OCTOBER 2018
CIGREF REPORT

Cigref
SUCCEED
WITH DIGITAL

CYBERSECURITY

visualize
understand
decide

Cybersecurity

Visualize, Understand, Decide

October 2018

Cigref is a network of major French companies and public administrations set up in order to develop its members' ability to acquire and master digital technology. It is a key player and federating body in the digital society, thanks to its high-quality thinking and the extent to which it represents its members.

Created in 1970, Cigref is a not-for-profit body in accordance with the French 1901 Law of Associations. It counts among its members some 150 major French corporations and public administrations across all business sectors. It is overseen by 15 board members who are elected by the General Assembly. Its day-to-day work is carried out by a team of ten permanent members of staff.

Browse all our publications at **www.cigref.fr** | Follow us on Twitter: **@Cigref**

Cigref, **21 avenue de Messine, 75008 Paris**, +33 1 56 59 70 00, **cigref@cigref.fr**

OVERVIEW

Today, the pressure of digital transformation and the dematerialization of physical processes means that **companies now hardly ever possess any essential functions operating independently of their information systems**. It is therefore of vital importance to the company that these systems are protected. Cybersecurity[1] is a response to this protection and trust issue, affecting customers and prospects.

Management demands – and needs to have – trust in the level of security in force for the business activity for which it is responsible. To ensure the **appropriate level of investment to cover cyber risks,** managers need a presentation or report enabling them to identify risks, qualify them and value them using relevant indicators.

IT security risks must be analysed **throughout every function of the company**. This is why cyber governance is the responsibility of a manager whose remit includes all of the company's activities. Depending on the organisation, it may be the Chief Information Officer (CIO), cyber manager or even the risk manager. The **mission of this manager is to educate** the leaders of companies or public bodies, in a way that applies to their own situation, **showing them how a cyberattack can have a significant impact on a company's business activity, its value, assets and reputation,** potentially even **putting its survival at risk, and to propose appropriate measures for covering such risk.**

The Cigref working group has identified and structured the essential strategic information and indicators in a cybersecurity dashboard to be presented to the Executive Committee and the Board of Directors. By adapting it to the specific context of his/her own company or public organisation, the CIO or cyber-governance manager has the information required to create a report which offers a very brief **summary which is accessible to non-specialists** and provides decision-makers with the right amount of information. This is based on a balance between current data, qualitative information, consolidated risk analyses, cost information and aggregated quantitative indicators. Its content must always include the following key information:

- A brief description of the most vulnerable activities and key data pertaining to the information system (IS);
- The SI's accessibility from outside, and an overview of its exposure;
- Level of threat and current information;
- The company's key areas of vulnerability;
- Summarised overview of IT security risks and risk analysis information by company sector;
- Operational key points;
- Current and future action plans.

[1] It is a key requirement for an information system, enabling it to withstand cyberspace events that may compromise the availability, integrity or confidentiality of stored, processed, or transmitted data, and related services provided or made accessible by these systems. Cybersecurity uses information systems' security techniques and is based on anti-cybercrime measures and the implementation of a cyberdefence system. (Source: ANSSI)

In addition to the question of securing information systems, it is also necessary to consider the issue of **resilience**. The situation arising in a number of companies in 2017 through attacks such as "NotPetya" has made it clear that even though some cyber risks currently carry a low probability, their occurrence is still a possibility, and **companies should start preparing for them right away**: we are entering a "cyber-warfare" era in which all companies are potential targets or liable to suffer collateral damage. **IT Directors**, **with the backing of their superiors and the assistance of their operations teams**, must **prepare now for a crisis resulting from a major successful IT attack**, and consider the emergency measures to be implemented in the first minutes/hours. After all, **in extreme situations, the direct involvement of the IT Director is the determining factor in the company's ability to handle the fall-out from such cyber-incidents.**

ACKNOWLEDGEMENTS

We would like to thank Jean-Claude Laroche, Chief Information Officer at ENEDIS, who steered this study as well as all those who participated and contributed to this Cigref working group:

Antoine ANCEL - SNCF RÉSEAU
Nicolas BAILLY - SAINT-GOBAIN
Christophe BLASSIAU - SCHNEIDER ELECTRIC
Eric BOUZOU - ORANGE
Maja BROQUÉ - IPSEN
Xavier CHAPELLE - TOTAL
Philippe CIROTTE - ERAMET GROUP
Philippe CLERICE - MINISTERE DE L'INTERIEUR
Eric CRESSON - NEXITY
Jérôme CUVILLIEZ - ENGIE
Mahmoud DENFER - VALLOUREC
Fatima DJOUBAR - IDEMIA
Marie DUVAL-SOYEZ - GRDF
Guillaume DUVEAU - MINISTERE DES ARMEES
Philippe ELBAZ – GROUP. DES MOUSQUETAIRES
Christophe FLOCH - DASSAULT AVIATION
Jean FLORIMOND - CNAF
Philippe FONTAINE - SMA
Robert FOUQUES - MACIF
David GARCIA - FRANCE TELEVISIONS
Emmanuel GARNIER - AG2R LA MONDIALE
Henri GUIHEUX - SCOR
Christian GOUILLOU - SOCIÉTÉ GÉNÉRALE
François GUYOT - PLASTIC OMNIUM
Florent HALBOT - VALEO
Coraline HAYRAUD - ARKEMA
Cyrille HERDHUIN - SCOR
Mylène JAROSSAY - LVMH
Philippe JURINE - MINISTERE DES ARMEES
Sylvie LE GALL - NAVAL GROUP
David LECARPENTIER - GRTGAZ
Jean-Yves LEMARCHAND - GRTGAZ
Pierre-Emmanuel LERICHE - REXEL
Marc LEYMONERIE - AIR FRANCE KLM
Christophe MAIRA - RAMSAY GÉNÉRALE DE SANTÉ
Marc MENCEL - NEXTER GROUP
Emmanuelle MOREAU - GROUPE 3M
Michel MORVAN - CONFORAMA
Hakim MOUFAKKIR - GROUPE PSA
Olivier RADIX - GROUPE SEB
Damien RESSOUCHES - CONFORAMA
Damir REZNICEK - LACTALIS
Antonio SILVESTRI - CNAF
Julien TORDJMAN - RENAULT
Marc TOURNIER - ERAMET GROUP
Eric VAUTIER - GROUPE ADP
Nicolas VERMUSEAU – KEOLIS

Cigref would also like to extend its sincere thanks to the following external individuals for their work and contributions to this research: Sébastien Héon – SCOR, Hélène Dubillot – AMRAE, François Beaume – Bureau Veritas – AMRAE, François Gratiolet – Cyrating, Charles d'Aumale – Cyrating.

This document was written by Marine de SURY, Cigref Mission Officer, with help from Jean-Claude Laroche.

TABLE OF CONTENTS

TABLE OF FIGURES

Preamble

In his introduction to the French Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI)'s 2017 activity report, Managing Director Guillaume Poupard pointed out an issue which will have a lasting impact on companies and public bodies:
"[…] the rise in digital technology is now being matched by a corresponding rise in digital threats. Given this reality, it is more useful than ever to remember the key role that can be played by political and economic leaders in devising security measures commensurate with the economic and strategic issues, or indeed their own image issues. "

And in fact, for a number of years now, Cigref has been placing the success of the digital transformation of our economy in general, and of our major corporations and public organisations in particular, at the heart of its strategic goals. Two of its nine stakes and challenges for companies[2] relate directly to cybersecurity[3]:

- Monetising data and **creating trust**. Data is a jewel which needs to be monetised, shared and protected. The protection aspect is important because, over and above ethical and legal issues (protection of privacy), what is at stake is the company's **contract of trust with customers and prospects**.
- **Controlling new digital risks**. **Cyber-resilience is becoming a key issue** which needs to be monitored by the company's general management to ensure that all stakeholders are sufficiently aware of, and engaged with, the issue.

In the fourth of its "7 digital resolutions for 2018", Cigref also undertook to: "**Make information systems security an essential condition for trust in the digital economy** and a strategic area for corporate competitiveness and efficiency in public organisations."

After all, there are two sides to digital technology: on the one hand, it offers possibilities for growth that were scarcely imaginable a few years ago; on the other, it puts powerful tools in the hands of potentially malicious players, generating new risks which must now be faced.

But before taking the appropriate measures in response to these new dangers, we need to assess cyber risks accurately for all corporate players who are responsible for mastering them; and, to this end, acquire a full suite of research, tools and indicators.

[2] "The 2020 enterprise in the digital age: the Stakes and Challenges", published by Cigref.
[3] It is a vital requirement for an information system, enabling it to withstand cyberspace events that may compromise the availability, integrity or confidentiality of stored, processed, or transmitted data, and related services provided or made accessible by these systems. Cybersecurity uses information systems' security techniques and is based on anti-cybercrime measures and the implementation of a cyberdefence system. (Source: ANSSI)

Introduction

This report builds on previous work. In 2007, a working group examining security indicators produced a practical guide for a strategic operational security dashboard. More recently, in 2016, the Cigref report entitled "Cyber risks in corporate governance; Why and how should they be discussed by the Executive Committee?" was published. One conclusion was obvious: not all managers are yet sufficiently aware of the IT security risk, despite several years of alerts issued on this subject. Cybersecurity often still appears to be the preserve of specialists, and remains delegated to the Information Systems Security (ISS) branch, even though a decision-making process actually involving all decision-makers (corporate officers, executive management, information systems management, etc.) would seem to be vital, given the intensification of the threat.

In addition, when managers do decide to take steps to manage this risk, they sometimes appear at a loss, and struggle to understand exactly **how** and **where to act**. It is therefore vitally important to inform decision-makers in companies and public institutions (Executive Management, Boards of Directors) of the key points enabling them to accurately identify the status of the threat and their exposure to it, as well as the investment they will need to make to provide the most appropriate security for their business activity.

But even when IT security risks are assigned their correct place in the hierarchy of risk priorities to be dealt with by the company, it is often the case that human and financial resources remain insufficient. After all, the return on investment on cybersecurity expenditure is still particularly hard to quantify: it is a matter of finding the right level of effort to invest in this area, while neither over- or understating the risk.

Consequently, one of the roles of the Chief Information Officer (CIO) or the person in charge of cyber governance is to **explain** the risks to the Executive Committee and Board of Directors, but also to **qualify** and **evaluate** them using appropriate indicators. This means establishing the right tools and indicators for a dashboard covering this area.

Cigref's intention has been to identify and structure strategic information and key indicators to enable CIOs to communicate information about cyber risks to the Executive Committee, Board of Directors or public authorities.

This report sets out a framework for work in this area and the key components of a dashboard which can be tailored to suit the company's characteristics. It then specifies the key points of cybersecurity governance, methodology and awareness training to be considered. Lastly, in addition to securing IT, there is also a need to consider resilience issues and **immediately** implement plans for an appropriate system to deal with a major IS attack.

1. Cybersecurity dashboard report and indicators for the executive committee

This section presents the information and indicators to be considered when producing the cybersecurity dashboard. The appropriate level of content for such a dashboard intended for use by the Executive Committee and Board of Directors is a subtle **balance of current data, quality information, consolidated risk analyses, cost information, and aggregated quantitative indicators**. It always includes the following items, which are presented in detail throughout this section:

- Activities with greatest exposure and key figures for the IS;
- The SI's outside access, and an overview of its exposure;
- Level of threat and current status in this area;
- The company's key areas of vulnerability;
- Overall analysis of cyber risks;
- Operational key points;
- Current and future action plans.

The cyber dashboard must be tailored to suit the characteristics of the economic entity in question (company – public organisation). The items for each of its components must be chosen to enable executives to take the appropriate decisions to cover the cyber risk: the cybersecurity dashboard report needs to be **highly summarised** (one or two pages), **and accessible to non-specialists.**

1.1. Describing the IS and the most exposed activities in brief

Rather than giving an overall description, participants in the Cigref working group aim to get straight to the heart of the matter by presenting the activities with the greatest exposure to risk, and why they are exposed. Current information can be used as a way of presenting the two or three IS activities or areas with the greatest exposure.

1.2. Giving information about the IS openness strategy

Because cybersecurity should never be an impediment to digital transformation, it is important **to analyse the development of cyber risks associated with the company's openness strategies**. Some strategies have an impact on the openness of the IS; e.g. increasingly extensive reliance on the public cloud, the growth of teleworking, etc. The CIO must therefore consider the answers that need to be provided, and assess the level of service and requirements as well as the resources to be implemented in support of this development. This is therefore a matter of showing the extent to which the company's IS is open, and how much of a genuine vulnerability is created by this openness.

1.3. Assessing the level of threat - Current news

The use of the daily news is a good way of presenting **the threat** and **its risks** by re-framing them in terms applicable to the company. There is a need to demonstrate the quality of its sources of information – which may be drawn from public or more specialised sources – and to show how the internal monitoring system is organised, and what its results are. In addition, this presentation of the threat will be **dynamic**, and **will demonstrate how it changes over time**. The aim here is to:

- Provide a very succinct account of current information;
- Describe the threat as it is perceived outside the company:
  - Most significant security incidents and development of the cyber threat (ransomware, known targets, etc.);
  - Known data violations.
- Describe the impact of external attacks and how they have changed recently.

1.4. Identifying the company's areas of vulnerability – Position in comparison to other companies in the sector

To qualify cyber risks, the company must identify its "Achilles heel" areas – its points of vulnerability and weakness, which may be intrinsic or context-related. Two examples of risk qualification are: what kind of vulnerabilities are currently being addressed, and how many? Classifying vulnerabilities provides a means of identifying the areas of greatest weakness. And by presenting an assessment of the financial impact of potential attacks wherever possible, it also establishes priorities for associated investments. In addition, the company must examine whether its current level of monitoring is appropriate for the current and future risk levels. The goal is to narrow the gap between the current and expected situations.

A focus on identifying key weaknesses should not lead to the assumption that everything else is satisfactory; these areas of weakness should simply receive extra attention.

It is also interesting to show, wherever possible, how the company's current position compares to other companies in the same sector.

1.5. Implementing the overall cyber risk analysis and steering mechanisms – Describing how risks change

In terms of risk management, two key points need to be shown:

- **the risk analysis mechanism**, which should incorporate a good understanding of what the company's key assets are;
- **the steering mechanism**, to show that the organisation is following the advice it receives.

The manager in charge of the IT security risk for the company must identify the company's key assets. Using the risk analysis, he/she must implement a mechanism for protecting these assets and measuring the effectiveness of this protective system. Managers of all the company's entities should work together to explain to him/her how business risks are managed. A risk handling plan (specified later in this document) must be implemented, accepted and used by all stakeholders.

The overall results of the risk analysis form part of the information to be presented to the Executive Committee. These results may cover the following points:

- Level of cyber threat for the company's various activities: low/medium/high
- Description of cyber threat changes in the company;
- Number of risk analyses updated;
- Number of new risk analyses;
- Reduction of risks in comparison to the established map:
  - Number of critical risks not covered
  - Number of critical risks currently being addressed
  - Number and type of recently-discovered new risks;
- Number of security alerts inside or outside the company;
- Number and scale of security incidents (targeted attacks, ransomware, etc.).

  With regard to the number of security incidents, it is important to note that the more efficient the exploration process, the more security incidents are identified. Growth in this indicator may reflect the company's ability and efficiency in detecting security incidents. In short, what is needed is not merely a knowledge of the number of security incidents, but an **understanding** and ability to explain how they **evolve and change**;
- Existence (or lack) of a mechanism to cover unknown risks (cyber-resilience tool)

Analyses of risks and how they change lend themselves very well to visual methods of presentation, and the choice of visual format should be selected to match the desired purposes.

Here are two possible presentation examples.

The first example shows a presentation of the impact of risks by frequency.

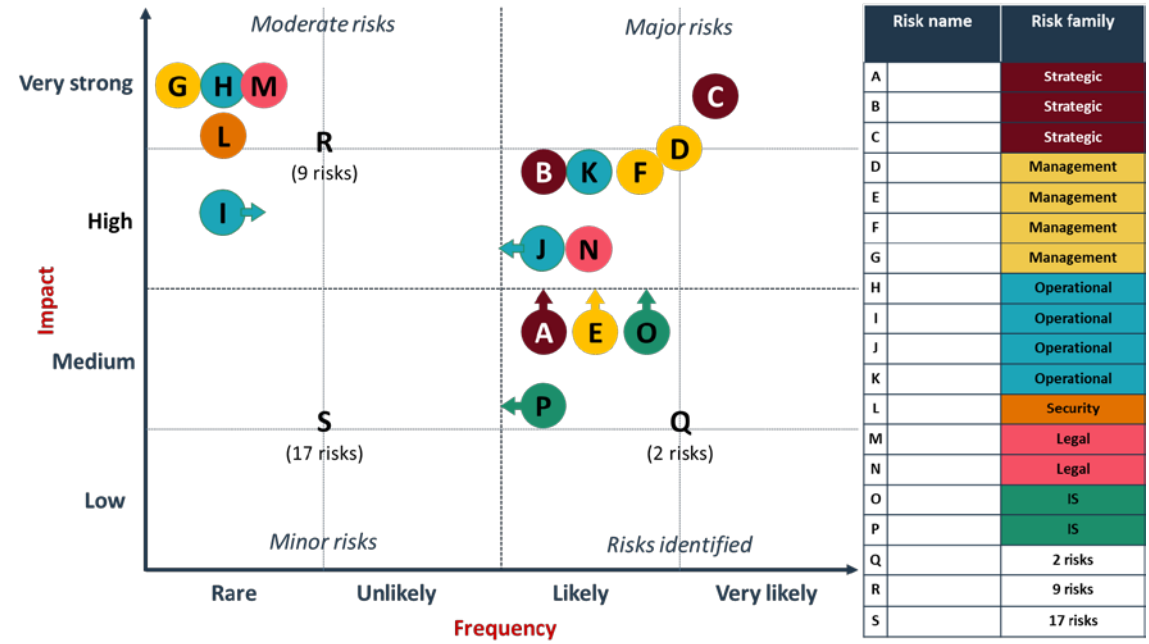

Figure 1: Risk Management Collection RISK MAPPING - AMRAE

The second example shows the security level applied by area in the form of a radar graph.

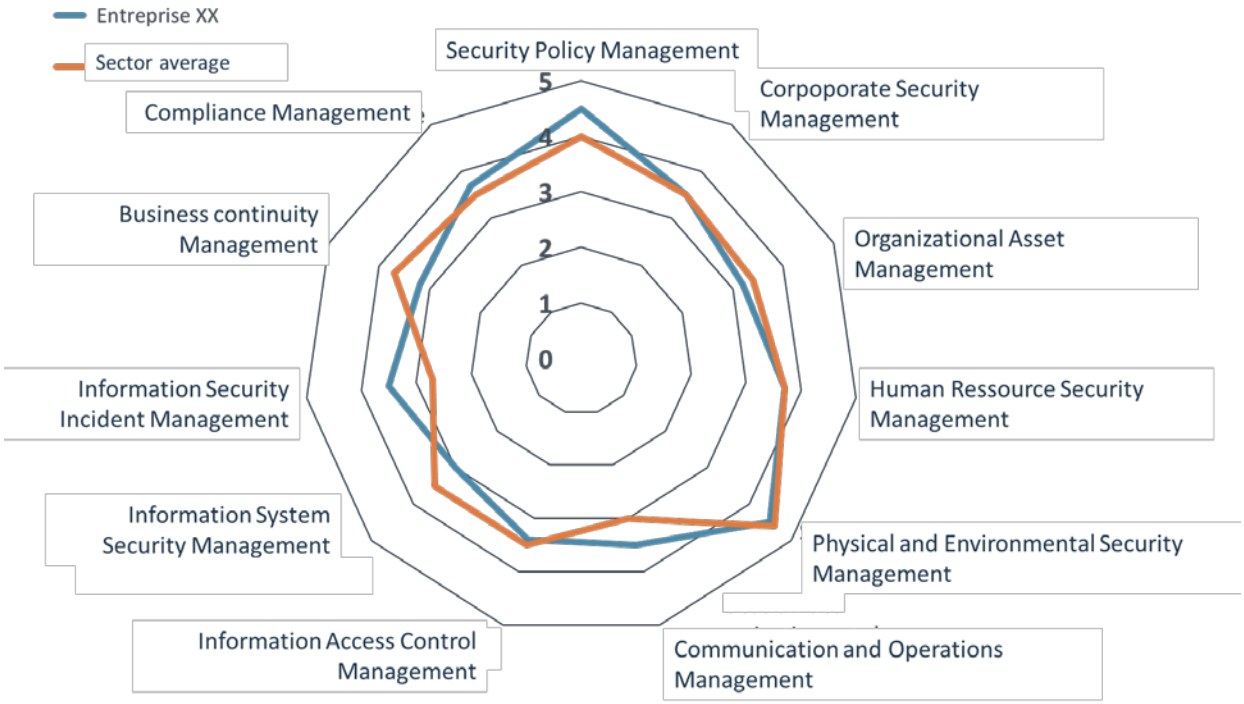

Figure 2: Visual radar graph representation – Source: Cigref

Other representations are available, and examples are given in the appendix.

1.6. Clearly specifying operational key points

The data supplied in the report to the Executive Committee must provide sufficient detail for the relevant context. Here are a number of key points which have been emphasised to show operational activities providing company security in the cyber domain.

1.6.1 Description of the security policy

The following indicators can be used to describe the security policy:

- Existence and implementation of a security policy;
- Date of most recent updates to:
    - The information charter for users, with rules to be followed (internet, email, passwords, social media, confidentiality, etc.);
    - The IS security policy (ISSP)[4];
    - Technical security policies (TSPs)[5];
- Level of compliance with key rules: indicator of compliance with the security policies of the various entities;
- Level of coverage of current subjects (business, operational, etc.). Does the ISSP cover them appropriately? If not, is it continuously improving?
- Where applicable, for certain organisations or operators of critical importance, the level of compliance with the Government's ISSP;
- Compliance with contractual systems representing the level of compliance required by customers. In other terms, this relates to how cybersecurity is handled within the company's ecosystem (customers, suppliers, etc.). After all, the ISSP does apply to a physical entity. However, it is becoming increasingly complex to implement within the context of an extended enterprise (i.e. with the whole of its ecosystem);
- Existence of a DRP (Disaster Recovery Plan)[6].

1.6.2 Description of the Business Continuity Plan (BCP) in the event of an attack, and resilience in the event of an information system failure

Each attack scenario is different, which calls for vigilance. There is therefore a need to ensure that the BCP and the DRP (Disaster Recovery Plan) are in step with ACTUAL company reality. This requires the involvement of all IT Department, digital and security-related participants, as well as management, and all business unit leaders (discussed later in this document). It is also important to point out the following:

- BCP for the company **and** the extended enterprise in the event of cyber attacks:
    - Number of tests conducted: production of BCP(s) in the past year;

[4] The ISSP reflects the strategic vision of the management of an organisation, small/medium company or industry, large company or government body in terms of IS security – Source: ANSSI
[5] The TSP describes all the applicable security rules for each of the technical domains (servers, PCs and laptops, network, printers, WiFi, telephony, etc.).
[6] The purpose of a Disaster Recovery Plan (DRP) is to plan for the recovery of IT infrastructure in the shortest possible timescale. Its aim is to enable the operational restoration of services in the event of an incident. Source: Cases.lu

  - Goals achieved: states whether the goals set for the tests have been achieved;
  - Achievement of recovery time: states whether the goals set for planned recovery time have been met;
  - Level of internal distribution of BCP test reports;
  - Development of resilience component. What is the business continuity mechanism for the extended enterprise, particularly in the event of a major cyber shock?
- For the IT recovery plan:
  - DRP tests conducted during the year;
  - Goals achieved for the tests;
  - Achievement of recovery time goal;
  - Achievement of maximum data loss goal;
  - Indicator specifying whether test reports have been distributed internally;
  - Cyber-compromise exercises;
  - Cold reconstruction ability. It is necessary to have the ability to remedy the situation then perform a cold reconstruction. In the meantime, an alternative system must be specified to make good the shortfall.

1.6.3 Threats, observed attacks and implemented responses

In some companies, the concept of "defendability" is promoted, which involves proving to key decision-makers that the company is capable of identifying attacks and security incidents to which it falls victim, analysing the unfolding crisis and rapidly resolving the issue. This primarily takes the form of an SOC (Security Operations Center)[7].

The following indicators can be used to present detected threats and attacks, and the related responses to them:

- Number of security alerts;
- Number of security incidents (viruses, targeted attacks, ransomware, etc.), and ability to process them. [See incident reference framework in the ETSI standard. The detailed list of security indicators: GS ISI 001-1 (Incidents) and ISI 001-2 (Vulnerabilities)];
- Number of incidents with a business impact, and ability to handle them;
- Number of major incidents, and ability to handle them;
- Actions taken in response to the incidents listed above;
- Incident resolution backlog (list of actions to be carried out) and changes to it;
- Cost of post-incident work in FTE (Full Time Equivalent) terms
- Intrusion attempts (number of attacks and number of service interruptions);
- Internet attacks (of DDOS: *Distributed Denial of Service* [8] type);
- Data loss/theft;

[7] A SOC is an information system security supervision and administration mechanism which gathers events in order to detect and analyse information security events, then determine what responses are to be taken in scenarios where alerts are issued or operational crisis mechanisms are deployed. Source: Sentryo.

[8] A Denial of Service attack is an electronic attack whose purpose is to render a service unavailable, preventing legitimate users of that service from using it. The vast majority of such attacks currently derive from multiple sources (hence the use of the term "Distributed Denial of Service" or DDoS, attack). Source: Wikipedia.

- Human errors (divergence from IT/user/administrator charters);
- Description of observations made by the SOC (Security Operations Center) team;
- Figures and data from SOC activities;
- Actions taken by the SOC team.

1.6.4 Audits and their outcomes

The working group has identified indicators for providing audit information to the Executive Committee.

- Number of audits started or in progress, and their outcome;
- Number of audits undertaken in last 5 years, and their outcome;
- Action plans in progress.

This assumes that the internal audit function is able to formulate the problem and question the business units on information systems issues. Internal auditors generally turn to specialist companies for this task. In this section, it is also possible to report on the cybersecurity-related consequences of audits by the statutory auditors.

1.6.5 A few vital indicators

It is also necessary to issue reports on the organisation's internal cyberactivity. The following indicators may be of use in this:

- Description of key actions undertaken by the main IS processes;
- Level of integration of "security by design" principles into projects
- Number of intrusion tests;
- Detection and correction of faults and vulnerabilities. For example:
  - Number of critical vulnerabilities to be handled as a priority (agreed vulnerabilities for priority consideration);
  - Number of critical vulnerabilities corrected in a six-month period;
  - Number of new vulnerabilities detected and assigned a high priority in the previous quarter;
  - Number of critical faults outstanding;
  - Number of vulnerabilities against number of machines in inventory;
  - Percentage and number of machines meeting security standards (patch management).
- Descriptions of actions undertaken regarding individuals, e.g. awareness training:
  - Existence (or lack) of financial incentives relating to cybersecurity in the goals set for the company's managers and staff, and incorporation of a cybersecurity dimension in delegations of authority;
  - Number of ISS (IS Security) messages to IS users. For example, one rule could be to send a quarterly awareness message to all users:
  - Percentage of individuals having been involved in an awareness campaign;
  - Level of awareness of all company participants by role;
  - Training initiatives.

1.6.6 Technical protection and authentication mechanisms – Permissions and permissions reviews

The indicators listed below provide reports on technical protection and authentication methods, plus permissions:

- Network protection mechanisms and security monitoring mechanisms
- Office software inventory status:
  - Antiviral protection (number of PCs and laptops with up-to-date antivirus)
  - Operating System protection (percentage of workstations with up-to-date operating system)
  - Encryption system
- Status of application inventory (application servers):
  - Antivirus protection
  - Operating system updated
  - Encryption system
- Permissions management system:
  - Reviews of permissions for access to the IS and sensitive applications
  - Corrections implemented following reviews
  - Existence of a unified authentification system: eligible applications / connected applications / monitored applications

Certain points may be added; e.g. establish how rights management and privileged account limitations are implemented, specify the functions and key people, etc.

1.6.7 Technical detection mechanisms

Description of suitable technological choices: level of SOC coverage, used tools, number of incident detection rules, use/non-use of artificial intelligence in incident detection, etc.

1.6.8 Technical and organisational tools for responsiveness

These technical and structural tools for responsiveness complement the Business Continuity Plan:

- Crisis mechanisms
- Number of exercises conducted and results

1.6.9 Compliance with the company's internal rules and compliance with legislation (GDPR, NIS, etc.)

To deal with the issue of compliance, the following information can be used:

- Positioning in comparison to other companies in the same sector;
- Protection of GDPR personal data; compliance discrepancies attributable to the IS;
- Compliance with directives (typically the NIS[9] *Network and Information Security)*, and sector regulations regarding safety.

[9] URL for the NIS directive: https://www.ssi.gouv.fr/entreprise/reglementation/directive-nis/

1.6.10 Visual representation of operational key points

Operational key points are good candidates for visual representation. An example of how to present them is given below, using green/orange/red dots to show the positioning of indicators. An arrow shows changes over time. In the following example, arrows show the change compared to the previous presentation.

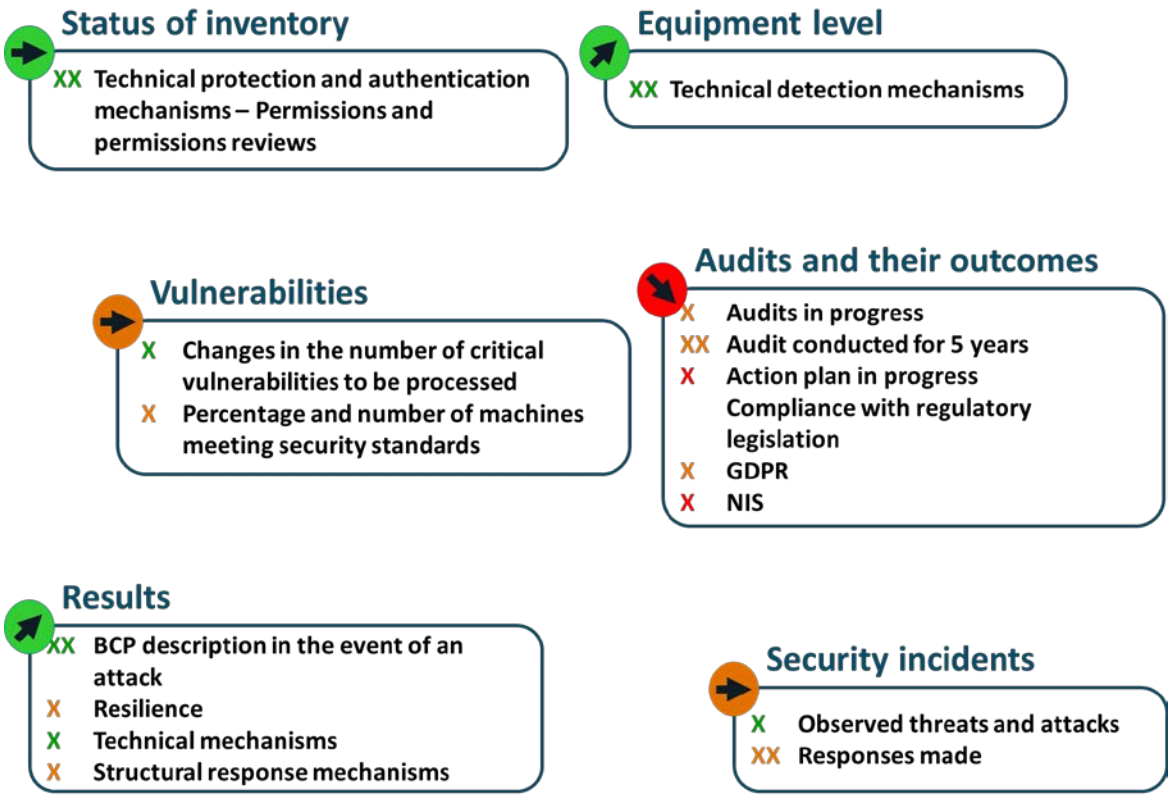

Figure 3: Sample presentation of operational key points – Source: Cigref

1.6.11 Establishing the action plan and monitoring it

Once the action plan has been determined, there is a need for regular monitoring of the agreed actions to reduce the exposure to cyber risk and recursively add new actions if necessary.

2. Governance, methodology and awareness training

Once the cybersecurity dashboard has been structured, a few questions regarding governance, methodology, trust and awareness training need to be answered.
But before that, it is important to consider the multifaceted nature of the threat, which can be either local or international. And crucially, it is likely to change over time. Anticipating future threats is a critically important exercise, even though the nature of attacks yet to come is not always known. However, it is still necessary to try to secure information systems against all risks, assigning the same importance to each.
This problem particularly affects insurance companies offering protection against IT security risks. They need a statistical basis for mutualising risk, and very often face this methodological difficulty. Fear of systemic risk – that is, of a cyber disaster that could potentially affect a very large number of players simultaneously, adding to the problem of anticipating a future threat – has made some insurers averse to cyber risks greater than those faced by their potential client, considerably hindering the development of insurance products in this area.

During the preparation of this report, the working group had the opportunity to discuss this issue with a reinsurer, obtaining an explanation of its methodology: the principle adopted is to assess the cyber maturity of businesses and understand their exposure to this risk. Depending on its area of activity, the company may be exposed to a variety of cyber risks: loss of data (personal, financial, strategic, etc.), extortion (ransomware, blackmail with denial of service), fraud, operating loss without material damage that characterises information technology damage, computer hacking that alters the characteristics of products, cyber attacks leading to physical damage (sabotage). Using this classification of impacts as a basis, the reinsurer seeks to structure the measurement of the client's exposure to risk in a way that ensures this measurement can be repeated for other prospects. It also seeks to establish the severity and incidence of the cyber risk as a first priority.

As mentioned above, the assessment of the risk to which the company is exposed can also be based on an assessment of the company's level of maturity compared to its counterparts (such as competitors). But once again, such information may be difficult to obtain, making this a somewhat risky exercise. In any event, the IS chain will need to try to correlate as much information as possible in order to arrive at a credible assessment of the state of exposure to the cyber threat.

2.1. Stakeholders to be involved in the cybersecurity strategy

Managers who have a direct role to play in the security of information systems require access at their level to specialised analytical indicators.

The **Chief Information Security Officer (**CISO) must have access on a very regular basis (at least monthly) **to technical indicators** which enable him/her to exercise fine control over operational actions to secure the information system.

Meanwhile, the **CIO** must accurately assess whether the security of all components of the IS is well suited to the missions and expected performance. He also needs to have **monthly indicators**, although probably fewer than those available to the CISO, and must be in possession of **the main risk analyses for the IS** for which it is responsible.

It may be useful to mandate a **cybersecurity director** responsible for overseeing the entire cyber risk, with a scope that extends beyond the mere information system. Digital technology is now spreading to all sectors of activity. Managers responsible for the equipment, products and systems on which the entire running of the company relies, need to consider the possible consequences of malfunctions related to computer security problems. The cybersecurity manager can be particularly useful in companies operating an industrial system (command and control of an industrial installation, for example), because he/she can provide an overview of the cyber risk and better control of the interfaces between organisations or between systems. At this level of responsibility, such managers require access to cyber risk analyses of all the company or administration's activities, sufficiently frequently to ensure that these risk analyses are valid; they are then to be adapted accordingly.

If the company does not have a Cybersecurity Manager, it can broaden the scope of its CISO's responsibilities to extend its oversight of cyber risk beyond the IS perimeter and designate a point of contact in each operational department.

At the overall company level, Executive Committee members need to know whether an IT attack is likely to cause significant harm to the company's business or even, ultimately, endanger its survival. The content of all activity reports submitted to the Executive Committee must be focused on providing this insight, ensuring that it obtains the most accurate idea of the **right level of investment to be made to cover the cyber risk**. The frequency of examination of this issue by the Executive Committee appears to be at least annual and at most quarterly.

Finally, every year, the **Board of Directors** must be informed of the possible impact of IT security breaches on the **company's actual value, assets and reputation**. The level of information which may be supplied to it is similar to the information supplied to the Executive Committee.

The cybersecurity dashboard must be tailored to the type of recipient: more focused on quantity, analysis and operational issues when it is intended for the CISO; more synthetic and strategic when aimed at the organisation's top management.

2.2. Cyber risk governance

IT now irrigates all of the company or public organisation's products, systems and processes. Threats to IT security cover a wide scope: **all internal information systems (office, industrial, management, etc.)** but also their interactions with **all ecosystem partners** (including maintenance, upkeep, etc.). Cyber threats therefore affect stakeholders across all company functions and individuals in charge of data governance (in particular the DPO[10] following the introduction of the General Data Protection Regulation) and asset quality and security. An IT crisis is not necessarily an information system crisis, in the traditional sense of IS management. It may affect other business units.

For this reason, the participants of the Cigref working group have all agreed that in order to correctly inform the highest levels of decision-making in the organisation (Executive Committee, Board of Directors), IT security risks must be analysed in a cross-functional way that covers the entire company.

There are a variety of stages involved in cyber risk governance, enabling actions of risk analysis and the steering of preventative and remedial measures (such as crisis mechanisms). These operations are conducted both at an overall level and at operational level within the various business units. At the overall, cross-functional strategic level, individuals in charge of risk management must have authority over all of the company's operational managers to ensure feedback is supplied and implemented initiatives are co-ordinated; they can co-opt the assistance of employees from the IS Department; it is also at this level that cyber risks straddling more than one department must be dealt with; e.g. at the interface between management information systems and industrial information systems; **all areas of uncertainty in organisations between divisions and/or subsidiaries should be considered as risk areas to be dealt with at this level**;

Cyber governance within the company can be driven by the CIO, the cyber director (a new feature in companies wishing to appoint a high-level executive specifically for the purpose of managing the e-risk plan across the entire company), the risk manager or the CISO. Those responsible for risk management must be strongly involved in this process. One Cigref member company has chosen to entrust this overall cyber risk assessment responsibility directly to its risk department. Others prefer to leave this responsibility to the CISO, given the specific nature of this risk and the technical skills required to assess it. Regardless of the organisational structure adopted, IT departments must also have risk analysis teams at their own level and for the information system itself; these teams pass on the information to the company's head of overall cyber risk management.

A point to note: in certain companies, some industrial activities may be subject to specific regulations; for example, the nuclear industry. In these specific areas, risk management is handled by the body subject to the specific regulations. However, this must be incorporated into the overall risk picture at company level.

[10] DPO: Data Privacy Officer

The most important point is that the party responsible for overall management must be able to bring together and control all players across all company functions in all matters concerning the evaluation and coverage of cyber risks.
Lastly, it is vital that the structure created to cover this cyber risk is:

- formally described;
- stable over time; i.e. it is immune to internal or external staff movements (executives and managers). However, an organisation that is too formally structured, and thus easy to read from outside, can represent a vulnerability;
- rapid modification and restructuring should be possible following business changes.

Lastly, this governance needs to be paired with a highly responsive mechanism providing the company's key executives with information on the risks faced by the company or organisations regarding attacks covered in the press.
The key component of a good cyber dashboard is therefore risk analysis, a point on which some clarification is needed.

2.3. Importance of risk analysis

Risk analysis mechanisms must be updated regularly and based on a precise, quantified methodology which can be supported by the company's internal reference frameworks. In any event, this methodology must enable the following points to be covered:

- **the status of the threat** to the company's business, and the level of the company's maturity regarding the threat in comparison to its counterparts;
- **the impact** of a cyber crisis, depending on the sensitivity of the systems under examination and the data being processed; the business units themselves must be involved in determining the sensitivity of their data and the processes which they manage, according to a reference framework established by the company. The governance mechanism must specify who bears this responsibility on the business side, and who controls the reference framework;
- the reality of the measures taken:
  - o to prevent a crisis and provide optimal protection; patch management forms a part of these preventive measures;
  - o to observe what is happening in the company's IS, and how threats are developing outside of the company, making it possible to anticipate crises and react quickly;
  - o to ensure business continuity and manage the crisis, if it arises;
  - o to return to normal operation as quickly as possible following a crisis.

However, it should be noted that IT security risk analysis is a particularly arduous task: it is always hard to form a clear picture of the current level of the threat, or indeed to quantify it precisely. In addition, for attacks which have already occurred in some companies, it is almost impossible for an outsider to know exactly which targets have been affected and what the impact has been, as this sensitive information remains covered by business secrecy. This is why the likelihood of cyber risks occurring remains difficult to establish. And it also explains why a company making investments in IT security may not see any changes in its risk level from year to year. This risk may remain high simply because of an increase in threat levels. This methodological problem can then lead to a certain level of

discouragement, despite the fact that this impression of a "futile effort" often - too often, in fact - proves to be wrong. In all cases, the CIO needs to **demonstrate the value of the investment to the Board of Directors and the Executive Committee**, e.g. because it has enabled a particular attack to be countered. Such communication work lends credibility to the need to invest in this area, in which return on investment is particularly difficult to calculate.

2.4. Mutualisation of cyber monitoring

Only the most spectacular examples of cyber attacks are given widespread publicity, often with the backing of the management of the companies concerned and within the context of a controlled external communication. The members of the working group thus perceive a need for **a small community of trusted players to be formed to allow sufficient information to be circulated to assess the true state of the threat.** This small community would comprise individuals from the management and IT departments of large companies.
Moreover, even with these risk analyses available in a usable form for discussions with the Executive Committee and the Board of Directors, before presenting a more detailed dashboard and a decision-making dossier on the subject, an examination of the level of awareness of the cyber issue among key decision-makers will be necessary; if cybersecurity has not been addressed before at governing body level, ways of raising awareness will need to be considered.

2.5. Raising the Executive Committee's awareness of cyber risks

In the aftermath of the high-profile attacks on the information systems of certain companies in 2017, some Executive Committees are very much aware of cyber risk, to such an extent that some of them are now referring to "denial of production" as a description for attacks that result in the shutdown of production plants.
However, in general terms, it remains difficult to raise Executive Committees' awareness of cyber risks, often because of the limited time available to decision-makers. Even so, a number of methods for informing/training/raising awareness among stakeholders at this responsibility level may be considered, such as:

- Cyber crisis exercises,
- Real-life scenarios: phishing[11],
- Simulations of interviews with journalists for post-crisis communication,
- Two-stage short training: an initial session with an external focus, delivered by specialists (e.g. ANSSI, or law firms) and a second session in which the company's main areas of weakness are presented by the risk and audit teams and cybersecurity specialists.

[11]Identity or confidential information theft (access codes, bank details) by subterfuge: an authentication system is simulated by a malicious user, who then attempts to persuade users to use it and hand over confidential information as if the system were legitimate. Source: Wikipedia.

The training must be tailored to the company's own circumstances: after all, information systems **security** is **not an obstruction to the business unit's work; it adapts to it, and secures it**.

Cyber scoring by a third party can also be a good tool for raising awareness. This service, performed by a specialist company, assesses the firm's cybersecurity performance. It is based on the firm's public footprint (tests are non-intrusive, and thus factual and objective). Scoring also makes it possible to set targets for internal departments, suppliers, customers, etc. In addition, it can produce a competitive scenario in which entities are ranked.

2.6. The question of trust

The question of trust is an issue for consideration during discussions with the governing bodies of companies or public bodies on the topic of cybersecurity.

While the IT security of business activities is on the one hand the "make or break" condition for **public trust in digital services** provided by government bodies, it is also the cornerstone for **customers' trust in their suppliers** of products, services and information systems. And it also influences the level of **trust employees have in their employer** when such employers collect their personal data. In short, it is impossible to imagine a digital society without trust, and that trust is possible only through the protection, control and monitoring of digital activities.

Given such expectations from all stakeholders (the public, customers, employees, etc.), the directors of companies and government organisations must be able to have confidence in the level of security of the activity for which they are accountable. However, cybersecurity issues sometimes require high levels of specialisation and technical skills which are out of the reach of managers. It is therefore important to facilitate communication between experts who understand the level of security to implement in order to support – and not slow down – the company's activity, and the managers who carry heavy key responsibilities for their organisation. This role of "go-between", liaising between the Executive Committee and the security division of the IT function, is one of the CIO's main functions. To gain recognition in this go-between role, the CIO must personally inspire confidence: this is dependent on his/her own knowledge of the company's business units and issues, and also his/her credibility in the information systems field.

2.7. The standards framework for cybersecurity

To complete this section on "Governance, methodology and awareness training", it should be pointed out that **IT security actions need to be implemented as part of an efficient standards framework.**

There is a need for a reference framework which describes **how the company responds to all risks and identifies those holding responsibilities.** This forms the foundation enabling each entity of the company to evaluate its progress in its reference framework compliance plan, e.g. in the form of a percentage, and to report that progress in a way that can be

audited. Consolidation of these results at the overall level then gives an insight into how the company handles cyber risk.

Because compliance must not be detrimental to responsiveness, this approach must be complemented by constant monitoring of actual events (e.g. cyber attacks) which are liable to affect the company or its environment. Observations from this monitoring work provide the basis for adjusting assessments of actual vulnerabilities putting business at risk, and for revising the priorities of actions to be undertaken. At the overall company level, there is a need to ensure that quick decisions can be taken, prioritising the cyber risk at the highest level and in a short timescale. This may, for example, consist of imposing a requirement for all business units to apply corrective patches promptly. Management also needs to provide for this type of mechanism.

Naturally, security event monitoring requires not only the right tools, but also high-level skills; ultimately, such skills are the determining factor which ensures high-quality monitoring and prediction, as well as a responsive organisational framework.

In addition, unlike a purely standards-compliant approach, the risk coverage approach is always the result of a **compromise between the security objectives pursued and the resources to provide them**, especially the skills and financial resources that the entity is able to allocate to this work. It must be possible for managers at the various levels of the organisation to demonstrate the way in which this trade-off is achieved.

Lastly, it is necessary to keep checking the relevance and usefulness of previously implemented initiatives.

Some Cigref members promote the concept of "defendability". This means the ability to show key decision-makers that the company is **capable of identifying the attacks** and **security incidents it faces**, **analysing the unfolding crisis and resolving it rapidly**. This is achieved mainly through the work of the SOC and operational crisis mechanisms.

In summary, a **standards-based mechanism** is needed, **demonstrating that the company is compliant**. This mechanism needs to be backed up by **monitoring of the actual cyber situation**, and an **order of priority must be drawn up**, stating which risks are to be prioritised over other company priorities. Lastly, the company must be able to reply quickly to questions from corporate officers and executive managers.

3. Major cyber attacks: what structures are needed?

In addition to traditional approaches to creating secure IT systems, which ultimately amount to comprehensive prevention strategies, it has now become **necessary to address the issue of resilience**. The situation arising in a number of companies in 2017 through the "NotPetya" attack has made it clear that even though some cyber risks currently carry a low probability, their occurrence is still a possibility, and **companies should be prepared for them.**

Now is the time for companies to start considering what structures they need in the event of a successful computer attack. The aim is to evaluate the requirements for maintaining a given level of activity in extremely degraded mode, and also to plan crisis communication under such circumstances. The textbook case study is the sudden failure of the entire IT system (e.g. through an Active Directory[12] paralysis).

Asking this question before a crisis means that alternatives can be considered and working solutions can be identified, particularly with regard to protecting the most critical sites and activities.

3.1. Geopolitical aspects

Regardless of which prevention methods are implemented, one of the reasons why the "cyber shock" scenario needs to be considered is geopolitical. Some attacks against information systems are now in line with state interests. Attackers can draw upon increasingly significant resources. And malicious IT attacks show ever-increasing levels of sophistication. Any company can fall victim to an attack. Cyber security is thus turning into a "military" battlefield. To put it another way, we are entering a "cyber-warfare" era in which all companies are potential targets or liable to suffer collateral damage.

The French national cybersecurity agency ANSSI is working on the detection of serious attacks against the economy and vital industries, and appropriate responses to these. Its focus is less on identifying attackers, and more on how such attacks work and what remedial solutions can be found. Most attacks are silent, but there is a high threat level all year round. Generally speaking, before acting, groups of attackers start by taking control of the network via patient, subtle observation methods.

ANSSI can provide large companies with certain support resources. However, if several critically important companies were to be affected simultaneously in France, they would need to rely first and foremost on their own resources, as the means of assistance available to ANSSI could potentially be insufficient.

[12] Active Directory is Microsoft's implementation of LDAP directory services for Windows operating systems. The main purpose of Active Directory is to provide centralised identification and authentication systems for a network of computers using the Windows system. It also allows the allocation and application of strategies, and the installation of critical updates by administrators.

3.2. Key points for planning action

The key points to be considered when preparing for a major cyber-shock are similar to those examined in a more traditional IT systems security approach; except that the solutions offered for these points are now specific in nature. In the following paragraphs, we offer a list of actions which can form the core of a resilience plan to be implemented by the company:

Figure 4: Stages in crisis management – Source: Cigref

3.2.1. Preparing for a crisis caused by a major successful cyberattack

- **Plan the crisis management team in advance**, and identify who will take the decisions. The chain of command needs to be simplified, shortened and clearly defined around the CIO.
- Establish a managerial core team: a plan must be put in place to mobilise internal and external resources, who will be 100% involved and know where/when/how to meet at the crucial time. Their availability must be known 3 months in advance, and their phone numbers must be accessible.
- **Assemble/centralise critical departments**: the telecoms and infrastructure teams. In cases where the company's infrastructure is fragmented, a centralised approach for monitoring them is needed, and the skills of potential support staff must be pooled.
- **Prepare emergency communication methods**: in particular, under extreme circumstances, it is critically important to be able to pass short messages down the chain of command to the key players. The messaging system may be unusable (and it is not a crisis management tool), and dedicated secure tools will be used instead by preference.
- **Develop an ecosystem of trusted private providers**: set up "cyber crisis" links with partners, service providers and suppliers BEFORE the cyber crisis to establish who to rely on, and for what. It is necessary to establish what will be required of these providers when the time comes.
- **Draw up Business Continuity Plans** specific to this type of circumstance: in a cyber crisis, the biggest problem is wherever business activity relies most on IT. It is therefore necessary to prepare all areas where work needs to continue without IT resources.
- **Test your detection/reaction capabilities** using high-level information attack scenarios, then hold debriefings with the teams on each of them.

3.2.2. Emergency measures to be implemented in the first minutes/hours

- Stop the spread: isolate all affected areas, vital components and critical company sites and – where applicable – shut them down to ensure they are closed off. After all, it is better to cease business activity for one day in order to protect the most critical sites and activities than to refuse to interrupt service, which may prove an extremely damaging decision in the longer term;
- Protect unaffected systems;
- Start the restore process with dedicated teams, taking particular care over organisational structure:
  - Make living arrangements for assistance personnel (24/7 food, accommodation for rest periods, etc.);
  - Oversee a daily steering committee with the MD/CEO, followed where applicable by a short communication to the company's key managers;
  - Form crisis resolution teams with the experts:
    - Dedicated project management team
    - Dedicated communication team
    - Use of several methods of communication
  - Follow ANSSI directions to the letter;
  - Limit the resolution timeframe for each problem beyond which it must be escalated to the CIO.
- Give resolution dates: the CIO must be able to give commitments on attack resolution dates for each business area, and a "return to normal" date.

In addition, it should be remembered that **in such circumstances, internal and external communication is a major issue**: therefore, be prepared to explain what has happened to top management, investors, business unit managers, customers, statutory auditors, etc.

Lastly, the CIO must make advance plans for the measures he/she will need to take to ensure his/her availability and clear focus throughout the crisis, e.g. to avoid becoming overwhelmed.

Conclusion

Managers of companies and public organisations demand – and need to have – trust in the level of security in force for the business activity for which they are responsible.

They therefore need to know in what ways a cyber attack is likely to have a significant impact on the company's activity and its value, assets and reputation, and even potentially threaten its survival. To do this, they require a **highly summarised report** giving them the right level of information to then be able to establish **the appropriate level of investment required to cover the cyber risk**.

By tailoring the cybersecurity dashboard described in this document to the specific characteristics of his/her company, the CIO will have the information needed to produce this summary report/presentation, which is accessible to non-specialists.

However, cybersecurity is becoming a military issue and a geopolitical weapon. We have entered a "cyber-warfare" era in which all companies are potential targets or liable to suffer collateral damage. **CIOs, supported by company executives and surrounded by their operational teams, must now start making plans for a crisis resulting from a successful major IT attack on information systems** and consider the emergency measures to be implemented during its first minutes/hours. Indeed, **in extreme situations, the direct involvement of the CIO is the determining factor in the company's ability to overcome cyber shock**.

Annex

Other examples of risk analysis presentation forms are shown in this annex.

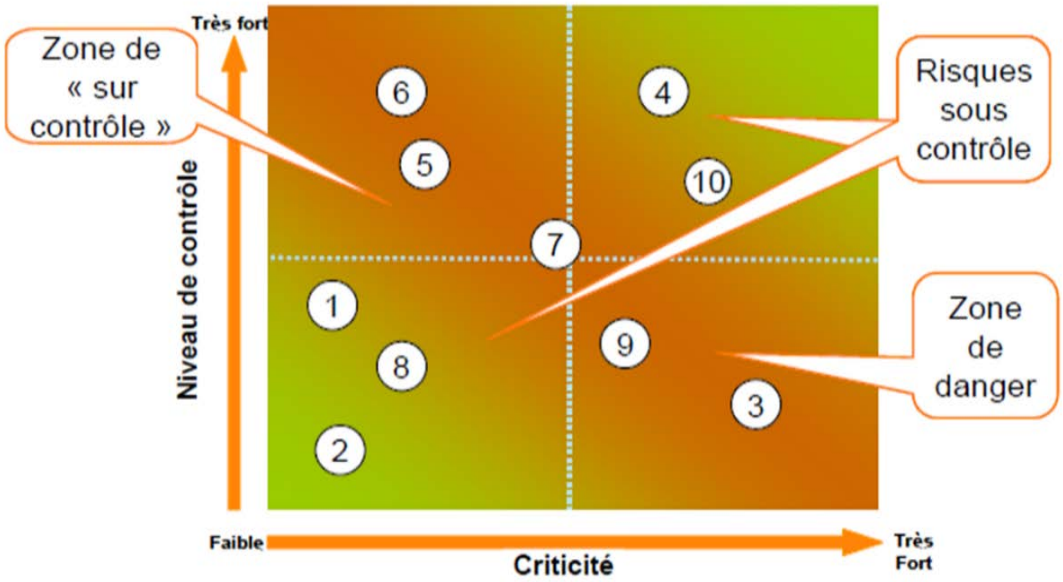

Figure 5: Risk Management Collection RISK MAPPING - AMRAE

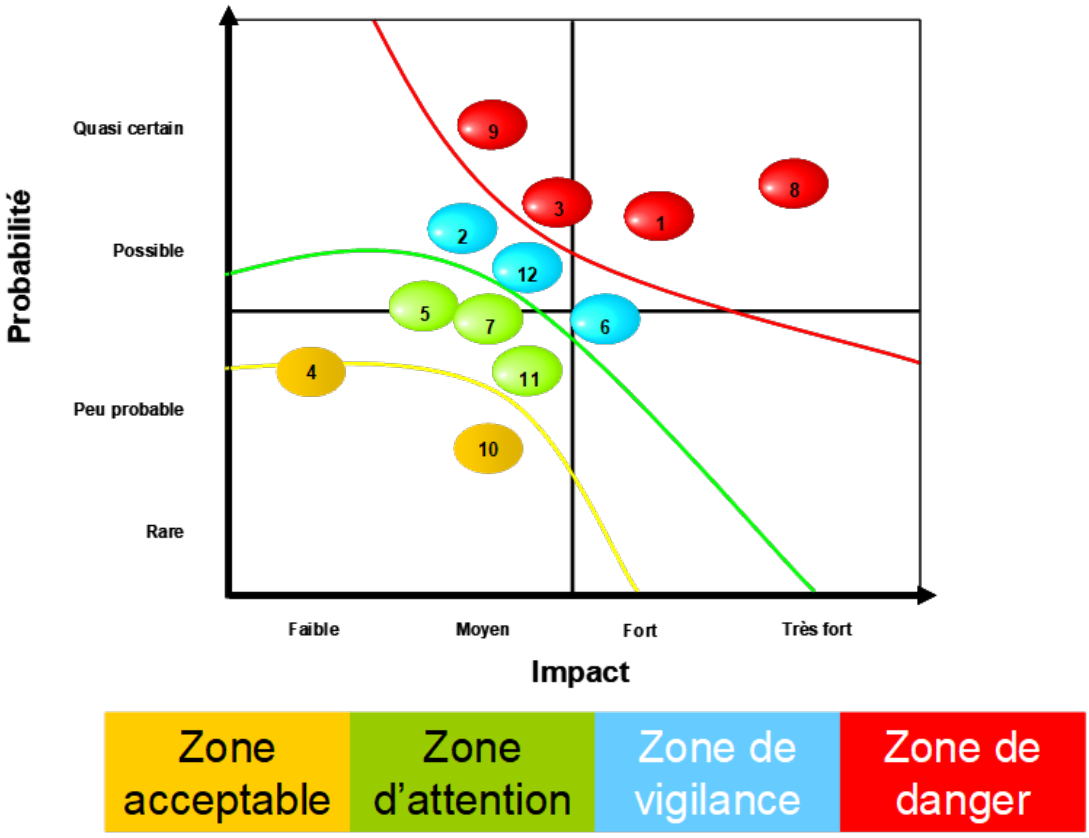

Figure 6: Risk Management Collection RISK MAPPING - AMRAE

Lastly, we can use an abacus (a graph which gives the solution to a calculation) that assesses risks according to 3 criteria: the level of prevention and the level of incident response mechanisms, assessed according to the threat level; an example is provided below:

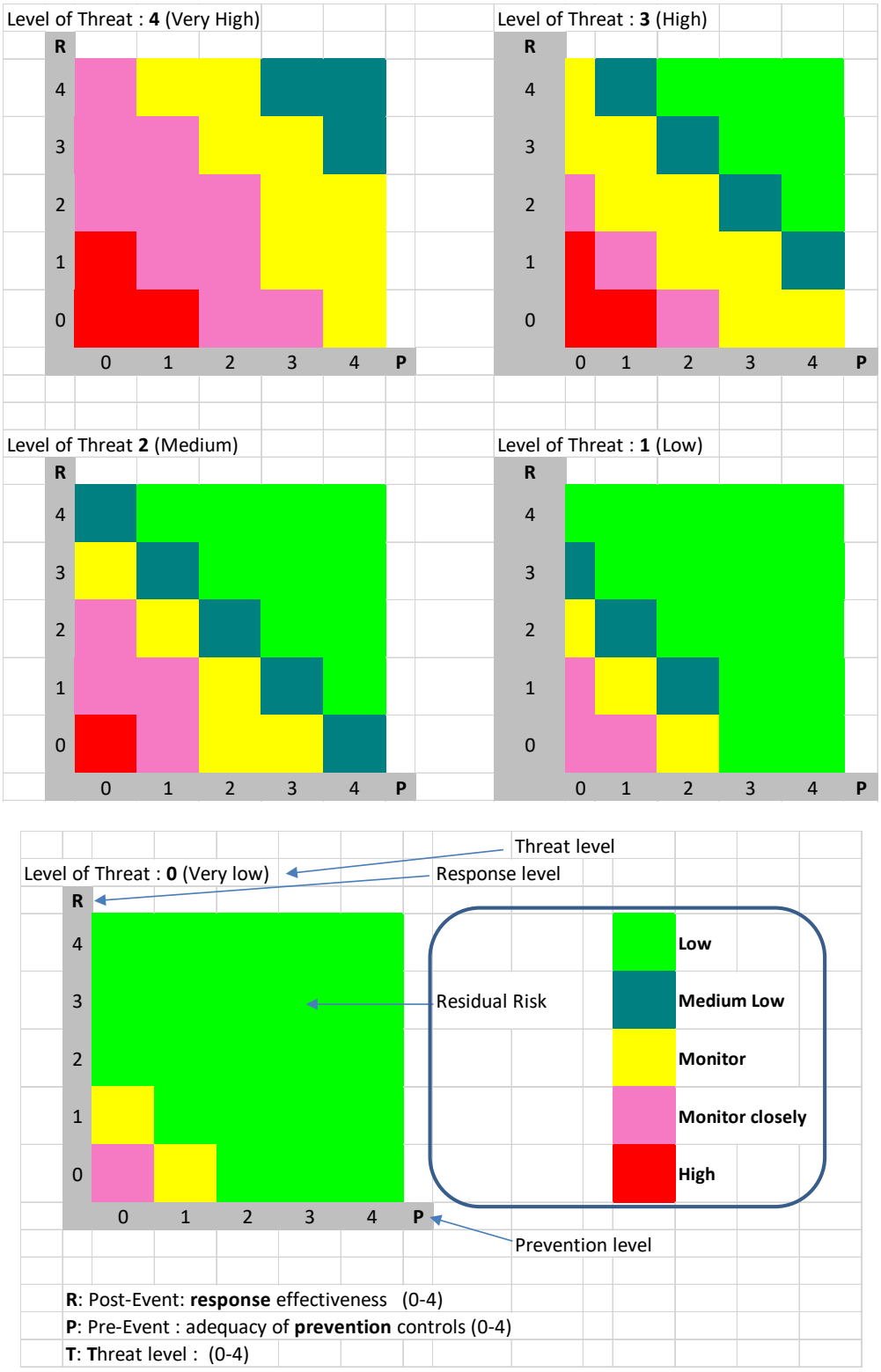

Figure 7: Visualisation of risks in abacus form – Source: Cigref

ABOUT CIGREF
KEY PLAYER IN THE DIGITAL SOCIETY

Cigref is a network of major French companies and public administrations set up in order to develop its members ability to acquire and master digital technology.

NETWORK OF MAJOR COMPANIES

Created in 1970, Cigref is a nonprofit organization. Its counts among its members some 150 major French corporations and public administrations across all business sectors, all users of digital services.

DIGITAL PLAYER

It is a key player and federating body in the digital society, thanks to its high-quality thinking and the extent to which it represents its members.

TO SERVE ITS MEMBERS

15 Board members, elected by the General Assembly, ensure its governance. A team of 10 permanent members leads the activities.