Guide pratique pour les PME/PMI : Méthodologie de gestion de crise cyber

Oscar ADEOSSI
Toussaint BASANTU MIESI
Léon-Darin MINTSA MI NZOGHE

Cette étude a été réalisée dans le cadre d'un projet pédagogique de l'École de Guerre Économique. La méthodologie présentée, bien que se voulant factuelle, ne prétend aucunement à l'exhaustivité. Il s'agit essentiellement d'une méthode d'analyse complémentaire des études menées jusqu'à présent sur le sujet. Elle ne saurait en aucun cas se substituer à ces dernières.

INTRODUCTION

Nous sommes le 11 Septembre 2017. La société *Clermont pièces* situé au Brézet à Clermont Ferrand vient de subir une cyberattaque d'envergure. En effet un virus a ciblé les systèmes d'information de l'entreprise et a réussi crypter les fichiers clients, fournisseurs, l'historique de production mais aussi les données comptables. En clair, plus aucune donnée de l'entreprise n'est utilisable. Devant cette situation dramatique, Eric Thomas, dirigeant de la société n'a autre choix que de cessé l'activité. *Clermont pièces* est mis en liquidation judiciaire au tribunal de commerce de Clermont-Ferrand après 30 ans d'activité[1].

Des PME et ETI qui subissent ce triste sort, il y en a des dizaines chaque année. Le chiffre est en constante augmentation. Lors du Forum International sur la Cybersécurité qui s'est tenu à Lille en Janvier 2020, le Directeur Général de l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI), Guillaume Poupard a déclaré[2] : « si toutes les TPE/PME françaises venaient à subir de vastes attaques informatiques sur une courte période de temps, cela pourrait engendrer un désastre économique ». La Confédération des Petites et Moyennes Entreprises (CPME) estime même que 4 entreprises sur 10 de moins de 50 salariés ont été victimes d'une cyberattaque en 2019. Etant donné que les TPE, PME et ETI représentent 99,8% des entreprises française et emploient 1 Français sur 5 le risque de déstabilisation de l'économie tout entière par des opérations de cyberattaques massives est réel. Si les grandes entreprises, à l'image de St-Gobain avec l'attaque NotPetya en 2017, ont la capacité d'absorber le choc (tout de même 220 millions de perte de chiffre d'affaire), les plus petites entreprises ne sont pas du tout armées pour surmonter de tels attaques.

Quelques chiffres clés expliquent l'engouement est cybercriminel pour les PME :

- **65%** des PME ne dispose d'aucune politique de protection des données.[3]
- **10**% des dépôts de plainte pour acte de cybercriminalité donnent lieu à des condamnations[4]
- **96%** des attaquants parviennent à percer les différents rideaux défensifs des PME[5]
- **58%** des dirigeants de PME ne mesurent pas le risque des cyberattaques.[6]

D'autant plus qu'avec les nouveaux usages qui s'installent dans les entreprises et notamment le télétravail, utilisation de multiples terminaux tels qu'ordinateurs personnels non sécurisés, téléphone portable, les risques ont explosé et les attaques aussi. Face à ce constat alarmant les PMEs française n'ont autre choix que de réagir très fortement. Il faut absolument en finir avec le discours de l'entreprise qui n'a pas de valeur pour des cybercriminels.

De trop nombreuses entreprises ont une sécurité des systèmes d'information totalement défaillante. Les investissements en solutions de cybersécurité ont certes augmenté, mais la bonne utilisation de ces outils et l'éducation des employés demeurent de trop gros points noirs.

Afin de permettre aux dirigeants de PME et aux responsables de la sécurité de ces entreprises d'avoir une meilleure ;

- Connaissance des enjeux
- Maitrise des outils à leur disposition

[1] *Victime d'un piratage informatique, la société Clermont Pièces va fermer boutique,* La Montage, 22/09/2017.
[2] Les cyberattaques contre les TPE/PME explosent… un danger pour notre économie, Silicon.fr, 03/06/2020.
[3] Office des Nations Unies contre la drogue et le crime.
[4] *Ibid.*
[5] Etude FireEye et Mandiant, une entreprise FireEye.
[6] Ponemon Institute.

- Prise de décision et mise en œuvre de la stratégie de défense

Nous proposons dans ce guide pratique une méthodologie de gestion de crise cyber qui permettra aux dirigeants de PME de prendre les premières mesures nécessaires pour protéger l'avenir de leurs sociétés et par conséquent de la sécurité économique de la France.

I. LES CONCEPTS DE L'ANALYSE DE RISQUES CYBER

1. Cadre et Méthodologie de l'étude

L'objet de la présente étude vise à guider de manière pratique les dirigeants de PME et PMI dans la « gestion des crises cyber ». Pour limiter au mieux le contour de ce sujet, il est essentiel dans un premier temps de préciser ce que nous entendons par :

- Risque IT.
- Gestion du risque.
- Crise.
- Gestion de crise.
- Cyber.
- PME et PMI.

1.1 Définition retenue pour décrire la notion de « Risque IT »

Selon le référentiel 31000 de l'International Standard Organisation (ISO) le « risque » est définit comme :

- « **L'effet de l'incertitude sur les objectifs**
  Un effet est un écart par rapport à un attendu. Il peut être positif, négatif ou les deux à la fois, et traiter, créer ou entraîner des opportunités et des menaces.
  Les objectifs peuvent avoir différents aspects, être de catégories différentes, et peuvent concerner différents niveaux.
  Un risque est généralement exprimé en termes de sources de risque, événements potentiels avec leurs conséquences et leur vraisemblance. »

- Le « COBIT 5 for Risk » de l'ISACA nous propose la définition suivante :
  « *Le risque informatique est défini comme le risque commercial, en particulier le risque commercial associé à l'utilisation, propriété, exploitation, implication, influence et adoption des Systèmes d'informations au sein d'une entreprise* »
  En nous appuyons sur cette base, la définition du « risque IT » que nous avons choisi de retenir est la suivante :

Le risque informatique est le risque commercial d'un écart positif ou négatif par rapport à un attendu, lié à l'utilisation, la propriété, l'exploitation, l'implication, l'influence et l'adoption des systèmes d'informations au sein d'une entreprise.

1.2 Définition retenue pour décrire la notion de « Gestion du risque »

Alors que le risque 0 n'existe pas, il parait évident voir même vitale pour l'entreprise de définir une approche de gestion des risques liés à l'informatique. L'ISO 31000[7] nous propose la définition suivante de la gestion du risque :

« La gestion des risques est l'identification, l'évaluation et la hiérarchisation des risques, suivies d'une application coordonnée des ressources pour minimiser, surveiller et contrôler la probabilité et / ou l'impact d'événements malheureux ou pour maximiser la réalisation des opportunités »

1.3 Définition retenue pour décrire la notion de « Crise »

[7] ANSI/ASSP/ISO 31000-2018 Risk.

De nombreux auteurs se sont penchés sur la notion de « crise » dans les entreprises. L'un des plus important est *Leonard Fuld*. Pionnier de l'intelligence économique et de la veille concurrentielle il écrit dans son ouvrage *The secret language of competitive* :
« *Le manque de transparence peut signifier que la direction ne voit pas ou ne veut pas voir des informations concurrentielles importantes et vitales. Parfois, cela peut conduire à une crise* »
Nous comprenons donc qu'une crise est essentiellement le fait du comportement et de la compréhension des réalités par les parties prenantes au sein d'une organisation. Par parties prenantes nous entendons toute personne, groupe ou entité morale qui a des intérêts ou une préoccupation dans l'entreprise. Il peut s'agir des directeurs, des employés, l'état, les fournisseurs et l'écosystème via lequel l'entreprise génère ses ressources.
Nous pouvons donc retenir la définition suivante pour le terme « crise » :

Un évènement brutal provocant l'effet de surprise et une déstabilisation considérable des ressources d'une organisation. Le degré de complexité de l'évènement fait perdre ses repères à l'organisation et rend incertain l'évaluation des résultats, ce qui par conséquent nécessite la mise en place de mesure extraordinaire par les différentes parties prenantes.

1.4 Définition retenue pour décrire la notion de « Gestion de crise »

En ce qui concerne le terme « gestion de crise » nous retenons la définition proposée par le portail de l'IE[8] :

« La gestion de crise est la méthodologie d'action d'une entreprise, d'un état ou de collectivité territoriale face à une crise ponctuelle, souvent violente, qui peut être de type naturelle (catastrophe), économique, physique, psychotique, ou encore les crises liées à l'information, la réputation ou les ressources humaines. La gestion va permettre de préparer, de réaliser et d'analyser de manière prospective les réactions de l'entreprise face à une crise. »

1.5 Définition retenue pour décrire la notion de « cyber »

Les outils et les réseaux informatiques ont pris une très grande part dans le fonctionnement des organisations et plus particulièrement des entreprises. Avec l'explosion de l'internet est apparu à la fin du XXème siècle l'expression cyber.
Le dictionnaire Larousse le définit comme :
Un préfixe servant à former de très nombreux mots relatifs à l'utilisation du réseau Internet.
Les anglo-saxons donnent une définition plus approfondie du terme « Cyber ». Le site internet Webopedia spécialisé en définition des termes TECH, propose la définition suivante :
Cyber est un préfixe utilisé dans un nombre croissant de termes pour décrire de nouvelles choses rendues possibles par la propagation des ordinateurs et des appareils. Tout ce qui touche à Internet relève également de la catégorie cyber.
Sur cette base, nous pouvons donc retenir la définition suivante :

Le préfix Cyber est utilisé pour matérialiser toutes les activités rendues possible par l'usage des ordinateurs et du réseau internet.

[8] Centre de ressources et d'information sur l'intelligence économique et stratégique.

Figure 1. Mots avec le préfixe « cyber ».

1.6 Définition retenue pour décrire la notion de « PME & PMI »

Pour cette étude nous retiendrons la définition de l'INSEE[9] :

« Les petites et moyennes entreprises (PME) sont celles qui, d'une part, occupent moins de 250 personnes, d'autre part, ont un chiffre d'affaires annuel n'excédant pas 50 millions d'euros ou un total de bilan n'excédant pas 43 millions d'euros. Elles incluent la catégorie des microentreprises. (MIC) qui occupent moins de 10 personnes et ont un chiffre d'affaires annuel ou un total de bilan n'excédant pas 2 millions d'euros. »

2. L'incident Cyber

Précédemment nous avons défini le cyber comme un environnement dans lequel les activités des organisations, notamment des entreprises sont rendu possible grâce l'utilisation des outils informatiques et l'internet. Par conséquent parler d'incident cyber c'est évoquer des événements qui surviennent par le canal de ces mêmes outils et impactent leur bon fonctionnement. Le COBIT va plus loin en précisant qu'il s'agit : « *de tout évènement qui ne fait pas partie du fonctionnement normal d'un service et qui cause, ou peut causer, une interruption ou une réduction de la qualité de service* ».

2.1 Approche phénoménologique de l'incident Cyber

L'incident Cyber dans la plupart des cas est le fait d'une action humaine visant à déstabiliser une organisation :

- Affecter les *systèmes d'informations et les réseaux de l'entreprise* ; IT, Serveurs, …
- Affecter les *processus de production* de la richesse ; Machine outils, robots…
- Vols de *données personnelles* ; base de données clients, données du personnels…
- Vols d'*informations sensibles* et vitale pour l'entreprise ; projet de recherche, brevet…

La dégradation des services informatiques ou des systèmes de productions d'une entreprise est une conséquence directe d'actions menées par un ou plusieurs **cybercriminels** toujours plus expérimentés et déterminés. Pour mener à bien ces activités nuisibles les cyberattaquants vont rechercher les **points d'entrés** du réseau informatique ciblé. La difficulté pour l'entreprise est d'anticipé ce type d'activité de d'exploration (physique ou numérique). Les failles de sécurité sont si nombreuses qu'un cybercriminel compétent et déterminé peut s'introduire dans le réseau de l'entreprise en quelques minutes et y installer un logiciel

[9] Institut national de la statistique et des études économiques

malveillant qui passera inaperçu pendant des mois. Une fois la ou les failles identifiées et le programme malveillant déployé, les cyberattaquants peuvent subtiliser des données et compromettre les infrastructures de l'entreprise. Il est donc primordial pour les entreprises de toute taille de mettre au point et déployer des stratégies fortes et performantes de cybersécurité afin de : **prévenir**, **détecter** et **neutraliser** ces menaces cyber.

2.2 Déroulements d'une cyberattaque

Pour développer les meilleurs stratégies cybersécurités dans une entreprise il est essentiel de comprendre le déroulement d'une attaque cyber. On ne le dira jamais assez mais il est établi que les cyberattaques les plus sophistiqués peuvent rester invisible sur le réseau de l'entreprise durant plus de 200 jours. Planification soignée et précision d'exécution sont les maitres mots. C'est pourquoi les cybercriminels les plus doués savent rester à couvert et exécuter leurs charges dévastatrices au bon moment. Même si les typologies des cyberattaques peuvent très différentes, généralement les schémas d'attaques suivent les mêmes logiques. Voyons ensemble ce schéma type.

Une cyberattaque peut être séquencé en 7 étapes[10] :

1-Reconnaissance

Avant de lancer d'une attaque, les attaquants s'appliquent d'abord à identifier la cible vulnérable et détermine le meilleur moyen de l'exploiter. Cette cible peut être n'importe quelle personne au sein de l'entreprise ; un dirigeant, un administrateur ou encore un prestataire externe. Les hackers ont simplement besoin d'un point d'entrée pour enclencher leur mission. C'est pourquoi les e-mails phishing sont très courant à ce niveau de la cyberattaque. Très efficace pour introduire efficacement un malware.

2-Exploration

Dès que la cible est identifiée par les cyber attaquants, l'étapes qui suit consiste à identifier le maillon faible leur permettant de s'infiltrer. En tirant profit d'outils facilement trouver sur internet les cybercriminels procède à l'exploration du réseau de l'entreprise. En fonction de la complexité du réseau de l'entreprise cette étape peut prendre du temps, parfois même des mois, le temps de repérer les vulnérabilités exploitables.

3-Accès et élévation

Une fois les failles de sécurité identifiée, les attaquants se frayent un accès et remontent. La plupart du temps, il est indispensable d'avoir un accès privilégié car cela permet aux agresseurs d'avancer en toute liberté au sein de l'environnement de l'entreprise cible. Afin de subtiliser les identifiants les infiltrés utilisent des tableaux Rainbow et d'autres outils comparables. L'objectif ici est de remonter les privilèges au niveau Admin et ainsi s'introduire dans tout système du réseau accessible au travers de ce compte Admin. Dès que les assaillants obtiennent les privilèges élevés, ils prennent investissent le réseau de l'entreprise, lequel est « à leur merci » désormais.

4-Exfiltration

Ayant tout, les droits et capacité de circuler sur le réseau, les cybercriminels sont susceptibles d'avoir accès aux systèmes détenant les données les plus critiques de l'entreprise qu'ils peuvent ainsi extraire à leur guise.

5-Attente

[10] Les sept étapes d'une cyberattaque réussie, William CULBERT, Beyond Trust.

Bien souvent pour que l'opérations soit la plus fructueuse possible, disposant d'un accès sans restriction au réseau ciblé, les assaillants adopte une stratégie de mise en « sommeil ». Durant cette période les hackers peuvent installer des programmes malveillants indétectable tel que des root kits. Ainsi ils peuvent faire des va et viens selon leurs envies. Les privilèges obtenus plus haut élimine la dépendance à un point d'accès unique.

6-Assault
C'est l'étape à laquelle le cauchemar de l'entreprise prend toute sa dimension. Même si ce n'est pas le cas de toutes les cyberattaques, c'est à ce moment que les cybercriminels risques d'altérer la fonctionnalité des équipements matériels d'une cible ou tout simplement les désactiver. L'exemple qui fait cas d'école aujourd'hui est l'attaque Stuxnet sur des infrastructures critiques (centrifugeuses d'enrichissement d'uranium) en Iran. Au moment de l'assaut, l'attaque n'a été que de courte durée. Bien souvent à ce stade de l'attaque, il est trop pour l'organisation cible d'organiser une autodéfense contre la compromission.

7-Obfuscation
Après l'attaque, les agresseurs numériques ont l'option d'adopter deux postures : Soit essayer d'effacer leurs traces ou bien au contraire laisser une carte de visite pour se vanter de leurs exploits. Le but principal de l'obfuscation est de brouiller l'enquête légale, de rendre l'investigation confuse et de désorienter les enquêteurs. De nombreux et techniques permettent d'appuyer cette stratégie tel que le nettoyage de fichiers journaux, de spoofing, de désinformation, de comptes zombis, de commandes de chevaux de Troie etc.

2.3 La typologie des attaquants

Il existe autant de motivations et de typologies d'attaquants qu'il y a de cibles. Les éléments qui permettent de baser une typologie des cybercriminels sont notamment la conjonction des mobiles interpersonnels et les mobiles comportementaux.
Cela nous permet dresser 3 catégories d'attaquant : Les amateurs, les professionnels et les activistes politiques.

2.3.1 Les amateurs

Au-delà de ce que l'on pourrait imaginer la différence entre les cybercriminels amateur et professionnel ne se situe pas sur le niveau de compétence technique à mener des actions malveillantes mais surtout sur leur degré de vénalité. En effet là où l'appât du gain est le moteur principal du professionnel, l'attaquant amateur sera plus à la recherche d'une forme de reconnaissance sociale.
Les cybercriminels en quête de reconnaissance sociale peuvent être catégorisé en 4 groupes :

a) Les curieux
Ce sont des personnes motivées par les nouveaux défis intellectuels généré par internet, les réseaux et l'informatique.

b) Les vandales
De la même manière les casseurs prennent du plaisir dans la délinquance classique, les vandales cyber délinquant tirent du plaisir dans la destruction des systèmes d'informations.

c) Les vengeurs

Un autre groupe de cyber attaquants mènent des opérations de nuisances par soucis de vengeance. La vengeance fait suite à une blessure morale subie dont le but est de se faire justice soi-même. Bien souvent il s'agit d'anciens employés en sécurité informatique ressentant le besoin de se venger en essayant de rationaliser leurs actes. Cette vengeance peut se matérialiser par le fait de s'en prendre à une entreprise ou encore à une personne en la manipulant ou en la harcelant.

d) Les antisociaux

Internet d'une certaine manière génère chez certains utilisateurs le besoin de célébrité et de pouvoir. Les cybers attaquants considérés comme antisociales recherchent la célébrité et le pouvoir, ils sont désadaptés socialement et recherchent la reconnaissance de leurs pairs. Dans cette catégorie on peut inclure les fanatiques qui s'attachent plus être reconnu socialement dans leur travail qu'à l'apport financier de leur acte qui sont très performant depuis le plus jeune âge[11] ainsi que les novices motivés par la notoriété que rapporte le crime, le besoin de reconnaissance et le défi.

2.3.2 Les professionnels

Comme vu plus haut le point différenciant entre les amateurs et les professionnels c'est le degré de vénalité : les professionnels recherchent le profit. En effet, ces profils sont essentiellement animés par la cupidité ou l'appât du gain. Dès lors, chez les criminels professionnels du cyberespace le mobile financier est le mobile le plus répandu ce qui les poussent à toucher toutes les cibles selon les besoins du « marché » : les personnes, les entreprises et les institutions. Pour les entreprises on distinguera les menaces émanant de l'intérieur de l'entreprise, les fraudeurs internes et les attaquants agissant depuis l'extérieur, les fraudeurs externes.

- *Les fraudeurs internes*
  Le fraudeurs interne n'est plus ni moins qu'un employé d'une compagnie qui infiltre les ordinateurs de son entreprise pour le compte d'un concurrent dans le but d'un gain financier. En effet, le fraudeur est commandité par une autre entreprise qui est son véritable supérieur hiérarchique. On parle plus communément d'espionnage industriel. On pourrait faire entrer dans cette catégorie les professionnels clandestins, c'est-à-dire les concurrents directs de l'entreprise visée, les fonctionnaires ou encore les mercenaires pouvant aussi bien agir pour le compte d'institutions privées ou publiques.

- *Les fraudeurs externes*
  A la différence du fraudeur interne, le fraudeur externe agit pour son propre compte et n'est salarié d'aucune entreprise. Ils sont le plus souvent ces cybercriminels professionnels qui pénétreraient les ordinateurs motivés pour un gain financier personnel. Ce peut être de simples personnes isolées ou des intermédiaires commandités ou engagés pour mener à bien des actions de nuisances sur une entreprise.

2.3.3 Les activistes politiques

[11] Net-profiling : analyse du comportement des cybercriminels, Nadine TOUZEAU.

Le troisième et dernier mobile du cybercriminel est complètement détaché de toute considération vénale. C'est un mobile qui touche une population beaucoup plus large et diverse comparé aux professionnels ou aux amateurs. Cette catégorie regroupe les cybercriminels motivés par l'aspect idéologique et politique. Ce sont donc des membres de toutes les sensibilités ou mouvance politique et idéologiques qui peuvent être amené à engager des opérations de cyberattaques contre des entités publiques, des entreprises ou toues organisation. L'activisme peut être définit comme une « doctrine ou une pratique qui met l'accent sur une action directe et vigoureuse pour exprimer son appui ou son opposition à l'égard d'une question controversée » ou encore « une théorie ou une pratique basée sur une action militante »[12].

2.4 Typologies des menaces cyber

Comme vu précédemment, la motivation première des cybercriminels de l'internet est l'appât du gain. Il y a les « ouvriers » qui fabriquent les logiciels malveillants tandis d'autres se les appropries afin de commanditer des œuvres criminelles. Il n'est pas aisé de dresser une typologie exhaustive de la cybercriminalité néanmoins on constate que les moyens à la disposition des cyber attaquants sont colossaux.

En effet, à l'origine vue comme de simples nuisances dans les organisations, les virus, les messages indésirables et autres logiciels espions sont aujourd'hui les outils de choix des cyber-délinquants. Les professionnels de la cybercriminalité n'hésitent pas à les vendre pour alimenter la fraude en ligne. Des actions d'envergures mondiales sont lancées à l'encontre d'entreprise et d'organisme publiques et de multiples infractions sont ainsi commises. Ces attaques sont produites de manière industrielle et les cybercriminels espèrent une réponse favorable d'une victime potentielle.

Il suffit par exemple aux cybercriminelles d'expédier massivement un message électronique non désiré contenant des codes malveillants, des vers, virus, chevaux de Troie et cela à des millions de personnes à travers le monde. Une fois ouvert par les victimes, le programme viendra s'installer sur leur poste de travail. Il ne reste plus qu'aux cybercriminel de remonter la route numérique pour subtiliser des données voir saboter l'outil de travail de sa victime.

Tout comme les trafiquant d'armes ou les narco trafiquants, les cybercriminelles sont désormais très structurées, ce qui en fait une délinquance **organisée** et **mondialisée**.

2.4.1 Une délinquance organisée

a) La boîte à outils des cybercriminels

Les cybercriminelles disposent de nombreux moyen pour structurer leurs attaques. Parmi ceux-ci on peut nommer ; les chevaux de Troie, les logiciels espions, les botnets, les virus, les vers et les keyloggers.

Les chevaux de Troie

Le cheval de Troie n'est pas un logiciel ayant la capacité de se reproduire. Sa dangerosité réside sur le fait qu'une fois installé sur l'ordinateur cible il permet d'ouvrir une « *porte* » qui permettra de prendre ultérieurement le contrôle ou activer à distance des programmes nocifs appelés « *malwares* ». Ce type de logiciel n'est rien d'autre que le véhicule, celui qui fait entrer le programme malveillant à l'intérieur de la machine. Il

[12] « De la passivité à l 'activisme des investisseurs institutionnels au sein des corporations », Raymonde Crete et Stéphane Rousseau.

n'est pas nuisible en lui-même car il n'exécute aucune action, si ce n'est de permettre l'installation du vrai programme malveillant. En soi le cheval de Troie n'est pas nuisible car il n'exécute pas d'action spécifique. C'est essentiellement l'installation du programme malveillant qu'il embarque qui fait toute sa force.
Le moyen le plus commun et favorable de sa propagation sont les messages électroniques. Le plus souvent ces programmes sont destinés au vol de données personnels.

Les logiciels espions
En anglais ces programmes sont connus sous la dénomination « spyware ». C'est un terme générique qui désigne l'ensemble des logiciels espions qui s'introduisent dans un système informatique afin de recueillir à des fins commerciales le profil d'un utilisateur au regard de sa navigation sur le réseau Internet, voire le cas échéant obtenir des informations personnelles comme les références d'une carte bancaire, d'un permis de conduire ou tout autre document personnel et sensible.

On retrouve très souvent ce type logiciels espions inclus dans des logiciels gratuits et s'installent généralement à l'insu de l'utilisateur en même temps qu'il télécharge le logiciel en question. Ils sont souvent développés par des sociétés proposant de la publicité sur Internet. Pour permettre l'envoi ultérieur de publicité ciblée, il est nécessaire de bien connaître sa cible. Cette connaissance est grandement facilitée par ces logiciels espions.

Les botnets
Le terme générique botnet vient de la contraction des mots anglais « ro**bot** » et « inter**net** ». Il désigne un groupe d'ordinateurs, de quelques milliers à plusieurs millions, contrôlés par un pirate à distance. Agissant comme des « zombies » ce sont en réalité des programmes informatiques destinés à communiquer avec d'autres programmes similaires pour l'exécution de différentes tâches.
La plus connue consiste à prendre le contrôle à distance, en exploitant une faille de sécurité via un cheval de Troie ; par exemple, des milliers d'ordinateurs zombies forment un réseau de milliers de robots appelés communément des "botnets"[13]. Ces milliers d'ordinateurs contrôlés seront autant de relais pour permettre des attaques puissantes puisque les pirates pourront alors depuis leur domicile diffuser des codes malveillants tout en cachant leur identité. Les enquêteurs, dans le meilleur des cas, arriveront sur des ordinateurs dont les propriétaires sont également des victimes. Ces botnets représentent aujourd'hui une réelle menace pour notre société[14].

Les virus et les vers
Les virus et vers sont les deux exemples de logiciels malveillants les plus répandus et les plus connus. Ils ont la capacité de s'autorépliquer sur les ordinateurs ou via les réseaux informatiques et d'infecter les ordinateurs à l'insu de leurs utilisateurs. Ils peuvent pour la plupart causer d'importants dégâts sur les réseaux informatiques ciblés.
Dans la mesure où chaque copie du virus ou du ver informatique peut à son tour s'autorépliquer, les infections peuvent se propager très rapidement. Il existe

[13] IFRAH (L.), « L'Europe face à la criminalité informatique », questions d'Europe, Fondation Robert Schumann, n° 70, 3 septembre 2007.
[14] IFRAH (L.), « Les nouvelles menaces criminelles numériques », Cahiers de la sécurité n° 6, pp. 59 et s.

énormément de catégories et sous-catégories de virus et vers informatiques. On peut citer les vers de courriel ou les vers de messagerie instantanée, les virus envoyés sous forme de pièces jointes ou via les réseaux de partages de fichier P2P (lors de téléchargement de musique ou vidéo par exemple).

Les Keyloggers

Imaginez une personne se tenant derrière vous, observant vos moindres faits et gestes jusqu'à prendre des notes de vos frappes de clavier. C'est exactement de cette manière que fonctionne un logiciel keyloggers. Il procède à l'enregistrement de frappes de touche du clavier d'un ordinateur dont les informations sont ensuite adressées au pirate agissant à distance. Il lui est ainsi possible de connaître les informations sensibles de sa victime comme des références bancaires, les mots de passe ou toutes autres données qui lui permettraient de commettre ultérieurement une escroquerie. Même s'il existe une multitude de KeyLoggers différents, leur mode opératoire est identique. Ils sont installés directement par le pirate sur la machine visée, si l'ordinateur n'a pas de connexion Internet permettant une installation à distance via un cheval de Troie.

Certains keyloggers sont capables d'enregistrer les URL visitées, les courriers électroniques consultés ou envoyés, les fichiers ouverts, voire de créer une vidéo retraçant toute l'activité de l'ordinateur infecté. Ils peuvent prendre la forme soit, d'un logiciel informatique soit, d'un support matériel. Dans le premier cas, il s'agit d'un processus furtif écrivant les informations captées dans un fichier caché. Dans le second cas, il s'agit alors d'un dispositif intercalé entre la prise clavier de l'ordinateur et le clavier. Malgré qu'il soit dangereux, il n'est pourtant pas répertorié parmi les virus, vers, ou chevaux de Troie car il ne modifie quoi que se soit dans la machine cible et permet simplement l'enregistrement d'informations.

b) Modus operandi des cybercriminels

A chaque minute qui passe une attaque cyber à lieu sur internet. Pour les entreprises la question n'est pas de savoir si elles ont déjà été attaquer ou si elles vont l'être mais d'être en mesure de faire face à la menace quand elle se présentera. En effet, selon une SOPHOS de l'éditeur de logiciel de sécurité ***SOPHOS*** et mené par l'agence ***Sapio research*** : c'est La moitié (49%) des entreprises françaises ont été la cible d'attaques d'hameçonnage (phishing) au cours des deux dernières années, tandis que plus de la moitié (52%) ont déclaré avoir identifié des cas d'employés qui avaient répondu à des emails non sollicités ou cliqué sur des liens contenus dans ces derniers, selon une étude réalisée pour Sophos[15]. Cette tendance confirme que l'intervention des cybercriminels est en train d'évoluer. Avant, leur activité consistait à diffuser du spam, à attaquer des serveurs pour se livrer au chantage ou à répandre des programmes publicitaires. Aujourd'hui, les pirates chassent en priorité les données personnelles qui, une fois collectées, sont revendues aux plus offrants. Des fichiers d'adresses de courriels électroniques donnent également lieu à un commerce très rémunérateur. Selon l'éditeur d'anti-virus Symantec, un réseau d'environ 5500 zombies se loue autour de 350 dollars la semaine.

Les cybercriminels ont recours à plusieurs techniques qui reposent généralement sur le facteur humain et que l'on nomme le social engineering ou ingénierie sociale. C'est l'art

[15] Global Security mag : « *La moitié des entreprises françaises ciblées par des attaques de phishing au cours des deux dernières années* », mars 2019.

d'obtenir des informations une personne en utilisant la ruse. Ces techniques peuvent prendre plusieurs formes. Il y a le spamming, le phishing, le pharming, et l'espionnage industriel.

Le Spamming

Le Spamming, qui renvoi en français à l'action d'envoyer des courriers indésirable ou pourriels est une forme de communication électronique non sollicitée, le plus souvent publicitaire. La CNIL est même plus précise et décris ce type d'action comme « *l'envoi massif, et parfois répété de courriers électroniques non sollicités, à des personnes avec lesquelles l'expéditeur n'a jamais eu de contact et dont il a capté l'adresse électronique de façon irrégulière* ».

Au-delà d'internet et des courriers électronique désormais, le spamming concerne aussi la téléphonie mobile, des messages invitant généralement à rappeler des numéros surtaxés envoyer par sms afin de réclamer un gain ou s'informer sur un colis pour lequel la cible serait dans l'attente.

Pour les adeptes du spamming c'est un moyen très peu onéreux de prospecter massivement de nouveaux clients. Mais cela représente également un coût pour les internautes, les entreprises, les fournisseurs d'accès à Internet en termes de connexions, de stockage de messages, de temps passé à les filtrer et à résoudre les problèmes techniques créés.

Ainsi, la prospection est interdite au moyen d'un courrier électronique utilisant, sous quelque forme que ce soit, les coordonnées d'une personne physique qui n'a pas exprimé son consentement préalable à recevoir des prospections directes par ce moyen.

Le phishing

Le phishing permet de subtiliser illégalement, auprès des internautes et des collaborateurs d'entreprises, des données personnelles en vue de leur utilisation au détriment des clients de banques ou de sites marchands. C'est une technique d'ingénierie sociale très apprécié des criminels du web puisqu'elle exploite non pas une faille informatique mais la crédulité humaine en dupant les internautes par le biais de courriers électroniques non sollicités semblant provenir d'une entreprise ou d'un service connu, comme sa banque ou un site de commerce dont la victime est cliente.

Les mails transmis par ces pirates usurpent l'identité d'une entreprise et invitent le destinataire à se connecter en ligne par le biais d'un lien hypertexte sur une page Web factice, copie conforme du site original afin de récupérer ses données personnelles.

Ces pratiques sont totalement illégales et sanctionnées par le biais de la collecte frauduleuse de données à caractère personnel, la contrefaçon de droits intellectuels, l'escroquerie, ou l'introduction frauduleuse de données dans un système de traitement automatisé ou la suppression ou la modification de données

Le pharming

Le pharming est une pratique frauduleuse similaire à l'hameçonnage. La différence est que, dans le cas du pharming, le trafic d'un site web légitime est manipulé pour diriger les utilisateurs vers des copies contrefaites qui installent des logiciels malveillants sur les ordinateurs des visiteurs ou qui recueillent (« pharm ») les données personnelles des utilisateurs, comme les mots de passe ou les détails financiers.

Il existe deux formes de pharming : Dans la première forme, les pirates informatiques utilisent différentes méthodes pour installer des virus ou d'autres logiciels malveillants dans votre ordinateur. Ce virus contrôle votre ordinateur pour qu'il n'atteigne pas le site

que vous voulez visiter, comme un site bancaire ou de commerce électronique, mais vous envoie à la place sur un site web contrefait qui a été conçu pour ressembler exactement au site que vous pensiez atteindre. La deuxième forme de pharming, cependant, est celle qui rend ce type de cybercrime particulièrement dangereux. Dans celle-ci, un cybercriminel empoisonne l'ensemble d'un serveur DNS, redirigeant ensuite tous les utilisateurs essayant de visiter un site légitime vers le site contrefait[16].

L'espionnage industriel

Espionner son concurrent afin de subtiliser sa recette de soda ou connaitre son organisation du travail n'est pas nouveau, mais l'extension d'Internet et des réseaux numériques a permis de la développer de façon plus sournoise, car dès lors que le système informatique de l'entreprise est pénétré illégalement, les documents deviennent accessibles. De plus avec la généralisation d'internet dans les entreprises, elle devient l'une des principales activités des cybercriminels[17].ok

Pour ce faire, les cybercriminels utilisent souvent des chevaux de Troie. La Chine est réputée pour s'adonner à cette pratique en lançant de multiples attaques vers ses concurrents avec pour objectif de rediriger les connexions vers leurs sites.

2.4.2 La mondialisation de la cybercriminalité

La cybercriminalité est l'une des formes de délinquance qui connait actuellement la croissance la plus forte. De plus en plus de malfaiteurs exploitent la rapidité, la fonctionnalité des technologies modernes, ainsi que l'anonymat qu'elles permettent, pour commettre des infractions sur le réseau Internet.

Pour lutter efficacement contre ce fléau qui a une dimension planétaire, les initiatives individuelles de chaque Etat ont montrés leurs limites. Le cyberespace offre au criminel non seulement la possibilité d'air sous couvert d'anonymat ou une fausse identité mais aussi de franchir les frontières et porter atteinte à des victimes dans le monde entier. Dès lors, la seule alternative pour lutter efficacement et durablement conter la cybercriminalité est la coopération entre les pays.

a) La dimension planétaire de la cybercriminalité

Grace à sa nature Mondial, le réseau Internet permet aux cybercriminels d'agir sans contrainte sur le plan international. Il est donc évident que les pays fassent évoluer leurs moyens de lutte afin de ne pas laisser impunie les infractions commises.

- La particularité de la criminalité commise sur les réseaux numériques est qu'elle a pour cible un territoire quasi sans limite puisque là où Internet est accessible, la criminalité l'est également. De ce constat nait une sombre réalité, à savoir que les cybers délinquants ont la possibilité de commettre des attaques dans un pays où la législation est encore inexistante ou beaucoup plus souple, et les effets de leurs actions vont pourtant se faire ressentir à l'autre bout du monde, ce qui rend souvent très complexe le déroulement des enquêtes.
- En effet, l'application du droit pénal est souvent rendue difficile en raison de la volatilité des sites et des informations circulant sur le Net, ainsi que des éléments

[16] *Qu'est-ce que le pharming ?* Avast.

[17] UnderNews Actu, « L'espionnage industriel priorité du cybercrime », éd. num., 2011.

d'extranéité[18] rendant complexes les investigations nécessaires à l'interpellation des auteurs et à l'identification des victimes.

- Une autre difficulté majeure tient par ailleurs à la recherche de la preuve des infractions commises. La réalité de la connexion à un site peut parfois se révéler difficile à établir. D'autant plus que les cybercriminelles font preuves de beaucoup d'imagination des méthodes de « brouillage » pour complexifier la remontée vers le point de départ de l'attaque.
- Toutes ces difficultés alliées à l'hétérogénéité du réseau Internet peuvent conduire à nuire à la coopération judiciaire internationale qui s'avère pourtant indispensable. A une agression de nature internationale, une riposte de nature internationale doit être mise en œuvre.

b) La coopération européenne et internationale

Au niveau européen, cette coopération s'inscrit dans le cadre de l'Espace de justice, de liberté et de sécurité des citoyens de l'UE. Les États ont compris que pour être plus efficace, la lutte contre la cybercriminalité doit être d'abord européenne. Des compétences dans ce domaine ont alors été confiées à EUROPOL, office de police criminel intergouvernemental facilitant l'échange de renseignements entre polices nationales en matière de cybercriminalité au sein de l'Union européenne. Depuis 2013 il a même été créé le Centre Européen du Cybercrime (EC3) afin de renforcer la loi et les moyens de lutte contre les « crimes en ligne ». Ce programme spécifique de l'EUROPOL est soutenu et dirigé par un bureau[19] de composé de 11 agences européenne dont l'ENISA, le conseil de l'Europe ou encore l'Agence de Défense Européenne. Chaque année est publiée l'*Internet Organized Crime Threat Assessment (IOCTA)*, le rapport stratégique phare sur les principales conclusions et les menaces et développements émergents en matière de cybercriminalité de l'agence.

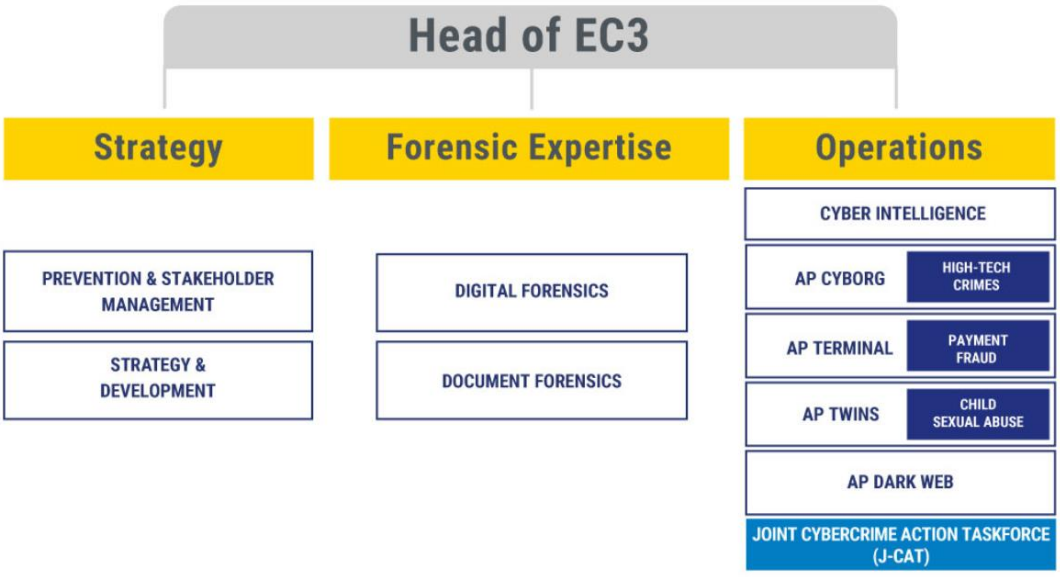


Figure 2. Organigramme de European Cybercrime Centre (EC3)

[18] Qualité juridique d'étranger, Larousse.

[19] EC3 Programme Board : CEPOL, CERT-EU, ECTEG, EDA, SEAE, ENISA, EUROJUST, Commission européenne, Conseil européen, EUCTF et INTERPOL.

Des compétences ont été également confiées à EUROJUST[20], organe de l'Union européenne ayant pour finalité l'amélioration de l'efficacité des autorités compétentes des États membres dans la lutte contre la cybercriminalité transnationale.
Au niveau international, la coopération s'inscrit principalement dans le cadre de la Convention de Budapest contre la cybercriminalité du 23 novembre 2001[21]. Il s'agit du premier traité international sur les infractions pénales commises contre ou à l'aide des réseaux informatiques. Cette convention réunit une trentaine de pays comme les États-Unis, le Japon, le Canada, l'Afrique du Sud ainsi que vingt-six des quarante-trois pays membres du Conseil de l'Europe, dont la France. Son objectif est de travailler à l'harmonisation du cadre légale des États signataires, à les moderniser, notamment en matière procédurale, et tend enfin à améliorer la coopération internationale en matière d'extradition et d'entraide répressive.
Des compétences, dans ce domaine, ont également été confiées à INTERPOL, l'organisation internationale de police criminelle la plus importante au monde, avec 194 pays membres, doté d'un pôle de lutte contre la cybercriminalité. En ce sens, elle s'emploie à suivre l'évolution des menaces tout en apportant une assistance aux pays membres en cas de cyberattaque ou dans le cadre d'enquêtes sur des affaires de cybercriminalité, en mettant à leur disposition des services en matière de recherches et de bases de données.

Figure 3. Réseau INTERPOL mondial

Cependant, les États ont dû faire face à des problèmes supplémentaires de compétences. En effet, si la poursuite d'une infraction informatique doit être engagée devant une juridiction pénale compétente, encore faut-il trouver la bonne juridiction. Cette question est très vite devenue assez complexe puisque la nature internationale des infractions est une véritable source de problèmes.

[20] Également connu sous « l'Unité de coopération judiciaire de l'Union Européenne ». Fondée en 2002 et composée de 28 membres, Eurojust a pour mission de promouvoir et renforcer la coordination et la coopération entre les autorités nationales dans la lutte contre la criminalité transfrontalière grave engagée dans l'Union Européenne.
[21] La Convention de Budapest et son rapport explicatif ont été adoptés par le comité des Ministres du Conseil de l'Europe à l'occasion de sa 109ème session, le 08 novembre 2001.

La question est de savoir si les infractions cybercriminelles peuvent être appréhendées par la justice d'un ou plusieurs États et, en cas de réponse positive, quelle devrait être finalement la juridiction compétente pour réprimer l'infraction. Certains auteurs ont d'ailleurs évoqué que « la structure du réseau Internet conduit à l'internationalisation pratiquement obligatoire des infractions ».

On peut relever que trois techniques législatives ont été utilisées :

- Les États qui ont promulgués des législations spécifiques autour de la cybercriminalité sans pour autant prendre en compte les textes déjà existants. C'est le cas des Etats-Unis.

- D'autres États ont simplement adapté la législation existante et les lois pénales pour les rendre applicable aux caractéristiques particulières de crimes du cyberespace.

- Enfin la troisième technique législative s'agit de s'appuyer sur les lois déjà existantes notamment sur les dispositions sur l'accès non autorisé aux données et aux informations.

Cette forme nouvelle de criminalité pousse évidemment les pays à revoir les fondements de leurs systèmes judiciaires. En effet, faces à ces menaces, il existe bel et bien des lois qui sont d'ores et déjà appliquées à l'Internet. Mais la question qui est posé ici c'est l'efficacité de ces dites lois pour lutter contre une cybercriminalité toujours plus professionnalisée.

Certains États disposent d'un nombre de lois qui permettent d'incriminer plus ou moins efficacement les actes illicites liés aux NTIC. En revanche, nombreux83 sont encore ceux qui se trouvent confronté à de terribles lacunes dans les textes législatifs et sont incapables de réprimer cette nouvelle forme de criminalité. Pourtant face à une criminalité devenue planétaire, une riposte coordonnée de la part des États doit se mettre en place.
Nous consacrons alors une première partie à l'étude de l'inadaptation du système judiciaire à la cybercriminalité, dans laquelle nous mesurerons l'efficacité de l'arsenal répressif mis en place par le législateur ainsi que les difficultés de compétence du système judiciaire pour sanctionner une infraction cybercriminelle. Dans une deuxième partie, consacrée à la difficulté de coopération entre États, nous montrerons comment ces derniers s'organisent pour faire face à la cybercriminalité et pourquoi cette coopération reste encore insuffisante. Nous proposerons plusieurs solutions pour essayer de pallier ces obstacles.
Nous ne pourrons que conclure par un constat d'échec lié essentiellement au manque de volonté des États, dont la souveraineté étatique reste un domaine inaliénable. S'il est souhaitable que la situation change, il faut constater l'insuffisance des moyens mis en œuvre, même si au demeurant des efforts ont déjà été accomplis.

3. Le patrimoine de l'entreprise

3.1 Le système d'information

Le système d'information est souvent vu comme un mal nécessaire par les dirigeants de PME. Face aux problèmes de fonctionnement, d'évolution et à des budgets élevés, les dirigeants de PME peinent à considérer l'informatique ou le système d'information autrement qu'un centre de coût. De plus, c'est un sujet qu'ils ont du mal à appréhender en raison de sa technicité et

de sa complexité. D'où un dialogue parfois difficile avec les collaborateurs internes ou les prestataires externes chargés de la gestion du système d'information.

3.1.1 Un actif essentiellement immatériel

Plus de 80% des actifs du système d'information d'une PME est immatériel. Mis à part les locaux et les composants matériels (postes de travail, serveurs, équipements réseau, téléphonie IP…), tout le reste est considéré comme immatériel.
Le capital immatériel se décompose en capital humain (intelligence, savoir-faire, créativité, … des employés internes comme des prestataires externes), en capital organisationnel (propriété intellectuelle, applications, bases de données, réseaux, processus métier, valeurs, culture, …) et en capital relationnel (relations externes avec clients, fournisseurs, partenaires, réseaux…).

3.1.2 Un élément central de la valeur de l'entreprise

Le système d'information est un actif clé du capital immatériel de l'entreprise, qui doit être mesuré, évalué, valorisé et bien sûr sécurisé.
Le système d'information est aujourd'hui un élément de mesure clé de la valeur de l'entreprise. Il permet de se différencier de la concurrence. Dans les opérations de fusion-acquisition, par exemple, un audit du système d'information est systématiquement effectué (due diligence IT) au même titre que tous les autres éléments de l'actif de l'entreprise objet du deal. Un système d'information bien géré et maîtrisé accroit la valeur de l'entreprise objet du rachat. A l'inverse, un système d'information mal maîtrisé, souffrant de problèmes de fonctionnement ou présentant des risques (exemple : obsolescence des technologies utilisées, difficultés d'évolution, dépendance vis à vis d'un petit nombre de personnes internes ou externes, …) diminue la valeur de l'entreprise et peut même conduire à remettre en cause la décision d'achat.
La contribution du système d'information à la création de valeur dépend du contexte de l'entreprise. Néanmoins nous pouvons mentionner les axes de contribution suivants :

- **Développement du CA** : capacité à gérer de nouveaux canaux de commandes, réduction du time to market, capacité à gérer la formation des employés

- **Amélioration de la marge** : meilleure rotation des stocks, permet aux équipes commerciales ou à l'adv de vendre plus, fidéliser les clients, maîtrise des outils par les employés, partage des informations avec clients et fournisseurs

- **Optimisation** des moyens : le système d'information facilite l'accès aux informations clés, la réactivité du support client, les échanges informatisés avec clients et/ou fournisseurs

- **Agilité opérationnelle** : capacité à intégrer une nouvelle société en cas de rachat/fusion, capacité à accompagner les modifications de processus internes, capacité à pérenniser les compétences clés au sein de l'entreprise, capacité à évoluer pour prendre en compte les évolutions du marché (traçabilité, règlementation relative au secteur d'activité et au périmètre géographique, …)

- **Prise de décision** : capacité à mettre à la disposition des managers les informations pertinentes au travers d'outils de *reporting* et de business intelligence permettant de faciliter la prise de décision.

3.1.3 Cas du système d'information externalisé

Lorsqu'une entreprise prend la décision d'externaliser son système d'information cela ne signifie pas qu'elle ne prendra plus part à la gestion du sujet ou qu'elle n'en supportera pas les investissements.

Le recours à l'externalisation doit être le résultat d'un arbitrage murement réfléchi et évalué entre « faire » et « faire faire ». En fonction de son contexte, la PME pourra sous-traiter tout ou partie de son exploitation informatique et/ou de la maintenance de ses applicatifs métier (ERP, applications spécifiques, sites web, …). Il faut savoir que le recours à la sous-traitance pour la maintenance des applications sera plus structurant que pour l'exploitation informatique. Par conséquent, ce n'est pas parce que l'on recourt à l'externalisation que l'on ne doit pas être vigilant. Bien au contraire, les bonnes pratiques en matière de sécurité doivent être préserver. Pour préserver la pérennité de ces actifs essentiels au bon fonctionnement de l'entreprise, il est primordial de définir les objectifs (et mesurer la bonne exécution) en matière de sécurité qui devront être tenu par le prestataire.

3.2 L'outil de production ou l'usine 4.0

Dans un monde qui se dirige à grand vers un appareil de production 4.0, c'est à dire hyperconnecté au système d'information et voir indirectement à internet, assuré la sécurité de celui-ci est quasiment vitale. Les dirigeants sont souvent peu préparés et désarmés face à ce nouveau phénomène. Les systèmes industriels utilisent aujourd'hui abondamment les technologies de l'information alors qu'ils n'ont pas été conçus pour faire face aux menaces qu'elles introduisent. Ces systèmes sont ainsi composés d'équipements physiques au sein de l'usine (moteurs, pompes, vannes, … et capteurs), pilotés par des systèmes logiques (automates et applications SCADA) – à distance parfois – et de systèmes informatiques dédiés à l'analyse des données.

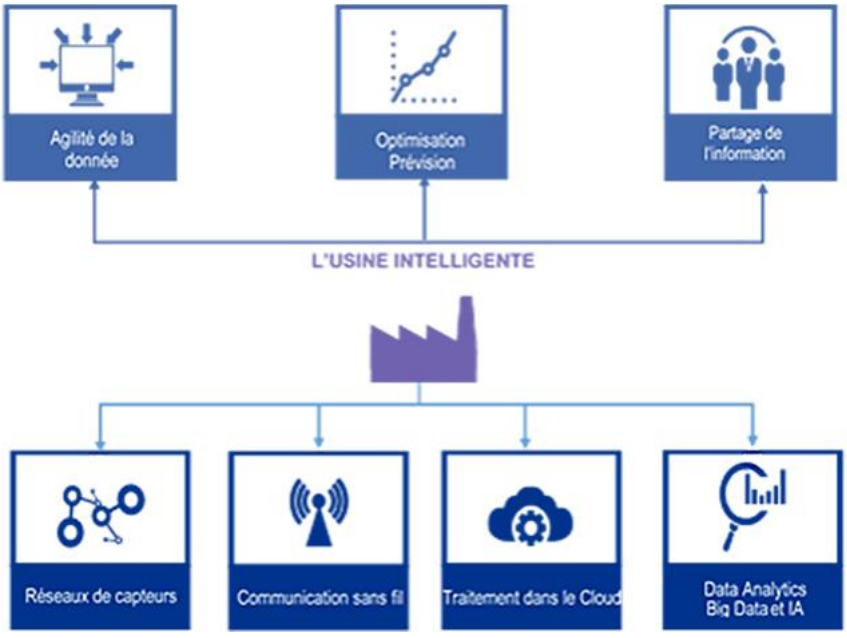


Figure 4 : L'usine 4.0[22]

Au-delà des ransomware et des vols de données, les pirates ciblent désormais jusqu'aux automates et contrôleurs de sécurité et menacent l'appareil de production, au risque de déclencher des catastrophes. A la manière d'un roseau, l'outils de production peut plier face à la menace cyber mais ne doit en aucun rompre au risque de mettre en danger l'avenir de l'entreprise.

Les attaques contre les entreprises sont de plus en plus fréquentes et les coûts induits augmentent. Dans une étude publiée le 25 Juin 2019, l'IRT SystemX estime ainsi que les attaques par cryptovirus, ou ransomwares, coûtent quelque 700 millions d'euros par an aux PME/TPE (moins de 50 personnes) françaises. Se protéger s'impose.

D'après une étude réalisée par la banque Morgan Stanley, la cybersécurité est considérée comme l'un des risques majeurs à l'adoption de l'IoT. Ce risque est multimodal et multi-source.

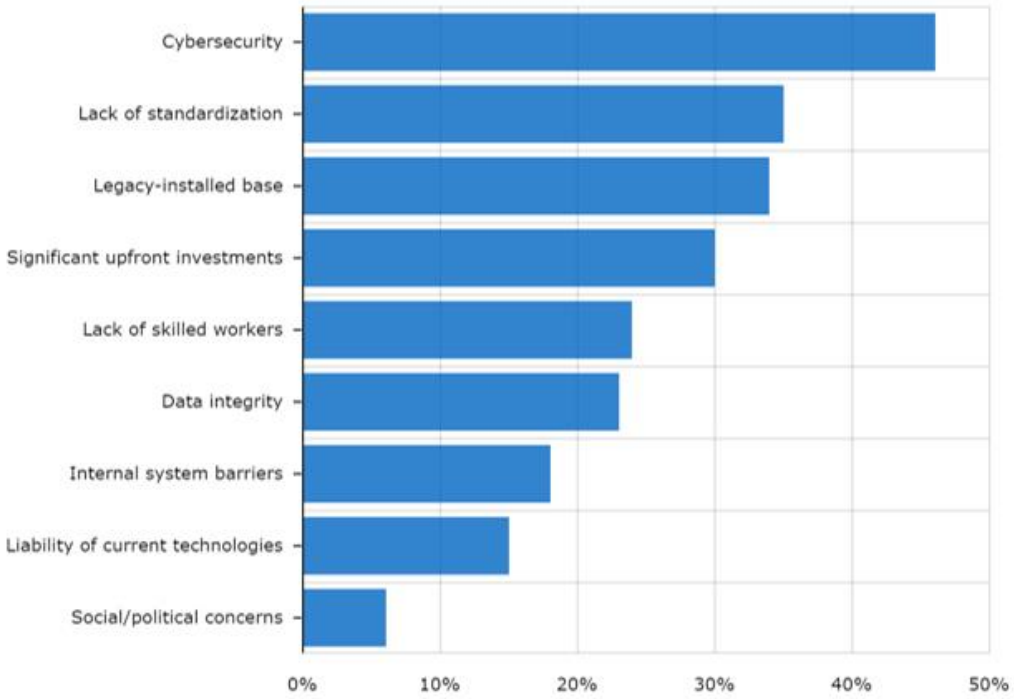


Figure 5. Challenges à l'adoption de l'IIoT[23]

« *Avec l'introduction de l'IIoT, la frontière entre les systèmes d'information d'entreprise (IT) et les systèmes industriels (OT) disparaît peu à peu et les systèmes OT ne disposent plus de la sécurité périmétrique (air gap) dont ils bénéficiaient à l'origine. Les automatismes industriels (robots, machines à commande numérique, automates programmables) deviennent beaucoup plus interconnectés, ouverts et accessibles depuis le réseau informatique de gestion d'une entreprise, voire depuis Internet. Des cyberattaques visant les réseaux de gestion se propageraient donc facilement vers les systèmes OT.* »[24]

[22] KPMG, L'usine 4.0 à l'ère du cloud et de l'hyperconnectivité.
[23] Morgan Stanley-Automation World Industrial Automation Survey, AlphaWise.
[24] KPMG, L'usine 4.0 à l'ère du cloud et de l'hyperconnectivité.

Dans ce contexte de surexposition de l'usine 4.0 à la cybermenace il apparait évident que la priorité pour les dirigeants de PME et les équipes de la direction des systèmes d'informations doit être la définition d'une stratégie solide de cyber résilience. Ainsi tous les acteurs (fabricants des capteurs, opérateurs de télécommunications, fournisseurs de solutions cloud et d'analyse de données, opérateurs et exploitants des systèmes industriels...) de l'écosystèmes doivent travailler main dans la main pour assurer une sécurité de bout en bout sur les plans technique et organisationnel.

3.3 Les données personnelles

Nous avons vu précédemment que les outils informatiques ont considérablement évolué ces dernières années dans le monde en générale mais plus particulièrement dans l'entreprise. Les ordinateurs, les téléphones portables se sont banalisés et Internet et les réseaux sociaux ont bouleversé les modes de communication. Effectivement, avec l'essor du commerce électronique, les données personnelles sont devenues un enjeu économique considérable. En effet, dans cet environnement numérique à impératif commercial, ces "matières premières" deviennent de nouvelles armes de marketing agressif. Une fois collectées, elles permettent aux entreprises de mieux connaître les marchés, de pratiquer toutes sortes de ciblages ou de chasses aux clients réels ou potentiels.

- Par faire Face à l'évolution des dangers liés à l'accroissement de l'informatique dans l'entreprise, la loi informatique et libertés du 6 janvier 1978, dite loi Godfrain, a dès son entrée en vigueur, confié à la Commission nationale de l'informatique et des libertés le soin de veiller à la protection des données personnelles. Le principe de cette loi c'est que toute personne souhaitant effectuer un traitement automatisé de données nominatives doit obligatoirement déclarer cette activité à la CNIL. En matière de collecte de données personnelles, le législateur s'est également montré ferme puisqu'il encadre strictement cette pratique jusqu'à punir de « *cinq ans d'emprisonnement et de 300 000 euros d'amende* » les contrevenants.
- Venant supplanter les lois nationales, l'union européenne via le parlement à adopter le 27 avril 2016, la loi dit : règlement général sur la protection des données (RGPD, ou encore GDPR, de l'anglais *General Data Protection Regulation*). Les principaux objectifs du RGPD sont d'accroître à la fois la protection des personnes concernées par un traitement de leurs données à caractère personnel et la responsabilisation des acteurs de ce traitement. Toutes les données permettant d'identifier directement ou indirectement un individu sont concernées : nom, courriel, adresse, date de naissance, etc. En outre, l'UE a considérablement élargi la définition des données à caractère personnel dans le cadre du RGPD. Les identifiants en ligne tels que les adresses IP sont désormais considérés comme des données personnelles. En ce sens, tous les fichiers contenant les types d'informations personnelles précités sont concernés par le RGPD, du simple fichier Excel utilisé pour des envois d'emailings aux bases de données de prospects, clients, salariés, etc.

Par ailleurs, les entreprises doivent obtenir le consentement de chaque individu dont elles collectent les informations, de manière licite et loyale. Le consentement doit être une action active de la part de la personne concernée. Les DPO (*Data Protection Officer* ou Délégué à la Protection des Données) doivent conserver une trace de comment et quand une personne a donné son consentement, laquelle peut s'en soustraire à tout moment.
Ces principes pourront être appliqués grâce à l'augmentation du pouvoir des autorités de contrôle et les sanctions liés au non-respect de ces dispositions sont très lourdes ;

« *Les violations des dispositions suivantes font l'objet, conformément au paragraphe 2, d'amendes administratives pouvant s'élever jusqu'à 20 000 000 EUR ou, dans le cas d'une entreprise, jusqu'à 4 % du chiffre d'affaires annuel mondial total de l'exercice précédent, le montant le plus élevé étant retenu* »[25]

Tandis que le Loi Informatique et Liberté Française reconnaissait déjà l'importance des droits aux individus au sujet du traitement de leurs données personnelle, la loi européenne reconnait désormais sept droits (dont deux nouveaux) qui sont mis en avant :

- Transparence des informations et des communications.
- Droit d'accès à la donnée de la personne concernée.
- Droit de rectification.
- Droit à l'oubli (nouveau).
- Droit à la limitation du traitement.
- Droit à la portabilité des données (nouveau).
- Droit d'opposition.

[25] Journal officiel de l'UE ; Règlement (UE) 2016/679 du Parlement Européen et du Conseil.

II. GESTION DES INCIDENTS CYBER : BOÎTE A OUTILS

Par essences la notion d'incident est très large et englobe des domaines divers. Incident de sécurité, incident fonctionnel, incident technique, incident financier etc. Plus précisément, un incident cyber peut être défini comme un évènement qui ne fait pas partie du fonctionnement standard d'un service et qui cause, ou peut causer, une interruption ou une diminution de la qualité de ce service.

1. 7 mesures de préventions des incidents cyber pour les PME et TPE

1 - Authentification forte

Afin de sécuriser l'accès aux réseaux, aux données (personnelles et sensibles) et aux applications de l'entreprise, la mise en place des solutions d'authentification fortes est un prérequis indispensable. Ce renforcement de la sécurité logique peut se matérialiser par m'imposition de mots de passe forts.

Néanmoins, la priorité dans les entreprises aujourd'hui reste la mise en place d'une solution d'authentification à deux étapes (*double factor authentification*), qui combine certificats numériques et des *tokens*. Cette solution pratique et sécurisée, permet de sécuriser l'accès à divers équipements ; serveurs de contrôleur de domaine, certificats de machines, terminaux mobiles, annuaire des collaborateur, services cloud, clés USB approuvées, VPN, passerelles et réseaux wifi.

2- Bluetooth Off

Très peu sécurisé, le Bluetooth est une porte d'entrée de choix pour les cyberattaquants. Sa porosité expose les entreprises au vol de données et même dans certains cas à la prise en main total de l'appareil par le pirate. Il est donc primordial d'inciter les collaborateurs de l'entreprise à le désactiver systématiquement sauf bien sûr pour un usage temporaire.

3- BYOD et contrôle des terminaux

Les pratiques du *jailbreaking* (déverrouillage) et du *rooting* (débridage) des terminaux mobiles sont devenues courantes auprès des utilisateurs. Le but de ces manipulations étant de lever les limitations logicielles des systèmes d'exploitation des terminaux, afin d'accéder à des fonctionnalités autrement interdites.

En débloquant ces fonctions avancées, surtout sur les appareils Android, les utilisateurs s'exposent à toutes sortes d'attaques. Lors de la phase de découverte de l'environnement ciblé, le cybercriminel ayant identifié l'appareil non-protégé pourrait notamment en prendre le contrôle, puis exécuter toutes sortes d'opérations : écoutes via le micro, accès à la connexion Internet, connexion aux applications via le compte de l'utilisateur.

4- Chiffrage de la connexion internet

Dans les TPE et les start-ups bien souvent on se contente des fonctions de sécurité basics embarquées dans le routeur fourni par le fournisseur d'accès internet, avec un trafic Internet non chiffré. Dans les entreprises de moins de 25 employés, la mise en place d'un VPN sur le routeur lui-même permet de chiffrer toutes les données transmises via le réseau. Les VPN peuvent légèrement ralentir la connexion Internet, mais avec un routeur de qualité, ce retard devrait être minime.

5- Règles pour les téléchargements et les antivirus

Cette pratique de base, généralement connue de beaucoup de salariés, est malheureusement souvent peu respectée dans les faits. Il revient donc à l'entreprise de responsabiliser ses collaborateurs, en rappelant régulièrement les menaces associées au téléchargement et les moyens de s'en prémunir, notamment sur les appareils personnels.

Chaque collaborateur doit ainsi disposer d'un antivirus à jour et de qualité sur les appareils utilisés dans le cadre du BYOD. À chacun également de s'assurer qu'une analyse de ses appareils est régulièrement effectuée. Tout fichier téléchargé individuellement doit enfin être analysé avant d'être ouvert.

6- Restriction de l'usage de la clé USB

Les clés USB sont pratiques, mais dangereuses. Leur absence de chiffrement et la facilité avec laquelle elles peuvent être égarées constituent les principaux facteurs d'inquiétude. Celles-ci peuvent également propager des programmes malveillants si elles sont connectées à un appareil du réseau interne de l'entreprise. Mieux vaut donc prévenir, en interdisant l'usage de clefs, à l'exception de solutions sécurisées.

7- Politique interne et formation du personnel

Les employés doivent avoir une meilleure connaissance du moment où les données professionnelles sont en sécurité ou non. Un des plus grands enjeux que les organisations doivent affronter est l'envoi par les employés des documents d'entreprise sensibles sur leur messagerie personnelle. Une fois qu'un document est divulgué, il n'est plus sous le contrôle de l'organisation, sa sécurité ne peut plus donc être contrôlée. Pour cela, un rappel permanent de ces enjeux par le chargé de la sécurité des données est indispensable.

2. Les mesures de gestion des incidents cyber

Une politique de gestion des incidents de sécurité est essentielle pour :

- Garantir que le mode d'alerte des évènements et des failles de sécurité est suffisamment efficace afin d'assurer la mise en œuvre d'actions complémentaires ou de correction dans les meilleurs délais.
- Garantir la mise en place d'une stratégie cohérente et efficace pour la gestion des incidents cyber.

Pour assurer la réussite d'un tel plan et atteindre ces deux objectifs plusieurs mesures doivent être mis en place.

2.1 Signaler tous les évènements liés à la sécurité de l'information

Le management de l'entreprise doit mettre en place des procédures formelles de signalement, de remontées des informations et de réponses lorsqu'un incident sur les systèmes d'informations est détecté. Les mesures de traitement doivent être clairement définis afin d'optimiser le temps de réponse suivant le signalement.

Généralement c'est le RSSI et le *Service Desk*, l'équipe de réponse aux incidents qui doivent être les points d'entrées privilégiés pour tous les signalements d'incidents. Par conséquents, tous les utilisateurs, collaborateurs, prestataires détachés, doivent être informés des

procédures de signalement et surtout de leur obligation à signaler tout évènement lié à la sécurité de l'information dans les délais les plus bref (session de sensibilisation, charte utilisateur...).

2.2 Signaler toutes les failles de sécurité identifiées

L'ensemble des collaborateurs, des contractants et utilisateurs des systèmes d'informations de l'entreprise doivent noter et signaler toute faille de sécurité identifiées ou soupçonnées.
Pour éviter tout incident lié à la sécurité de l'information, comme pour le point précédent, l'ensemble des collaborateurs sont tenus de signaler au *Service Desk* dans les meilleurs délais ces failles. Aussi, pour ne pas suscité de rejet de la part des utilisateurs et avoir un taux de déclaration élevé le mécanisme de signalement doit être le plus simple, accessible et disponible possible. Par ailleurs, après indentification d'une faille de sécurité il est recommandé aux collaborateurs de ne pas essayer de ne pas tenter d'apporter la preuve de l'existence du dit risque de sécurité.

2.3 Mise en place des procédures et détermination des responsabilités

Toujours dans un souci de garantir une réponse rapide, efficace et pertinente les responsabilités et les procédures doivent être clairement établies. Ainsi, au-delà du signalement des évènements et des failles liés à la sécurité des systèmes d'information il plus que recommandé de mettre en place une politique de surveillance des systèmes, des alertes et des vulnérabilités afin de détecter plus efficacement les incidents liés à la sécurité de l'information de l'entreprise. Aussi, le RSSI de l'entreprise doit établir des priorités de traitement, une description des incidents mais aussi un mode opératoire de résolution spécifique pour gérer au mieux les différents types d'incidents liés à la sécurité du système d'information. Dans ce mode opératoire il est de la responsabilité du RSSI de confirmé de la clôture d'un incident de sécurité et d'apprécié la qualité de la résolution (délai de résolution, solution proposée, les axes d'amélioration…).

2.4 Mise en place de mécanismes de surveillance et de comptabilisation des incidents

Pour quantifier et surveiller les différents types d'incidents liés à la sécurité de l'information en prenant en compte le volume et les coûts associés, il est recommandé à la RSSI de mettre en place des mécanismes adaptés.
Afin d'identifier les éventuelles actions préventives à engager, une analyse « à froid » des incidents ayant donné lieu à une cellule de crise est réalisé lors des comités exécutifs. Les informations recueillis lors de la résolution d'incidents liés à la sécurité de l'information sont réévaluées à la fin de l'incident. En effet, cette réévaluation peut faire apparaitre la nécessité d'améliorer les mesures existantes ou encore d'en définir de nouvelles, dans le but de réduire la fréquence des futurs incidents ainsi que les dommages et les coûts associés. De plus, cette activité de revue si elle est réalisée régulièrement permet notamment de quantifier et surveiller les différents types d'incidents liés à la sécurité de l'information.

2.5 Mise en place d'une assurance pour la protection des ressources de l'entreprise

Dans le but de protéger les collaborateurs, les investissements, les informations et plus largement l'ensemble des actifs de l'entreprise il est capital pour la direction de souscrire à une police d'assurance adaptée. Ainsi, la détermination du périmètre à assurer fait en règle générale l'objet d'une analyse de risques menée avec l'assureur. La mission est d'analyser le plus précisément possible la nature des risques encourus, les conséquences financières auxquelles ils exposent, et ainsi faire l'arbitrage entre l'auto-assurance (provision, franchise)

et le transfert de risque à l'assureur. Ceci nécessite une mis à jour régulière du périmètre à assurer pour ainsi réviser les contrats en conséquence. D'ailleurs afin de mieux négocier des tarifs préférentiels sur les contrats il est important de démontrer de l'efficacité de l'organisation en place de gérer les incidents liés à la sécurité des systèmes d'information.

2.6 Collecte et conservation des preuves d'un incident cyber

Lorsque l'entreprise a la capacité de mener une action en justice civile ou pénale contre un collaborateur, une personne extérieure à l'entreprise ou encore une organisation criminelle, à la suite d'un incident lié à la sécurité du système d'information, Il est essentiel de collecter, conserver et présenter conformément à la législation les preuves. Par conséquent, pour que cela soit possible la RSSI doit mettre en place une procédure interne qui définit les exigences de sécurité en matière de collecte des traces techniques de sécurité, de leur conservation, de leur protection et de leur accès. A noter que seules les autorités judiciaires sont mandatées à collecter les preuves légales.

III -Cartographie des risques cyber actifs & Méthode d'analyse du risque Cyber

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 [26]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"*.

1-La méthode et les principes de l'analyse

« Si on n'a pas de bonnes bases méthodologiques, on ne peut pas construire des scénarios de protection. On arrive à un stade de maturité sur le sujet parce que les dirigeants sont sensibilisés depuis des attaques comme le ransomware **Wanacry** » plaide Guillaume Poupard de l'ANSSI.
Bien que le lancement de de EBIOS Risk Manager, **une nouvelle méthode d'analyse de risque** conduite par l'ANSSI et le **Club EBIOS** qui regroupe des experts de la gestion des risques. Nous essayerons d'établir une marche à suivre pour mener à bien la compréhension de la gestion des risques cyber et surtout de bien tirer ce qui est l'essentiel pour nous dans cette notion complexe.

1.1. Les étapes de l'analyse du risque cyber : ce qui requiert une défense

Au quotidien, on peut constater une augmentation des menaces et des attaques cyber contre les biens informatiques que l'on soit dans des entreprises de taille modeste dans les grands groupes du CAC-40. Dans la plupart des cas, les efforts de défense permettent de contenir ces attaques et de continuer le cycle normal des opérations de l'entreprise. Mais il y'a des cas où

[26] État recherché pour un système d'information lui permettant de résister à des événements issus du cyberespace susceptible 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).

les cyberattaquants parviennent à perturber fortement l'activité ou provoquent complètement l'arrêt des opérations d'une entreprise. Ces cyber-attaques peuvent évoluer vers une crise-cyber, en particulier lorsque l'attaque touche aux ressources informatiques vitales de l'entreprise, ce qui est susceptible de causer des dommages critiques aux opérations de routine et à la réputation, des dommages économiques et de mettre en danger des vies humaines. Par conséquent, une menace réelle de dommage à une ressource informatique vitale, ou un dommage réel à celle-ci, est le point d'entrée pour identifier une crise-cyber et déterminer sa gravité.

Afin de minimiser la probabilité de l'arrivée d'une crise cyber et de formuler une réponse adéquate qui minimisera ses dommages et ses ramifications tout en définissant et en utilisant efficacement les ressources et les capacités de l'entreprise, chaque organisation devrait, dans un premier temps, dresser la liste des ressources informatiques vitales les plus pertinentes pour elle. Il s'agit des ressources dont les fonctions régulières sont essentielles pour maintenir la continuité fonctionnelle des processus de base qu'elle gère au sein de l'entreprise.

Selon la méthodologie EBIOS Risk Manager de l'ANSSI, la défense doit être proportionnelle aux dommages potentiels ; c'est-à-dire que l'investissement dans la défense de chaque actif doit être proportionnelle avec le niveau de sa criticité par rapport à l'organisation et à ses objectifs. Par conséquent, la majorité de l'investissement dans les capacités de défense doit se concentrer sur les ressources informatiques vitales.
De la part de l'agresseur ces ressources constituent une cible attrayante pour les cyber-attaques, et donc, ce qui en fait un objectif à atteindre.

1.2. Définition des ressources informatiques vitales

En Israël, chaque organisation peut utiliser la *" Cyberdéfense Methodology for an Organization"* pour dresser une cartographie correcte et efficace des ressources informatiques vitales qu'elle détient et de les classer par ordre de criticité, d'évaluer les risques auxquels ces ressources sont exposées et d'élaborer un plan visant à renforcer le niveau de "*cybersécurité"* qui leur est applicable.
Dans notre analyse, nous avons deux axes principaux pour la cartographie des ressources informatiques vitales comme définis dans la charte de "*Israeli National Cyber Directorate*" :

- Définition par la méthode ascendante des ressources informatiques vitales
  Le long de cet axe, l'analyse commence par le bas. Nous regardons les processus de base de l'organisation et identifions les ressources informatiques dont les fonctions normales sont essentielles pour maintenir la continuité des processus de fonctionnement. Par la suite, nous examinons les ressources informatiques qui ont été identifiées par rapport aux critères formulés par "*Cyberdéfense Methodology for an Organization"*, qui sont utilisés comme un mécanisme proactif de cartographie pour définir les organisations qui, si elles sont touchées par une cyberattaque, sont susceptibles de causer des dommages importants à l'organisation et par ricochet à l'Etat. Les ressources numériques qui répondent aux critères sont définis comme des ressources informatiques vitales et sont divisés en deux groupes d'organisations :
- Organisation de l'Infrastructure critique ;
  Une entreprise détenant des actifs informatiques critiques devrait se rapprocher de l'ANSSI pour demander conseil ou soumettre le plan de défense de son infrastructure afin de recevoir tous les prérequis pour la mise en conformité de ce plan. Le rôle de

l'ANSSI consiste notamment à déterminer quelles organisations doivent être définies comme "critiques" et ont donc besoin d'un niveau élevé de cyberdéfense.

- Organisation de “Groupe A ” ;
- Afin de construire des capacités efficaces pour augmenter le niveau de la surveillance des entreprises contre les menaces cyber, l'ANSSI prend des mesures pour définir divers groupes de discussion, et fournit à chacun d'eux une orientation différentielle. La majorité des orientations, les ressources seront allouées à un petit groupe de discussion appelé "Groupe A", fondé sur l'idée qu'ils détiennent des ressources informatiques vitales qui ont un impact majeur sur les processus clés de l'économie (de leur entreprise) et une cyber-attaque à leur encontre est susceptible de provoquer des dommages considérables pour eux et pour les autres.

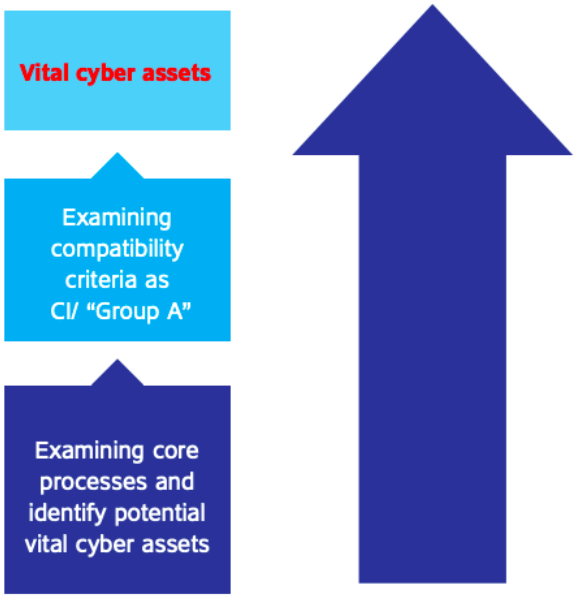


Figure 6. Méthode ascendante des ressources informatiques vitales
Source : Deloitte France Cyber Risk Services

- Définition par la méthode descendante des ressources informatiques vitales
  Un autre axe de définition des ressources informatiques critiques au niveau plus large de l'organisation concerne le travail effectué par l'autorité de régulation (ANSSI) et les ministères du gouvernement correspondant dans le domaine de la continuité fonctionnelle de l'économie.

Selon cet axe, l'analyse commence au sommet, puisqu'il commence par les "objectifs de service national" dans tout ce qui concerne la question cyber, qui sont les définitions pratiques des services et des fonctions des systèmes qui doivent se poursuivre même pendant les crises, afin d'assurer la continuité fonctionnelle et la routine au sein de l'organisation même. En tant que dérivé des "Objectifs de service national" et afin de permettre leur réalisation, l'ANSSI travaille avec les ministères du gouvernement (Intérieur et Économie) pour définir les objectifs ministériels et les niveaux de service, qui sont les définitions pratiques et quantitatives des capacités fonctionnelles dans ces ministères et dans les organisations sous leur responsabilité. Capacités qui doivent être maintenues dans la mesure du possible, même en cas de crise.

La réalisation des objectifs et des niveaux de service définis par l'Etat dépend de la continuité des processus de base mis en œuvre dans les organisations, et la continuité fonctionnelle de nombre d'entre elles dépend des ressources informatiques. Il est demandé à chaque organisation de travailler avec les autorités de régulation afin de cartographier et d'identifier ressources informatiques vitales, puis définir quelles ressources qui devront maintenir un niveau élevé de niveau de défense-cyber.

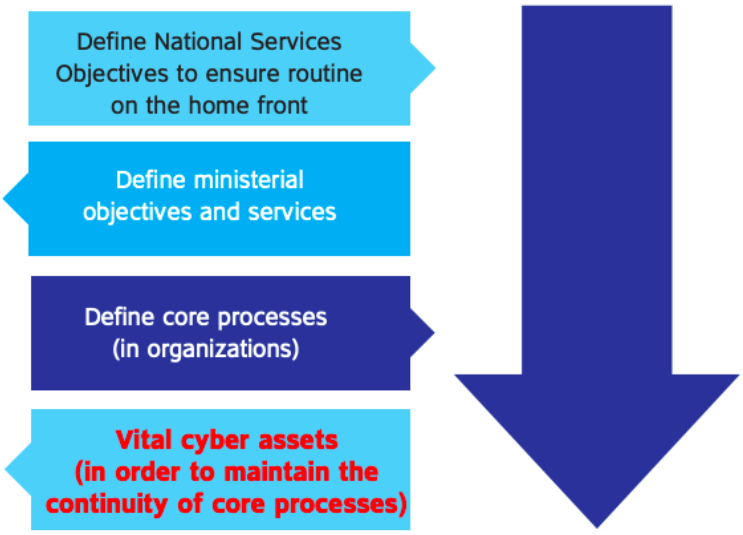


Figure 7. Méthode descendante des ressources informatiques vitales
Source : Deloitte France Cyber Risk Services

1.3. Le système « risque cyber » dans une entreprise

Lorsque Monsieur Imade Elbaraka, Associé Cyber Risk Services chez Deloitte France dit que "*la gestion de la sécurité du système d'information (SI) ne suffit plus lorsqu'on parle de dispositif de gestion des risques cyber*", nous comprenons que la gouvernance de la sécurité s'inscrit dans une approche plus globale et selon un cycle bien défini << ***préparer les évènements inattendus, Enseigner ou former ses collaborateurs à ces éventualités et savoir répondre en cas de risque majeur*** >>.

Il existe deux grands types de cyberattaques :

- La compromission des systèmes et données : ces attaques impactent la confidentialité des données, et souvent sans que les systèmes attaqués n'en ressentent les effets.
- L'indisponibilité des systèmes et données : ces attaques paralysent les systèmes d'information de l'entreprises ou rendent indisponibles ses données.

Lorsque notre organisation rencontre l'un des cas de figure cité dessus, le dispositif de gestion de crise doit être mis en route et ainsi que la mobilisation des capacités d'urgence. D'où l'importance vitale aujourd'hui d'insérer la dimension cyber dans la façon de gérer les crises de l'entreprise en impliquant notamment les bons acteurs et les bons outils.
Il est par exemple nécessaire d'anticiper ces situations en constituant un système de gestion de crise indépendant du réseau nominal afin de s'émanciper du réseau initial en cas d'attaque l'ayant rendu hors d'usage ou compromis. Cette même réflexion doit permettre d'identifier des

solutions d'échanges alternatives par messageries ou autres tout en garantissant leur confidentialité.

Ainsi, comme le dit le comité Risques & Entreprises de Euro Disney, " *Maîtriser le risque de cyberattaque demeure aujourd'hui indispensable pour éviter que l'intégralité des bénéfices économiques et humains liés à la transformation numérique ne se trouvent compromis. Les entreprises, quelle que soit leur taille, doivent assurer la mise en place de nouveaux schémas organisationnels et techniques pour palier à ces nouvelles problématiques dont les impacts potentiels sont toujours croissants.*"

1.4. Les scénarios d'attaque cyber

Selon l'étude « Attack Landscape H2 2019 » réalisée par F-Secure en mars 2020, 5,7 milliards de cyberattaques ont été enregistrées à l'échelle mondiale, c'est à dire 5 fois plus qu'en 2018. Les attaques de déni de service distribué [27]sont montées en puissance.
De la cybercriminalité à l'espionnage industriel, nous avons retenu 5 types de cyberattaques dont nos différentes organisations devraient se méfier.

#1 Les ransomwares

Ce type d'attaque a explosé ces dernières années avec des pertes conséquentes affligées aux entreprises. Nous avons en mémoire l'attaque subie par l'industriel français Saint-Gobin, touché par un cryptolocker dont les pertes ont été évaluées à plus de 300 millions d'euros.
La grande vague d'attaques provoquée par Wannacry, CryptoWall et TeslaCrypt qui sont des rançongiciels mettant les données d'une organisation sous clé et exigeant de l'argent pour les libérer.

#2 Le déni de service (DOS et DDOS)

Les attaques par déni de service sont provoquées par un utilisateur qui envoie massivement des requêtes à un serveur qui va vite se retrouver saturé quand il tentera de répondre. Il y'a tout de même deux attaques différentes :

- Les attaques par déni de service volumétrique, qui submergent la bande passante pour provoquer une latence dans les réponses des serveurs ou un arrêt total ;
- Les attaques par déni de service applicatif, qui envoient de nombreuses requêtes erronées pour que le serveur ne puisse pas les traiter et devienne hors d'usage.
- Ce type d'attaque est complexe à atténuer et demande des investissements de sécurité plus lourds.

#3 La compromission d'identité et/ou de mot de passe

C'est le phishing qui est à la fête dans cette attaque : l'attaquant envoie massivement les mails en se faisant passer pour un fournisseur d'accès ou une personne ou institution de confiance comme les impôts. Et lorsque la victime se connecte avec le lien ou les informations laissées, l'attaquant vole les données avec les conséquences connues.

[27] Un déni de service distribué (DDoS, Distributed Denial-of-Service) est une attaque dans laquelle de nombreux systèmes sont compromis et réunis pour attaquer une seule cible, afin de submerger les ressources du serveur et de bloquer les utilisateurs légitimes.

C’est généralement un type de mail facilement reconnaissable mais les attaquants aussi continue de se perfectionner.

#4 Les attaques indirectes

Ce genre d’attaques trouve sa source dans la négligence comme par exemple un collaborateur qui infecte son sa machine en étant mobile et en se connectant à un réseau peu sécurisé (déplacement à l’étranger, télétravail, etc.), puis vint le tour d’infecter les autres machines dès qu’il se connecte au réseau de l’entreprise.
Ce type d’attaque se fait en deux phases : d’abord à l’extérieur avec internet puis en utilisant la compromission initiale qui permet à l’attaquant d’avoir toutes les informations pour passer à l’attaque.

#5 Les menaces opérationnelles

Dans ce cas, les attaquants ciblent tout simplement les réseaux mal protégés pour s’introduire dans une infrastructure et d’en prendre le contrôle.
Avec ces scénarios divers et variés, il est plus qu’important d’investir dans des solutions de défense qui vont tenter d’enrayer ou de ralentir ces attaques. Tout cela passe par une bonne politique de cybersécurité que les entreprises doivent adopter et surtout prendre conscience de la valeur des ressources dont elles disposent.

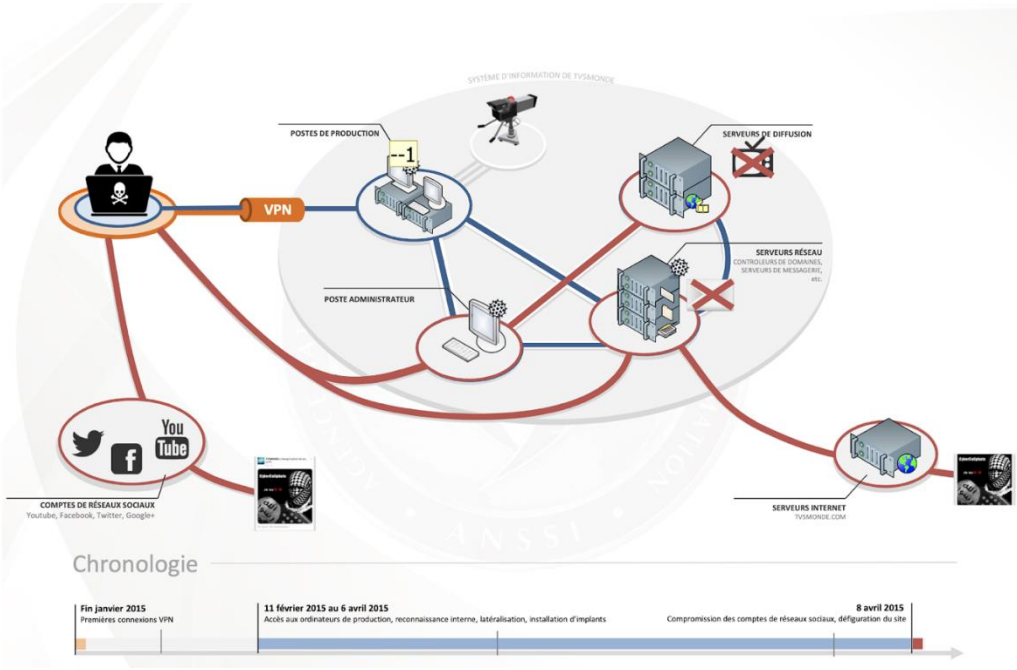
1.5. Action de réduction des risques : les chaînes d’approvisionnement

Une étape importante dans le processus de cartographie des ressources informatiques vitales et de leur protection, dans chacun des axes décrits ci-dessus, consiste à examiner la chaîne d'approvisionnement. Le fonctionnement de nombreuses organisations dépend des services qu'elles achètent ou reçoivent de fournisseurs externes, tels que les sous-traitants qui fabriquent des composants informatiques, les fournisseurs de services informatiques et autres. Comme ces services peuvent être connectés aux systèmes de l'organisation, ils sont également connectés aux ressources informatiques vitales. Par conséquent, chaque organisation est tenue de cartographier et d'identifier les menaces et les risques contenus dans les systèmes et les services de ses fournisseurs, et de les inclure dans son investissement et dans la protection des ressources informatiques vitales.

2. Etude de cas : France Télévision

Au cours de l’année 2015, les médias en France ont subi quelques attaques autant mineures que considérables. L’ANSSI nous retrace ici une petite chronologie de ces attaques.

#Schéma de compromission du système d'information de TV5 (ANSSI)



Source: ANSSI

Le 8 avril 2015 à 20 h 50 HAEC, l'infrastructure de diffusion de TV5 Monde (le multiplexage) est la cible d'une cyberattaque. Même si l'infrastructure principale et celle de secours sont neutralisées d'un seul coup, le directeur informatique de la chaîne et son équipe croient tout d'abord à une panne technique. Mais quelques minutes plus tard, le serveur de messagerie électronique est détruit, confirmant une cyberattaque. Pour le directeur informatique, il s'agit d'une « *agression fulgurante qui a probablement été très bien préparée* ».
Pour limiter les dégâts, les équipes techniques coupent l'ensemble du réseau informatique vers 22 h, interrompant les diffusions télévisées de la chaîne dans le monde.

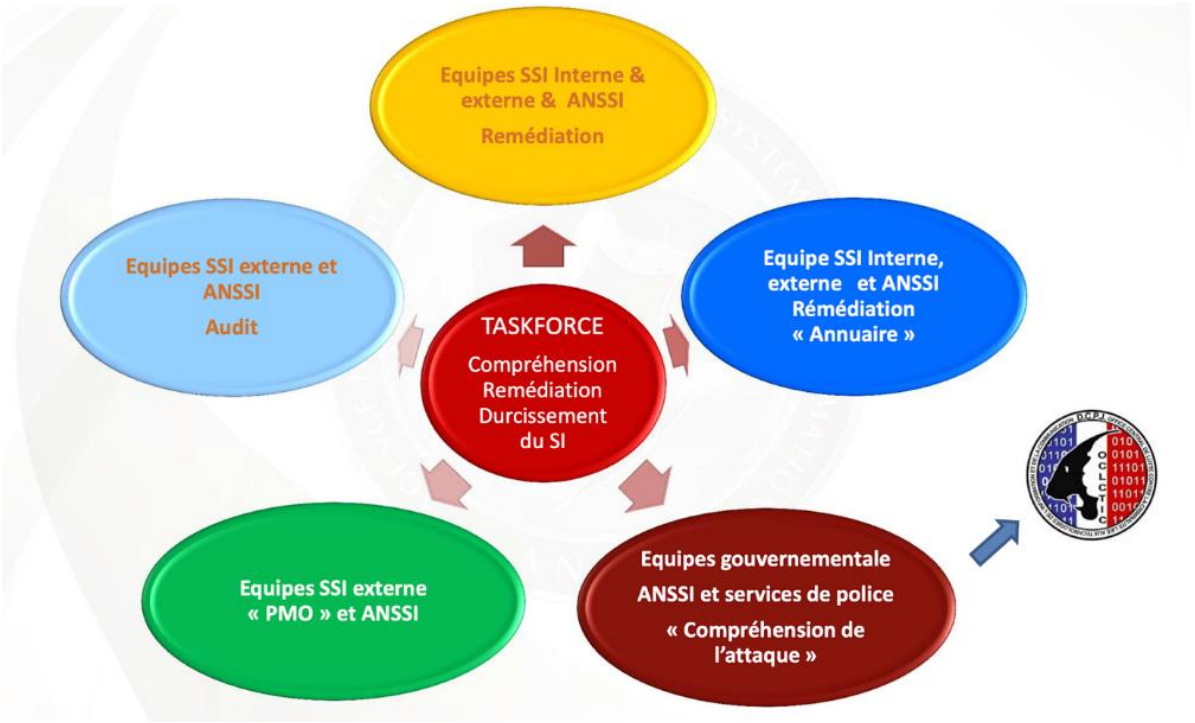
En parallèle, les comptes Twitter et Facebook de la chaîne sont également piratés. Des messages de soutien à l'État islamique en anglais, arabe et français y sont publiés, ainsi que des documents présentés comme des pièces d'identité et des CV de proches de militaires français impliqués dans les opérations contre l'État Islamique.
Un message accuse le président de la République François Hollande d'avoir commis « *une faute impardonnable* » en menant « *une guerre qui ne sert à rien* », récompensée par les « *cadeaux de janvier à Charlie Hebdo et à l'Hyper Cacher* », faisant référence aux attentats de janvier 2015 en France.

Peu avant minuit, les équipes techniques arrivent à reprendre le contrôle des réseaux sociaux et postent des messages d'explication à destination des internautes. Le directeur général de TV5Monde, Yves Bigot, poste une vidéo sur Facebook et parle d'une « *cyberattaque extrêmement puissante* ».

- Le 9 avril à partir de 5h HAEC, le système informatique et les signaux télévisés sont progressivement relancés avec l'aide d'une quinzaine d'ingénieurs en sécurité informatique de l'ANSSI dépêchés sur place.

- Vers 10 h, toutes les chaînes du réseau sont rétablies mais elles ne peuvent diffuser que des programmes préenregistrés, et pas les journaux en production propre.
- À 18 h, la chaîne reprend une diffusion normale avec son programme d'information en direct le "*64' Le Monde en Français*".

#Taskforce " Compréhension Remédiation Durcissement"
Il est important de se référer aux prérequis de l'ANSSI. C'est pourquoi face à l'urgence, l'ANSSI fait partie intégrante de la composition des équipes spécialisées devant l'urgence de combler les failles de sécurité et de corriger les dégâts.



Source : ANSSI

En ce qui concerne les prestataires d'audit de la sécurité des systèmes d'informations (PASSI) qualifiés, l'ANSSI propose une liste consultable sur son site : [Prestataires d'audit de la sécurité des systèmes d'information (PASSI) qualifiés].

#Plans d'actions de TV5 validés par l'ANSSI

- Remédiation et durcissement.
- Bascule de l'Active Directory.
- Mise en place d'une supervision pour la Sécurité du Système d'Information (SSI).
- Audits complémentaires.
- Campagne de sensibilisation.
- Quelques règles d'hygiène informatique pour une défense en profondeur.
- Utilisation des machines connectées à internet.
- Sécurité renforcée en fonction des métiers.
- Imposer une politique de mot de passe.

3-L'état d'alerte et les principes du changement

Les états d'alerte constituent un signal reflétant le degré requis de vigilance et préparation à la lutte contre les circonstances qui prévalent dans les entreprises. Ils seront déterminés sous réserve d'une évaluation de la situation, qui devrait permettre de mieux comprendre ce qui se fait sur la base d'informations, de faits et de l'analyse, après quoi, les actions à réaliser seront définies.
Déclarer un état d'alerte le plus tôt possible en cas de menace correspond à un seuil déjà défini, et les actions ou prédispositions à prendre rapidement contribueront à réduire la probabilité de dommages sur les biens essentiels ainsi qu'à l'activité globale de l'organisation. Ainsi, l'on peut aider à minimiser le développement d'une crise-cyber, et, si cela s'est déjà produit - à minimiser les dommages qui ont été causés.
D'autre part, l'absence de déclaration d'un état d'alerte approprié entraînera des dommages à grande échelle - dommages qui auraient pu être évités ou réduits.

4-Description des différents niveaux d'alerte

Tant qu'elle n'a pas été déclarée autrement, une organisation reste dans un état de "routine de défense", elle mène des opérations de routine. Dans cette situation, aucune perturbation du fonctionnement normal des biens essentiels de l'organisation n'est indiquée.
Une menace importante de dommage à un bien essentiel ou une perturbation possible de ses opérations normales (même s'il n'a pas encore été prouvé qu'elle découle d'un incident cyber), reflète une escalade possible et augmente la probabilité de l'apparition d'une crise-cyber.
Dans un scénario extrême, des dommages étendus et prolongés à grande échelle sur un ou plusieurs bien essentiels causent des dommages importants aux processus de base (routine de défense) et à la continuité des activités de l'organisation.

Etat d'alerte	Description
Routine de défense	Vert : aucun signe de perturbation de la continuité fonctionnelle des ressources informatiques vitales
Escalade	Jaune : une menace importante pour les ressources informatiques vitales. Leur continuité fonctionnelle est compromise. Rouge : les dommages causés aux ressources informatiques vitales peuvent entraîner leurs dysfonctionnements. Noir : les dommages étendus et prolongés causés à grande échelle aux ressources informatiques vitales avec de gros dégâts dans leurs fonctionnements et à celle de l'entreprise.

5-Indicateurs clés de la prise de décision

Un état d'alerte cyber sera déterminé en utilisant des indicateurs qui classent la gravité de la menace et la probabilité de sa réalisation, donc en indiquant les mesures à prendre et les ressources et les outils à utiliser. Les situations d'urgence causées par un déclencheur non-cyber (comme : guerre, phénomène naturel, activités terroristes, pandémie etc.) servent souvent d'opportunités pour les cyberattaquants pour intensifier leurs efforts, précisément lorsque le fonctionnement normal des ressources informatiques devient vraiment essentiel ou vital. L'état d'alerte cyber sera déterminé non seulement par les circonstances dans le

cyberespace, mais aussi par les circonstances dans l'espace physique que les ressources occupent.

Deux points importants dans la corrélation entre les indicateurs et l'état d'alerte :

- La mise en avant d'un indicateur particulier ne dicte pas nécessairement un niveau spécifique d'alerte cyber, mais les indicateurs sont plutôt des outils utilisés en conjonction avec une évaluation de la situation pour décider du niveau d'alerte.
- Une alerte cyber peut être déclarée avant même qu'un cyber incident ne se produise et sans qu'il n'y ait pas d'indications de dommages causés aux ressources informatiques vitales. Cela peut être le résultat d'alertes informationnelles ou de circonstances qui augmentent la dépendance et l'importance du fonctionnement normal des ressources informatiques vitales. En d'autres termes, une organisation peut être définie dans une alerte cyber de niveau A ou B (ou Level A ou B) en même temps qu'elle a le "feu vert" dans le système d'escalade.

Partant du fonctionnement normal et optimal des ressources vitales de l'entreprise, nous allons voir évoluer le niveau d'alerte jusqu'au plus élevé faisant ainsi appel à l'organisme national qui intervient pour comprendre et maîtriser la crise cyber lorsqu'elle est avérée et persistante. Le tableau suivant nous en donne un aperçu et définit l'état des niveaux d'alertes tels que décrit par Deloitte France par son Cyber Risk Services :

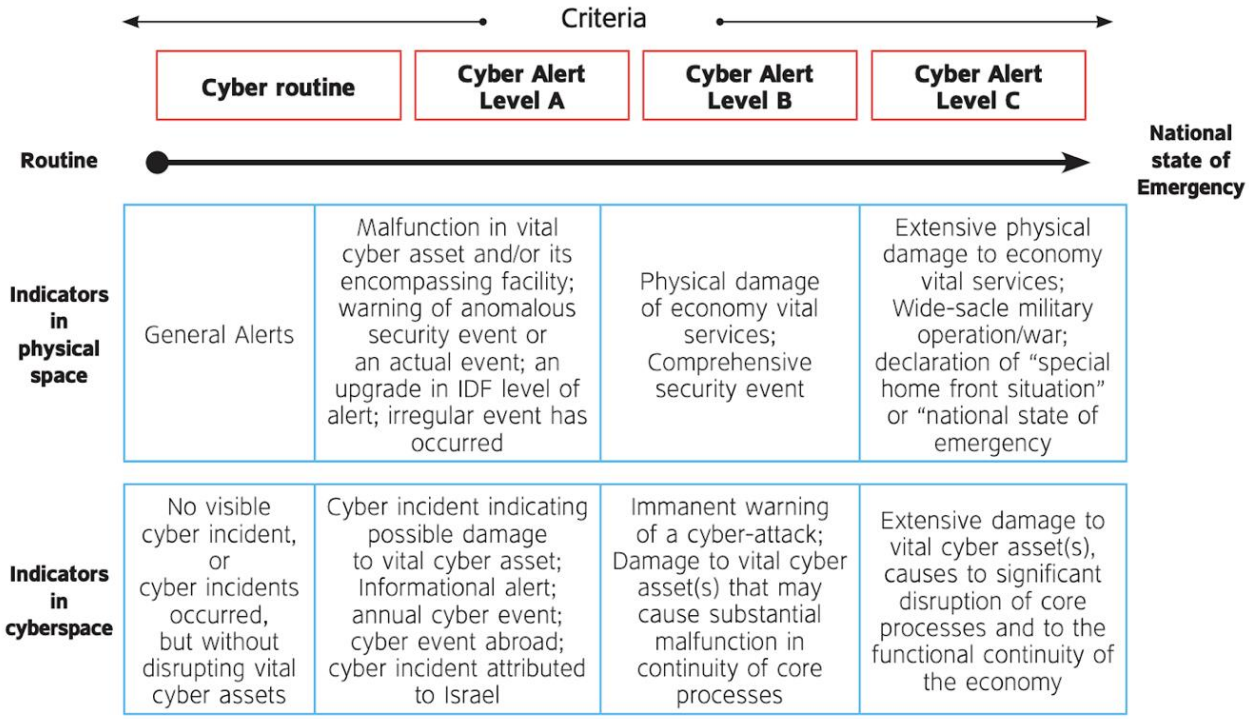


Figure 8. Critères d'évaluation et changement d'état d'alerte

.

 # La routine cyber ou Absence de crise-cyber

C'est la situation par défaut, lorsque les circonstances dans l'environnement cyber et de l'infrastructure ne montrent aucun signe de perturbation du fonctionnement normal des ressources informatiques vitales, ni aucun besoin de renforcer la défense. Dans ces circonstances, les indicateurs de niveau d'alerte semblent être normaux.

Indicators in cyberspace : soit aucun incident informatique visible ne s'est produit, soit des incidents informatiques se sont produits, mais sans perturber les ressources informatiques vitales.
Indicators in physical space: Alertes générales ou pas d'incidents connus.

 # Alerte Cyber "Level A"
Le niveau d'alerte "Level A" sera déterminé à la suite d'une évaluation de la situation, et à condition qu'au moins un des indicateurs suivants ait été respecté.

Indicators in cyberspace : un incident informatique s'est produit indiquant une possible perturbation du fonctionnement normal d'une ressource informatique vitale ; la notification d'une alerte informative ; une cyber-attaque annuelle ; un événement informatique s'est produit à l'étranger qui ne s'est pas encore propagé (tel que "WannaCry") ;
Indicators in physical space : un dysfonctionnement opérationnel/technique d'une ressource informatique vitale et/ou du site où elle se trouve ; l'alerte d'un événement de sécurité à grande échelle ou l'arrivée d'un événement de sécurité aberrante.

 # Alerte Cyber "Level B"
Le niveau d'alerte "Level B" sera déterminé si au moins l'une des conditions suivantes est satisfaite.

Indicators in cyberspace : avertissement imminent d'une cyber-attaque ; dommages des ressources informatiques vitales et, par conséquent, perturbation réelle potentielle de la continuité opérationnelle des opérations.
Indicators in physical space : des dommages physiques aux services vitaux pour l'économie de l'entreprise (tels que : panne d'électricité, perturbation des services de fonctionnement) ; un événement cyber de grande envergure s'est produit telle la corruption des services de l'organisation.

 # Alerte Cyber "Level C"
Le niveau d'alerte "Level C" est le niveau d'alerte le plus élevé, de sorte que les circonstances qui ont motivé la déclaration de cet état d'alerte sont susceptibles de dégénérer en un état d'urgence global ou national. Ce niveau d'alerte sera déterminé à la suite d'une évaluation de la situation, et à condition qu'au moins un des indicateurs suivants ait été respecté.

Indicators in cyberspace : des dommages importants et/ou persistants aux ressources informatiques vitales, entraînant une perturbation importante des processus opérationnels et de la continuité fonctionnelle de l'économie (tels que les dommages étendus dans l'organisation tout entière).
Indicators in physical space: des dommages physiques importants et/ou persistants à des services vitaux pour l'économie de l'entreprise ; la déclaration d'une "situation spéciale de d'arrêt complet des ressources opérationnelles de l'entreprise".

IV-Gestion de la crise cyber

Selon l'Institut national des hautes études de la sécurité et de la justice, la gestion de crise est l'ensemble des moyens humains, juridiques, techniques et matériels permettant à une organisation de se préparer aux risques et de faire face aux impacts pouvant affecter le bon fonctionnement de cette dernière. Il affirme en plus que tirer les enseignements de l'évènement est une bonne chose mais il faut que ce retour d'expérience serve de base solide à des procédures visant à l'anticipation des risques, la réponse aux impacts et ce, dans une vision prospective.

Gérer une crise n'est donc pas un évènement à improviser. La gestion de crise doit être anticipée par l'entreprise avec la mise en place en amont d'une évaluation des risques qui servira de base à la mise en place d'un plan.

Nous allons aborder le traitement de la gestion de crise au sens large du terme. Puis, nous aborderons spécifiquement la question des crises cyber.

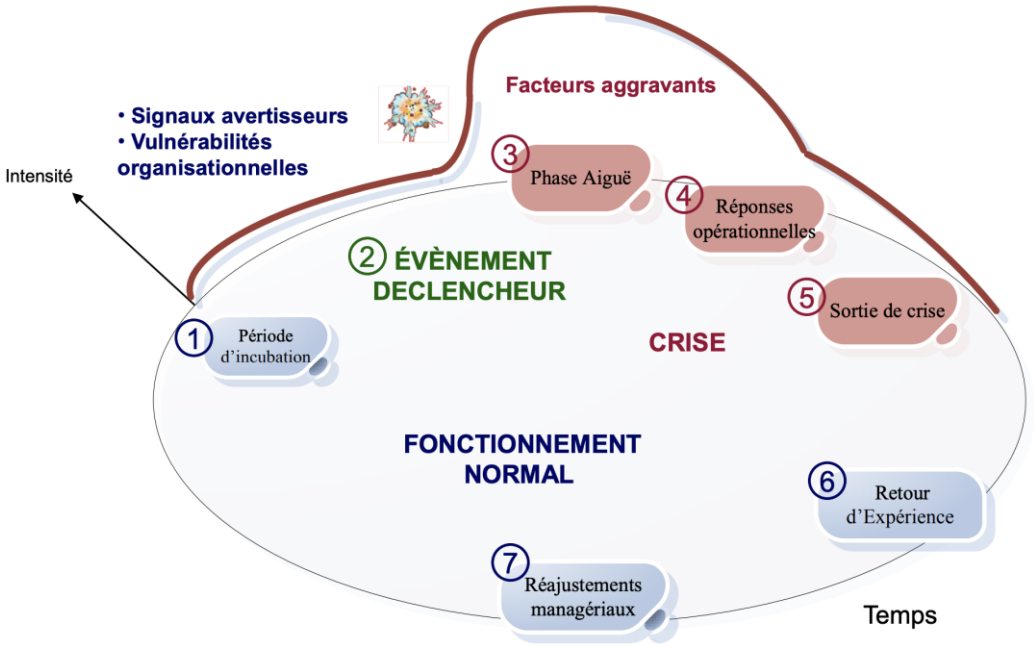


Figure 9. Fondamentaux de la gestion de crise
Source : Institut National des Hautes Études de la Sécurité et de la Justice

Dans ce schéma ci-dessus que l'Institut National des Hautes Études de la Sécurité et de la Justice a publié dans son étude, la crise représente une situation anormale au fonctionnement normal de l'entreprise : et le début de la crise est bien caractérisé par un évènement déclencheur dont la sévérité ou l'état est amplifié par des facteurs ou niveau d'alertes définis plus haut.

1. Organisations, moyens et processus

Les bonnes pratiques en termes d'organisation recommandent de scinder les rôles entre une cellule de direction de crise et une ou plusieurs cellules opérationnelles de crise, qui assumeront respectivement des responsabilités de pilotage et d'exécution.

Figure 10. Organisation de la gestion de la crise
(Source : Institut National des Hautes Études de la Sécurité et de la Justice)

La collaboration et la coordination entre les deux types de cellule doivent être établies avec soin. Un pilotage surdimensionné conduit au piège de la **pyramide inversée** qui étouffe la capacité d'exécution du dispositif (les opérationnels passent plus de temps à rendre compte qu'à traiter). Et, *a contrario*, un pilotage sous-dimensionné peut être tout aussi inefficace en laissant les ressources et énergies se disperser dans de mauvaises directions.
La composition de ces cellules dépend évidemment du contexte de chaque entreprise et de la nature de chaque crise mais on retrouvera, de manière très classique, les participants suivants :

Cellule de direction de crise :
➢ Pilote de crise (*en liaison avec la Direction générale*).
➢ Directions Métiers *(en fonction de la nature de la crise).*
➢ Direction Communication.
➢ Direction des Ressources humaines.
➢ Direction des Systèmes d'information.
➢Direction juridique.
➢ Direction Gestion des risques ;

Cellule(s) opérationnelle(s) de crise :
➢ Ressources opérationnelles « Métier ».
➢ Ressources « informatiques et sécurité ».
➢Ressources « Communication ».
➢Partenaires externes en cas de besoin (expertise légale, expertise sécurité...).

Ces cellules doivent ensuite disposer de **moyens** pour assurer leur mission. Parmi ces moyens, on notera tout d'abord les salles de crise. Ces salles devront permettre aux cellules de se réunir en un même lieu et devront également être équipées de moyens de communication (système de téléphonie, site web pour échanger des documents) et de moyens de traitement opérationnels (ordinateurs connectés aux réseaux de l'entreprise et à internet...). Mais il faudra également fournir aux cellules les informations, documents de référence et outils qui

leur permettront de piloter et coordonner leur activité (annuaire de crise, journal de crise, tableaux de bord de pilotage).
Et enfin, ces cellules doivent pouvoir opérer en se référant à des guides opératoires et processus de fonctionnement qui auront été définis au préalable. Cela concerne aussi bien les **processus** de déclenchement (procédures d'alerte et d'escalade, procédure de qualification du niveau de crise) que les processus de traitement (fiches réponses décrivant les modes opératoires de traitement et correction, guide de communication rappelant les messages clefs et règles à respecter dans toute communication externe).

2. Les phases importantes de la crise : début et fin de la crise

Dans toute gestion de crise, l'entreprise va être confrontée aux enjeux suivants.
Comment :

- Détecter et gérer l'entrée en crise ?
- Évaluer la gravité de la crise ?
- Répondre à la crise ?
- Détecter la fin de la crise ?
- Capitaliser ?

Détecter et gérer l'entrée en crise est une tâche délicate. Cela impose aux organisations d'avoir établi les processus et/ou les réflexes qui permettent d'identifier, dans leurs lots d'incidents quotidiens, ceux qui sont générateurs de risques importants et qui sont des déclencheurs potentiels de crises. Cela suppose de mettre en place une discipline de qualification des événements et incidents qui permette de faire rapidement ce tri et de donner l'alerte quand il le faut.

L'évaluation de la gravité de la crise est également une étape importante. En effet, c'est cette évaluation (avec par exemple des classifications du type niveau Rouge ou niveau Orange) qui permettra non seulement de décider s'il faut déclencher une crise mais également de dimensionner le dispositif de réponse.

Répondre à la crise nécessite d'identifier et mobiliser toutes les ressources pour enrayer le développement de la crise et exécuter les actions qui en corrigeront les impacts. Cela réclame une grande capacité de pilotage et de coordination ainsi qu'une bonne communication interne et externe.

Détecter la fin de la crise permettra de mettre fin au dispositif exceptionnel de gestion de crise. Cela ne doit pas être fait trop tôt (attention à l'effet boomerang d'un problème supposé résolu qui resurgit) mais il faut également veiller à ne pas prolonger le dispositif inutilement.

Capitaliser, après la sortie de crise, consiste à faire une analyse *post-mortem* ou un **retour d'expérience** sur l'ensemble du déroulement et des événements de la crise. Cette activité est essentielle pour permettre à chaque organisation d'identifier des axes d'amélioration et ajuster leur plans et processus de gestion de crise en conséquence.

Ce retour d'expérience doit se faire :

- À chaud, pour recueillir ce qui est bien présent dans la mémoire de chacun des acteurs.

- À tiède (quelques semaines plus tard), pour valider les enseignements et propositions de plan d'actions post-crise à engager.
- À froid (par exemple à la date d'anniversaire), pour évaluer plus sereinement l'impact réel de la crise initiale et vérifier que les leçons et plan d'action post-crise du Retour d'expérience ont bien été appliquées.

3. Ce qu'il faut retenir d'une gestion de crise cyber

La gestion de crise cyber doit être pluridisciplinaire : elle est notamment au croisement de la gestion du risque et de la sécurité informatique (donc technique). Les experts techniques seront au service du décisionnaire dans cette gestion. Plus les choses auront été préparées en amont, notamment la cartographie des risques, l'analyse des vulnérabilités et des vecteurs et modes d'attaques, plus la gestion de la crise pourra être efficiente.
Et cette gestion doit naturellement prendre en compte les spécificités d'une attaque cyber qui sont de plusieurs natures :

- Les attaques cyber sont généralement **invisibles** ou difficiles et longues à identifier contrairement à d'autres types classiques de crises tels qu'un séisme, un incendie, une crue, les entreprises doivent donc développer leur capacité de détection des signes précurseurs et des « signaux » faibles d'attaques avant que celles-ci ne deviennent majeures.
- La deuxième spécificité tient au fait que l'étendue des attaques est bien souvent très difficile à évaluer et qu'elle peut évoluer très vite. En effet, les attaques ont pu être détectées longtemps après leur occurrence et ont donc pu « contaminer » de multiples parties du Système d'information de l'entreprise. De plus, ces attaques peuvent également continuer à se propager très rapidement. Cela doit conduire les cellules de crise à définir des plans d'actions pour confiner les attaques et enrayer leur propagation. Elles devront ensuite mener des opérations de correction et de reconstruction, tout en continuant à garder sous surveillance les parties du Si qu'elles vont progressivement « assainir ».
- La troisième spécificité est directement liée à la dimension technique des attaques. La cellule de crise doit pouvoir mobiliser une multiplicité d'expertises et de compétences technologiques pour pouvoir contenir et remédier à une attaque cyber. il lui faudra donc pouvoir solliciter très rapidement un grand nombre de spécialistes en interne ou en externe tels que: des experts en analyse technique post-incident, des équipes CeRt, des agences nationales de lutte contre la cybercriminalité tels que l'Office Central de lutte contre la Criminalité liée aux technologies de l'information et de la Communication (OClCtiC), la Brigade d'enquêtes sur les fraudes aux technologies de l'information (BeFti), l'Agence nationale de la sécurité des systèmes d'information (ANSSi), voire même la Direction centrale du renseignement intérieur (DCRi).

Une autre particularité des crises cyber est que l'attaque, en altérant le Si de l'entreprise, peut directement diminuer sa capacité de réponse. Il convient donc de disposer d'un dispositif de gestion de crise qui permette de pallier à cette possibilité et par conséquent :

- de prévoir des moyens de gestion de crise hors Si ;
- de se doter de postes de travail durcis hors des domaines d'administration ;

• d'exploiter des services d'échange et de communication externes (par exemple des services *cloud*).

4. La communication

Depuis l'avènement du Web 2.0 et des media sociaux, les entreprises se trouvent bien souvent dans une situation de communication externe « asymétrique » : c'est-à-dire qu'elles continuent majoritairement à utiliser des canaux de communication traditionnels alors que l'opinion publique devient de plus en plus sensible et influencée par la viralité des informations diffusées sur internet. Les entreprises comprennent désormais qu'internet doit devenir pour elles un canal de communication « officiel » et elles doivent adapter leur stratégie de communication en conséquence.
C'est particulièrement vrai en temps de crise quand la communication externe doit veiller à préserver la notoriété de l'entreprise et que cette dernière peut se retrouver menacée sur internet. Des organisations, des groupes d'internautes ou même de simples individus peuvent ternir directement l'image d'une entreprise et déclencher ou aggraver une crise en diffusant de fausses informations ou des informations confidentielles sur internet. Il faut être capable de détecter ces menaces/attaques mais également de proposer une riposte « symétrique », c'est-à-dire dont l'impact positif sur internet permettra d'éteindre l'impact négatif initial sur le public.
Mais cela ne s'improvise pas et chaque entreprise devra, dans un premier temps, établir sa présence, développer ses propres réseaux et asseoir sa crédibilité sur ces nouveaux media. Pour cela, il lui faudra :

- Organiser une **veille continue sur les communications sur internet** ayant un rapport avec son activité et pouvant constituer des signaux faibles ou éléments déclencheurs de crise.
- Comprendre et apprendre les **bonnes pratiques de communication** sur les réseaux sociaux.
- Identifier les **communautés, cercles et *leaders* d'opinion** ayant une influence sur son activité.
- Créer les liens et établir la communication et les échanges avec ces acteurs.

L'enjeu consiste ensuite à tirer les fruits de ce travail de veille en élaborant des messages ou stratégies de communication qui soient personnalisés pour chaque audience visée et qui puissent être diffusés directement par l'entreprise ou relayés par les communautés et groupes avec lesquels elle a établi un lien.
Tout va très vite sur internet. Aussi pour pouvoir réagir rapidement en cas de crise, l'entreprise devra définir en amont la liste des personnes habilitées à communiquer en son nom.
Communiquer en interne en période de crise est primordial pour coordonner l'ensemble des acteurs mobilisés dans la gestion de la crise (ex : équipes de supports locales, spécialistes de la cellule de crise, équipes techniques, juristes). Il convient donc de donner à chacun les informations dont il a besoin pour assumer ses activités et responsabilités mais également maintenir son engagement et investissement dans la gestion de l'événement.
Il faut néanmoins veiller à trouver la bonne limite dans le partage d'informations. Communiquer plus que nécessaire peut s'avérer contre-productif car cela peut créer des risques supplémentaires de fuite d'information vers l'extérieur avec toutes les conséquences décrites précédemment sur un public recevant un message qui n'a pas été conçu pour lui. Il

est donc préférable de communiquer de façon **ciblée** plutôt que globale afin de rendre l'information **parcellaire** et ainsi limiter les impacts négatifs en cas de propagation au-delà du cercle des personnes habilitées.
Il faut là encore être capable d'agir vite. Cela impose à nouveau de définir soigneusement au préalable la liste des personnes habilitées à communiquer en interne et de rappeler aux autres acteurs (internes mais aussi aux partenaires externes) leur devoir de réserve et leur obligation de confidentialité. Il est d'ailleurs conseillé de faire signer à tous un engagement de non-divulgation (*Non Disclosure Agreement* – NDA). Cela donnera les leviers juridiques de réponse aux fuites éventuelles d'information hors de la cellule de crise. On pourra également organiser une veille informationnelle dans l'entreprise afin de détecter et gérer les rumeurs, fuites, et être capable soit de les démentir, soit de les stopper.

> « *La cellule de crise est la forteresse de l'organisation qui traverse la crise. Le but de la cellule de crise est de pouvoir abriter les réserves stratégiques de l'organisation dans un lieu inaccessible aux attaques nées de la crise. Les activités tactiques de défense de l'organisation y sont coordonnées. C'est dire à quel point sont importants les travaux de fortification de cette cellule lors de l'anticipation des crises.* » dixit **Florian Silnicki**.

CONCLUSION

La lutte contre la cybercriminalité est-elle perdue ? [28] Le simple fait de se poser la question montre clairement l'étendue du problème pour les entreprises. Et l'analyse du contexte actuel et de l'évolution de la cybercriminalité peut venir renforcer nos doutes et notre pessimisme sur la question.

En effet, l'attaque a toujours un temps d'avance sur la défense. En innovant et créant continuellement de nouvelles armes, les cybercriminels peuvent contourner les mécanismes de défense que les entreprises ont bâtis sur la base des menaces « anciennes » qu'elles connaissaient. De plus, la confrontation est déséquilibrée car asymétrique.

D'un côté, les cybercriminels dédient toutes leurs ressources et leur énergie aux attaques cyber. Alors que de l'autre, les entreprises sont concentrées sur leur métier et la conduite de leurs affaires et ne voient donc les enjeux de défense cyber que comme un « mal nécessaire » et une affaire de spécialistes.

Mais alors, à quoi bon investir dans la cyber sécurité et dans la gestion de crise cyber ?

Friedrich Nietzsche nous donne la réponse au travers de son adage : « ***tout ce qui ne nous tue pas nous rend plus fort*** ». En effet, la première mission d'un dispositif de gestion de crise est de faire en sorte que la société « survive » à une attaque et à ses conséquences. Et comme nous l'avons vu tout au long de ce mémoire, sa capacité à répondre et à contenir les impacts négatifs des attaques dépendra fortement de son niveau de préparation et d'anticipation. Mais sa mission consiste également à tirer les enseignements de chaque crise pour améliorer son dispositif. Nous ne souhaitons évidemment pas aux entreprises d'être attaquées pour progresser mais nous les invitons néanmoins à considérer chaque incident de sécurité auquel elles sont déjà confrontées aujourd'hui comme une opportunité d'apprendre, de s'améliorer mais également d'éduquer et de sensibiliser l'ensemble de leur organisation.

La capacité d'une entreprise à répondre et à contenir les impacts négatifs (sur les métiers, les activités, le personnel, l'image et la réputation de la société) d'une crise dépend de son niveau de préparation et d'entraînement. Voici, en résumé, la marche à suivre pour se préparer au mieux à une crise cyber :

- Analyser les faiblesses de l'entreprise.
- Identifier les données les plus sensibles.
- Rédiger une politique de gestion de crise.
- Rédiger un kit documentaire.
- Constituer des cellules de crises, nommer des membres et leurs suppléants.
- Définir leur rôle et leurs responsabilités, leurs limites ;
- Penser la coordination entre les différents membres et les différentes cellules de gestion de crise.
- Former chaque membre à la gestion de crise ainsi qu'à de nouveaux outils de communication sécurisés.
- Créer un scénario d'exercice basé sur une vulnérabilité connue de la société et sur la menace la plus probable et ayant le plus d'impacts.
- Pendant la simulation, cadrer le périmètre d'intervention afin d'éviter le risque de suraccident.
- Observer les actions de chacun, les noter avec soin ;

[28] Huffington Post.

- Cadencer l’exercice par des stimuli ayant pour but de recréer la tension d’une crise.
- À la fin de l’exercice, réaliser une session d’analyse post-mortem à chaud.
- Écrire un rapport d’exercice et un plan d’action pour favoriser l’amélioration continue.
- Réaliser régulièrement des sessions de formation.
- Mener des exercices de gestion de crise au moins une fois par an.
- Mettre à jour régulièrement tous les documents évoqués plus haut.

WEBOGRAPHIE

- Juin 2013 – *Business les Echos* – Cyber-attaques: se préparer pour réagir efficacement.
- Juin 2014 – MacAfee & CSiS – *Net Losses: Estimating the global cost of cybercrime*.
- Juillet 2014 – *Huffington Post* - la lutte contre la cybercriminalité est-elle perdue ?
- 2005 – *Le magazine de la communication de crise et sensible* – Christophe ROuX- DuFORt – Gestion de crise – Premiers réflexes pour le pilotage – Guide pour les managers.
- 2013 – MacAfee – *Creating and maintaining a SOC*
- 2016 - Cyber crisis management : Readiness, response and recovery
- 2020 – Insider Threat Report