOLOGICO NACIONAL, c=ES
2021.02.25 22:48:50 +01'00'

National Cryptologic Centre, 2021

Release date: January 2021

Index

	page
1. About CCN-CERT,National Governmental CERT	4
2. Introduction	5
3.Case studies	9
4. Best practices in crisis management caused by cyber incidents	10
BP.1 Leadership, values and control	10
BP.2 Structural plans and protocols	11
BP.3 Crisis Committee. Configuration	12
BP.4 Permanent control of the exposure area	15
BP.5 Appropriate stakeholder management	16
BP.6 Initial diagnosis and possible scenarios	18
BP.7 Coordination	19
BP.8 Initiative and proactivity	20
BP.9 Unified discourse and official source of information	21
BP.10 Transparency, empathy and accountability	23
BP.11 Valorization of the actions implemented	24
BP.12 Formal closure of the crisis	25
BP.13 Implementation of lessons learned	26
5. Conclusions and recommendations	27
Annex 1. Cyber espionage case study	29
Annex 2. Ransomware case study	34
Annex 3. Case study of attempted theft of funds	40
Annex 4. Guidance on levels and criteria for assessment and classification of cyber crises	46

1. About CCN-CERT, National Governmental CERT

The CCN-CERT is the Computer Security Incident Response Team of the National Cryptologic Centre, CCN, assigned to the National Intelligence Centre, CNI. This service was created in 2006 as the **Spanish National Governmental CERT** and its functions are set out in Law 11/2002 regulating the CNI, RD 421/2004 regulating the CCN and in RD 3/2010, of 8 January, regulating the National Security Framework (ENS), modified by RD 951/2015 of 23 October.

Its mission, therefore, is to contribute to the improvement of Spanish cybersecurity, being the national alert and response center that cooperates and helps to respond quickly and efficiently to cyber-attacks and to actively confront cyber-threats, including the coordination at the national public level of the different Incident Response Teams or existing Cybersecurity Operations Centers.

Its ultimate aim is to make cyberspace more secure and reliable, preserving classified information (as stated in art. 4. F of Law 11/2002) and sensitive information, defending Spanish Technological Heritage, training expert personnel, applying security policies and procedures and using and developing the most appropriate technologies for this purpose.

In accordance with these regulations and Law 40/2015 on the Legal Regulation of the Public Sector, the CCN-CERT is responsible for the management of cyber-incidents affecting any public body or company. In the case of critical operators in the public sector, the management of cyber-incidents will be carried out by the CCN-CERT in coordination with the CNPIC.

2. Introduction

Crisis is understood as any circumstance, deliberate or fortuitous, internally caused or not, which produces an imbalance in an organization regarding its service, clients, shareholders, workers and union representatives, authorities or other companies or entities, affecting or damaging its public image and reputation, with the consequent economic loss or legal non-compliance, and which may jeopardize its economic viability and/or professional future.

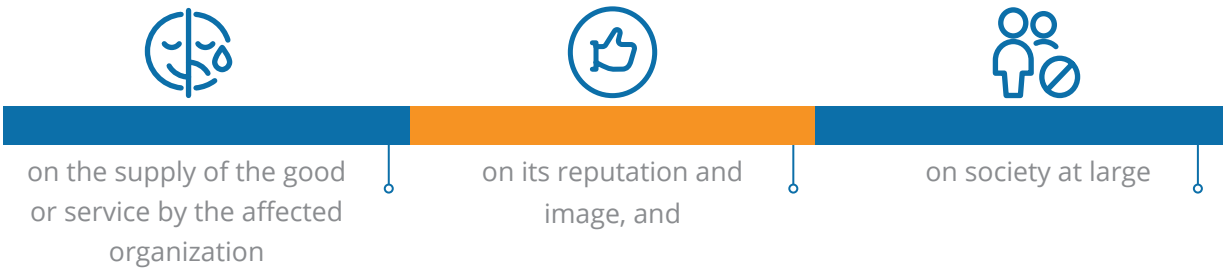
A shorter definition could be: a **low-probability** situation which, when it occurs, generates a **large impact** and whose effects **last for a long time**.

There are three elements to consider in a crisis: the **threat** to the organization, the element of **surprise** (unforeseeable and unexpected) and the **short period** of time required for decision-making. In any case, threats or circumstances must be managed before, during and after they occur, bearing in mind that a crisis situation can happen even without a real problem. It is enough for any rumor or event to reach public opinion for the crisis to unravel, and given the present growth of social networks, it can even spread uncontrollably, causing panic among the aforementioned stakeholders. This will make crisis management even more difficult.

The management of all types of crisis is a discipline that has evolved significantly in the last decade and from very different fields, particularly those related to Information Security (ISMS) and Communication. As these are particularly serious situations, which can compromise not only the functioning of the organization, but even its future, crisis management has become an increasingly essential capability for a growing number of organizations. Among the many factors that have led to its development are the greater demands in terms of service provision, the increase in social responsibility and the potential impact of social networks on reputation and image.

In this context, there is already a body of knowledge, with a very heuristic base, that provides guidance on the **most appropriate resources** for organizations to develop this management capacity and on **the most advisable management practices** in order to successfully face crisis of any kind.

The effects of a crisis in an organization occur:



Every crisis involves **decision-making under pressure**, with **limited time and information**, on **several fronts in parallel**, and with many actors and people involved.

Regardless of the origin of the crisis, **the management component** required for its resolution is obvious. In order to do so, the organization affected needs to have the appropriate **management capacities and structures** in place to deal with the crisis successfully.

In any crisis, therefore, **two distinct spheres** of action are identified:

- **Operational and technical response to the incident** related to the reason for the incident and whose immediate effects must be contained and resolved by a specialized response team. A cyber-incident response team that, by rapidly detecting attacks and threats, minimizes the loss or destruction of technological or information assets, mitigates the malicious exploitation of weak points in infrastructures and helps recover services as quickly as possible[1]. This complex activity involves data and event collection and analysis methods, monitoring methodologies and procedures to classify threats and prioritize them.
- **Organizational and strategi** insofar as its impact affects different areas of the organization (service, operations, image and reputation, relationship with the regulator, stakeholders, presence in social networks, etc.) and requires a coordinated response at a high level, determining the channels of communication with other units or entities, whether in-house and/or external.

The management capabilities and structures required to deal with a crisis are not improvised when a crisis arises, they must be developed in advance so that everything is ready when that moment comes.

The management capabilities and structures required to deal with a crisis are not improvised when a crisis arises, they must be developed **in advance** so that everything is ready when that moment comes.

1 CCN-STIC Guide 817_Cyber incident management: https://www.ccn-cert.cni.es/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/988-ccn-stic-817-gestion-de-ciberincidentes/file.html

As a frame of reference, Figures 1 and 2 show the generic profile of a crisis and its main phases, on which the good practice proposal developed in this document is based:

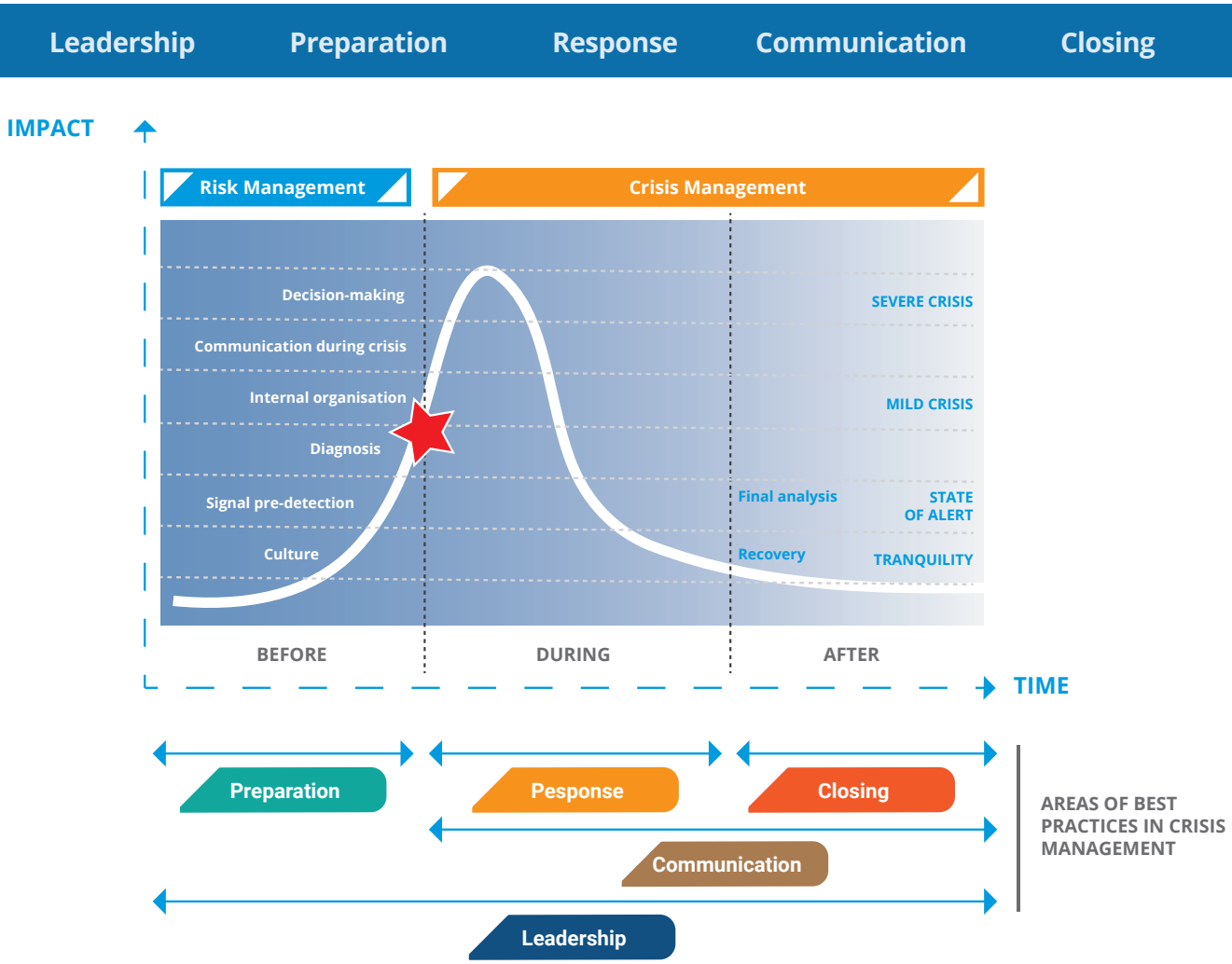


Figure 1. Profile of a crisis[2]

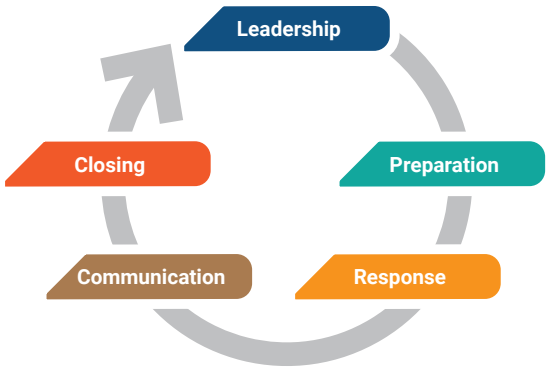


Figure 2 Key areas for addressing a crisis

2 Good practices in crisis management Institut Cerdá

In this regard, it is important to insist on the importance of the **prior work** required to ensure that the organization is prepared when a crisis arises: **risk analysis**, the **development of action plans** and the definition of appropriate management structures shall indicate that a **foresight exercise** is constantly developed so that it is possible to estimate the most likely type of cyber-attack in order to anticipate the problem by designing a way to manage it at the slightest sign of materialization.

Focusing on the subject of this report, we can therefore **define** a **cyber crisis** as a cybersecurity event that has a **major impact** on the organization's activity and requires **prompt decision-making** with limited information. The likelihood of such an event will depend on the degree of prior preparation of the organization: it will be very small if a large number of preventive measures have been taken, and progressively higher as the volume of prevention work decreases.

This guide of good practices in cyber incident management is based on detailed analysis of recent real-life episodes from which recommendations were collected for dealing with crisis in general, it also includes specific good practice for each case on the governance of crisis arising from cyber security incidents.

To this end, a decalogue of thirteen (13) good practices[3], summarized in Figure 3, is proposed, which are considered fundamental components of the success model for dealing with a crisis and which is organized into the five areas outlined above - l**eadership, preparation, response, communication and closure** - related to the generic profile of a crisis.

These good practices for cyber incidents crisis management are set out in section 4.

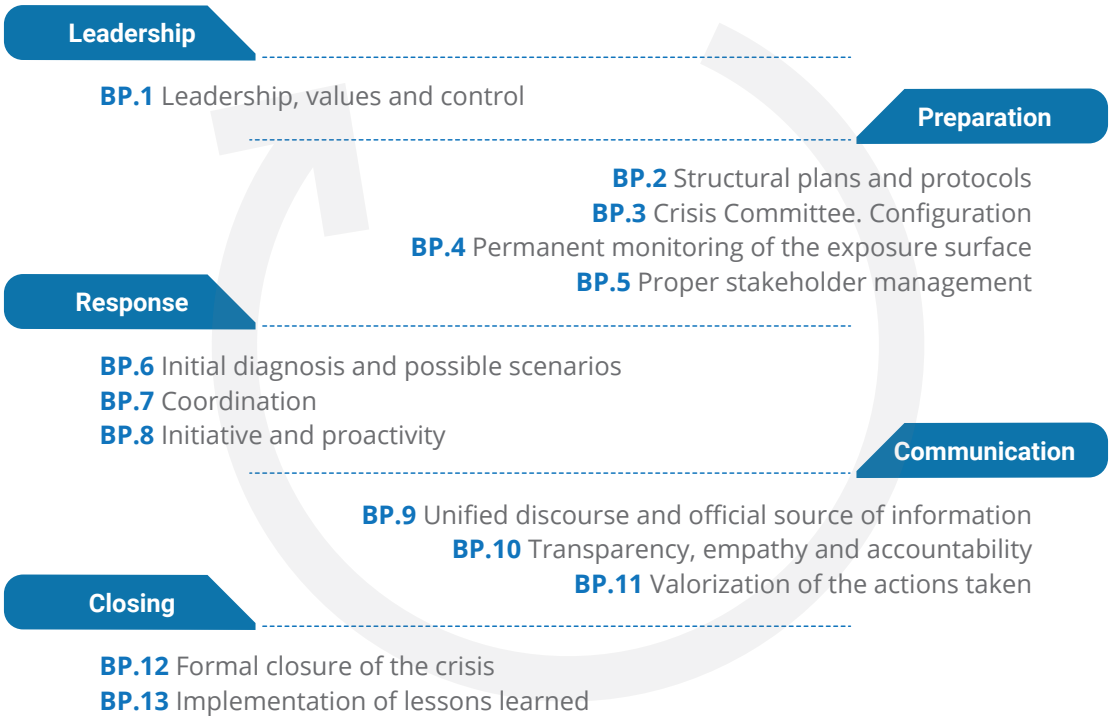


Figure 3. Summary of good practices

3 This Decalogue of good practices is adapted from the Institut Cerdà publication "Monografía 4. Buenas practices en la gestión de crisis" of December 2018.

3. Case studies

In order to illustrate in a concrete way the good practices detailed in the following sections, Annexes 1, 2 and 3 develop didactic examples on cyber crisis that summarize CCN-CERT's recommendations for this type of situations. Although these good practices are common to all cyber-crisis management cases, not all crisis caused by cyber-incidents require the same type of actions.

The aim of these case studies is to show in a practical way the main actions to be taken in the specific situations detailed.

1

Cyber espionage:

this annex explains the issues to be taken into account for the management of cyber crisis in the event of cyber espionage.

2

Ransomware:

this annex explains the necessary issues to be taken into account in the management of a cyber-crisis caused by a targeted attack via ransomware malware.

3

Extortion and theft of funds:

this annex explains the necessary issues to be taken into account in the management of cyber-crisis in the face of possible attacks aimed at extortion and theft of funds.

4

Summary of main findings:

this annex summarizes the main conclusions of the case studies described above.

4. Best practices in crisis management caused by cyber incidents

BP.1 Leadership, values and control

It is important to lead, take and maintain the initiative during the crisis and, if lost, to look for opportunities to regain it. Taking reasonable measures is almost always better than doing nothing, but **on the basis of a previously agreed plan and preparation**. It will be easier to take appropriate action in a short period of time (which is usually the case in such situations) if there is some kind of prior work than if there is not. In this way, nervousness or improvisation, which are all too common at this time, can be avoided.

In the case of cyber-incidents, the role of the Information Security Manager is fundamental, he/she will be the first to categorize the event and decide whether convening the Crisis Committee or not.

On the other hand, if prior to a crisis, organizations have built a **reputation** with explicit values that they respected throughout their activity, they will be more trustworthy, credible and empathetic than those that did not. Whether it is a large or small organization, if its history is based on ethical and professional principles, it will be much easier for it to gain the trust of all its stakeholders and, therefore, to overcome the situation.

Decision-making shall be done by senior management, who are the ones with the capacity to ensure the material and human resources required, as well as from the different levels of decision-making. In the case of cyber-incidents, the role of the **Information Security Manager** is fundamental, he/she will be the first to categorize the event and decide whether convening the **Crisis Committee** or not, assuming that the prompt notification of the event not only benefits the organization itself, but also results in an increase in the general, industry and national security, which is why its implementation is an ethical commitment to society.

BP.2 Structural plans and protocols

Crisis plans shall be developed in normal times. Anything that is not foreseen previously is practically impossible to improvise during the emergency. It is true that perfect prevention is practically unattainable: zero risk does not exist; but one of the keys to effective crisis management is determined by the ability to **anticipate and identify the most vulnerable areas (risk management)** that may lead to critical situations. Identifying these potential risks in the business will be key to knowing how to respond and reduce their impact as much as possible.

Crisis plan shall be developed in normal times.

From this point of view, cyber threats require a **constant foresight exercise** in order to be aware of the organization's weaknesses and thus anticipate and prepare.

Many crisis analysis find that the main problem is that **the risk that triggered the crisis was not considered** previously and therefore there was no rigorous planning to manage the risk, leaving the organization in a state of permanent vulnerability.

In this sense, many organizations (this is reflected, for example, in international standards such as ISO 27001 and 22301 for the implementation of an ISMS[4]) draw up **Crisis Management Plans**, following various methodologies such as BCM[5], which describe the tasks required to develop crisis management capability and to identify the main actions to be taken in response to a serious situation or a disaster. These plans usually include a **Crisis Manual** that serves as a reference framework to count on a script of actions to be carried out in terms of continuity, contingency, communication, human resources, etc., with a clear assignment of responsibilities.

These plans should be properly disseminated among the organization and its management through exercises or training sessions.

BP.2

4 Information Security Management System that includes a set of policies, procedures and guidelines for the correct protection of the information assets of any organization.
5 *Business Continuity Management* (BCM), a comprehensive program that incorporates business continuity, disaster recovery and crisis management.

BP.3 Crisis Committee. Configuration

A **Crisis Committee** should be the highest decision-making body for the unified management of a crisis situation and should be previously defined. Its main task will be to accelerate the decision-making process to resolve incidents by defining priorities and establishing the strategy and tactics to be followed. The committee shall set the main scenarios to be taken into account, determine how to act and report the situation and lead all the recovery and communication teams.

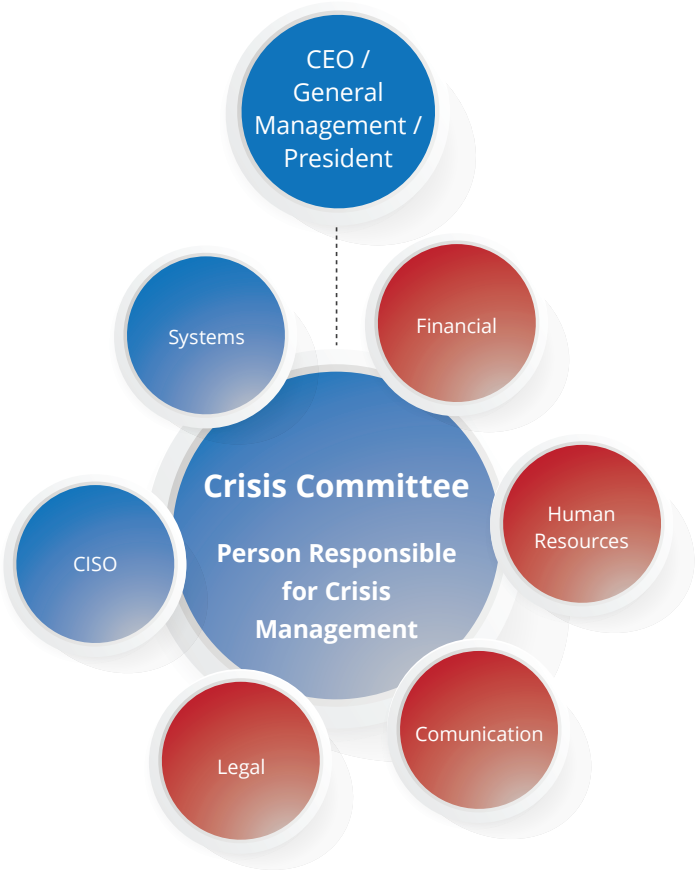


Figure 4. Crisis Committee

It should be made up of a small group of people with different profiles, executive and highly decisive, with the capacity to react to stressful situations and agility in team management and decision-making. It will be led by the Head of the Crisis Committee, a figure with maximum decision-making capacity (CEO of the company or head of the organization, in the case of the public sector). Each of the basic areas in an organization should be represented alongside them: the person responsible for Information Security (CISO), Infrastructure, Processes, Human Resources, Legal and Communication. Because the management of a crisis, even if its origin is a cyber incident, is not something exclusive to the security team, but involves the entire organization.

This Committee will decide whether or not the organization is facing a crisis, its level or degree (depending on the previously agreed levels), the establishment of measures and the distribution of responsibilities, as well as the different levels of committees, with different people responsible in each case; from the operational committee that must contain and resolve the incident, to the coordination and communication committee that will safeguard the organization's reputation, establish the information policy, with the most appropriate messages and channels.

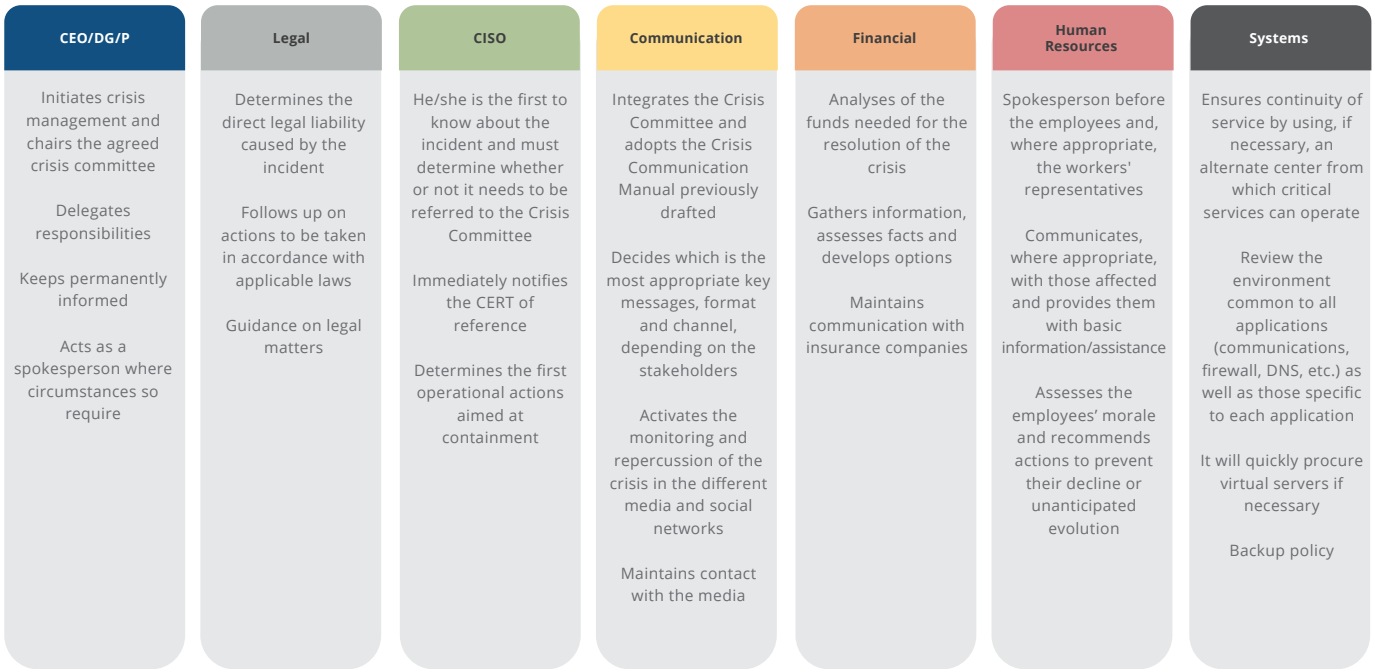


Figure 5. Crisis Committee and its managers

From an operational point of view, it can be expected that, depending on the cyber incident level established on the basis of the criteria of danger and impact, the appropriate management committee is set up in advance.

As a guideline, although it depends on the size and capacities of the organization, a management scheme is presented below.

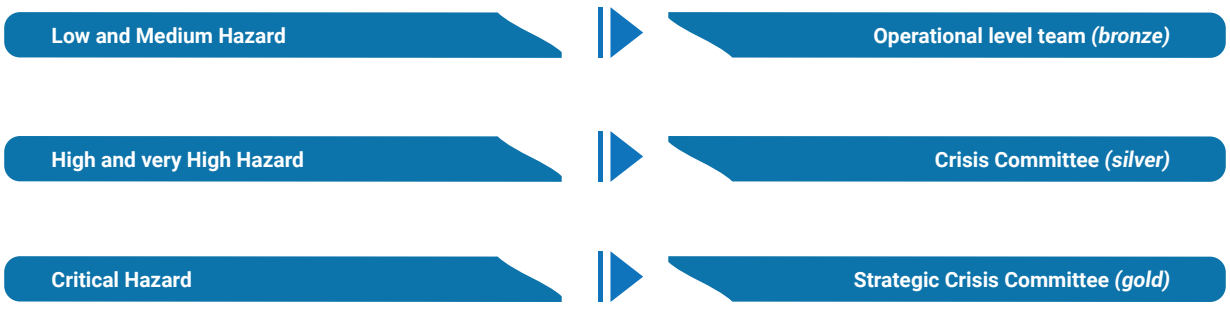


Figure 6. Crisis Committee by Level

In reality, low and medium hazard incidents do not require the convening of a crisis committee, because they do not present a situation that can be defined as a crisis. Under the direct responsibility of the CISO, the technical teams have sufficient knowledge to solve the problem from an operational point of view.

This configuration of committees is not exclusive; the constitution of one of the higher levels implies, in general, the maintenance of the activity of the previous ones. That is to say, in a critical category cyberattack, the top of the organization (CEO, General Management and previously designated members) will be the final decision-maker within the *gold* committee, according to the contributions of both the *silver* committee, composed - for example - of representatives of functional directorates and with probably more than one *bronze* team working on very specialized and specific operational aspects. In contrast, other cyber-incidents will only require the intervention of a *bronze* committee, and maybe with the occasional involvement of the *silver* committee.

When the organization is large, the size and complexity associated with its operations justifies the existence of the different levels of committees mentioned above, while small or medium-sized companies will have a single Crisis Committee.

In this sense, deciding which level of the organization and which structure to manage will contribute to determine the level of the incident/crisis (see table).

Established / Origin	Attribute	Level 1 LOW	Level 2 MEDIUM	Level 3 HIGH	Level 4 VERY HIGH	Level 5 CRITICAL
Other attributes of crisis management	Crisis declaration	No	No	Optional	Yes, of High Level	Sí, of Critical Level
	Area of crisis management / governance	No crisis committee required / IHR / Incident response team	It requires crisis committee / Bronze team	It requires crisis committee / SILVER TEAM	It requires crisis committee / SILVER TEAM	It requires crisis committee oh high management / GOLD TEAM

Figure 7. Management criteria

BP.4 Permanent control of the exposure area

A key element in crisis management is to constantly test the designed plans, procedures and configurations. This should be done through initiatives to assess the exposure area of entities, identifying vulnerabilities associated with their services and applications.

In this approach, the essential objective is to promote citizens' confidence in the use of electronic media, while promoting their use in a secure manner where the surface of exposure to cyber threats is measurable, controlled and adapted to the ecosystem in question: public sector, critical infrastructures, research centers, universities, health sector, etc...

A key element in crisis management is to constantly test the designed plans, procedures and configurations.

In short, to be able to measure security. If we measure, we can manage, and if we manage, we move towards a balance between the capabilities and functionalities provided by technology and the secure use of the same.

On the other hand, it should be borne in mind that dealing with a crisis is essentially a management exercise involving different types of human resources (physical intervention, resource allocation, internal and external communication, stakeholder management, coordination, etc.) and that for a team to perform adequately at the moment of maximum pressure, it must be well trained. It is therefore advisable to carry out periodic **simulations** of different types (operational or desktop) that subject their components to the management situations that real crisis will most likely impose on them, so that the team can practice in a simulated incident environment and make improvements that could be applied in a real situation.

BP.4

BP.5 Appropriate stakeholder management

Stakeholders are people or groups in the organization's environment that may be affected by any activity carried out by the organization. During a cyber crisis it is very likely that there will be interaction with some of them, either because they are an active part of the situation or because they are as much or more affected than the organization itself.

For this reason, it is advisable to develop a so-called **"*Stakeholder* Map"** where the different hierarchical levels of the organization should identify those who may be affected by the crisis.

The traditional concept of stakeholders included customers, suppliers and public authorities, in addition to the *shareholders* themselves. Today - and, once again, as a consequence of the ubiquity of communication possibilities and the weight of public opinion - additional groups must be considered according to three main areas and, of course, according to the activity of the organization:

Groups

- **Internal** ..... *members of the Board of Directors/shareholders, current and former employees by category and department; family members and trade union representatives.*
- **External** ..... *authorities and governments, regulatory and supervisory bodies, reference CERTs or CSIRTs[6], Spanish Data Protection Agency, customers, suppliers, patients, general public, investors, insurance companies, associations, competitors, prescribers, etc.*
- **Media** ..... *including traditional and online media (social networks, blogs, etc.).*

Depending on the incident, it will be necessary to review all stakeholders, their expectations and the strategy to be followed with each of them.

In the specific case of cyber-incidents, the Security Incident Response Teams **(CERTs)**, which provide support and management services for this type of event, are of **fundamental importance**. In some cases, and depending on the danger or impact on the organization, notification to the CERT of reference will be mandatory. For example, in Spain, all incidents classified as High, Very High or Critical[7], within the Public Sector, must be notified to the CCN-CERT, the National Cryptologic Centre. This classification is based on different criteria such as the type of threat, its origin, the systems and users affected or the impact that the incident may have on the organization[8].

6 CERT *(Computer Emergency Response Team)* and CISRT *(Computer Security Incident Response Team)* are terms used to refer to the same type of Teams or Capabilities. The term CERT is registered by the CERT Coordination Center (CERT/CC) so it is necessary to have their permission to use it.
7 Within a scale of five values: Low, Medium, High, Very High and Critical.
8 See: Classification/Taxonomy of cyber incidents. CCN-STIC Guide 817 Cyber Incident Management (ccn-cert.cni.es/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/988-ccn-stic-817-gestion-de-ciberincidentes/file.html)

Beyond this notification, it is **essential to be aware of their availability** and their r**ole in ensuring information security** both at the level of individual companies and the organizational and institutional framework of the country.

It should be borne in mind that since the mission of CERTs is to be a **permanent cybersecurity resource**, their knowledge and means of action are **constantly** being **updated**.

In this context, another key stakeholder is the **Competent Authority** managing cyber security at national level. As discussed in BP7 on Coordination, in certain situations organizations are obliged to report the incident. For this reason, it is good practice to plan this communication: the relevant body, the information to be provided, etc.

Another issue is the impact that a cyber incident generating crisis may have on a relevant supplier. The dependency on the supply chain shall be considered and, in certain cases, certifications or assurances should be required from suppliers regarding their protection against cyber-attacks. Figure 8 summarizes generic supplier management strategies on cyber security.

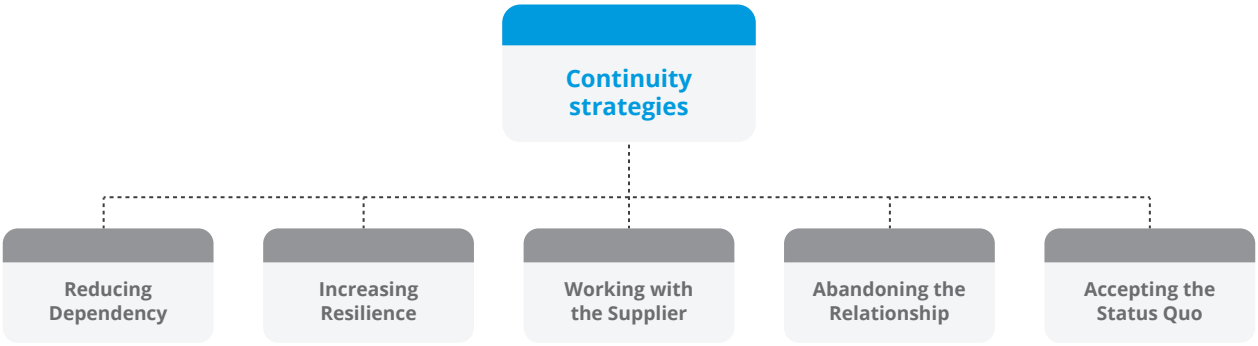


Figure 8. Strategies of Supply Chain Continuity

BP.6 Initial diagnosis and possible scenarios

The first step in the management and subsequent resolution of cyber crisis is to carry out a **diagnosis**[9] of what is happening. In the analysis of real crisis, it is very often observed that without an initial diagnosis, the organization shows erratic behavior during the emergency, loses initiative, lags behind events and suffers a clear loss of reputation.

Despite the fact that, in the early stages of the crisis, information is often confusing and incomplete, it is very important to understand what is happening and its possible effects in the short and medium term (possible scenarios). This exercise allows **prioritizing actions and making the first decisions**, and as more information becomes available, the process will be refined.

In the diagnose phase, it is also very necessary to classify the crisis in progress according to its perceived severity and possible impact so that subsequent management decisions can be anticipated. To this end, it is essential to **previously define an incident classification and escalation scheme**. This scheme should include severity and impact levels, as well as the evaluation and classification criteria to be used.

Annex 4 shows an example of **evaluation and classification criteria** that can serve as inspiration for such a design, taking as a starting point the classification of the Level of Danger and the Level of Potential Impact of the ICT Security Guide CCN-STIC 817 and the National Guide for Notification and Management of Cyber incidents[10]. Other concepts are added to the mentioned guides, as a suggestion, to help discern the nature of the crisis and the advisability of activating the respective crisis committee.

This first diagnosis should include the **initial notification to the CERT** of reference to receive support, specific indications and complementary and updated diagnostic and operational tools. All of this allows a rapid response that, in many cases, will either stop the attack in its entirety or significantly limit its impact on the organization and the affected business fabric.

Depending on the nature of the organization concerned and the type of incident that is occurring, there may be an obligation to notify[11]. the situation, in which case the competent authorities may request any information about the incident that they deem necessary for its resolution and for the minimization of its impact on national security[12].

9 If possible, it should be accurate, but it is more important to do it, as it is a prospective exercise that allows to anticipate action areas that by merely focusing on the problem won't be identified.
10 National Guide on Cyber Incident Notification and Management and the aforementioned CCN-STIC Guide 817.
11 By the NIS Directive, transposed into Spanish law by Royal Decree-Law 12/2018, of 7 September, for Essential Services Operators, or by the GDPR in case of data leakage.
12 In some cases, given the seriousness or the media situation of the cyber incident, the Permanent Cybersecurity Commission has been activated as the supreme body at national level where certain cyber incidents have been dealt with.

BP.7 Coordination

Coordination is the key to the successful resolution of a cyber crisis. Even organizations that have adequately prepared to deal with such a serious situation tend to improvise. **And improvisation and lack of coordination are ingredients in a recipe for failure.**

For this reason, having a **Crisis Committee**, as outlined above, with experience and management capacity is one of the first and most important steps to take during a crisis, as these people will be the ones to assume and assign responsibilities, competencies and resources to solve the problem.

This coordination is indispensable in decision-making and its implementation, as well as in communication tasks, which is why the figure of the Committee's spokesperson is so important.

In the most operational sphere, the figure of the **Chief Information Security Officer** (CISO) is fundamental, as he/she will be the focal point for this coordination as the point of contact for the operational action teams *(bronze*[13]), the **Crisis Committee** itself (*silver* or *gold*) and the **CERT of reference**.

On the other hand, in this context it is important to mention that cyber crisis frequently involve the loss of confidential information, the management of which is subject to the General Data Protection Regulation (GDPR). For this reason, it is good practice that, in addition to the CISO, the **Data Controller** is also directly involved in the resolution of the crisis, being part of the Crisis Committee to ensure that confidential information receives the appropriate treatment and ensuring proper coordination with the other members.

This coordination is to a large extent conditioned by aspects such as:

Aspects

- *The values of the organization and its culture, , i.e. that these values are shared.*
- *The prior work done to identify risks and determine action plans, which inevitably requires coordination.*
- *The degree to which the committee is exercised and its good team dynamics.*
- *The existence of a mature relationship with stakeholders, which facilitates coordination tasks with the different crisis actors.*

It can therefore be seen that **crisis management is a holistic discipline** that goes beyond the existence of specific tools and resources (crisis manual, committees, etc.) and is based on the **awareness of cyber risk** and a **general culture of coverage** of this and other identified risks.

13 See Annex 6 for definitions of types of committees.

BP.8 Initiative and proactivity

Analysis of a wide variety of cyber crisis shows that in many cases, cyberattacks find an organization lacking the tension to shift its priority from the day-to-day towards the crisis. It does not carry out a proper diagnosis and loses initial time, which, on the one hand, gives the attackers an advantage by not ensuring **the rapid intervention of the CERT** and, on the other hand, makes it lag behind events.

This implies the adoption of an **essentially reactive policy**, more focused on responding to criticism or pressure from the environment than on defining and communicating the strategy to solve the situation.

This is why it is so important that, at the first warning of a crisis, the organization **reacts quickly and decisively** by making an initial notification without undue delay and takes the initiative. It is therefore about the organization being proactive rather than reactive, making decisions quickly and positioning itself to take the lead in the crisis management.

One aspect that demonstrates initiative and proactivity in the face of cyber-risks is when the organization - in the event that it does not have its own resources - has previously agreed on rapid intervention by a specialized service company in the event of a cyber-attack. In this way, the response of the specialized company, which will know the organization's systems and protections, will allow - in coordination with the reference CERT - very rapid action, which is essential in this type of situation.

As discussed in BP-7 on coordination, the incorporation of the CERT's expertise in the response facilitates awareness and proactivity. This is evident in the cases described in the annexes.

BP.9 Unified discourse and official source of information

Once an incident is considered to have passed into the crisis category, it is essential to proceed with the preparation of the most appropriate information, taking into account: time or priority and stakeholder. Depending on these two parameters, and with the advice of the Communication department, the following will be defined: type of information to be offered, key messages, the format and the channel or medium (informal meetings, videoconferences, e-mails, distribution lists, calls, face-to-face interventions, speeches, shareholder meetings, *Dark Site*[14], messaging such as WhatsApp or Telegram, etc.)

It should not be forgotten that the best thing that can happen in a crisis is that the main source of information is the **organization itself**. For this to happen, it is essential for the company to be proactive and take the initiative, but without acting hastily. It is also very important that the Crisis Committee establishes clear messages that no one in the organization should deviate from, so that whatever format and channel is chosen, the information is the same, without contradictions.

It should not be forgotten that the best thing that can happen in a crisis is that the main source of information is the organization itself.

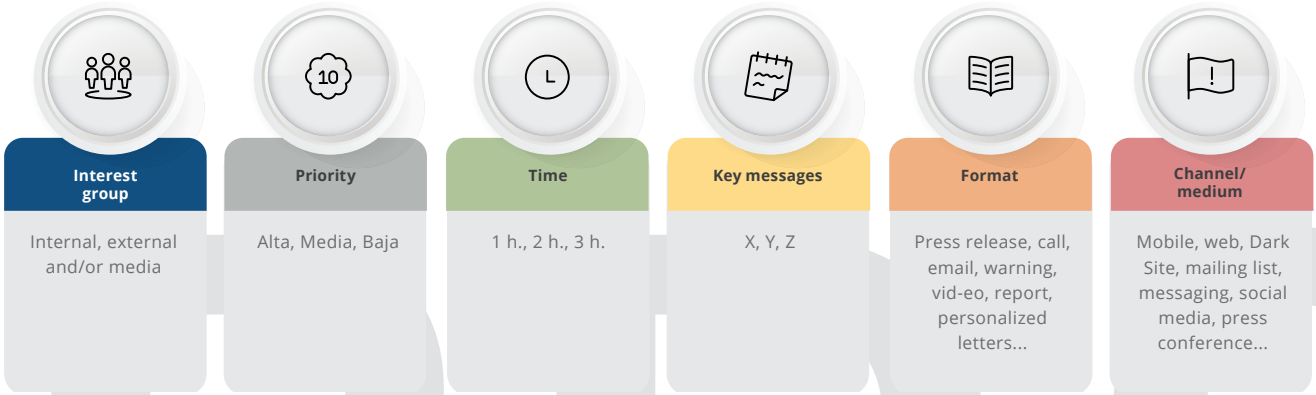


Figure 9. Example of matrix for crisis communication plannin[15]

14 Websites that have been prepared in anticipation of a possible crisis that could damage the image and reputation of an organization, but which are not publicly visible until a difficulty arises and it is decided to put them online. Its objectives are:
Be prepared to react immediately in the event of crisis.
Protect and maintain the normal functioning of the organization's website.
Have one place accessible to all the parts involved in a crisis (journalists, authorities, family members, etc.).
15 Carles Montaña, "Crisis Communication Workshop".

Dichos mensajes deben tener las siguientes características:

- *Never deny reality. Never lie and be transparent.*
- *Always give the organization's side of the story, positioning itself as the most credible and accurate source of information.*
- *Convey confidence. Act with serenity, firmness and professionalism.*
- *Demonstrating careful attention, respect and total commitment to all those involved.*
- *Apologizing and taking responsibility if necessary (not blaming others).*
- *To highlight the value of the actions taken.*
- *Ensuring that the activity/business is viable.*

Proactivity and unified discourse

Therefore, **proactivity and unified discourse** are very important components of the communication policy that must take into account not only external information (media, web, social networks, etc.) but also that this unified message is also practiced internally, among the staff, suppliers and/or customers. It must be borne in mind that, in the event of a crisis, any employee can act - voluntarily or involuntarily - as a source of information about what is happening.

In the case of cyber-incidents, special consideration must be given to the need for a **balance between open external communication** - which can alert the attackers that the attack has been discovered and action is being taken, which may not be desirable at first - and s**haring it quickly with the CERT of reference** who, in turn, will coordinate with other national and international organizations and agencies.

Therefore, it is important to design a **unique discourse** and, at the same time, to modulate the rhythm and cadence of communication.

BP.10 Transparency, empathy and accountability

As noted above, lying, biased reporting, silence or passivity are the worst communication options in the event of cyber incident. To protect the reputation of the organization, uncertainty must be avoided. This attitude is also relevant for the rapid notification to the CERT of reference as this results in overall benefit.

In general, a mature society can accept that things do not always work as desired and that imponderables may arise in any organization. What is not understood, nor is it accepted, is that those in charge do not react in time or inadequately.

Maintaining transparency during a crisis is not easy, but the damage can be offset or minimized by adopting an **open and accountable policy** that, while it may raise criticism in the short term, will ultimately lead to an improvement in the organization's credibility and reputation.

This approach does not mean that absolutely everything has to be told. As a general rule, it is necessary to gain time until the extent of the situation is better understood. Therefore, any communication shall avoid mentioning the causes of the incident, the person responsible for it, information that the investigation may reveal or the possible consequences for the organization or another stakeholder.

Any communication shall avoid mentioning mentioning the causes of the incident, the person responsible for it, information that the investigation may reveal or the possible consequences for the organization or another stakeholder.

BP.10

BP.11 Valorization of the actions implemented

Crisis have many moments when, despite the intense work and the many simultaneous actions being carried out, no results can be presented to the public and stakeholders.

In the context of proactivity and transparency described above, this is a good time to **highlight all the measures taken** so far by the organization, both preventive (coordination with the CERT and other institutions, development of previously designed plans, investment in resources) and corrective (intervention teams, crisis committees, subcontracting, execution of contracts, review of protocols, etc.).

In this way a multiple message is conveyed:

Multiple message

The organization is concerned about its immediate environment and its stakeholders, which is why it has prepared in advance and has protocols for action, a crisis committee, etc.

Although concrete results are not yet available, every effort is being made to achieve them through the deployment of means and resources, as planned.

The organization is working closely with other agencies, institutions or authorities for early resolution.

Therefore, the company is doing everything in its power to resolve the situation and, under these conditions, it will certainly succeed.

In short, **any crisis represents an opportunity** to demonstrate the organization's ability to deal with a complex situation, showing that the disruptive event is being properly managed.

BP.11

BP.12 Formal closure of the crisis

The crisis does not end with the crisis. In many cases the pressure of day-to-day life means that these events are not closed in the most appropriate way. The main practice for a correct closure is to dedicate time and resources to assess the damage and, above all, to collect **lessons learned** and implement them in the reality of the organization, as well as to communicate the closure, both internally and externally.

Therefore, carrying out the **relevant analyses**, drawing **conclusions**, **defining an action** plan and **monitoring its implementation** are indispensable steps in closing the cyber crisis and are often only half-finished.

Subsequent communication about the activities that were carried out and about the formal closure of the episode is a good way to convey the message to both *stakeholders* and the general public that **lessons have been learned** and that the organization is better prepared for the future. It is also a good time to **show gratitude** to any person or institution that assisted in the resolution of the situation.

This communication is not only relevant externally, but also makes sense **internally**. In this way, messages of appreciation for the work done and of the importance of being prepared for such situations are sent, which enhances the alertness of the members of the organization.

The crisis does not end with the crisis.

BP.12

BP.13 Implementation of lessons learned

This good practice is closely related to the previous one and, in fact, is an extension of it. In any case, we would like to emphasize the need to summarize what has happened, synthesizing it into **concrete actions to be implemented**. As indicated, on many occasions, day to day may hinder detailed analysis, and the immediate adoption of the most urgent and necessary measures may lead one to think that conclusions have already been drawn from what has happened and that action has been taken accordingly.

This attitude is a very superficial reaction; it is necessary to develop in-depth analyses and **improvement plans with concrete objectives and measurable evolution**, avoid sticking with the most immediate cause-effect relationships (e.g. "it was a human error" but why did the person make a mistake?) but also look for **systemic origins** of the problem that can be related to existing legislation (so, should we go beyond what is merely normative? should we look for new collaborations with the regulator?), to abandoned good practices (why did we stop doing that?), to inadequate communication structures (why didn't they understand us? did we explain ourselves correctly?), etc.

Not settling for **simple explanations** is a characteristic that is part of the values of a resilient organization and, at the same time, a necessary condition for achieving resilience.

In short, crisis should be treated as a source of organizational learning, drawing lessons from what has happened through in-depth analysis and adjusting future action and investment plans accordingly.

BP.13

5. Conclusions and recommendations

The different cases described in the annexes reflect the crisis management from the CCN-CERT's point of view in a way that clearly shows how to deal with a cyber crisis and the importance of having adequate technological support.

As a synthesis of the cases, the **following main conclusions** can be drawn:

- In order to manage a hypothetical crisis, it is necessary to have foreseen it, to have a Crisis Committee and different plans and manuals for it, and even to carry out exercises or simulations.

- There is insufficient awareness of the importance of information security in organizations, either because it is not among their priorities or due to a false sense of security caused by the availability of resources (systems and protections) which turn out to be insufficient.

- In many cases, there is not a person who clearly assumes the role of Information Security Officer. This role, whether in-house or external, is indispensable in today's world.

- It is essential that the organization's senior management is aware of the overall threat, the potential impact on the service and the level of preparedness and therefore, its shortcomings.

- Investment in cybersecurity should be a priority for organizations. Despite the difficulty in calculating the exact financial return (as with any investment in security, whatever the type), given the increasing frequency of cyber-attacks and the great impact they have both on the services provided and on the organization's information and reputation, it should be done.

- In this context, it is necessary to have systems that, while protecting, facilitate attack management (firewalls, SIEM, EDR), as well as the availability of human resources (in-house or external) for the permanent supervision of the network.

- Prompt notification of a cyber-attack to the relevant CERT is a critical step in resolving the incident and minimizing its impact.

- Training and awareness of the organization's staff is essential. Many attacks can be prevented if IT staff are aware of the risks involved and the threats to the organization.

- Communication is key to the correct management of a crisis. The organization shall previously identify all the interest groups or stakeholders to whom it is necessary to inform and it shall know what to say and how to say it at all times. This requires a single discourse shared by the different members of the organization, showing total transparency while assuming responsibilities if necessary and highlighting the value of the actions performed.

- The "information security" factor must be taken into account in any strategy adopted by the organization. The massive adoption of teleworking during the Covid-19 crisis is an example of it, as not everyone took into account the risk of working from home. This led to a higher incidence of threats.

Annex 1.
Cyber espionage case study

The geopolitical situation of recent years marks a growing trend in cyber espionage operations. These capabilities are made up of the so-called APT (*Advanced Persistent Threat*) groups, which consist of highly specialized personnel with extensive technical knowledge and financial and material resources, who carry out intrusions into targeted networks in order to remain hidden for as long as possible while they extract information from them. This capability is targeted at both the public and private sectors, and usually comes from countries wishing to improve their political, strategic or economic position.

In short, cyber espionage is a specific and targeted cyber attack that tries to be as stealthy as possible and to stay as long as possible, unlike cybercrime which is noisier and seeks short- and medium-term financial gain.

What does usually happen in such a crisis?

In the most common case, attackers send targeted emails to trick users into opening the malicious attachment or link. In this way, they manage to infect the user's computer which allows them remote control of the machine and, once inside the network, they keep advancing. To do this, they execute additional commands and/or tools that seek to obtain credentials of users with administrator privileges in the domain and thus take complete control of the attacked organization's network.

It may also be the case that the APT group has obtained legitimate remote access credentials to the victim's systems, such as VPN or remote desktop sessions.

Once the attacker has managed to penetrate the target network, he/she carries out reconnaissance work to detect where the information of interest to him is located and how he can access it. This information theft can be done using the same malicious code that infected the recipients of the email or through alternative routes, such as email or cloud services on the internet, to make its detection more difficult.

Normally, the attacker's modus operandi makes it very difficult to detect him, as he seeks to stay for long periods of time within the targeted network in order to steal as much information as possible.

Detection of such attacks

In a large number of cases, the intrusion is reported by third parties to the organization. However, it is possible that the intrusion is detected by the victim organization when inconsistencies or strange behavior are found on the network.

Objective

The objective of this type of attack is usually the theft of information, technology or any kind of documentation. It is important to note that the activity of APT groups is not limited to their victims, but they also compromise other systems to use them as part of their attack infrastructure, either as command and control servers or as hop and/or management machines.

What should an organization do in such situations?

Preventive measures to avoid such attacks:

As a general rule, it has been observed that, in order to penetrate systems, APT groups obtain access credentials through phishing techniques or, increasingly, by obtaining credentials available on the internet and the dark web.

This is successful, in part, due to the **malpractice of password reuse** by users. Obtaining such credentials does not require sophisticated operations. In the end, human error is the main entry point. For this reason, it is essential to implement robust policies that include the regular change of passwords, as well as to raise awareness and sensitize the employees about the main threats and procedures that cyber attackers use to achieve their goals.

Training and awareness-raising of the organization's staff is also essential. Many attacks could be prevented if the staff that works with computer systems was aware of the risks involved and the threats to the organization.

Recommendations in the initial phase of crisis management

Recommendations

Act promptly. The rapid notification of a cyber-attack to the reference CERT is a fundamental step for the resolution of the incident and impact minimization. It should be noted that this type of incident is usually classified as Very High and Critical due to its serious impact on the organization and, therefore, in the case of the Spanish Public Sector, it is mandatory to report it to the CCN-CERT, as mentioned above.

A meeting should be held with the information security officers.

The company's management must be notified and kept informed of progress in the investigation.

Meeting of the Crisis Committee previously set up for this purpose. This group will be responsible for managing the situation and implementing the plans put in place for this purpose.

Actions taken in the management of this type of crisis:

The first steps in the management of this type of crisis is to **detect when the attacker has been stealing information** in order to assess the breach generated. To do this, in most cases, the following actions are carried out:

Actions

*The incident response team **will analyze** available **logs**, primarily from perimeter security equipment with the corporate firewalls and browser proxy. At this point it is important to note that many organizations delete logs regularly and therefore complete information may not be available. **It is** therefore **recommended to increase the log retention capacity**. In some cases, intrusions are discovered a long time after attackers accessed the network, so having as many logs as possible helps to identify the source of the infection and to reconstruct the attackers' actions since then. **The organization's security team should continuously review these logs in order to detect anomalies**.*

- ***The first step requires the organization to communicate internally** with ICT staff. It may happen that, for the deployment of specific tools or access to the logs of specific systems, the incident response team investigating the incident may need the support of the organization's ICT staff. For this reason, and in order to avoid delaying the timeframe, the organization in question must warn these teams about this situation and inform them of the need to send the information requested and necessary to carry out the investigation as soon as possible.*

- ***Network diagrams and schematics** will be essential to uncover new clues as the investigation progresses. It should be borne in mind that analyzing the network for strange movements of information between computers is time-consuming. It will also be necessary to install specific tools.*

Actions

- *While prompt action is recommended, **trying to mitigate the situation too quickly could be a main failure of an organization in this situation**. The attacker must feel safe to act normally. This is the only way to gather evidence and to know how far he/she has accessed the network, and where he has deployed backdoors or other mechanisms to access the network.*

    - *The CCN-CERT has verified the criticality of this aspect in different situations of this type. If the attacker is aware that he has been discovered, he may choose to cease his activity temporarily or use other means of access unknown to the incident response team, which greatly complicates the investigation. Changing mail access credentials is not sufficient to resolve such an incident, for example.*

    - *This results in a complex situation: on the one hand, it takes time to find out to which extent the attacker has control of the network; on the other hand, the representative of the organization wants to correct the security breach as soon as possible.*

    - *At this point it is essential to **manage time** to thoroughly investigate how far the attacker went, his knowledge of the network and his various plans to stay inside. It is necessary to install monitoring tools and have time to study the situation.*

- *Once the scope is known, a detailed mitigation plan is drawn up, which must be approved by the Management.*

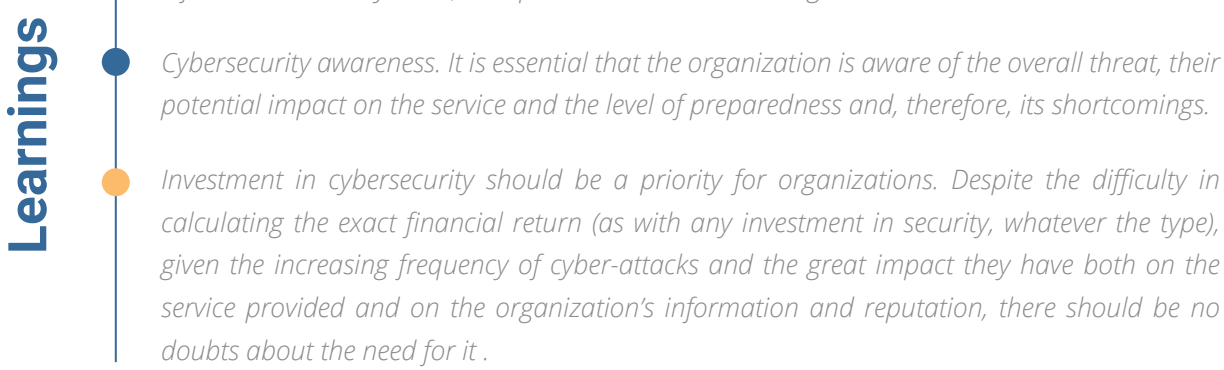
    - *At this point, it should be borne in mind that too early mitigation without sufficient investigation time means that it is not possible to perform the necessary clean-up of the attacker's various plans.*

    - *The mitigation plan should be as radical as possible and should be executed on weekends to try not to affect the normal functioning of the organization. This way, in general, systems are not affected and there are no changes to the employee's activities: no services are down and no systems are blocked. No obstante, una vez que se decide ejecutar el plan de mitigación los empleados tendrán que cambiar sus credenciales de acceso, después de que se haya actuado.*

    - *However, once the decision is made to implement the mitigation plan, employees will have to change their access credentials after the action has been taken.*

    - *It may happen that the management does not approve the mitigation plan and decides to take insufficient measures, which could lead to a new attack in the future or even to the attacker remaining active and maintaining access to the attacked network.*

Learnings



- *Organizations should keep the network diagrams and schematics constantly updated.*
- *It is not enough to have extensive security measures in place in an organization. Resources and personnel must be dedicated to monitoring suspicious activity on an ongoing basis.*
- *It is important for the organization to create a network monitoring team that becomes the information security team, with permanent tools and budget.*
- *Cybersecurity awareness. It is essential that the organization is aware of the overall threat, their potential impact on the service and the level of preparedness and, therefore, its shortcomings.*
- *Investment in cybersecurity should be a priority for organizations. Despite the difficulty in calculating the exact financial return (as with any investment in security, whatever the type), given the increasing frequency of cyber-attacks and the great impact they have both on the service provided and on the organization's information and reputation, there should be no doubts about the need for it .*

Annex 2.
Ransomware case study

Ransomware has been the most destructive type of malicious code in the last decade. It started affecting personal computers, and it has become a major threat to businesses and critical infrastructures (hospitals, energy infrastructures, etc.).

In recent years, the capabilities of this malware have evolved from encrypting user machines to blocking complex networks with heterogeneous technologies, which are present in the large companies and structures of a country.

The popularity of this type of malware, as well as the growth of its variants, is due in part to what is known as Ransomware as a Service, a service whereby criminals create this malicious code on request, in exchange for a percentage of the campaign's profits.

Sectors such as pharmaceuticals, finance and commerce have been the favorite victims of cyber-criminal groups in recent years, in which, in addition to the theft and leak of information, they have also caused the disruption of activity by infecting the network with ransomware. Moreover, the attackers use extortion techniques after infecting the network to monetize the attack by demanding a ransom to prevent the release of the stolen information and/or to decrypt the files affected by this malicious code.

In this regard, it is important to note that making a payment to a criminal group does NOT guarantee the victim that their data will not be published or sold on the black market.

What usually happens in such crisis?

Traditionally, this type of cybercrime was very noisy; short-term financial gain was sought. Nowadays, however, large cybercrime groups act according to a more sophisticated modus operandi, trying to colonize the network in the first instance, locating the victim's vital assets, stealing valuable information for further extortion and, finally, deploying ransomware that makes access to the information impossible.

Detection of such attacks

In most cases, the victim is aware that he or she has suffered a ransomware-related attack because of the inability to access multiple files from multiple computers or the disabling of several of his or her essential services.

Objective

The main objective of cybercrime is to monetize the infection in several ways:

- Extorsión directa hacia la víctima amenazando con la publicación de la información sensible sustraída.
- Disruption of the availability of information and the provision of vital services to the affected party. The attacker will offer the key to decrypt the information in order to restore the organization's operation.

What should an organization do in such situations?

Preventive measures to avoid such attacks:

To prevent this type of infection, it is usually recommended to follow security policies at the domain level which, for example, disable the execution of macros in office documents (Emotet's main means of infection) and of Powershell on all computers that do not require it (thus partially limiting the attacker's execution of a multitude of tools)[16].

Likewise, it is also recommended to establish policies at the network level that allow granular control of the connections between the different points and computers within the network, thus giving the security team greater visibility and traceability of all the events generated, detecting in a timely manner anomalous activity that could denote a malfunction or a possible intrusion in the network.

Similarly, prior awareness and sensitization of the staff is vital to prevent the success of such attacks.

Recommendations in the initial phase of crisis management:

Recommendations

- *Act promptly. Prompt notification of a cyber-attack to the CERT of reference is shown to be a fundamental step in resolving the incident and minimizing its impact. The urgent establishment of a communication channel with the CERT is key to start managing the security incident.*
- *A meeting should be held with the information security officers.*
- *The company's management must be notified and kept informed of the progress in the investigation.*
- *Meeting of the Crisis Committee that shall manage the situation and implement the plans previously created. This group will decide on the actions to be taken and whether the situation requires the formation of a dedicated team.*
- *An initial assessment must be made on the state of the network, equipment, assets and services that make up the network.*

16 For more detailed information, we recommend reading the following reports: CCN-CERT BP/04 Ransomware and CCN-CERT IA-11/18 Security measures against ransomware (https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos.html?limit=25&limitstart=25).

Recommendations

It is often very useful to draw up a diagram of the architecture of the computer systems in order to know the situation at the time the investigation is started. In addition, all affected equipment should be inventoried, so that it is clear which critical information and services have been compromised.

Draw up the Stakeholder Map and clearly define who should be notified of the incident. Both employees and all the organization's external connectivity (customers, suppliers, users, etc.) should be notified immediately to avoid the danger of collateral infections. Depending on the scope of action of the affected party, whether it is a public body or a private company that offers IT services to third parties, for example, it will be necessary to consider scenarios in which, after appropriate communication with the affected parties, the access that connects the victim with the rest of the entities will be blocked.

It is possible to imagine the case of a city council that provides citizen-facing services, such as access to municipal data (census, telematic procedures, etc.), and that after falling victim to a ransomware infection it has to review the resources that are publicly accessible and that may contain harmful code that could spread the infection.

Likewise, some public bodies delegate certain tasks such as payroll or personnel management to third party companies, with which they share network resources, remote desktop access, VPN tunnels, etc. It is essential both to block these accesses to prevent the spread of malware and to alert the third party in order to prevent or mitigate at an early stage any collateral infection they may have suffered.

In the case of MSPs (*Managed IT Services Providers*), the need to contact all their customers and partners is even more critical in order to avoid a total collapse that could magnify the ultimate impact of the infection.

Actions taken in the management of this type of crisis:

Actions

Containment of the threat

It is necessary to contain the propagation of malicious code through the network (encryption of shared folders, lateral movement to equipment with visibility, etc.) to prevent a potential remote attacker with access to the systems from continuing his activity (information leaks, deployment of additional backdoors, elimination or destruction of evidence, etc.). To do this, depending on the volume of equipment affected in the network and its nature, the connections will be blocked physically (disconnecting the network cable) or logically (blocking at Firewall level).

If the victim organization's firewall does not effectively segment the different subnets located in the pool, an attacker that gains access to one of the organization's systems could access all computers. To remedy this, the network segmentation is redesigned together with the organization's system administrators, fortifying the existing policies in the Firewall, and adding an additional firewall to increase the level of security.

The speed with which action is taken to stop the infection and avoid a more severe impact is key to resolving the incident. Likewise, involvement at all levels within the affected company, from the technical team to senior management, will allow to obtain results from the outset.

Threat detection

The next step after the containment phase is to determine which computers have been affected by the malicious code, which the attacker may have used to pivot through the network or to encrypt and/or delete their content.

At this point, in cases where the CCN-CERT collaborates in the resolution of the incident, the Early Warning System (EWS) is installed in the organization's Internet gateway to detect, based on the patterns known by the CCN-CERT, if there is traffic categorized as malicious on the network, so that timely action can be taken to locate and subsequently neutralize the threat.

In parallel, while the forensic analysis of the affected computers is being carried out, the malicious code samples found are sent to the reverse engineering specialists, who shall find out which is the functionality of each malware sample. This point is fundamental to characterize the threat, to know its capabilities, what persistence points it establishes in the systems, whether it consists of malware or tools used in other incidents, etc

Threat mitigation

In addition to redesigning the network by segmenting the different environments and restoring the affected equipment (mail service, Domain Controller, database server, client equipment, etc.), all the equipment is updated, focusing on those services exposed to the Internet, which are the most susceptible to vulnerability.

In this type of attack, the Mimikatz tool is commonly employed during a network intrusion to obtain the local and domain credentials cached on the infected computer. If the cached credentials on the infected computer are the same on the rest of the domain, it is assumed that all computers have been potentially compromised. The solution is to reset the domain credentials, after rebuilding the Domain Controller together with the Active Directory (AD). It is also recommended to review and remove those users with administrative privileges that may have been created by the attacker.

Therefore, to effectively mitigate the threat, and in order to prevent future cases of similar infection, it is suggested to change all credentials in the domain, both in the infrastructure exposed by the company or organization in the cloud (webmails, VPN access, etc.), and internally (Active Directory, local administrators, etc.). Likewise, in this phase, which implies reviewing and cleaning the equipment pool, it is important to introduce the concept of a clean network in order to keep proper control of the assets that have not yet been reviewed, those that are infected, and those that have already been cleaned.

This logical network will be created on an internal address different from that of the main network, and it will be isolated using a firewall, for example, and its function will be to progressively host each and every one of the computers from the main network that have been checked and cleaned. This way, a suitable separation is obtained that will allow the network to be rebuilt without the risk of reinfection.

Actions

Information and services retrieval

After a security incident that involved the encryption and erasure of assets, it is essential to determine the extent of the impact, assessing what information can be recovered and what services have been affected.

In some cases, it is possible to recover much of the information that has been encrypted, using isolated, unaffected backups and through forensic work. In addition to this, it is necessary to reconstruct the organization's essential services that may have been damaged, seizing the opportunity at this point to perform a clean and secure installation that allows clearer monitoring and traceability by the security team.

Learnings

Learnings

- *Incidents such as these make it clear that investment in security is a necessity. Unfortunately, on many occasions, it is only when incidents of this relevance take place that top management begins to pay attention to requests for more security personnel, who can monitor and maintain systems and networks. It is necessary to have a prepared security team, with the appropriate material resources, who proactively carries out network audits and raises awareness among all users who make use of technical resources.*
- *It is essential to equip the organization with security systems such as firewalls, SIEM, EDR, etc. in order to ensure security in a more agile manner.*
- *However, it is not enough to have dedicated IT security staff or physical means to implement the relevant measures, a deep awareness on the part of top management is also required, so that in extraordinary situations such as teleworking, appropriate procedures are put in place to ensure that work is carried out with the same security guarantees as when working from the daily workstation.*
- *In general, the experience of recent years shows that there is a lack of a culture of security among the top management of organizations and companies..*
- *In the world of IT security, while it is almost impossible to prevent an intrusion (either due to the lack of knowledge of all the vulnerabilities that are not public, or because the user is the weakest link in the chain), the means and people must be available to detect as quickly as possible that an attack is taking place, so that a potential critical incident can be managed at an early stage.*
- *Attempting to resolve an incident in a company or organization with a large equipment pool too quickly can lead to hasty technical decisions. It is important not to overlook possible additional backdoors deployed by the attacker that would allow him to re-infect the network in a short space of time.*
- *Working on-site from the outset with the affected organization and having a team of people who are clear about the steps to be taken to deal with the incident is the key to succeed in resolving the incident.*

Learnings

- *Coordination between all those involved is essential to be able to explain research progress in a simple and timely manner.*
- *These incidents highlight the need to review network design, security policies and the method of teleworking applied.*
- *All companies, and in particular those in the field of critical infrastructure or essential services, need to keep maturing in the field of IT security in order to avoid security incidents that could ultimately seriously affect the service they provide.*

Annex 3.
Case study of Attempted Theft of Funds

The attack group known as "Carbanak/Cobalt Gang" is named after the malicious code it used in its attacks: known as Carbanak until 2014 and Cobalt Strike Beacon[17] from 2015 onwards. This group has been active since at least 2014[18] and is estimated to have stolen at least €1 billion from banks worldwide by 2019. Initially, its activity focused on Russian and Ukrainian banks, but given the profitability of its attacks, it soon expanded its illicit activities to the rest of the international banking sector.

17 https://www.cobaltstrike.com
18 Kaspersky Labs - "Carbanak APT, the great bank robbery".

What usually happens in this type of crisis

For some years now, technically savvy cybercriminal groups have been carrying out targeted attacks. Once they have penetrated the network and gained control of its systems, the attackers transfer funds to accounts controlled by themselves at other institutions.

To do so, they use tactics, techniques and procedures (TTPs) more typical of state-sponsored actors engaged in cyber-espionage (known as APT groups). Although the motivation of the attack is not to obtain information but to make money, cybercriminals carry out similar actions to those of APT groups in the networks under attack: thorough reconnaissance work to identify the assets of interest and learning how the entity's employees operate them. In this way, they can replicate their actions and remain unnoticed.

What should an organization do in such situations?

Preventive measures to avoid such attacks:

Measures

- *Staff awareness: Many attacks can be prevented by making IT staff aware of the risks involved and the threats to the organization.*
- *Creation of a dedicated team to handle the situation.*

Recommendations in the initial phase of crisis management:

Recommendations

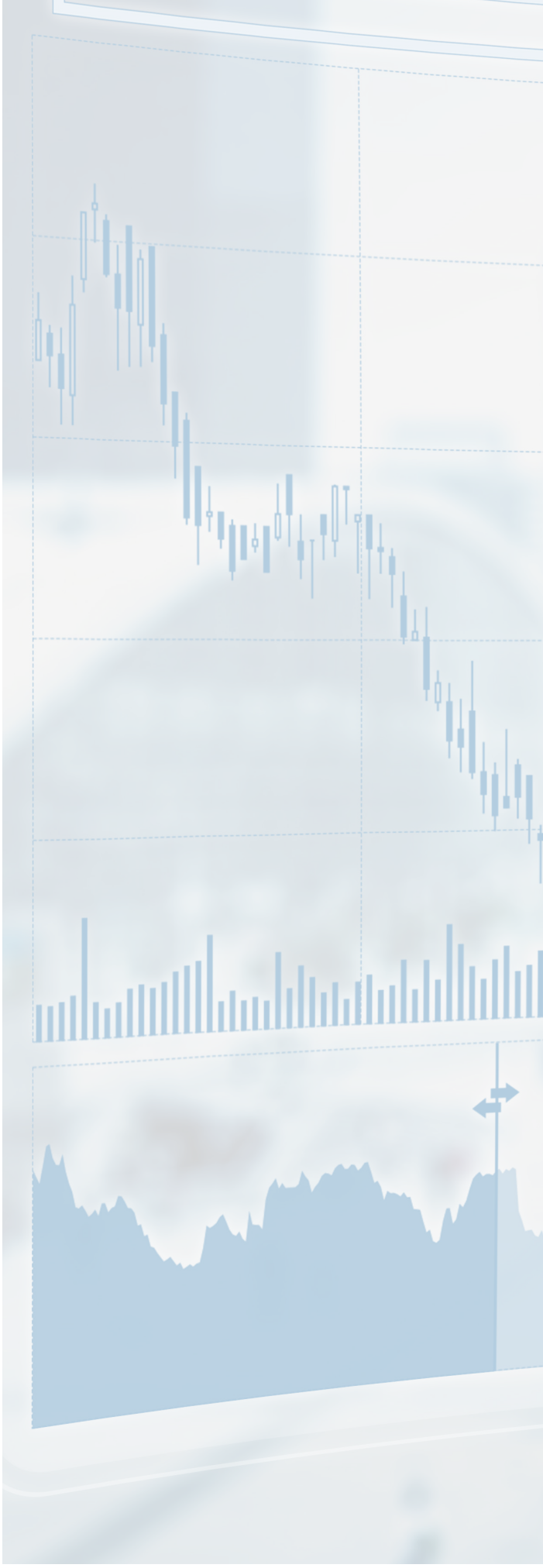
- *Act promptly. Prompt notification of a cyber-attack to the CERT of reference is a fundamental step in resolving the incident and minimizing its impact. The urgent establishment of a communication channel with the CERT is key to start managing the security incident.*
- *It is essential to prioritize all tasks related to the investigation with the support of Management, to act promptly and to set up a dedicated team to handle the situation, which is crucial to deal with this type of attacks. The full and sincere cooperation of the victim is crucial too, as it is their staff who know the network, which systems are part of it, etc.*
- *In addition, the creation of a crisis cell at the corporate level, involving the minimum essential staff, is often a positive step. This is important in order to avoid information leaks when rumors start to spread. The cell should report in real time to Management on the status of the investigation and the measures being taken. This point is crucial, as the support of Management is essential for the information to flow and for the investigation to be successful, especially in this type of investigation in which an external entity requests very sensitive information about the network.*

Actions taken for the management of this type of crisis:

Firstly, the machines that are making or have made connections to the command and control servers are identified in order to carry out a forensic analysis and thus find out what tools and TTPs the attackers are using. These analyses reveal that this type of attack uses *spear phishing* as an infection vector.

In most cases, the malicious email contains a Word attachment that, once opened, would exploit various Microsoft Office vulnerabilities and infect the user's computer with *malware* that provides attackers with control over the machine.

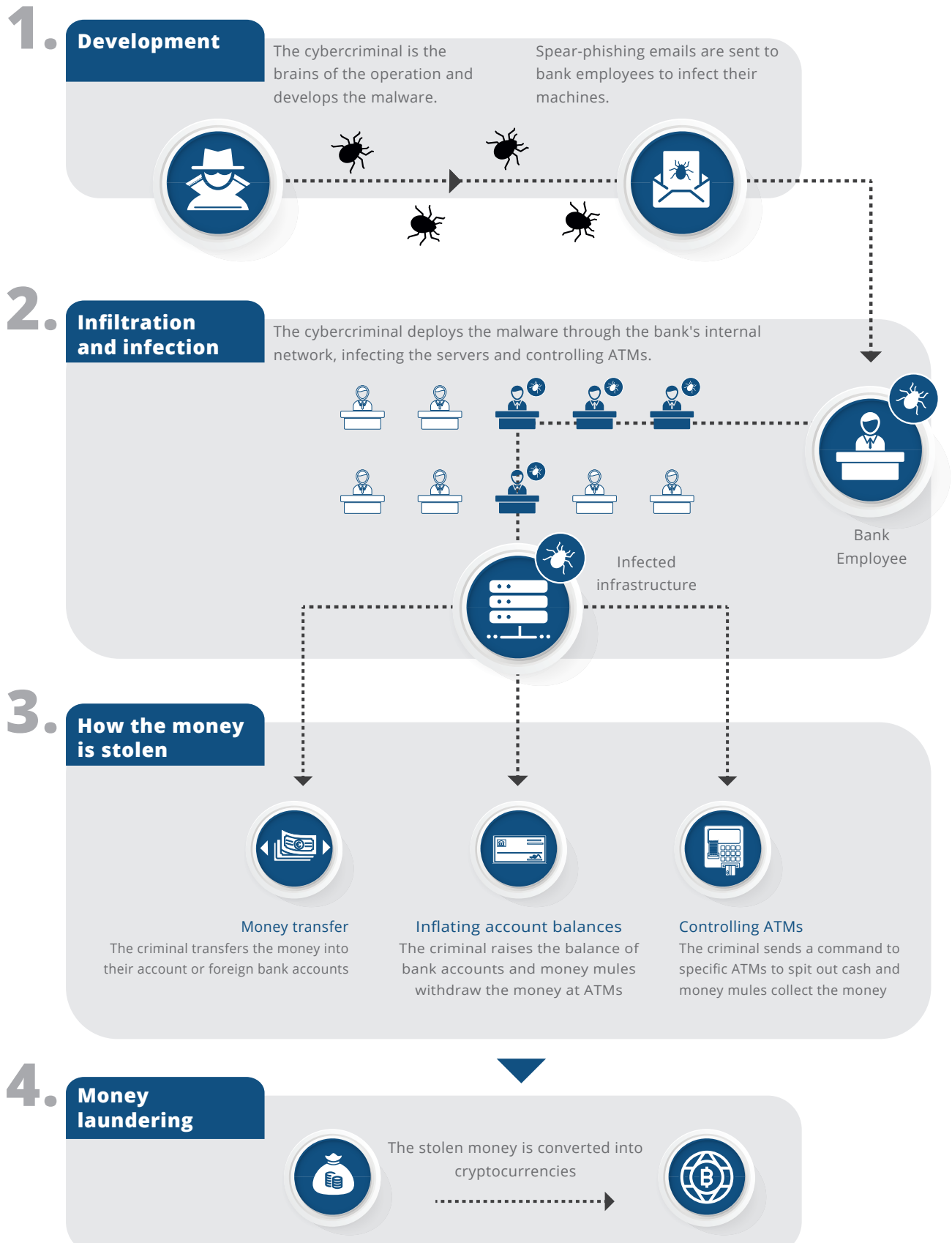
The installation of the malware gives the attackers full access and control over the machine. Once the attackers access the network they quickly progress through it and in a very short space of time they may obtain user credentials with network administrator permissions, allowing them to move around freely and install their tools without any problems.



The attack would follow the pattern shown in the Europol's chart below:

Carbanak / Cobalt

How it works



Once the full scope of the incident is defined, the containment and mitigation phase is started, in which the following actions are taken:

Actions

- *Disconnection of the main servers, which paralyses the organization's activity for a few hours. This point is important as measures must be taken while the attacker does not have access to the network.*
- *Reinstallation and re-platforming of all affected non-critical equipment. On some servers this is not possible and a manual clean-up is performed, removing malicious code and modifying the configuration to secure them properly.*

Learnings

Lessons learned at the technical level are:

Learnings

- *The need for a dedicated security team: constant monitoring and vigilance is essential to prevent this type of attack. Security must be dealt with proactively, not reactively. An organization without such a team, will not be able to detect the intrusion in its early stages.*
- *Increase log retention capacity: In some cases, intrusions are discovered when attackers have been inside the network for a long time, so having as many logs as possible helps to identify the source of the infection and to reconstruct the attackers' actions since then. It is the task of the aforementioned security team to continuously review these logs to detect anomalies.*
- *Network segmentation: this can limit attackers' access if they infect a user performing a non-essential task.*
- *Application of the principle of least privilege: users must have the permissions strictly necessary to carry out their functions.*
- *Staff awareness: Many attacks can be prevented if IT staff are aware of the risks involved and the threats to the organization.*

Learnings

Lessons learned for crisis management are:

- *Report to management, as soon as possible, clearly, and with the maximum transparency and information available. Their support is essential to take decisions and implement the actions required.*
- *Formalization of the crisis management cell/structure: it is essential to know "who to call" at any given moment.*
- *Maintain control over the information, establish secure channels to deal with the ongoing incident so that the attacker does not know that he has been discovered until it is possible to stop him from accessing the network.*
- *Most of the time, organizations have a false sense of security. They have a large number of security products, but do not have the right staff to manage and exploit them, so they hardly take advantage of them.*

Annex 4.

Guidance on levels and criteria for assessment and classification of cyber crises

Established / Origin	Typology of impacts	Attribute	Level 1 LOW
CCN-STIC 817	External	Affecting national security	---
	External	Affection public security	---
	Internal	Affecting critical infrastructure/ essential service	---
	Internal	Affecting systems	Affects the organisation's systems
	Internal	Service interruption	Interruption of the provision of a service
	Internal	Resources in working days by employee	The cyberincident requires less than 1 person-day to resolve
	Internal	Economic impact	Between 0.0001 % and 0.002 % of current GDP
	External	Geographical coverage	More than 1 AC
	External	Reputational impact	Punctual, no media coverage
OTHER CRISIS MANAGEMENT ATTRIBUTES	Internal / activity / operations	Affecting critical processes	No impact on critical processes
	Social	Affecting stakeholder relations	Stakeholders' expectations and trust are not affected.
	Social	Social alarm	No alarm
	Economic	Damage to third parties / environment	No damage to third parties / environment
	Economic	Economic losses (estimate)	No or negligible losses. Cost within acceptable budgetary parameters
	Legal	Legal implications	No implications
	Management	Crisis declaration	No

Level 2 MEDIUM	Level 3 HIGH*	Level 4 VERY HIGH*	Level 5 CRITICAL*
---	---	Significantly affects official activities or missions abroad	Significantly affects national security
---	---	Affects public security with potential danger to material assets	Affects public security, potentially endangering people's lives
---	---	Affects an essential service	Affects critical infrastructure
Affects more than 20 % of the organisation's systems	Affects more than 50 % of the organisation's systems	Affects classified systems RESERVED	Affects classified systems SECRET
		Affects more than 75 % of the organisation's systems	Affects more than 90 % of the organisation's systems
Interruption in service provision of more than 5 % of users	Interruption in service provision of more than 1 hour and more than 10 % of users	Interruption in service provi-sion of more than 8 hours and more than 35% of users	Interruption in service provision of more than 8 hours and more than 50 % of users
The cyberincident requires between 1 and 5 person-days to resolve	The cyberincident requires between 5 and 50 person-days to resolve	The cyberincident requires between 50 and 100 Person-Days to resolve	The cyberincident requires more than 100 Person-Days to resolve
Between 0.001 and 0.05 % of current GDP	0.05 % to 0.07 % of current GDP	0.07 % to 0.1 % of current GDP	More than 0.1% of current GDP
More than 2 ACs	More than 3 ACs	More than 4 ACs	Supranational geographical spread
Significant reputational damage, with media coverage (extensive media coverage)	Reputational damage that is difficult to repair, with media coverage (extensive media coverage) and affecting the reputation of third parties	Reputational damage to the country's image (Spain brand) and continuous coverage in the national media	Very high reputational damage and continuous international media coverage
Affecting critical processes and recovering interrupted activity within its RTO	Recovery from interrupted activity slightly above its RTO (%)	Recovery of a discontinued activity above its RTO (%)	Recovery from interrupted or unknown activity or well above its RTO (%)
Stakeholders' expectations and trust are not affected	Stakeholders' expectations and confidence will be minimally affected	Stakeholders' expectations and trust will be significantly affected	Stakeholder expectations and trust and the relationship with stakeholders will be strongly affected over a long period of time
No alarm	Principle of alarm in the population with/without due cause	Alarm in population with/without just cause	Panic in the population with/without good cause
Minor material damage (valuation €?)	Moderate damage (valuation €?)	Serious damage (valuation €?)	Very serious damage (valuation €?)
Impairment losses up to replacement cost	Impairment losses up to replacement cost	Impairment losses up to replacement cost	Impairment losses up to replacement cost
No implications	No implications	Isolated third party claims and/or indications of wrongdoing	Mass claims by third parties and/or materialisation of crime
No	**Optional**	**Yes, of very HIGH LEVEL**	**Yes, of CRITICAL level**

www.ccn.cni.es
www.ccn-cert.cni.es
oc.ccn.cni.es

CCN
centro criptológico nacional