OCTOBRE 2018
PUBLICATION CIGREF

Cigref
RÉUSSIR
LE NUMÉRIQUE

CYBERSÉCURITÉ

visualiser

comprendre

décider

Positionner la **cybersécurité** comme condition indispensable de la **confiance** dans l'économie numérique et comme **domaine stratégique** pour la compétitivité des entreprises et la performance des administrations.

— 4ème résolution numérique du Cigref


Cigref
RÉUSSIR
LE NUMÉRIQUE

Cybersécurité

Visualiser, comprendre, décider

Octobre 2018

Le Cigref est un réseau de grandes entreprises et d'administrations publiques qui a pour mission de développer la capacité de ses membres à intégrer et maîtriser le numérique. Par la qualité de sa réflexion et la représentativité de ses membres, il est un élément fédérateur et acteur important de la société numérique.

Association loi 1901 créée en 1970, le Cigref n'exerce aucune activité lucrative. Il regroupe à ce jour près de 150 grandes entreprises et administrations publiques françaises dans tous les secteurs d'activité. Sa gouvernance est assurée par 15 administrateurs, élus en Assemblée générale. Son activité est animée par une équipe de 10 permanents.

Retrouvez toutes nos publications sur **www.cigref.fr** | Suivez-nous sur Twitter : **@Cigref**

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

SYNTHÈSE

Aujourd'hui, sous l'effet de la transformation numérique et de la dématérialisation des processus physiques, **les entreprises ne disposent quasiment plus de fonctions essentielles indépendantes de leurs systèmes d'information**. Il est donc vital pour l'entreprise que ceux-ci soient protégés. La cybersécurité[1] répond à cet enjeu de protection et de confiance avec les clients et les prospects.

Les dirigeants demandent et doivent avoir confiance dans le niveau de sécurisation de l'activité dont ils portent la responsabilité. Pour assurer le **niveau adéquat d'investissement pour couvrir le risque cyber,** ils ont besoin d'une présentation ou d'un rapport qui leur permette d'identifier les risques, de les qualifier et de les valoriser à l'aide d'indicateurs pertinents.

L'analyse des risques de sécurité informatique doit être **transverse et globale à l'entreprise**. C'est pourquoi la gouvernance cyber est portée par un manager qui couvre l'ensemble des activités de l'entreprise. Selon l'organisation, ce sera le directeur des systèmes d'information (DSI), le directeur cyber ou encore le *risk* manager. Ce manager a pour **mission de sensibiliser les dirigeants** des entreprises ou des administrations publiques en fonction du contexte, **de leur présenter comment une cyberattaque est susceptible de porter atteinte de manière significative à l'activité de l'entreprise, à sa valeur, à ses actifs et à sa réputation,** voire de manière ultime **à mettre en danger sa survie, et de proposer des mesures adaptées pour couvrir ce risque.**

Le groupe de travail Cigref a identifié et structuré les informations stratégiques et les indicateurs indispensables dans un tableau de bord cybersécurité à présenter au COMEX et au Conseil d'administration. En l'adaptant aux spécificités de son entreprise ou administration publique, le DSI, ou le manager responsable de la gouvernance cyber, a les éléments pour construire un rapport qui présente de manière **extrêmement synthétique** et **accessible à des non spécialistes** le bon niveau d'information aux décideurs. Cela repose sur l'équilibre entre des données d'actualité, des informations qualitatives, des analyses de risques consolidées, des éléments de coûts et des indicateurs quantitatifs agrégés. Son contenu doit comporter systématiquement les rubriques suivantes :

- Description succincte des activités les plus exposées et chiffres clés du système d'information (SI) ;
- Niveau d'ouverture du SI à l'externe et aperçu de son exposition ;
- Etat de la menace et éléments d'actualité ;
- Points essentiels de vulnérabilité de l'entreprise ;

[1] État recherché pour un système d'information lui permettant de résister à des événements issus du cyberespace susceptibles de compromettre la disponibilité, l'intégrité ou la confidentialité des données stockées, traitées ou transmises et des services connexes que ces systèmes offrent ou qu'ils rendent accessibles. La cybersécurité fait appel à des techniques de sécurité des systèmes d'information et s'appuie sur la lutte contre la cybercriminalité et sur la mise en place d'une cyberdéfense. (Source ANSSI)

- Synthèse de l'analyse globale des risques de sécurité informatique et éléments sur les analyses de risques par secteur de l'entreprise ;
- Points clés opérationnels ;
- Plans d'action en cours et à venir.

En complément de la sécurisation des SI, il devient nécessaire d'aborder la question de la **résilience**. La situation générée en 2017 dans certaines entreprises par des attaques comme « NotPetya » oblige à considérer que même si certains risques cyber ressortent aujourd'hui avec une probabilité faible, leur réalisation doit être considérée comme possible et **l'entreprise doit s'y préparer dès à présent**. Nous entrons en effet dans une époque de « guerre cybernétique » dont chaque entreprise peut être soit une cible soit une victime collatérale. Le **directeur des SI**, **soutenu par ses dirigeants et entouré par ses équipes opérationnelles**, doit **dès à présent se préparer à une crise résultant d'une attaque informatique majeure réussie** et réfléchir aux mesures d'urgence à mettre en place dès les premières minutes/heures. En effet, **dans les situations extrêmes, l'implication directe du directeur des SI est le facteur déterminant de la capacité de l'entreprise à surmonter le choc cybernétique.**

REMERCIEMENTS

Nos remerciements vont à Jean-Claude Laroche, Directeur des systèmes d'information de ENEDIS, qui a piloté cette réflexion, ainsi qu'à toutes les personnes qui ont participé et contribué à ce groupe de travail Cigref :

Antoine ANCEL - SNCF RÉSEAU
Nicolas BAILLY - SAINT-GOBAIN
Christophe BLASSIAU - SCHNEIDER ELECTRIC
Eric BOUZOU - ORANGE / DSI
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

Le Cigref remercie également sincèrement les personnalités extérieures suivantes pour leurs interventions et leurs contributions aux réflexions : Sébastien Héon – SCOR, Hélène Dubillot – AMRAE, François Beaume – Bureau Veritas – AMRAE, François Gratiolet – Cyrating, Charles d'Aumale – Cyrating.

Ce document a été rédigé par Marine de SURY, chargée de mission Cigref, avec la participation de Jean-Claude Laroche.

TABLE DES MATIÈRES

TABLE DES FIGURES

Préambule

Dans le rapport d'activité 2017 de l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI), son Directeur Général, Guillaume Poupard, rappelait en introduction un des points qui toucheront durablement la vie des entreprises et des administrations :
« […] le développement du numérique s'accompagne désormais du développement concomitant de la menace numérique. Dans un tel contexte, il est plus que jamais utile de rappeler le rôle essentiel que les responsables politiques et économiques ont à jouer pour penser la sécurité à la lumière des enjeux économiques, stratégiques ou encore d'image qui sont les leurs. »

Or précisément, depuis plusieurs années déjà, le Cigref a placé la réussite de la transformation numérique de notre économie, et plus spécifiquement des grandes entreprises et administrations publiques, au cœur de ses enjeux stratégiques. Deux de ses 9 enjeux et défis pour l'entreprise[2] touchent directement la cybersécurité[3] :

- Valoriser les données et **créer la confiance**. La donnée est un joyau qui doit être valorisé, partagé et protégé. Elle doit être protégée, car au-delà des aspects éthiques et légaux (protection de la vie privée), c'est le contrat de **confiance avec les clients et les prospects** qui est en jeu.
- **Maîtriser les nouveaux risques numériques**. La **cyber-résilience devient un enjeu majeur** devant être supervisé par la direction générale (DG) de l'entreprise pour assurer le bon niveau d'investissement et de sensibilisation de l'ensemble des acteurs.

Dans ses « 7 résolutions numériques pour 2018 », le Cigref s'engage également dans sa quatrième résolution à : « **Positionner la sécurité des systèmes d'information comme condition indispensable de la confiance dans l'économie numérique** et comme domaine stratégique pour la compétitivité des entreprises et la performance des administrations. »

En effet, le numérique présente deux faces : d'une part, il offre des possibilités de développement peu imaginables il y a encore quelques années ; d'autre part, il met à la disposition d'acteurs potentiellement malveillants des outils puissants, générant de nouveaux risques auxquels il faut désormais faire face.

Mais avant de prendre les dispositions adaptées répondant à ces nouveaux dangers, il convient de positionner correctement le risque cyber, pour tous les acteurs de l'entreprise qui ont à le maîtriser, et pour ce faire disposer d'un canevas de réflexion, d'outils et d'indicateurs.

[2] Publication Cigref « Entreprise 2020 : Enjeux et défis »
[3] État recherché pour un système d'information lui permettant de résister à des événements issus du cyberespace susceptibles de compromettre la disponibilité, l'intégrité ou la confidentialité des données stockées, traitées ou transmises et des services connexes que ces systèmes offrent ou qu'ils rendent accessibles. La cybersécurité fait appel à des techniques de sécurité des systèmes d'information et s'appuie sur la lutte contre la cybercriminalité et sur la mise en place d'une cyberdéfense. (Source ANSSI)

Introduction

Le présent rapport s'inscrit dans la continuité de travaux antérieurs. En 2007, un Groupe de Travail (GT) sur les indicateurs de la sécurité a rédigé le guide pratique pour un tableau de bord sécurité stratégique et opérationnel. Plus récemment, en 2016, le rapport Cigref intitulé, « Le cyber risque dans la gouvernance de l'entreprise ; Pourquoi et comment en parler en COMEX ? » a été publié. En effet, un constat s'impose : les dirigeants demeurent plus ou moins bien sensibilisés au risque de sécurité informatique malgré les alertes lancées depuis plusieurs années à ce sujet. La cybersécurité semble encore parfois une affaire de spécialistes et reste déléguée à la filière Sécurité des Systèmes d'Information (SSI), là où une prise en compte réelle par l'ensemble des décideurs (mandataires sociaux, directions exécutives, direction des systèmes d'information…) apparaît comme indispensable, compte tenu de l'intensification de la menace.

Par ailleurs, lorsque les dirigeants décident de prendre à leur charge ce risque, ils se révèlent parfois désarmés, et en difficulté pour apprécier précisément **comment** et **où agir**. Il est donc primordial de pouvoir communiquer aux décideurs des entreprises et des organismes publics (Directions exécutives, Conseils d'administration), les points de repères leur permettant d'apprécier de la manière la plus juste possible, l'état de la menace et de leur exposition à cette menace, ainsi que les investissements qu'il leur appartient de mettre en œuvre pour sécuriser de la manière la plus adéquate leur activité.

Lorsque les risques de sécurité informatique sont bien positionnés sur l'échelle des priorités des risques à traiter par l'entreprise, il apparaît bien souvent que les moyens humains et financiers restent insuffisants. Car le retour sur investissement d'une dépense dans le domaine de la cybersécurité demeure particulièrement difficile à établir : il s'agit donc de trouver le bon niveau d'efforts à consentir dans ce domaine, sans survaloriser ni sous-estimer le risque.

En conséquence, un des rôles du directeur des systèmes d'information (DSI) ou de la personne en charge de la gouvernance cyber, est bien d'**expliquer** au COMEX et au Conseil d'administration les risques, mais également de les **qualifier** et de les **valoriser** à l'aide d'indicateurs pertinents. Ce qui nécessite de déterminer les outils et les indicateurs d'un tableau de bord dans ce domaine.

Le Cigref a souhaité identifier et structurer les informations stratégiques et les indicateurs indispensables pour permettre aux DSI de communiquer vers le COMEX, le Conseil d'administration ou les pouvoirs publics sur le risque cyber.

Ce rapport propose une structuration de la réflexion et des éléments de tableau de bord à adapter en fonction des caractéristiques de l'entreprise. Il précise ensuite les points clés de gouvernance, de méthode et de sensibilisation à prendre en compte en matière de cybersécurité. Enfin, en complément de la sécurisation des systèmes d'information, il devient nécessaire d'aborder la résilience et d'anticiper **dès à présent**, la mise en place d'une organisation adéquate en cas d'attaque majeure des SI.

1. Rapport et indicateurs du tableau de bord cybersécurité pour le COMEX

Cette partie présente l'ensemble des éléments et indicateurs à considérer lors de l'élaboration du tableau de bord cybersécurité. Le bon niveau de contenu d'un tel tableau de bord adressé au COMEX et Conseil d'administration repose sur un subtil **équilibre entre données d'actualité, informations qualitatives, analyses de risques consolidés, éléments de coûts, et indicateurs quantitatifs agrégés**. Il comporte systématiquement les rubriques suivantes qui sont détaillées tout au long de cette partie :

- Activités les plus exposées et chiffres clés du SI ;
- Niveau d'ouverture du SI à l'extérieur, et aperçu de son exposition ;
- Etat de la menace et actualité dans ce domaine ;
- Points essentiels de vulnérabilité de l'entreprise ;
- Analyse globale des risques cyber ;
- Points clés opérationnels ;
- Plans d'action en cours et à venir.

Le tableau de bord cyber doit être adapté en fonction des caractéristiques de l'entité économique concernée (entreprise – administration). Les éléments dans chacune de ses parties doivent être choisis pour permettre aux dirigeants de prendre les bonnes décisions pour couvrir le risque cyber. En effet, le rapport du tableau de bord cybersécurité doit être **extrêmement synthétique,** une page ou deux, **et accessible à des non-spécialistes.**

1.1. Décrire rapidement le SI et les activités les plus exposées

Plutôt qu'une description globale, les participants au groupe de travail Cigref proposent d'entrer directement dans le vif du sujet en présentant les activités les plus exposées aux risques et pourquoi elles le sont. S'appuyer sur l'actualité est un angle que l'on peut prendre pour décrire les deux ou trois activités ou organes du SI les plus exposés.

1.2. Donner les éléments sur la stratégie d'ouverture du SI

La cybersécurité ne devant pas être un frein à la transformation numérique, il est important **d'analyser l'évolution des risques cyber en fonction des stratégies d'ouverture de l'entreprise**. Certaines stratégies ont un impact dans l'ouverture du SI par exemple le recours plus large au cloud public, l'extension du télétravail, etc. Le DSI doit donc examiner les réponses à apporter et évaluer le niveau de service et d'exigence ainsi que les moyens à mettre en place pour accompagner cette évolution. Il s'agit donc bien d'indiquer à quel degré le SI de l'entreprise est ouvert et dans quelle mesure cette ouverture génère une réelle vulnérabilité.

1.3. Evaluer l'état de la menace - Eléments d'actualité

S'appuyer sur l'actualité est un bon moyen de présenter **la menace** et **ses risques** en la re-contextualisant par rapport à l'entreprise. Il faut démontrer la qualité de ses sources d'information, qui peuvent être grand public comme plus spécialisées, montrer comment est organisée la veille interne et le résultat de cette veille. Cette présentation de la menace sera par ailleurs **dynamique** et **montrera son évolution dans le temps**. Il s'agit donc ici de :

- Rendre compte très succinctement des éléments d'actualité ;
- Décrire la menace telle qu'elle est perçue en dehors de l'entreprise :
  - Incidents de sécurité les plus significatifs et évolution de la menace cyber (ransomwares, cibles connues, …) ;
  - Violations de données connues.
- Décrire l'impact des attaques externes et leur évolution dans la période passée.

1.4. Identifier les terrains de vulnérabilité de l'entreprise – Position par rapport aux autres entreprises du secteur

Pour qualifier le risque cyber, l'entreprise doit identifier ses talons d'Achille, ses terrains de vulnérabilité et de faiblesses qui peuvent être intrinsèques ou contextuelles. La nature et le nombre des vulnérabilités en cours de correction sont deux exemples de qualification du risque. Le classement des vulnérabilités permet de déceler les endroits de plus grandes fragilités. Il permet également de proposer les investissements prioritaires associés, en présentant une évaluation de l'impact financier d'attaques potentielles toutes les fois que cela sera possible. De plus, l'entreprise doit regarder si son niveau de contrôle existant est optimisé par rapport au risque actuel et à venir. L'objectif est de diminuer l'écart entre l'existant et l'attendu.

Se focaliser sur l'identification des principales faiblesses ne doit pas conduire à estimer que tout le reste est satisfaisant… Ces faiblesses doivent simplement faire l'objet d'une attention particulière.

Il est intéressant de présenter également lorsque c'est possible, où se positionne l'entreprise par rapport à celles du même secteur.

1.5. Mettre en place le dispositif global d'analyse des risques cyber et de pilotage - Décrire l'évolution des risques

En termes de gouvernance des risques, deux points clés sont à mettre en évidence :

- **le dispositif d'analyse des risques** qui doit intégrer une bonne compréhension de ce que sont les biens essentiels de l'entreprise ;
- **le dispositif de pilotage** pour montrer que l'organisation suit les consignes.

Le manager en charge du risque de sécurité informatique pour l'entreprise doit identifier les biens essentiels de l'entreprise. Fort de l'analyse de risque, il devra mettre en place un dispositif pour protéger ces biens, et mesurer l'efficacité de cette protection. Les managers de toutes les entités de l'entreprise doivent collaborer en lui précisant comment les risques métiers sont pilotés. Un plan de traitement des risques (précisé ultérieurement dans ce document) doit être mis en place, accepté et pris en compte par l'ensemble des acteurs.

Les résultats globaux de l'analyse des risques font partie des éléments à présenter au COMEX Ils peuvent décrire les points suivants :

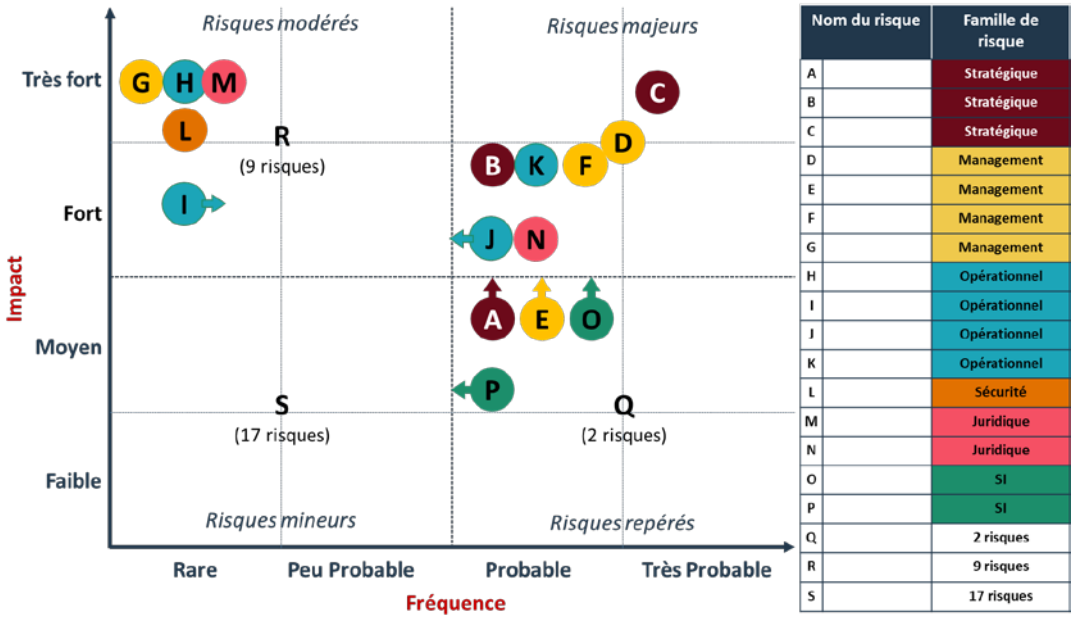
- Niveau de la menace cyber pour les différentes activités de l'entreprise : faible / moyenne / importante
- Description de l'évolution de la menace cyber dans l'entreprise ;
- Nombre d'analyses de risques mises à jour ;
- Nombre de nouvelles analyses de risque ;
- Réduction des risques par rapport à la cartographie établie :
  - Nombre de risques critiques non couverts
  - Nombre de risques critiques en cours de traitement
  - Nombre et type de nouveaux risques nouvellement découverts ;
- Nombre d'alertes de sécurité interne ou externe à l'entreprise ;
- Nombre et poids des incidents de sécurité (attaques ciblées, *ransomware*, …).

  Concernant le nombre d'incidents sécurité, il est important de noter que plus on est performant dans l'exploration, plus on détecte les incidents de sécurité. L'évolution croissante de cet indicateur peut refléter la capacité et l'efficacité de la détection d'incidents de sécurité. En résumé, il ne s'agit pas seulement de connaître le nombre d'incidents de sécurité, mais de **comprendre** et de pouvoir expliquer sa **variation et son évolution** ;
- Existence ou non d'un dispositif qui couvre les risques inconnus (Outil de cyber résilience)

Les analyses des risques et leur évolution se représentent très bien visuellement et la représentation est à choisir en fonction des finalités souhaitées.

Voici deux exemples de représentation possible.

Le premier exemple montre une représentation de l'impact des risques en fonction de la fréquence.



	Nom du risque	Famille de risque
A		Stratégique
B		Stratégique
C		Stratégique
D		Management
E		Management
F		Management
G		Management
H		Opérationnel
I		Opérationnel
J		Opérationnel
K		Opérationnel
L		Sécurité
M		Juridique
N		Juridique
O		SI
P		SI
Q		2 risques
R		9 risques
S		17 risques

Figure 1 : Collection Maitrise des Risques LA CARTOGRAPHIE DES RISQUES - AMRAE

Le deuxième exemple montre le niveau de sécurisation en fonction du domaine sous forme de radar.

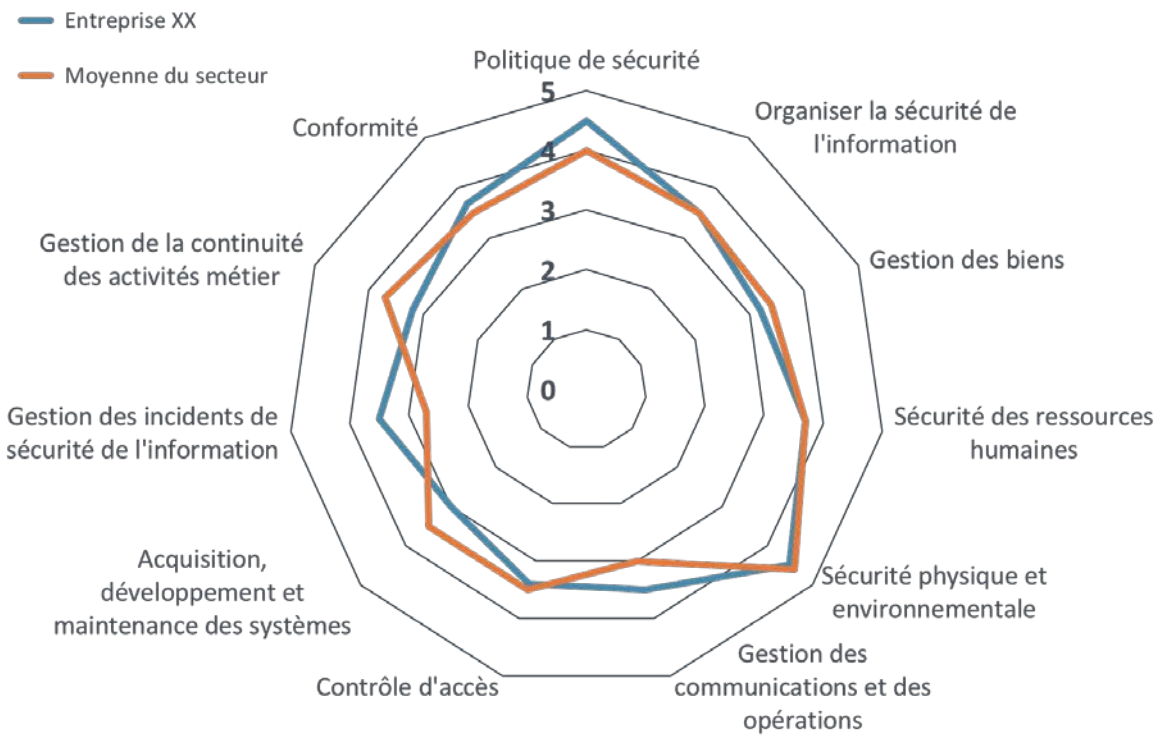


Figure 2 : Représentation visuelle radar – Source Cigref

D'autres représentations existent et des exemples sont donnés en annexe.

1.6. Expliciter les points-clés opérationnels

Les données fournies dans le rapport au COMEX doivent avoir un niveau de détails suffisant en fonction du contexte. Voici un certain nombre de points-clés qui ont été mis en évidence pour rendre compte de l'activité opérationnelle permettant de sécuriser l'entreprise dans le domaine cyber.

1.6.1. Description de la politique sécurité

Les indicateurs suivants peuvent être utilisés pour décrire la politique de sécurité :

- Existence et mise en place d'une politique sécurité ;
- Dates des dernières mises à jour de :
    - La charte informatique destinée aux utilisateurs avec les règles à respecter (internet, mails, mots de passe, médias sociaux, confidentialité…) ;
    - La politique de sécurité des SI (PSSI)[4] ;
    - Les politiques techniques de sécurité (PTS)[5] ;
- Niveau de respect des règles principales : indicateur de suivi de la conformité à la politique sécurité des différentes entités ;
- Niveau de couverture des sujets actuels (business, opérationnel, etc.). La PSSI les couvre-t-elle bien ? Sinon, est-elle en amélioration continue ?
- Le cas échéant, pour certaines administrations ou opérateurs d'importance vitale, niveau de conformité par rapport à la PSSI de l'Etat ;
- Suivi des dispositifs contractuels qui correspondent au niveau de conformité exigé par les clients. En d'autres termes, il s'agit de présenter comment est abordée la cyber sécurité dans l'écosystème de l'entreprise (clients, fournisseurs, etc.). En effet, la PSSI s'applique bien à une entité physique. Mais elle devient plus compliquée à établir dans le contexte de l'entreprise étendue (c'est-à-dire avec l'ensemble de son écosystème) ;
- Existence d'un PRA (Plan de Reprise d'Activité)[6] .

1.6.2. Description du Plan de Continuité d'Activité (PCA) en cas d'attaque et résilience en cas de panne du système d'information

Chaque cas d'attaque est différent, ce qui implique d'être agile. Il faut donc veiller à ce que le PCA et le PRA (Plan de Reprise d'Activité) soient en phase avec la VRAIE vie de l'entreprise. Il est donc nécessaire d'impliquer

[4] La PSSI reflète la vision stratégique de la direction d'un organisme, PME, PMI, grande entreprise, administration en matière de sécurité des SI – Source ANSSI
[5] La PTS décrit toutes les règles de sécurité applicables pour chacun des domaines techniques (serveurs, PC et portables, réseau, imprimantes, wifi, téléphonie, etc.)
[6] Un plan de reprise d'activité (*Disaster Recovery Plan – DRP*) a pour objectif de planifier le rétablissement, dans les meilleurs délais, d'une infrastructure informatique. Il vise à permettre la reprise opérationnelle des services en cas de sinistre. Source Cases.lu

tous les acteurs de la DSI, du numérique et de la sécurité ainsi que les dirigeants et tous les responsables métiers (abordé ultérieurement dans le document). Il est également important de porter son attention sur les points suivants :

- PCA de l'entreprise **et** de l'entreprise étendue en cas d'attaques cyber :
  - Nombre de tests effectués : réalisation de PCA(s) dans l'année écoulée ;
  - Objectifs atteints : indique si les objectifs fixés pour les tests ont été atteints ;
  - Respect du temps de rétablissement : indique si le temps de rétablissement prévu est respecté ;
  - Niveau de diffusion des comptes-rendus des tests de PCA en interne ;
  - Evolution de la partie résilience. Quel dispositif de continuité d'activité dans le cadre de l'entreprise étendue, notamment en cas de choc cyber majeur ?
- Pour le plan de secours informatique :
  - Réalisations de tests de PRA dans l'année ;
  - Objectifs fixés atteints pour les tests ;
  - Respect du temps de rétablissement ;
  - Respect perte maximale de données ;
  - Indicateur qui indique si les comptes rendus de test ont été diffusés en interne ;
  - Exercices de compromission cyber ;
  - Capacité de reconstruction à froid. Il est nécessaire d'avoir la capacité de nettoyer la situation puis de reconstruire à froid. Il faut, en attendant, pouvoir déterminer un système alternatif qui prenne le relais.

1.6.3. Menaces, attaques constatées et réponses apportées

Dans certaines entreprises, la notion de « défendabilité » est mise en avant : il s'agit de démontrer aux principaux décideurs que l'entreprise est capable d'identifier les attaques dont elle est la cible et les incidents de sécurité, d'analyser la crise en cours et d'y remédier rapidement. Cela passe notamment par l'existence d'un SOC, *Security Operations Center*[7].

Les indicateurs suivants peuvent être utilisés pour présenter les menaces et les attaques constatées ainsi que les réponses associées apportées :

- Nombre d'alertes de sécurité ;
- Nombre d'incidents de sécurité (virus, attaques ciblées, *ransomware*, etc.) et capacité à les traiter. [Cf. le référentiel d'incidents de sécurité dans la norme ETSI. La liste détaillée des indicateurs de sécurité : GS ISI 001-1 (Incidents) et ISI 001-2 (Vulnérabilités)] ;
- Nombre d'incidents avec un impact business et capacité à les traiter ;
- Nombre d'incidents majeurs et capacité à les traiter ;
- Actions prises pour répondre aux incidents listés ci-dessus ;

[7] Un *SOC* est un dispositif de supervision et d'administration de la sécurité du système d'information permettant, grâce à la collecte d'événements, de détecter des incidents de sécurité informatique, de les analyser et de définir les réponses en cas d'émission d'alertes et de dispositifs opérationnels de crise. Source : Sentryo.

- *Backlog* (liste d'actions à conduire) de résolution d'incidents et son évolution ;
- Coût du traitement après incident en terme ETP (Equivalent Temps Plein) ;
- Tentatives d'intrusion (nombre d'attaques et nombre d'interruptions de service) ;
- Attaques internet (type DDOS : *Distributed Denial of Service attack*[8], déni de service) ;
- Pertes de données/vols ;
- Erreurs humaines (écarts aux chartes informatiques, utilisateurs, administrateurs) ;
- Description de ce qui a été observé par l'équipe SOC (*Security Operations Center*) ;
- Chiffres et données des activités SOC ;
- Actions prises par l'équipe SOC.

1.6.4. Audits et leurs résultats

Le groupe de travail a identifié des indicateurs permettant d'informer le COMEX sur les audits.

- Nombre d'audits en cours de réalisation ou initialisés et leur résultat ;
- Nombre d'audits réalisés depuis 5 ans et leur résultat ;
- Les plans d'actions en cours.

Cela suppose que l'audit interne a la capacité de poser le problème et d'interroger les entités sur les questions relatives aux SI. Les auditeurs internes font généralement appel à des sociétés spécialisées pour cela. Dans cette partie, on pourra également rendre compte des conséquences des audits des commissaires aux comptes en matière d'exigences de cybersécurité.

1.6.5. Quelques indicateurs vitaux

Il est également nécessaire de rendre compte de l'activité cyber interne à l'organisation. Les indicateurs ci-dessous peuvent y aider :

- Description des actions clés prises sur les principaux process du SI ;
- Niveau d'intégration de la « *security by design* » dans les projets (taux de prise en compte de la sécurité dans les projets) ;
- Nombre de tests d'intrusion ;
- Détection et correction des failles et des vulnérabilités. Par exemple :
  - Nombre de vulnérabilités critiques à traiter en priorité (vulnérabilités retenues et à traiter en priorité) ;
  - Nombre de vulnérabilités critiques corrigées dans le semestre ;
  - Nombre de nouvelles vulnérabilités détectées dans le trimestre écoulé et retenues en haute priorité ;
  - Nombre de failles critiques restant à corriger ;
  - Nombre de vulnérabilités par rapport au nombre de machines du parc ;

[8] Une attaque par déni de service (abr. *DoS attack* pour *Denial of Service attack* en anglais) est une attaque informatique ayant pour but de rendre indisponible un service, d'empêcher les utilisateurs légitimes d'un service de l'utiliser. À l'heure actuelle la grande majorité de ces attaques se font à partir de plusieurs sources, on parle alors d'attaque par déni de service distribuée (abr.*DDoS attack* pour *Distributed Denial of Service attack*). Source : Wikipedia.

- Pourcentage et nombre de machines respectant la sécurité *(patch management)*.

- Description des actions prises concernant les personnes, notamment en matière de sensibilisation :
  - Existence ou non d'incitations financières liées à la cybersécurité dans les objectifs des managers et des collaborateurs de l'entreprise, et intégration d'une dimension cybersécurité dans les délégations de pouvoir ;
  - Nombre de messages SSI (messages de Sécurité des SI) vers les utilisateurs du SI. Une règle peut être par exemple d'envoyer un message de sensibilisation trimestriel à tous les utilisateurs ;
  - Pourcentage de personnes ayant participé à une campagne de sensibilisation ;
  - Niveau de sensibilisation de tous les acteurs de l'entreprise en fonction de leur rôle ;
  - Actions de formation.

1.6.6. Dispositifs techniques de protection et d'authentification - Habilitations et revues d'habilitations

Les indicateurs inventoriés ci-dessous rendent compte des dispositifs techniques de protection et d'authentification ainsi que des habilitations :

- Dispositifs de protection du réseau et des dispositifs de supervision de sécurité
- Etat du parc bureautique :
  - Protection antivirale (nombre de PC et portables avec antivirus à jour)
  - Protection Système d'exploitation (pourcentage de postes avec système d'exploitation à jour)
  - Système de chiffrement
- Etat du parc applicatif (serveurs applicatifs) :
  - Protection antivirale
  - Système d'exploitation mis à jour
  - Système de chiffrement
- Dispositifs de gestion des habilitations :
  - Revues d'habilitations d'accès au SI et aux applications sensibles
  - Corrections réalisées suite aux revues
  - Existence d'un système d'authentification unifiée : applications éligibles / applications raccordées / applications suivies

Certains points peuvent être ajoutés, par exemple, déterminer comment est effectuée la gestion des droits et la limitation des comptes à privilège, préciser quelles sont les fonctions et personnes clés, etc.

1.6.7. Dispositifs techniques de détection

Description des choix technologiques adoptés : niveau de couverture du SOC, outillage utilisé, nombre de règles de détection d'incidents, utilisation ou non de l'intelligence artificielle dans la détection d'incidents…

1.6.8. Dispositifs techniques et organisationnels de réaction

Ces dispositifs techniques et organisationnels de réaction viennent en ajout au plan de continuité d'activité.

- Dispositifs de crise
- Nombre d'exercices effectués et résultats

1.6.9. Conformité aux textes internes de l'entreprise et conformité aux textes réglementaires (RGPD, NIS, etc.)

Pour aborder la conformité, les éléments suivants peuvent être utilisés :

- Positionnement par rapport aux autres entreprises du secteur ;
- Protection des données personnelles RGPD : écarts à la conformité dus au SI ;
- Conformité aux directives (typiquement la directive NIS[9] : *Network and Information Security)* et aux régulations sectorielles en matière de sécurité.

1.6.10. Visualisation des points clés opérationnels

Les points clés opérationnels se représentent bien visuellement. Un exemple de présentation est donné ci-après avec des pastilles de couleurs vert/orange/rouge, qui précisent le positionnement des indicateurs. Une flèche permet de visualiser l'évolution dans le temps. Dans l'exemple suivant, les flèches précisent l'évolution par rapport à la présentation précédente.

[9] Url de la directive NIS : https://www.ssi.gouv.fr/entreprise/reglementation/directive-nis/

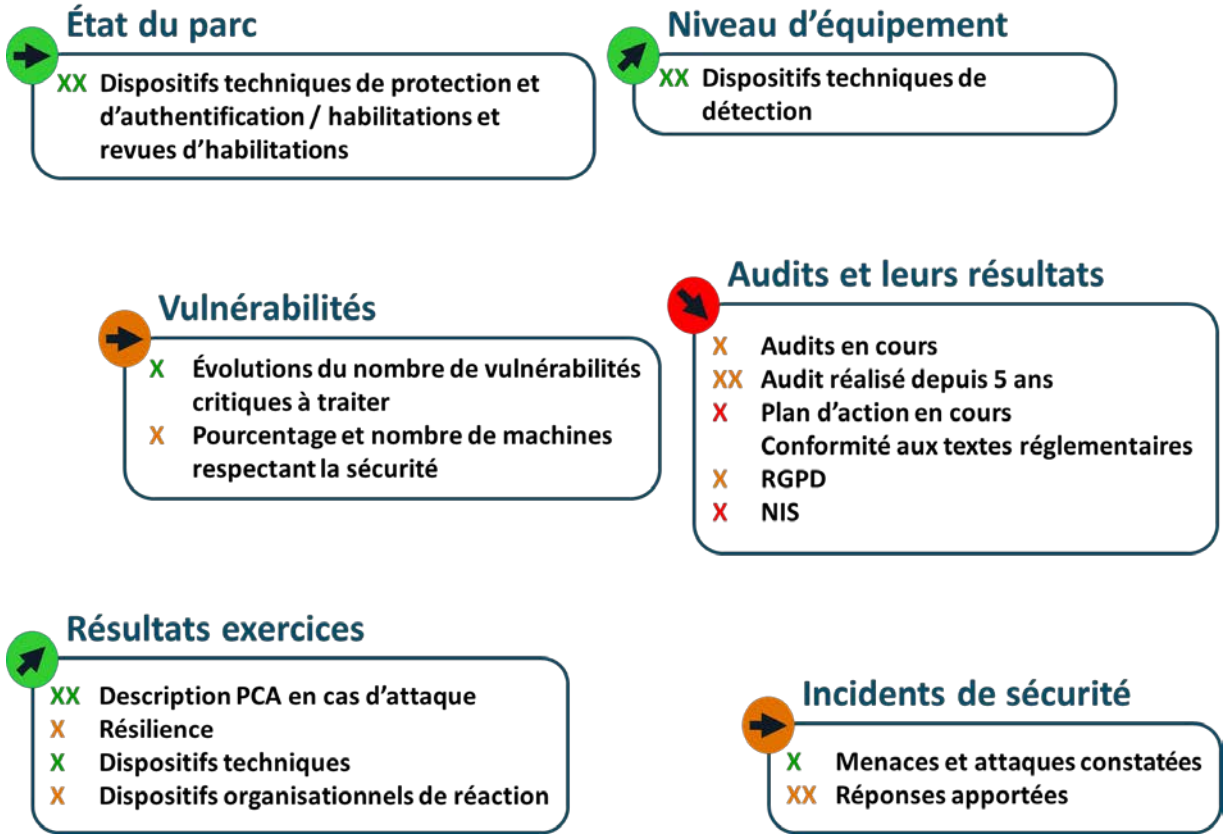


Figure 3 : Exemple de présentation des points clés opérationnels – Source Cigref

1.6.11. Déterminer le plan d'action et faire le suivi

Une fois le plan d'action déterminé, il s'agit de faire régulièrement un suivi des actions décidées pour réduire l'exposition au risque cyber et de manière récursive ajouter de nouvelles actions si nécessaire.

2. Gouvernance, méthode et sensibilisation

Suite à la structuration du tableau de bord cybersécurité, il convient de préciser quelques questions de gouvernance, de méthode, de confiance et de sensibilisation.

Auparavant, il faut prendre en considération le caractère protéiforme de la menace qui peut se révéler locale ou internationale. Elle est surtout susceptible d'évoluer au fil du temps. Anticiper la menace future est un exercice primordial bien que la nature des attaques à venir ne soit pas toujours connue. Il demeure néanmoins nécessaire d'essayer de sécuriser les SI face à tous les risques avec la même importance.

Cette problématique touche particulièrement les compagnies d'assurance lorsqu'elles proposent des produits couvrant le risque de sécurité informatique. Elles ont besoin de disposer de bases statistiques pour mutualiser le risque et se heurtent très souvent à cette difficulté méthodologique. La peur du risque systémique, c'est-à-dire d'une catastrophe cyber qui affecterait simultanément un très grand nombre d'acteurs, s'ajoutant à la problématique d'anticiper une menace future, conduit certains assureurs à une aversion au risque cyber supérieure à celle de leur client potentiel : cela freine considérablement le développement de produits assuranciels en la matière.

Le groupe de travail a eu, au cours de la préparation de ce rapport, l'occasion d'échanger avec un réassureur, qui a exposé sa méthodologie : il s'agit bien pour lui d'évaluer la maturité cyber des entreprises et de comprendre leur exposition à ce risque. Selon son domaine d'activité, l'entreprise est exposée à des risques cyber différents : pertes de données (personnelles, financières, stratégiques, etc.), extorsion (rançongiciel, chantage au déni de service), fraude, perte d'exploitation sans dommage matériel qui représente une vraie caractéristique des dommages informatiques, piratage informatique qui modifie les caractéristiques des produits, cyber-attaque donnant lieu à des dommages physiques (sabotage). Partant de cette classification des impacts, le réassureur cherche à structurer la mesure de l'exposition client au risque pour rendre cette mesure répétable pour d'autres prospects. Il cherche ainsi à déterminer prioritairement la sévérité et l'incidence du cyber risque.

Comme indiqué plus haut, l'appréciation du risque auquel est exposée l'entreprise peut également reposer sur l'appréciation du niveau de maturité de celle-ci par rapport à ses homologues (concurrents par exemple). Mais là encore, l'information peut se révéler difficile à obtenir, rendant l'exercice quelque peu hasardeux. Quoiqu'il en soit, la filière des SI devra tenter de corréler le maximum d'informations pour parvenir à une appréciation crédible de l'état de l'exposition à la menace cyber.

2.1. Acteurs à impliquer dans la stratégie de cybersécurité

Les managers qui agissent directement dans le domaine de la sécurité des systèmes d'information ont besoin à leur niveau de disposer d'indicateurs analytiques et spécialisés.

Le **Responsable de la Sécurité des Systèmes d'Information (**RSSI) doit disposer très régulièrement (au minimum mensuellement) **d'indicateurs techniques** lui permettant de piloter finement des actions opérationnelles de sécurisation du système d'information.

Le **DSI**, lui, doit apprécier précisément si la sécurisation de l'ensemble des composantes du SI est bien adaptée aux missions et aux performances attendues. Il doit également disposer **d'indicateurs mensuels**, en nombre sans doute plus limité que ceux dont dispose le RSSI, et il doit disposer **des principales analyses de risque portant sur le SI** dont il est responsable.

Il peut être utile de mandater un **directeur cybersécurité** en charge de la supervision de l'ensemble du risque cyber, avec un périmètre dépassant le simple système d'information. Le numérique s'étend aujourd'hui à tous les secteurs d'activité. Les responsables des équipements, produits et systèmes sur lesquels repose le fonctionnement complet de l'entreprise doivent se préoccuper des conséquences éventuelles de dysfonctionnements liés à des problèmes de sécurité informatique. Le directeur cybersécurité peut être particulièrement utile pour les entreprises disposant d'un système industriel (contrôle commande d'une installation industrielle par exemple), parce qu'il apporte une vision d'ensemble du risque cyber et une meilleure maîtrise des interfaces entre organisations ou entre systèmes. A ce niveau de responsabilité, il lui est essentiel de disposer des analyses de risques cyber de l'ensemble des activités de l'entreprise ou de l'administration, à une fréquence garantissant la validité de ces analyses de risques, à adapter en conséquence.

Lorsque l'entreprise ne dispose pas d'un directeur cybersécurité, elle peut élargir le périmètre de responsabilités de son RSSI afin d'étendre sa vision du risque cyber au-delà du périmètre du SI, et lui désigner un correspondant dans chaque direction opérationnelle.

Au niveau global de l'entreprise, les **membres du COMEX** doivent savoir si une attaque informatique est susceptible de porter atteinte de manière significative à l'activité de l'entreprise voire, de manière ultime, de mettre en danger sa survie. La teneur de tout compte rendu d'activité communiqué au COMEX doit être orientée vers cet éclairage, de manière à lui donner une idée la plus juste possible du **bon niveau d'investissement à consentir pour couvrir le risque cyber**. La périodicité d'examen de cette question en COMEX paraît être à tout le moins annuelle, au plus trimestrielle.

Enfin, annuellement, le **Conseil d'administration** doit être informé des conséquences éventuelles d'atteintes à la sécurité informatique sur la **valeur même de l'entreprise, ses actifs et sa réputation**. Le niveau d'informations qui peut lui être transmis est de même nature que les informations transmises au COMEX.

Le tableau de bord cybersécurité doit être adapté au type d'interlocuteur : davantage quantitatif, analytique et opérationnel lorsqu'il est destiné au RSSI ; plus synthétique et davantage stratégique lorsqu'il s'adresse au top management de l'organisation.

2.2. Gouvernance du risque cyber

L'informatique irrigue aujourd'hui tous les produits, systèmes et processus de l'entreprise ou de l'administration publique. Les menaces visant la sécurité informatique couvrent un large périmètre : tous les **systèmes d'information internes (bureautique, industriel**, **de gestion, etc.)** mais aussi leurs interactions avec **l'ensemble des partenaires de l'écosystème** (y compris ceux de la maintenance, de l'entretien, etc.). La menace cyber concerne donc les acteurs de toutes les fonctions de l'entreprise et les personnes en charge de la gouvernance des données (en particulier les DPO[10] suite à l'arrivée du Règlement Général sur la Protection des Données personnelles), de la qualité et de la sécurité du patrimoine. Une crise informatique n'est donc pas forcément une crise du système d'information, au sens traditionnel du SI de gestion. Elle peut porter sur les autres métiers.

C'est pourquoi, les participants au groupe de travail du Cigref sont unanimes à considérer que pour informer correctement les niveaux décisionnels les plus élevés dans l'organisation (COMEX, CA), l'analyse des risques de sécurité informatique doit être **transverse et globale à l'entreprise.**

Différents étages interviennent dans la gouvernance du risque cyber pour mener les actions d'analyse du risque, de pilotage des mesures de prévention et de remédiation (comme les dispositifs de crise). Ces actions s'effectuent au niveau global et aux niveaux opérationnels dans les différents métiers. Au niveau global, transverse et stratégique, les personnes en charge du management du risque doivent avoir autorité sur l'ensemble des managers opérationnels de l'entreprise pour imposer la remontée d'informations et assurer l'alignement des actions entreprises ; ils peuvent s'adjoindre le concours de collaborateurs issus de la DSI ; c'est aussi à ce niveau que doivent être traités les risques cyber apparaissant à la frontière des directions, par exemple à la frontière entre les systèmes d'information de gestion et les systèmes d'information industriels ; **toutes les zones de flou dans les organisations entre directions et/ou filiales, doivent être considérées comme des zones à risques à traiter à ce niveau** ;

La **gouvernance cyber** au sein de l'entreprise peut être portée par le DSI, le directeur cyber (fonction nouvelle dans les entreprises qui souhaitent nommer un dirigeant de haut niveau, précisément pour piloter le plan de traitement des risques cyber à l'échelle de l'ensemble de l'entreprise), le directeur des risques ou encore le RSSI. Elle doit fortement impliquer les responsables du « *risk management* ». Une des entreprises membres du Cigref a choisi de confier directement cette responsabilité d'évaluation du risque cyber global à sa direction des risques. D'autres préfèrent laisser au RSSI cette responsabilité, en raison de la spécificité de ce risque et de la technicité requise pour l'appréhender. Quelle que soit l'organisation mise en place, les DSI doivent aussi avoir, à leur niveau et pour le système d'information proprement dit, des équipes responsables d'analyses de risques, qui transmettent les éléments au responsable chargé du management global du risque cyber de l'entreprise.

Point à noter : dans certaines entreprises, une partie des activités industrielles peut faire l'objet d'une réglementation spécifique, par exemple, le domaine du nucléaire. Dans ces domaines particuliers, la gestion du

[10] DPO : Délégué à la protection des données

risque est assurée par l'entité soumise à la réglementation spécifique. Cependant, il est nécessaire de l'intégrer dans la vision globale du risque, au niveau de l'entreprise.

Point le plus important : celui qui assure le pilotage global doit impérativement pouvoir joindre et piloter tous les acteurs de toutes les fonctions de l'entreprise pour tout ce qui concerne l'évaluation et la couverture des risques cyber.

Enfin, il est primordial que l'organisation mise en place pour couvrir ce risque cyber soit :

- décrite de façon formelle ;
- stable dans le temps, c'est-à-dire qu'elle résiste aux mouvements internes ou externes des collaborateurs (dirigeants et managers). Une organisation trop figée et donc trop lisible de l'extérieur peut toutefois représenter une vulnérabilité ;
- révisable et reformalisée rapidement lors de changements dans l'activité.

Pour finir, il conviendra d'assortir cette gouvernance d'un dispositif permettant d'apporter aux principaux dirigeants de l'entreprise une information sur les risques pour l'entreprise ou sur les organisations d'attaques relayées dans la presse et ce, avec une grande réactivité.

La pièce maîtresse d'un bon tableau de bord dans le domaine cyber est donc l'analyse des risques, sur laquelle il convient d'apporter quelques précisions.

2.3. Importance de l'analyse de risques

L'analyse de risques, régulièrement actualisée, doit s'appuyer sur une méthodologie précise et quantifiée, pouvant reposer sur des référentiels internes de l'entreprise. Dans tous les cas, cette méthodologie devra permettre d'aborder les points suivants :

- **l'état de la menace** sur l'activité de l'entreprise, et le niveau de maturité de celle-ci face à la menace par rapport à ses homologues ;
- **les incidences** d'une crise cyber, en fonction de la sensibilité des systèmes examinés et des données traitées ; ce sont les métiers qui doivent être impliqués dans la détermination de la sensibilité de leurs données et des processus qu'ils gèrent, selon un référentiel fixé par l'entreprise. La gouvernance doit décrire à la fois qui porte cette responsabilité côté métier et qui fixe le référentiel ;
- la réalité des mesures prises :
  - pour prévenir la crise et se protéger au mieux ; la gestion des correctifs ou « *patch management* » fait partie de ces mesures de prévention ;
  - pour observer ce qui se passe dans le SI de l'entreprise et comment évoluent les menaces en dehors de l'entreprise, pour pouvoir anticiper les crises et réagir au plus vite ;
  - pour assurer la continuité de l'activité et gérer la crise si elle survient ;
  - pour revenir au plus vite dans un état nominal après une crise.

Il convient toutefois de noter que l'analyse de risque de la sécurité informatique est particulièrement ardue à réaliser : en effet, il est toujours difficile d'apprécier réellement, voire de quantifier précisément, l'état de la

menace. En outre, pour les attaques déjà survenues dans certaines entreprises, il est quasiment impossible pour une personne extérieure, de connaître exactement les cibles qui ont été touchées et leurs conséquences, tant cette information sensible demeure couverte par le secret des affaires. C'est la raison pour laquelle la probabilité d'occurrence du risque cyber demeure difficile à établir. Et c'est aussi pourquoi une entreprise qui consent à des investissements en matière de sécurité informatique peut ne pas voir son risque évoluer d'une année à l'autre. Ce risque peut rester à un niveau élevé, tout simplement en raison d'une appréciation à la hausse de l'état de la menace. Cette difficulté méthodologique peut alors conduire à un certain découragement, même si cette impression d'un effort vain s'avère être – trop – souvent erronée. Dans tous les cas, il est nécessaire pour le DSI de **démontrer au Conseil d'administration et au COMEX que les investissements consentis sont utiles**, par exemple parce qu'ils ont permis de parer à telle ou telle attaque. Cet effort de communication permet de crédibiliser le besoin d'investir dans ce domaine où le retour sur investissement est particulièrement difficile à calculer.

2.4. Mutualisation de la veille cyber

Seuls les exemples les plus spectaculaires des attaques cyber ont fait l'objet d'une communication large, souvent avec l'aval des Présidents des sociétés concernées et dans le cadre d'une communication externe maîtrisée. Il apparaît donc nécessaire aux membres du groupe de travail qu'**une petite communauté d'acteurs de confiance soit constituée pour qu'une information suffisante permettant d'apprécier l'état réel de la menace puisse circuler**. Cette petite communauté serait constituée de personnes de l'administration et de la filière des systèmes d'information de grandes entreprises.

Par ailleurs, disposant de ces analyses de risques utilisables dans un dialogue avec le COMEX et le Conseil d'administration, et avant de présenter un tableau de bord plus circonstancié et un dossier décisionnel en la matière, il conviendra de s'interroger sur le niveau de sensibilisation à la question cyber des principaux décideurs ; si la cybersécurité n'a pas été abordée auparavant dans les instances dirigeantes, il conviendra de réfléchir à des moyens de les sensibiliser davantage.

2.5. Sensibilisation du COMEX aux risques cyber

À la suite d'attaques retentissantes sur les SI de certaines entreprises survenues en 2017, certains COMEX sont très sensibilisés au risque cyber, au point que certains d'entre eux parlent désormais de « déni de production », pour qualifier des attaques qui conduisent à l'arrêt d'usines de production.

Mais d'une manière générale, la sensibilisation des COMEX au risque cyber demeure difficile à effectuer, souvent en raison du manque de temps des décideurs. Toutefois, on peut envisager différentes méthodes de sensibilisation / information / formation des acteurs de ce niveau de responsabilité comme :

- Des exercices de crise cyber,
- Des mises en situation réelles : *phishings*[11] (ou hameçonnages),
- Des simulations d'exercices d'interviews avec un journaliste, pour la communication post-crise,
- Une formation courte en deux temps : une première session avec un regard externe donné par des spécialistes (par exemple l'ANSSI, ou des cabinets juridiques) et une deuxième avec les principaux points de faiblesse de l'entreprise présentés par les équipes de risques et d'audit et les spécialistes de la cybersécurité.

La sensibilisation doit être adaptée au contexte de l'entreprise : en effet, la **sécurité** des systèmes d'information **ne bloque pas mais s'adapte au métier et le sécurise**.

La **notation cyber par un tiers peut également constituer un bon outil de sensibilisation**. Celle-ci, effectuée par une société spécialisée, évalue la performance cybersécurité de l'entreprise. Elle s'appuie sur l'empreinte publique de l'entreprise (les tests ne sont pas intrusifs et donc factuels et objectifs). La notation permet par ailleurs de fixer des objectifs chiffrés pour des directions internes, des fournisseurs, des clients, etc. Elle permet également d'établir une émulation avec un classement des entités.

2.6. La question de la confiance

La question de la confiance est un point à considérer lors d'un échange sur la question de la cybersécurité avec les instances dirigeantes des entreprises ou des administrations.

Si la sécurisation informatique des activités est la condition *sine qua non* de **la confiance des administrés dans les services numériques** offerts par les administrations, elle est aussi la pierre angulaire de la **confiance des clients, envers leurs fournisseurs** vendeurs de produits, services ou systèmes informatisés. Et elle conditionne également la **confiance des salariés envers leur employeur** dans la mesure où ce dernier collecte des données personnelles les concernant. En résumé, il n'est pas possible d'envisager une société numérique sans confiance, et la confiance n'est possible qu'à travers la sécurisation, la maîtrise et le contrôle des activités numériques.

Face à une telle attente de l'ensemble des acteurs (administrés, clients, salariés, etc.), les dirigeants des entreprises ou des administrations doivent acquérir la confiance dans le niveau de sécurisation de l'activité dont ils portent la responsabilité. Or, les problématiques de cybersécurité sollicitent parfois des niveaux de spécialisation et de technicité élevés, inaccessibles aux dirigeants. Il est donc important d'assurer la communication entre les experts qui apprécient le niveau de sécurisation à mettre en place pour soutenir – et non freiner - l'activité de l'entreprise, et les dirigeants qui portent des responsabilités lourdes et vitales pour leur entité. Ce rôle de « passeur » entre le COMEX et les filières sécurité du système d'information constitue l'une des fonctions notables du DSI. Pour être reconnu dans ce rôle de passeur, le DSI devra lui-même inspirer confiance : cela passe par sa propre connaissance des métiers et des enjeux de l'entreprise, et sa crédibilité dans le domaine des systèmes d'information.

[11] Vol d'identité ou d'informations confidentielles (codes d'accès, coordonnées bancaires) par subterfuge : un système d'authentification est simulé par un utilisateur malveillant, qui essaie alors de convaincre des usagers de l'utiliser et de communiquer des informations confidentielles, comme s'il s'agissait d'un système légitime. Source Wikipédia.

2.7. Le dispositif normatif dans lequel s'inscrit la cybersécurité

Pour compléter ce chapitre sur la « Gouvernance, méthode et sensibilisation », il convient de préciser que **le déploiement d'actions de sécurisation informatique doit s'inscrire dans un dispositif normatif efficace**.

Il est nécessaire de disposer d'un référentiel qui décrit **comment l'entreprise répond à l'ensemble des risques** et **identifier les responsables**. Sur cette base, il devient possible pour chaque entité de l'entreprise d'évaluer son degré d'avancement dans son plan de mise en conformité au référentiel, par exemple par un pourcentage, et d'en rendre compte de manière auditable. La consolidation de ces résultats au niveau global donne alors un aperçu de la manière dont l'entreprise maîtrise le risque cyber.

Comme la conformité ne doit pas nuire à la réactivité, cette approche doit être complétée par une observation permanente de la réalité des événements (attaques cyber par exemple) qui peuvent affecter l'entreprise ou son environnement. En effet, c'est sur la base de cette observation que l'appréciation des vulnérabilités réelles exposant l'activité peut être ajustée et la priorisation des actions à entreprendre révisée. Il est nécessaire qu'au niveau global de l'entreprise, des décisions immédiates puissent être prises, priorisant au plus haut niveau et pour un temps court le risque cyber. Cela peut consister, par exemple, à imposer à l'ensemble des métiers une démarche de mise en place de « patches » dans les meilleurs délais. La gouvernance doit aussi prévoir ce type de dispositif.

Naturellement, pour assurer l'observation des événements de sécurité, il faut pouvoir disposer de compétences de haut niveau, au-delà de l'outillage ; ce sont elles qui, *in fine*, permettent d'apporter la garantie de la qualité de la veille et de l'anticipation, ainsi que de la réactivité de la structure.

De plus, venant infléchir une démarche de pure conformité aux référentiels, la démarche de couverture du risque résulte toujours d'un **compromis entre les objectifs de sécurisation poursuivis et les moyens**, notamment les compétences et les moyens financiers que l'entité peut allouer à cette activité. La manière dont ce compromis est effectué doit pouvoir être exposée par les responsables aux différents niveaux de l'organisation.

Enfin il est nécessaire de s'assurer régulièrement de la pertinence et de l'utilité des actions déjà effectuées.

Chez certains membres du Cigref, la notion de « défendabilité » est mise en avant. Il s'agit de démontrer aux principaux décideurs que l'entreprise est **capable d'identifier les attaques** et les **incidents de sécurité dont elle est la cible**, **d'analyser la crise en cours et d'y remédier rapidement**. Cela passe notamment par l'existence de SOC et de dispositifs de crise opérationnels.

En résumé, il faut un **dispositif normatif** et **montrer que l'entreprise y est conforme**. Il faut compléter ce dispositif par une **observation de la réalité cyber** et avoir **établi une priorisation** : le traitement de tel risque est prioritaire par rapport au reste des priorités de l'entreprise. Il est enfin nécessaire pour l'entreprise d'être en mesure de **répondre dans les plus brefs délais aux questions des mandataires sociaux et directeurs exécutifs**.

3. Cyber attaque majeure : quelle organisation ?

En complément des approches classiques en matière de sécurisation des SI, qui peuvent en dernière instance s'assimiler à des démarches globales de prévention, il devient aujourd'hui **nécessaire d'aborder la question de la résilience**. La situation générée en 2017 dans certaines entreprises par l'attaque « NotPetya[12] » oblige à considérer que même si certains risques cyber ressortent aujourd'hui avec une probabilité faible, leur réalisation doit être considérée comme possible et **l'entreprise doit s'y préparer**.

Les **entreprises doivent réfléchir dès à présent à leur organisation en cas d'attaque informatique réussie**. Le but est d'évaluer les conditions de poursuite d'un certain niveau d'activité en mode extrêmement dégradé et de prévoir également la communication de crise dans ce type de circonstance. Le cas d'école type est la disparition soudaine de l'ensemble du SI (par exemple par une paralysie des *Active Directory*[13]).

Se poser la question en amont permet de réfléchir aux alternatives et d'identifier les solutions d'organisation, notamment en vue de protéger les sites et les activités les plus critiques.

3.1. Aspects géopolitiques

Quelles que soient les démarches de prévention mises en œuvre, une des raisons pour lesquelles l'hypothèse du choc cyber doit être prise en compte, est de nature géopolitique. Certaines attaques ciblant les SI répondent aujourd'hui à des intérêts étatiques. Les attaquants disposent de moyens de plus en plus importants. Enfin, les attaques informatiques malveillantes revêtent un niveau sans cesse accru de sophistication. Toutes les entreprises peuvent être victimes d'une attaque. La cyber sécurité devient donc un champ de bataille « militaire ». En d'autres termes, nous entrons dans une époque de « guerre cybernétique » dont chaque entreprise peut être soit la cible, soit une victime collatérale.

L'ANSSI travaille sur la détection des attaques graves pour l'économie et les secteurs vitaux, et sur la réaction à y apporter. Elle se positionne sur le fonctionnement des attaques et sur leur remédiation davantage que sur l'identification des attaquants. La plupart des attaques sont silencieuses mais le niveau de menace est élevé toute l'année. En général, avant d'agir, les groupes d'attaquants commencent par maîtriser le réseau par une observation patiente et discrète.

L'ANSSI peut mettre à disposition des grandes entreprises certains moyens d'appui. Néanmoins, si plusieurs entreprises d'importance vitale venaient à être touchées simultanément en France, elles devraient compter prioritairement sur leurs propres capacités parce que les moyens de secours mobilisables par l'Agence pourraient ne pas suffire.

---

[12] L'article « *The untold story of notpetya, the most devastating cyberattating cyberattack in history*", disponible sur l'url https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world décrit l'attaque informatique majeure de NotPetya et son impact dans deux grandes entreprises.

[13] L'*Active Directory* est la mise en œuvre par Microsoft des services d'annuaire LDAP pour les systèmes d'exploitation Widows. L'objectif principal d'*Active Directory* est de fournir des services centralisés d'identification et d'authentification à un réseau d'ordinateurs utilisant le système Windows. Il permet également l'attribution et l'application de stratégies, l'installation de mises à jour critiques par les administrateurs.

3.2. Points clés pour préparer l'action

Les points clés à aborder en préparation d'un choc cybernétique majeur sont de même nature que ceux examinés dans une approche plus classique de sécurisation des SI ; simplement, les réponses apportées à ces différents points deviennent spécifiques. Nous proposons une liste d'actions pouvant constituer le cœur d'un plan de résilience à mettre en œuvre dans l'entreprise, dans les paragraphes suivants.

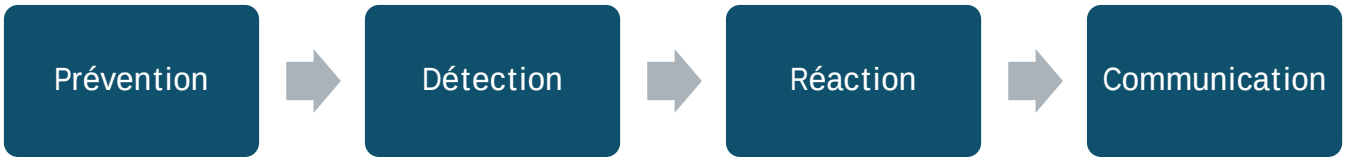


Figure 4 : Etapes de gestion de crise – Source Cigref

3.2.1. Préparer la crise résultant d'une cyberattaque majeure et réussie

- **Anticiper la direction de crise** et identifier qui prendra les décisions. La chaîne de commandement doit être simplifiée, raccourcie et clairement définie autour du DSI.
- **Constituer une *core team* managériale** : un plan doit être mis en place pour mobiliser des ressources internes et externes qui seront à 100% impliquées et qui savent où/quand/comment se retrouver à l'instant T. On doit connaître leur disponibilité sur les 3 mois à venir, et avoir leur numéro de téléphone.
- **Rassembler/centraliser les départements critiques** : équipes télécoms et infrastructures. Lorsque les infrastructures de l'entreprise sont fragmentées, il est nécessaire de centraliser leur supervision et de mutualiser les compétences des personnes pouvant intervenir.
- **Préparer les moyens de communication de secours** : en particulier, dans des circonstances extrêmes, il est vital de pouvoir communiquer de manière descendante des messages courts aux principaux acteurs concernés. La messagerie risque d'être inutilisable (et ce n'est pas un outil de gestion de crise), et on privilégiera des outils sécurisés dédiés.
- **Développer un écosystème de prestataires privés de confiance** : établir des liens « crise cyber » avec ses partenaires, prestataires et fournisseurs AVANT la crise cyber pour savoir sur qui compter et de quelle manière. Il est nécessaire d'anticiper sur ce qui sera demandé à ces prestataires le moment venu.
- **Préparer des Plans de Continuité d'Activité** spécifiques à ce type de circonstance : en crise cyber, on est le plus bloqué là où l'activité est la plus informatisée. Il est donc nécessaire de préparer partout où c'est nécessaire une poursuite du travail sans l'outil informatique.
- **Tester ses capacités de détection/réaction** avec des scénarios d'attaques informatiques de niveau élevé, puis débriefer sur chacune d'elles avec les équipes.

3.2.2. Mesures d'urgence à mettre en place dès les premières minutes/premières heures

- **Bloquer la propagation** : isoler ce qui a été touché, les organes vitaux, et les sites critiques de l'entreprise et le cas échéant les arrêter pour assurer cette séparation. En effet, il vaut mieux stopper l'activité pendant une journée pour protéger les sites et activités les plus critiques que de refuser une interruption de service pouvant se révéler à terme extrêmement dommageable ;
- Protéger ce qui n'a pas été touché ;
- Démarrer le « *restore* » avec des équipes dédiées en soignant particulièrement l'organisation :
  - Organiser la vie des personnes mobilisées (nourriture 24h/24h, base vie pour repos, etc.) ;
  - Gouverner jour par jour un *steering committee* quotidien avec le DG/PDG, suivi éventuellement d'une communication courte vers les principaux managers de l'entreprise ;
  - Constituer des équipes de résolution de crise avec les experts :
    - Equipe de gestion de projet dédiée
    - Equipe communication dédiée
    - Utilisation de plusieurs fils de communication
  - Respecter à la lettre les consignes de l'ANSSI ;
  - Limiter le temps de résolution de chaque problème, au-delà duquel une escalade auprès du DSI doit être assurée.
- **Donner des dates de résolution** : le DSI doit pouvoir s'engager sur des dates de résolution de l'attaque par segment et sur une date de retour à la normale.

Par ailleurs, il est nécessaire d'avoir à l'esprit le fait que **dans ce type de circonstances, la communication interne et externe est un enjeu majeur** : il faut donc prévoir d'expliquer ce qui s'est passé au top management, aux investisseurs, aux directeurs métiers, aux clients, aux commissaires aux comptes, etc.

Enfin, le DSI doit anticiper les dispositions qu'il devra prendre pour assurer sa propre disponibilité et lucidité pendant toute la durée de la crise, et ce pour éviter son propre épuisement par exemple.

Conclusion

Les dirigeants des entreprises ou des administrations demandent et doivent acquérir la confiance dans le niveau de sécurisation de l'activité dont ils portent la responsabilité.

Ils doivent donc savoir comment une cyber-attaque est susceptible de porter atteinte de manière significative à l'activité de l'entreprise, à sa valeur, à ses actifs et à sa réputation, voire de manière ultime à mettre en danger sa survie. Ils ont besoin pour cela d'un **rapport extrêmement synthétique** qui leur donne le bon niveau d'information pour être à même de déterminer ensuite, **le niveau d'investissement adéquat à consentir pour couvrir le risque cyber**.

En adaptant aux spécificités de son entreprise le tableau de bord cybersécurité défini dans ce document, le DSI a les éléments pour construire ce rapport ou cette présentation synthétique et accessible à des non spécialistes.

Cependant, la cybersécurité devient un enjeu militaire et une arme géopolitique. Nous sommes entrés dans une époque de « guerre cybernétique » dont chaque entreprise peut être soit la cible, soit une victime collatérale. **Le DSI, soutenu par les dirigeants et entouré par ses équipes opérationnelles, doit dès à présent se préparer aux risques d'une crise résultant d'une attaque informatique majeure réussie des systèmes d'information** et réfléchir aux mesures d'urgence à mettre en place dès les premières minutes/heures de celle-ci. En effet, **dans les situations extrêmes, l'implication directe du DSI est le facteur déterminant de la capacité de l'entreprise à surmonter le choc cybernétique**.

Annexe

D'autres exemples de visualisation d'analyses de risques sont donnés dans cette annexe.

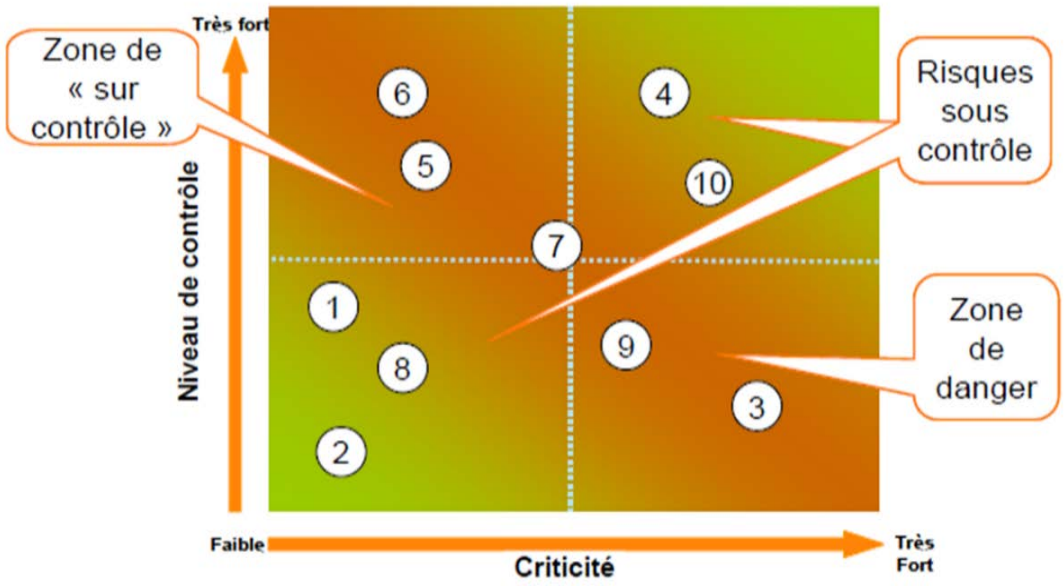


Figure 5 : Collection Maitrise des Risques LA CARTOGRAPHIE DES RISQUES - AMRAE

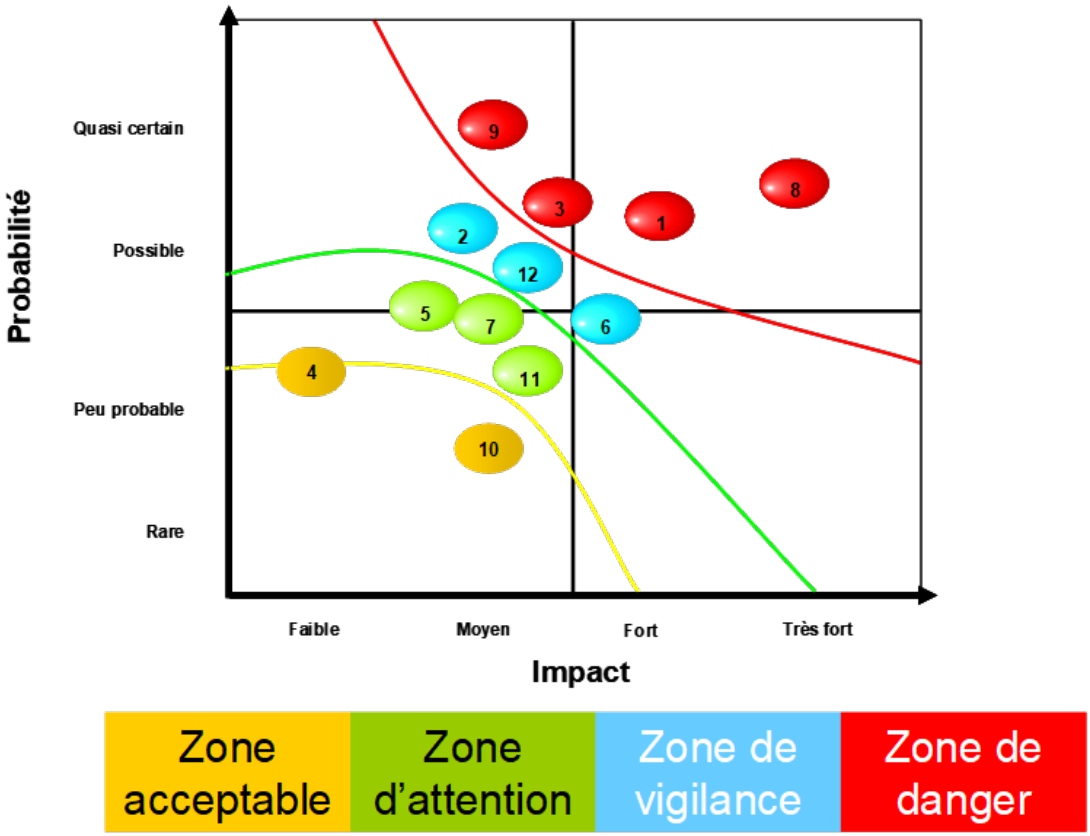


Figure 6 : Collection Maitrise des Risques LA CARTOGRAPHIE DES RISQUES - AMRAE

On peut enfin, s'appuyer sur un abaque (graphique permettant de donner la solution d'un calcul) qui permet d'évaluer les risques selon 3 critères : le niveau de la prévention et le niveau des dispositifs de réponse à incident, appréciés en fonction du niveau de la menace ; un exemple est fourni ci-dessous :

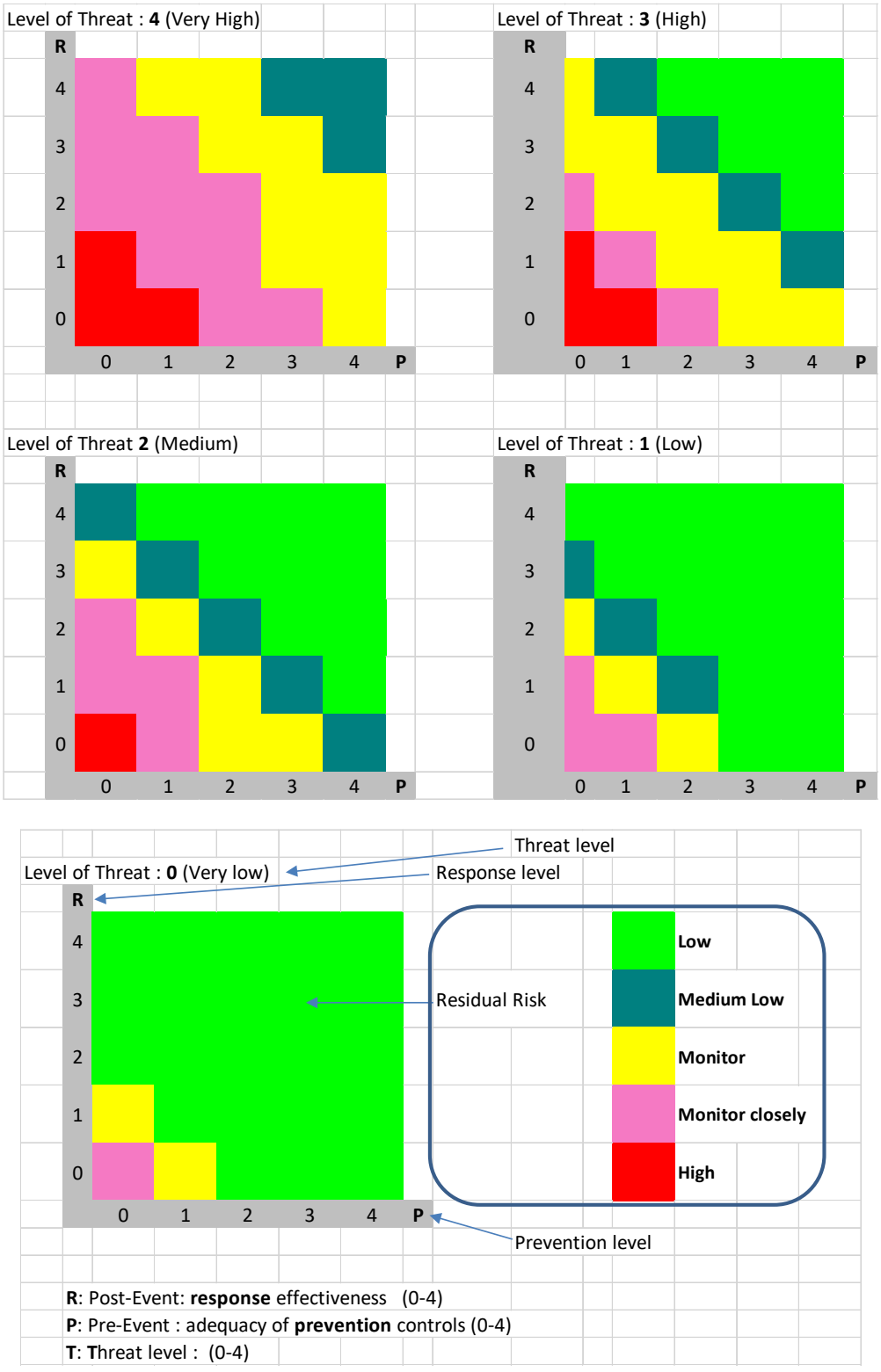


Figure 7 : Visualisation des risques sous forme d'abaque - Source Cigref


Cigref
RÉUSSIR
LE NUMÉRIQUE

À PROPOS DU CIGREF
ACTEUR DE LA SOCIÉTÉ NUMÉRIQUE

Association des grandes entreprises et administrations publiques françaises, le Cigref se donne pour mission de développer leur capacité à intégrer et maitriser le numérique.

RÉSEAU DE GRANDES ENTREPRISES

Association loi 1901 créée en 1970, le Cigref n'exerce aucune activité lucrative. En 2018, il regroupe près de **150 grandes entreprises et organismes français utilisateurs de systèmes numériques**, dans tous les secteurs d'activité.

ACTEUR DU NUMÉRIQUE

Par la qualité de sa réflexion et la représentativité de ses membres, **il est un élément fédérateur et acteur important de la société numérique.**

AU SERVICE DE SES MEMBRES

Sa gouvernance est assurée par **15 Administrateurs**, élus en Assemblée générale. Son activité est animée par une équipe de **10 permanents.**