MASTER EN SCIENCES DE GESTION

Gestion du risque cyber au sein des entreprises

Claeys, Manu

Award date:
2019

Awarding institution:
Universite de Namur

Gestion des risques cyber au sein des entreprises

Manu Claeys

Directeur: Prof. E. Dauvin

Mémoire présenté
en vue de l'obtention du titre de
Master 60 en Sciences de gestion
à finalité spécialisée

ANNEE ACADEMIQUE 2018-2019

Université de Namur, ASBL
Faculté des Sciences économiques, sociales et de gestion – Département des Sciences de gestion

Rempart de la Vierge 8, B-5000 Namur, Belgique, Tel. +32 [0]81 72 48 41/49 58, Fax +32 [0]81 72 48 40

Table des matières

1 Avant-propos 3

2 Introduction 4

2.1 Délimitation de ce mémoire et question de recherche 6

2.2 Problématique 7

2.3 Plan du mémoire 7

3 Ampleur de la menace cyber 8

3.1 Historique des attaques et évolution du contexte 8

3.2 Etat des lieux des risques informatiques et indices de cybersécurité 11

3.2.1 Risques informatiques 11

3.2.2 Indices de cybersécurité 12

3.3 Coût et fréquence des attaques cyber et pertes encourues actuelles 13

4 Management des risques cyber 18

4.1 Volet prévention et culture d'entreprise 18

4.1.1 Introduction 18

4.1.2 Les pratiques à adopter 21

4.2 Volet gestion des risques 29

4.2.1 Introduction 29

4.2.2 Approche de gestion des risques par l'OCDE 31

4.2.3 Approche de gestion des risques par le « Centre de Cybersécurité Belge » 36

4.3 Veille technologique et réglementaire 37

4.4 Solutions logicielles 38

5 Gestions des crises 40

5.1 Introduction 40

5.2 Le cycle de la gestion de crises 42

5.3 Plans et outils 46

5.3.1 Plan de continuité des activités (PCA) 47

5.3.2 Cellule de crise 49

5.3.3 Plan de communication 51

5.4 Conclusion de la section 54

6 Externaliser la gestion des risques à une partie tierce 54

7 Modèle de cybersécurité 56

8 Limites de ce mémoire 57

9 Conclusion 58

10 Bibliographie 59
10.1 Bibliographie de la littérature 59
10.2 Bibliographie des figures 65
11 Annexe 67
11.1 Figure 67
11.2 Revue du mémoire par un professionnel de la cybersécurité 73

1 Avant-propos

Je tiens à exprimer toute ma gratitude envers mon promoteur de mémoire, Monsieur Emmanuel Dauvin, qui m'a épaulé durant ce travail, grâce à ses remarques, critiques, et suggestions.

J'adresse un sincère remerciement à Monsieur Frédéric Gelissen, professionnel de la cybersécurité, qui a consacré du temps à lire mon travail et m'a proposé quelques pistes de réflexion et d'amélioration, avec l'œil critique du professionnel.

Je remercie également toutes les personnes qui ont pris le temps de lire mon mémoire, et de me donner leur avis, pour certains avec un œil externe aux études de gestion ainsi qu'au thème abordé.

2 Introduction

De l'apparition du téléphone en 1886, à celle de l'ordinateur ne comportant plus de pièces mécaniques en 1943, 57 années se sont écoulées. Le début du 20ème siècle jusqu'à la fin des années 70 n'a pas connu de bouleversement majeur dans le domaine des technologies de communication. Les 50 dernières années, en revanche, ont connu une accélération du progrès technologique et numérique, avec l'apparition du téléphone portable en 1973, de l'iPhone à partir de 2007, de la tablette moderne en 2010… Ces changements introduisent de profonds bouleversements dans la manière que nous avons d'échanger, de communiquer, de faire parvenir des données en un rien de temps à l'autre bout de la planète. Ces bouleversements profonds ne tiennent pas tant dans l'invention de nouveaux outils numériques, que dans l'utilisation et l'usage quotidien que nous faisons de ces outils. Il est chose courante, désormais, de vérifier, grâce au numérique, la qualité d'un service avant de l'utiliser, de commander un produit sans contact réel avec un vendeur, et même de consulter des livres sous leur forme virtuelle.
Les entreprises, quant à elles, sont également de plus en plus présentes sur le volet numérique (Agence du numérique, 2018), utilisant le cloud computing (service offert sous forme de serveurs à distance), les progiciels (outils généraux permettant un multi-usage), les processus métiers (ERP, CRM), etc.

Nous assistons donc à une accélération du « tout informatique » et un changement brusque dans nos manières d'échanger de l'information.

Nous sommes à l'aube d'une révolution numérique, comparable à la révolution industrielle qui a bouleversé le paysage de la production et a repoussé les frontières du possible en matière technologique, et, dans ce cadre, il est prévisible que cette tendance s'accélérera et que pas un domaine ne sera épargné par la révolution numérique, allant de la maison connectée aux accessoires individuels, passant par la voiture, frigo, lunettes, puces connectés[1]. Tant les outils numériques, destinés aux particuliers, que les machines professionnelles seront interreliées, envoyant et recevant de nombreuses données en temps réel. *« Une étude (AON et Ponemon Institute, publiée en avril 2017) révèle d'ores et déjà le changement de paradigme qui s'opère actuellement* », annonce le dossier sur la couverture du cyber risque (Scor, 2017 : 3). En effet, cette étude (Ponemon Institute, 2017) montre que la valorisation que les entreprises font de leur information (appelés actifs intangibles en comptabilité) est supérieure

[1] Ce que reflète le concept d' « internet of Things » (IOT)

à celle de leur équipement de manière générale (actifs tangibles, appelés PP&E, soit « Property, Plant and Equipment »). Dans ce contexte, et au rythme de l'évolution de la situation actuelle, il est également possible que demain, pourquoi pas, le niveau général de cybersécurité d'une entreprise devienne une nouvelle variable de compétitivité !

Dans ce cadre, la numérisation de l'économie, apportant son lot de bénéfices grâce à l'immédiateté de l'échange d'information et l'automatisation, offre un gain de temps non négligeable à la détection d'une panne, l'anticipation de problèmes, …. Cette révolution numérique s'accompagne également d'une exposition permanente à un risque d'un genre relativement nouveau : le cyber risque. Celui-ci se définit par « *tout ce qui touche à l'atteinte, la violation ou la perte de données, ainsi qu'à des intrusions de réseau ou à la détérioration d'actifs aussi bien matériels qu'immatériels* » (Institut des actuaires, 2017 : 4).
Toujours selon cette même source (Institut des actuaires, 2017), le risque cyber se distingue par 5 caractéristiques :

- Le caractère invisible, ainsi qu'un temps de latence entre l'inoculation du virus et sa détection[2]
- La distance géographique entre le lieu d'attaque et le lieu du sinistre
- Le caractère contagieux d'une attaque
- La dimension technologique
- La difficulté à évaluer les coûts des dégâts matériels et immatériels (Institut des actuaires, 2017)

Il est à parier que la multi-connectivité de nos appareils courants et professionnels ira de pair avec l'exposition aux risques, et les pertes potentielles liées à des accidents ou attaques informatiques seront inestimables. D'après l'Apref (Association des professionnels de la réassurance en France), le risque cybernétique peut même, dans certains cas, se transformer en risque systémique, en raison de son caractère multiplicatif (APREF, 2016)[3], étant donné le développement de la multi connectivité dans le monde et des outils intelligents, communicant de manière automatique. Particulièrement critique, dans ce cadre, seront les opérateurs d'importance vitale (OIV) qui seraient déjà victimes de plusieurs millions d'attaques chaque jour (APREF, 2016).

[2] En effet, il faut en moyenne trois mois aux entreprises avant de détecter qu'une brèche dans la sécurité a été commise (ICC et al., 2016)
[3] Nous pouvons penser par exemple au logiciel malveillant Wannacry (le logiciel Wannacry a infecté de nombreuses machines à travers le monde en 2017, exposant le caractère pandémique des virus)

Toute organisation se doit de faire face aux risques. En effet, « *ce risque appelle un besoin fondamental de protection pour les acteurs de la vie sociale et économique, dont le fonctionnement, les moyens financiers, la réputation, voire la survie même pour les entreprises ou, pour les individus, en cas de dysfonctionnement entrainant des dommages corporels, peuvent être menacés* » (APREF, 2016 : 4). La force d'une entreprise n'est pas seulement l'adaptation de sa production à l'évolution du marché, mais réside également dans l'adaptation au nouveau et futur contexte de l'échange de données, impactant les *outils* de production. Il est temps que les entreprises prennent la mesure du danger qui pèse sur le déroulement de leur activité.

2.1 Délimitation de ce mémoire et question de recherche

La thématique de la gestion des risques cyber, ou plus généralement de la cyber sécurité s'articule autour de trois domaines fondamentaux : l'informatique, la gestion assurantielle (le métier d'actuaire), et le management. L'informatique se concentre sur la défense des systèmes d'informations, la modélisation mathématique entre en jeu dans le cadre du calcul des coûts et de l'optimum concernant la couverture assurantielle, et enfin le management s'occupe de la gestion et des solutions à mettre en place d'un point de vue managérial, afin de coordonner les différents acteurs et d'optimiser la planification de la gestion du risque. Ce mémoire se concentrera sur l'aspect managérial de la gestion des risques, en s'articulant autour de plusieurs domaines : la prévention, la culture d'entreprise, la gestion des risques, la veille technologique et réglementaire, la gestion des crises. Ce mémoire abordera essentiellement des outils qualitatifs, exposant les *bonnes pratiques et les outils* à mettre en place dans le contexte de la cybersécurité.

Ce mémoire vise à contribuer à la gestion du risque cyber faite par les entreprises. En effet, le « Baromètre 2018 de maturité numérique des entreprises wallonnes » pointe le manque « *d'éducation cyber* » de la part d'employés (10% [Digital Wallonia, 2018 : 25]), et ce indépendamment de la taille de l'entreprise. Ainsi, de nombreux accidents cyber sont commis par des employés, et / ou facilités par des employés : mauvaise gestion du mot de passe, ouverture de liens provenant de destinataires inconnus, transmission de données sensibles … Ce mémoire s'inscrit également dans la dynamique actuelle de la digitalisation et plus

particulièrement à la sensibilisation des acteurs à la cyber sécurité comme facteur de réduction des risques. En effet, d'après un graphique [Voir Annexe Figure A] les entreprises sont peu ou pas (« *Somewhat aware* » « *Not aware* » [Ponemon Institute LLC, 2017 : 10]) conscientes des impacts d'une brèche informatique. Peu d'entreprises sont conscientes du changement à venir et ne prendront donc pas les mesures adaptées, en termes de formation du personnel, gestion des crises, etc. Ce mémoire porte sur la gestion des risques au sens large, qu'ils soient du fait d'une attaque ou d'une erreur humaine.

Par conséquent, la contribution de ce mémoire est triple :

- Sensibiliser aux enjeux cyber et conscientiser à l'évolution du paysage numérique
- Proposer des outils afin de gérer les risques
- Offrir un recueil de la littérature principale sur le sujet

2.2 Problématique

A ce besoin de protection des entreprises face aux menaces présentes et futures d'ordre cyber répond donc une préparation en amont face aux incidents. Je réponds, dans ce mémoire, à la question suivante : *Quels sont les outils de sensibilisation à la cyber sécurité à destination des managers et des utilisateurs du système d'information qui peuvent être mis en place pour réduire les risques avérés ou supposés auxquels l'entreprise est soumise ?*

2.3 Plan du mémoire

La gestion des risques cyber forme un tout qu'une entreprise sensibilisée aux enjeux cyber se doit de mettre en place. Cependant, au sein de ce mémoire, j'aborderai les différentes mesures (prévention et culture d'entreprise, gestion des crises, etc) de manière scindée afin d'analyser et de décortiquer un par un les outils que l'entreprise a à sa disposition afin de faire face aux menaces. Il est donc normal qu'il y ait des liens, des interactions entre les mesures, voire même des chevauchements d'idées.

Tout d'abord, une brève historique des attaques sera présentée afin d'exposer l'ampleur de la menace cyber grandissante. Il est fort probable que cela soit un sujet qui gagne de plus en plus en attention dans l'actualité à venir, au fur et à mesure que notre quotidien se digitalisera.

Ensuite, je passerai en revue l'état des lieux des risques informatiques et les pertes encourues, afin de quantifier les pertes subies. Il s'avère que le risque informatique ne relève pas du seul fait des pirates informatiques, mais qu'une part relativement substantielle (35 % [ICC et al. 2016 : 12]) serait dûe à une erreur humaine, mettant au jour la nécessité d'une meilleure gestion humaine du risque. Ces pertes ne sont pas seulement financières, mais s'expriment également en termes de vol de données, affectant la réputation de l'entreprise.

Ensuite, j'aborderai les éléments centraux de mon mémoire. Je vais axer la gestion des risques au sein de l'entreprise sur plusieurs piliers différents. Tout d'abord, il semble que la prévention et la culture d'entreprise ont un rôle majeur à jouer dans la réduction des risques (ICC et al., 2016), mettant au jour les *bonnes pratiques* à adopter au sein des entreprises. Le management des risques, la gestion des crises, et la veille technologique ont également leur part à jouer (OCDE, 2015 : Cyber Security Coalition, 2015). En effet, gérer les risques et faire face aux crises (i.e. après l'impact d'une attaque) sont des domaines qui devraient également être « codifiés » afin de se préparer au mieux à l'adversité.

3 Ampleur de la menace cyber

3.1 Historique des attaques et évolution du contexte

Une cyberattaque est définie comme étant « *[…] une atteinte à des systèmes informatiques réalisée dans un but malveillant. Elle cible différents dispositifs informatiques : des ordinateurs ou des serveurs, isolés ou en réseaux, reliés ou non à Internet, des équipements périphériques tels que les imprimantes, ou encore des appareils communicants comme les téléphones mobiles, les smartphones ou les tablettes* » (Clusif, 2017 : 52). Les dégâts occasionnés au système informatique ne sont cependant pas le fait exclusif d'un acte malveillant, puisque des erreurs, de la négligence, peuvent aussi porter atteinte à la sécurité de l'entreprise. Une autre source (Jean Marc Lehu, 2018) définit la cyberattaque comme étant « *une action individuelle ou collective délibérée, qui vise à porter atteinte à l'intégrité du système d'information informatisé d'une personne, d'une entreprise, d'une organisation ou d'un État, à l'aide de tout ou partie du réseau Internet (ou de tout autre réseau cybernétique) […] Une cyberattaque s'assimile à un acte de piraterie moderne, dont le but est essentiellement le vol et/ou la destruction d'informations, via un accès réseau. Elle constitue un acte criminel ou, dans ses formes extrêmes, une action terroriste […] Dans tous les cas, elle exploite une ou plusieurs vulnérabilités […] de l'ensemble de la sécurité cyber* » (Jean Marc Lehu, 2018 : 42-43).

Concernant les cyberattaques, il y a essentiellement trois catégories de victimes : les particuliers, disposant d'ordinateurs portables, de téléphones, tablettes, … les entreprises, utilisant l'informatique à des fins professionnelles, et les états, victimes et coupables d'attaques cyber.

Ces dernières années ont connu une accélération des attaques qui ont parfois fait la une des journaux. Ainsi, comme le rapporte le journal Le Monde (2019), des exemples récents montrent l'ampleur que prend la menace cyber, lorsqu'elle est exécutée avec succès : « *le logiciel malveillant Blackenergy priva, en 2015, les ménages ukrainiens d'électricité. Un an plus tard, le virus Industroyer, mettait à l'arrêt un transformateur au nord de Kiev. Moins de six mois plus tard, le rançongiciel WannaCry se répandait comme une traînée de poudre et infectait des milliers d'entreprises et d'organisations, le système de santé britannique au premier chef. Rebelote un mois plus tard, lorsque le logiciel NotPetya partait d'Ukraine pour se répandre dans le monde entier, occasionnant, selon les estimations les plus conservatrices, plus d'un milliard de dollars de dégâts. En 2017 apparaissait Triton, un logiciel conçu spécifiquement pour s'attaquer aux mécanismes de sûreté industrielle. L'année suivante, des chercheurs mettaient la main sur OlympicDestroyer, un programme malveillant destiné à perturber le fonctionnement des Jeux olympiques de Pyeongchang. Peu de temps après, à la veille de la Ligue des champions (en Ukraine, encore), les mêmes chercheurs retrouvent la trace de VPNFilter, capable de « couper l'accès à internet à des centaines de milliers de victimes* ». (Le Monde, 2019)

Une autre source (Revue d'économie financière, 2017) parle d'attaque informatique, menée en 2012, ayant permis de voler les plans de l'avion de chasse F-35 américain, ainsi que le système antimissile AEGIS. Parmi les attaques les plus connues se trouve également l'attaque des centrales nucléaires iraniennes par le virus Stuxnet (APREF, 2016).

Ces exemples, en rien exhaustifs, très probablement exécutés par une puissance étatique, mettent au jour la vulnérabilité de notre exposition permanente à la toile numérique. Bien que les exemples précédents montrent essentiellement des attaques d'origine étatique, la plupart des attaques informatiques touchent les entreprises et les particuliers. Ainsi, en 2013, l'un des principaux acteurs de la distribution aux Etats-Unis, Target, se serait fait subtiliser 40 millions de données bancaires, pour un coût de 20 millions d'euros (APREF, 2016). En cause, une faille chez le sous-traitant qui s'occupait de la surveillance de la climatisation dont le dispositif « *n'était pas suffisamment isolé du système informatique principal* (de Target)

(Nicolas Arpagian, 2016 : 38) ». Un très bon reportage est d'ailleurs consacré aux cyberattaques (France 2, 2017), mettant un scène un dirigeant d'une PME française spécialisée dans le petit électroménager qui a été victime d'un logiciel de rançon (ransomware) et dont l'entreprise, déjà en difficulté, a dû fermer ses portes, mettant sur le carreau 8 employés.

De plus en plus d'articles publiés dans la presse sur les risques cyber montrent une prise de conscience de ce phénomène, sujet qui émerge dans la conscience collective. Ainsi est né en 2018 « l'Appel de Paris », sorte de charte énonçant divers principes visant à pacifier le cyberespace, mettant en avant la coordination concernant la sécurité cyber.

Malheureusement, le contexte actuel va certainement aller vers une dégradation de la situation en termes de sécurité. Cette même source (Revue d'économie financière, 2016) pointe le contexte défavorable vers lequel on se dirige, en mettant en avant une dynamique structurelle. En cause, les milliers de failles dans les logiciels les plus courants, les nouveaux objets connectés très peu sécurisés, mais également la pression de la concurrence (les clients ne sachant pas juger la sécurité entre deux produits, une situation d'antisélection[4] apparaitrait), et enfin la relative impunité des attaquants (Revue d'économie financière, 2016). Mais également le « tout connecté » qui va très rapidement apparaitre, le développement rapide de l'e-commerce (Le Monde, 2019), la nouveauté des produits connectés (IoT, internet of Things) dépassant la prudence qui devrait être de mise. A cet égard (Le Monde, 2019), il semble d'ailleurs que la réalité dépasse parfois la fiction, lorsque l'on annonce l'arrivée d'algorithmes dans le secteur de la beauté, scannant votre peau et proposant automatiquement des produits adaptés. Au regard de différents articles de presse, il est visible également que les états utilisent désormais l'outil informatique à des fins hostiles. Enfin, le « Hiscox Cyber Readeness Report 2018 » pointe également le fait que les groupes criminels auront accès à des outils plus sophistiqués et seront plus déterminés (Hiscox Ltd, 2018). La monétisation des données volées serait désormais également rendue plus facile, grâce à l'existence de marchés noirs (black markets) où les données pourraient être échangées via une série de transactions faisant intervenir plusieurs intermédiaires (McAfee, 2018).

[4] « Market for Lemmons »

Si l'on souhaite d'ailleurs mesurer la perception de l'évolution du risque, l'indice de cybersécurité (« index of Cybersecurity[5]» [NYU, 2016]) montre, au-delà des limites méthodologiques habituelles, une perception du risque qui s'accroit dans le temps.

Figure 1. Note : reproduit à partir de « Index of Cybersecurity », New York University. (Avril 2019). Consulté sur http://cybersecurityindex.org/

3.2 Etat des lieux des risques informatiques et indices de cybersécurité

3.2.1 Risques informatiques

De nombreux domaines, sur lesquels l'entreprise est présente, peuvent être sujets à une perturbation. Etant donné que ce domaine relève de l'informatique, et que ce sujet est hors cadre de mes études, je n'exposerai qu'à titre illustratif les principaux risques informatiques de l'entreprise[6]. Ces risques ne sont bien entendu pas exclusifs à l'entreprise, des particuliers, ainsi que des états, peuvent être victimes de ces menaces. L'ENISA, agence européenne, identifie les menaces suivantes (ENISA, 2018 : 27 – 31, 64) :

- Les malwares : les malwares sont des programmes nuisibles qui visent à porter atteinte au système informatique. Le terme « Malware » est un terme générique englobant de nombreux virus tels qu'un « cheval de Troie » et des « Ransomware », ou encore logiciel de rançon. Assez connus ces dernières années, les Ransomware sont petit à petit remplacés par du « Cryptojacking », infectant les ordinateurs de manière furtive afin d'utiliser la puissance de ceux-ci pour créer des monnaies virtuelles. Le

[5] Cet indice est référencé dans des articles académiques. Il est mis à jour chaque mois depuis avril 2011.
[6] Bien que ce mémoire soit délimité à l'étude du management des risques cyber, abordant principalement les outils managériaux, ma problématique ne peut, par définition, faire totalement abstraction de l'exposition des entreprises sur le volet informatique.

Cryptojacking et les Ransomware restent les principales menaces faisant partie de la catégorie des malwares.

- Les « Web based attacks », ou encore les attaques provenant du web : ces attaques visent à utiliser les vulnérabilités des outils utilisés en ligne.
- Phishing : le Phishing, ou encore les tentatives d'hameçonnage est une technique ayant pour but d'usurper l'identité d'une entreprise ou d'un organisme, dans le but de collecter les données fournies par les utilisateurs. Une tentative d'hameçonnage peut se réaliser via un email, afin que la victime donne (par exemple) ses coordonnées bancaires. Le Phishing fait partie de l'ingénierie sociale, c'est-à-dire des tentatives de manipulation afin d'obtenir certaines données.
- DDoS (Distributed Denial of Services) ou encore « attaque par déni de service » : cette attaque est une technique visant à empêcher l'accès à un service informatique, de perturber son fonctionnement normal. C'est une attaque très répandue.
- Data Breaches, ou encore un vol de données : les entreprises sont régulièrement victimes de vol de données (voir point 3.3). De manière rigoureuse, le vol de données n'est pas vraiment une menace mais plutôt une attaque réussie contre une entreprise. Le but de cette attaque est d'ordre pécunier mais également de nuire à la réputation d'une entreprise.
- Insider Threat, ou encore une « menace provenant d'un interne à l'entreprise » : cette menace couvre des actes intentionnels ou non intentionnels (voir point 4.1). Ils sont le fait d'employés agissant par inadvertance ou malintention.

3.2.2 Indices de cybersécurité

A l'heure actuelle se développent aussi de nombreux indices de cybersécurité. Les indices sont actuellement des outils indispensables à l'évaluation de process et se trouvent dans de nombreux domaines en entreprise, notamment dans les process de pilotage de la performance, où ils sont très présents pour mesurer différents paramètres, tels que le taux de satisfaction client, taux de retour sur une campagne promotionnelle, etc. Dans le domaine de la cybersécurité, des indices émergent et servent à qualifier le niveau de cybersécurité, et celui-ci devient même, avec l'accroissement des risques liés au numérique, « *l'une des variables d'appréciation de la valeur des entreprises* » (Daniel Ventre, 2016 : 5). Il n'existe

actuellement malheureusement pas encore d'indices génériques, applicables à toute entreprise, simplement sous forme de ratio (comme en finance par exemple). C'est à l'entreprise de quantifier son exposition aux risques sur une échelle afin de déterminer son niveau de cybersécurité. C'est ce qui rend la gestion cyber complexe et demande la mise en place de véritables procédés de management !

Il y a plusieurs sortes d'indices pour différents destinataires. Il existe des indices qui mesurent le degré de sécurité cyber des états, et d'autres qui mesurent le degré de sécurité des entreprises.
Concernant les entreprises, l'indice « Breach Level Index » réalisé par l'entreprise Gemalto et Safenet (s.d.) permet de quantifier, à partir des données fournies par l'entreprise, son niveau sur une échelle de risques, allant de 1 (minimal) à 10 (catastrophique). Dans le même genre, l'indice proposé par KPMG (2018) permet à l'entreprise de s'autoévaluer dans son avancement en termes de cybersécurité (de « Immature » à « Maitrise », Immature to Leading). De nombreuses autres références sont qualifiées d'« indices », mais sous forme de service extérieur ou de sorte d'applications proposés aux entreprises, à des fins commerciales[7].

3.3 Coût et fréquence des attaques cyber et pertes encourues actuelles

D'après le rapport « Cyber Readiness Report » (Hiscox Ltd, 2018), le coût moyen des attaques était de 229.000 $ parmi les entreprises interrogées se souvenant des coûts[8]. Mais ce chiffre cache en réalité une ventilation plus précise entre les différentes entreprises.

En effet, les petites et les grandes entreprises ne sont pas affectées de la même façon, ces dernières percevant un coût par attaque plus important. Alors que l'Allemagne semble la plus touchée dans les entreprises de taille inférieure à 250 employés, ce sont les Etats-Unis qui remportent la palme des coûts, tout autant concernant l'estimation des coûts de tous les incidents des 12 derniers mois par organisation que des coûts engendrés par l'attaque la plus virulente des 12 derniers mois par organisation. Notons la fourchette les coûts totaux très

[7] Exemple: The CTU Cyber Security Index (CSI), qui détermine le niveau de sécurité à partir des données de l'entreprise proposant ce service, voir https://www.secureworks.com.au/about/counter-threat-unit , ou encore un indice proposé par la société SRC, spécialisée dans la sécurité Cyber, voir https://www.srcinc.com/pdf/Technical-Services-Cybersecurity.pdf .
[8] 4100 entreprises interrogées dans cinq pays : l'Espagne, les Pays-Bas, les Etats-Unis, la Grande-Bretagne.

élevés allant jusqu'à 25 millions de dollars aux Etats-Unis. Au niveau mondial, le coût des attaques cyber serait de 450 milliards de dollars[9]. Une autre source (McAfee, 2018) évalue ce montant à 600 milliards de dollars, plaçant la cyber criminalité en troisième place, après la corruption et le trafic de stupéfiants. Les estimations restent cependant délicates, étant donné la difficulté à avoir des données précises, dû à l'incomplétude des données, la peur d'un dégât réputationnel, etc (McAfee, 2018).

Cost of all cyber security incidents
Average estimated cost of all of an organisation's incidents in the past 12 months

	249 or fewer employees	250 or more employees	1,000 or more employees	Overall range
Germany	$55,067	$406,653	$640,408	$500 – $20m
Netherlands	$32,760	$280,784	$531,158	$1,000 – $10m
Spain	$22,175	$259,230	$355,761	$500 – $5m
UK	$33,787	$462,633	$554,596	$1,000 – $20m
US	$34,604	$578,762	$1,047,465	$350 – $25m

Cost of largest cyber security incident
Average estimated cost of an organisation's largest incident in the past 12 months

	249 or fewer employees	250 or more employees	1,000 or more employees	Overall range
Germany	$11,918	$86,834	$150,891	$10 – $5m
Netherlands	$4,489	$66,767	$127,417	$10 – $2.5m
Spain	$3,789	$31,359	$41,733	$20 – $800,000
UK	$4,063	$56,870	$65,668	$10 – $1.2m
US	$4,883	$60,258	$106,583	$20 – $2m

Figure 2. Note : reproduit à partir de « 2018 Hiscox Cyber Readiness Report », Hiscox Ltd. (2018). Consulté sur https://www.hiscox.com/sites/default/files/content/2018-Hiscox-Cyber-Readiness-Report.pdf

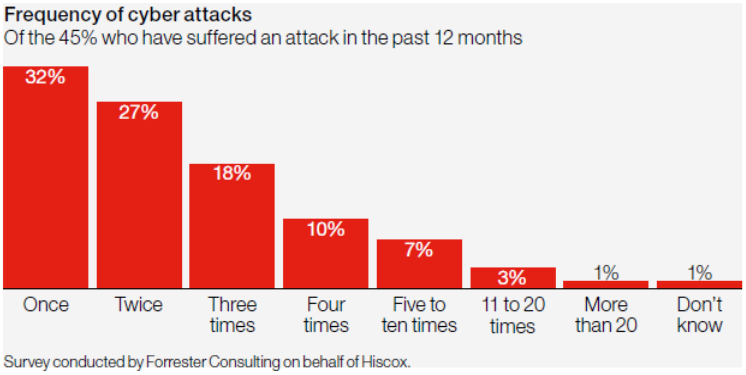


Figure 3. Note : reproduit à partir de « 2018 Hiscox Cyber Readiness Report », Hiscox Ltd. (2018). Consulté sur https://www.hiscox.com/sites/default/files/content/2018-Hiscox-Cyber-Readiness-Report.pdf

Au niveau de la fréquence des attaques, celle-ci semble relativement élevée, puisque 32 % des entreprises interrogées[10] déclarent avoir été victime d'une attaque cyber lors des 12 derniers mois.

Notons également qu'il y a 66 % d'entreprises (parmi celles qui se déclarent avoir été attaquées) déclarant avoir été attaquées plus d'une fois durant les 12 derniers mois. Encore ici, au niveau de la ventilation des attaques par pays, certains pays semblent plus vulnérables que d'autres (Hiscox Ltd, 2018). En effet, l'Espagne, les Pays-Bas et l'Allemagne semblent les plus touchés [Voir Figure B Annexe], devant la Grande-Bretagne et les Etats-Unis, malgré que ces

[9] D'après le CEO des « Hiscox assurances ».
[10] Parmi les 45 % des entreprises se déclarant avoir été attaquées, sur un total de 4100 entreprises interrogées dans cinq pays, selon le 2018 Hiscox Cyber Readiness Report (Hiscox Ltd, 2018).

derniers perçoivent le coût par attaque le plus élevé au sein des grandes entreprises (voir supra).

Enfin, les pertes de données à la suite d'un vol, consécutif à une attaque, ne sont pas à négliger. En effet, la réputation d'une entreprise peut être grandement affectée par le vol des données. Un intéressant article académique est d'ailleurs consacré à l'analyse de l'attaque de Sony Pictures en 2014, faisant la une des journaux dans le monde entier. A l'origine de l'attaque, le lancement du film « The Interview » par Sony Pictures, mettant en scène la mort du dirigeant Nord-coréen, qui entraina l'attaque d'un groupe de hackers GOP, appelés « Guardian of Peace ». Cette attaque occasionna la divulgation de 306 287 documents internes, diffusé sur Wikileaks (Jean Marc Lehu, 2018). Toujours selon la même source, le vol de données introduit une variable temps différente, autre que lorsqu'un évènement se produit et appartient au passé, en laissant les pirates divulguer l'information quand bon leur semble, « *prenant en otage l'entreprise pour une durée indéterminable, même si le temps passant, la valeur de la plupart des informations s'altère* » (Jean Marc Lehu, 2018 ; 45). Le tableau suivant propose une liste des entreprises à avoir fait l'objet d'un vol de données :

5.1.3. Hitparade des violations de données 2014-2015

ENTREPRISES	DONNÉES DÉROBÉES	TYPE DE DONNÉES
PREMERA BLUE CROSS Date d'annonce : 18 mars 2015	11 M	Numéro de compte bancaire Numéro de sécurité sociale
ANTHEM Date d'annonce : 05 février 2015	80 M	Numéro de sécurité sociale Adresses email Adresses physique
SONY Date d'annonce : 25 novembre 2014	47 000	Information de l'entreprise Données d'employés
HOME DEPOT Date d'annonce : 02 septembre 2014	109 M	Numéro de carte de crédits Adresse email
JP MORGAN Date d'annonce : 27 aout 2015	83 M	Adresses email Adresses physique
Ebay Date d'annonce : 21mai 2014	145 M	Adresses email Adresses physique Identification de connexion
TARGET Date d'annonce : 13 décembre 2013	110 M	Numéro de carte de crédits
ADOBE	2014	150 M

Figure 4. Note : reproduit à partir de « Etude sur les « cyber risques » et leur (ré)assurabilité », Apref. (2016). Consulté sur https://www.apref.org/sites/default/files/espacedocumentaire/note_apref_cyber_risque.pdf

Ces vols de données concernent des entreprises de grande taille, pourtant réputée pour leur sécurité, ce qui laisse présager une vulnérabilité encore plus importante des entreprises de

petites et moyennes tailles. Concernant Sony Pictures, le vol de données a eu de nombreuses répercussions, tels que la « mise en place d'urgence d'une messagerie électronique parallèle temporaire, et de demander à l'ensemble des employés un nouveau mode de travail « *non-numérique […] Le système de comptabilité n'étant plus opérationnel, le paiement des fournisseurs, des prestataires et des employés dut être réinventé avec des supports physiques oubliés* » (Jean Marc Lehu, 2018 ; 47).

Le graphique suivant montre le temps de réaction moyen des entreprises interrogées (Hiscox Ltd, 2018), et est ventilé selon le temps de « Découverte, Investigation, Eradication de la menace, Recouvrement, et Résolution ». Le temps de réaction après un incident, ne semble, à première vue, pas être excessivement catastrophique, mais cache que ces perturbations se traduisent souvent en centaines de milliers d'euros (229.000 $, cf supra).

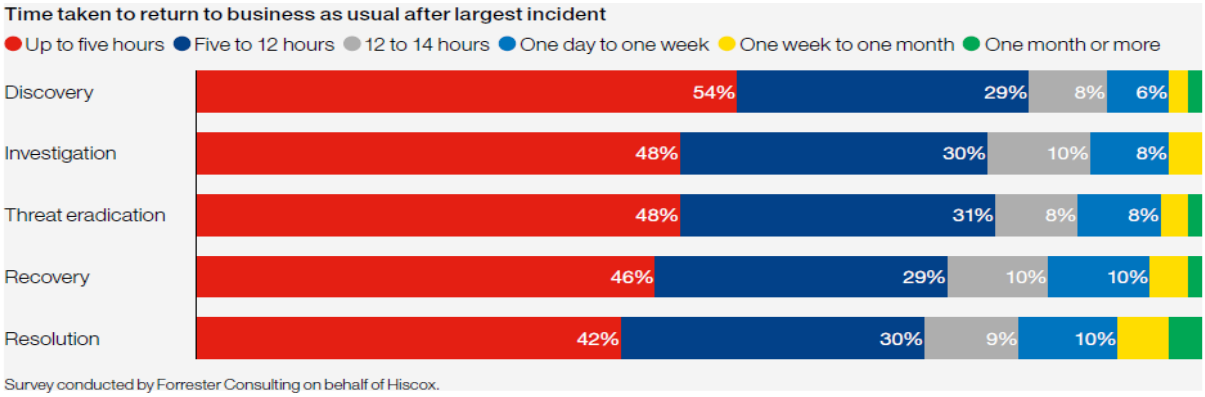


Figure 5. Note : reproduit à partir de « 2018 Hiscox Cyber Readiness Report », Hiscox Ltd. (2018). Consulté sur https://www.hiscox.com/sites/default/files/content/2018-Hiscox-Cyber-Readiness-Report.pdf

Cependant, une autre source (Jean Marc Lehu, 2018) pointe des temps de réaction différents, allant de 23 jours le temps moyen nécessaire pour un ransomware (logiciel de rançon) à 50 jours pour une Cyberattaque par logiciel malveillant, nécessitant la mise en place de modélisation de la part des entreprises (Ponemon et Accenture, 2017 : Cité par Jean Marc Lehu, 2018). Le Guide Belge de la Cybersécurité, lui, avance que « *les entreprises ne réalisent souvent pas qu'un incident de sécurité est en train de se produire. Il arrive que des systèmes restent infectés et pillés pendant des mois, ou même des années, avant que l'intrusion ne soit détectée…quand elle est effectivement détectée* » (ICC et al., 2016 ; 33).

En conclusion, les chapitres précédents montrent l'impérative nécessité de protéger au mieux l'entreprise pour faire face à l'adversité. Des coûts importants, une paralysie, la réputation, une crise interne et externe sont les conséquences possibles d'une intention malveillante, ou même une fermeture définitive, comme dans le reportage consacré à la PME piratée par un

logiciel de rançon, lorsque le chef d'entreprise refusa de payer pour récupérer ses données encryptées par un pirate (France 2, 2017). Une gestion efficace du risque cyber peut donc faire économiser des capitaux importants dont l'entreprise a besoin pour continuer à se développer et mener à bien sa stratégie. Je propose, dans les chapitres suivants, une gestion en amont et en aval du risque au sein des entreprises, ou, dit autrement, une gestion a *priori* et a *posteriori* du risque, en mettant en avant la prévention et la culture d'entreprise afin d'exposer les *bonnes pratiques* à acquérir « ante-incident » ainsi que la gestion des crises pour faire face à la situation « post-incident ».

4 Management des risques cyber

4.1 Volet prévention et culture d'entreprise

4.1.1 Introduction

Dans de nombreux domaines, la prévention reste le moyen le plus économe afin d'éviter la plupart des problèmes de survenir. La gestion des risques cyber n'est pas exempte de cette sagesse[11]. Il est logique qu'éviter toute attaque ne sera pas faisable, mais s'y préparer reste le meilleur moyen d'y faire face. Cette même source (Hiscox Ltd, 2017) pointe le fait que les dégâts occasionnés par une attaque informatique vont en général bien au-delà du simple aspect financier, impactant la réputation, la relation client sur le long terme. Ne sont pas pris en compte également les coûts d'opportunité qui surviennent, obligeant une entreprise à mettre en place des procédures de recouvrement des données, plutôt que de pouvoir continuer son travail normalement.

Sur le graphique suivant (Hiscox Ltd, 2018), nous pouvons apercevoir que la majorité des entreprises se classent comme « Novices », après évaluation, en termes de « technologie et procédures » ainsi que la « surveillance et les ressources ». Même si la méthodologie utilisée ne laisse pas clairement entrevoir quelles questions ont été posées et que les exemples présents montrent davantage une concentration sur l'aspect technique de la sécurité[12], il est raisonnable de penser que l'aspect humain de la

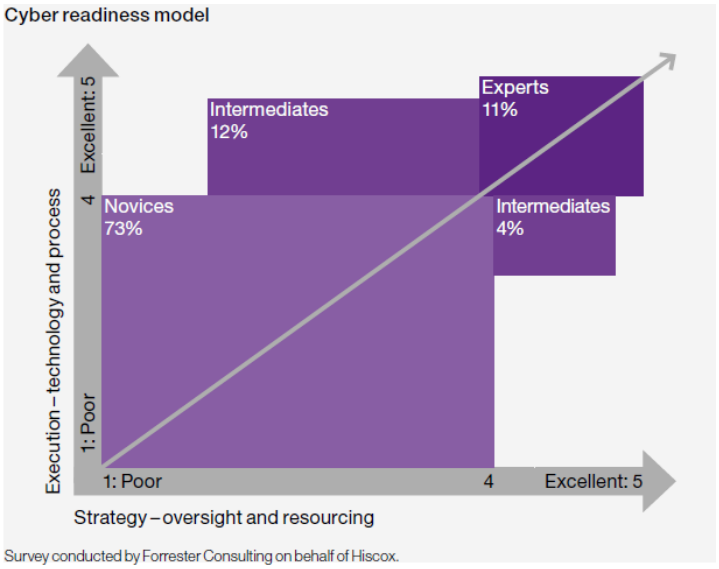


Figure 6 Note : reproduit à partir de « 2018 Hiscox Cyber Readiness Report », Hiscox Ltd. (2018). Consulté sur https://www.hiscox.com/sites/default/files/content/2018-Hiscox-Cyber-Readiness-Report.pdf

[11] "It is an old saying, but a true one: prevention is better than cure. In the age of e-commerce and the connected business, it has a particular ring to it. Robust defences against cyber intruders and strong processes for eliminating careless or rogue behaviour internally are now the keys to business continuity and consumer trust. Without investment in prevention, detection and training, firms leave themselves exposed to costly business interruptions and possible brand impairment." (Hiscox Ltd, 2017: 1)

[12] "Cyber readiness model methodology: Respondents were shown a series of statements relating to cyber security strategy and execution. Each statement represents best practice in its area. The strategy statements were broken down into two sections – oversight and resourcing. Two examples: 'Cyber security has a formal

gestion des risques soit encore plus négligé, étant donné que l'aspect technique de la gestion arrive très régulièrement en première position, une erreur selon le Guide Belge de la Cybersécurité[13].

Le graphique (Figure 6) montre également une surestimation de la capacité des entreprises à évaluer leur gestion en matière de sécurité, puisque 57 % ont déclaré être « assez confiantes » en la matière (Hiscox Ltd,2018). Après évaluation, il s'avère que 73 % des entreprises sont classées comme « Novices » en matière de sécurité, 16 % comme étant « Intermédiaires » et seulement 11 % « Experts », cette dernière catégorie devant avoir un score supérieur à 4 concernant la surveillance (oversight and resourcing) ainsi que la technologie (technology and process).

Par conséquent, il semble important que les entreprises mettent en place une véritable culture d'entreprise en impliquant l'ensemble du personnel concernant la sécurité, culture identique à celle désormais exigée concernant les programmes appelés *Secure by design,* dont la sécurité est le socle sur lequel ils ont été construits depuis le début. La culture d'entreprise, définie comme l'ensemble des « *valeurs partagées dans l'entreprise* » (FONCSI, 2015 ; 3) est entendue comme un état d'esprit partagé par les membres de celle-ci, dans le domaine de la sécurité mais pas seulement, état d'esprit positif pour la sécurité accompagnant chaque activité de l'entreprise. Il s'agit donc de modifier les attitudes, afin d'arriver vers des « *comportements désirés, (fruits du) suivi des procédures et (de) l'observance des bonnes pratiques* »(FONCSI, 2015 ; 1). L'ENISA (European Union Agency For Network and Information Security) rejoint cette définition et énonce quant à elle la culture (de cybersécurité) comme étant « *la connaissance, les croyances, les perceptions, les attitudes, les normes et valeurs des personnes concernant la cybersécurité et la façon dont elles se comportent vis-à-vis des technologies de l'information* » (ENISA, 2017 ; 5). Le point central de ces définitions semble être donc le comportement humain.

budgeting process which is integrated into all security projects and activities' and 'Cyber security competencies are regularly reviewed using established metrics according to roles and responsibilities'. The execution statements were similarly split between processes and technology."(Hiscox Ltd, 2018 : 16)

[13] « La cybersécurité doit être perçue comme l'affaire de toute l'entreprise, et pas seulement de l'informatique. La mise en oeuvre de mesures de sécurité ne doit pas être limitée au département IT : elle doit être répercutée dans toute l'organisation, et se refléter dans chacune de ses actions. Le périmètre de la cyber-sécurité doit donc couvrir les personnes, les produits, les installations, les processus, les politiques de l'entreprise, les procédures, les systèmes, les technologies, les réseaux et l'information. » (ICC et al., 2016 : 12).

En effet, la pyramide de Bird, outil proposé en 1969, appelée également « pyramide des risques », énonce le principe que la probabilité d'un accident majeur (« attaque réussie ») survienne augmente avec l'accroissement de la fréquence des comportements à risques. L'entreprise peut donc en s'attaquant à la base (« comportements à risques », par exemple ouvrir une pièce jointe d'un email provenant d'un destinataire inconnu) diminuer la probabilité de l'occurrence d'un accident majeur de sécurité (un logiciel de rançon bloquant l'ensemble de ses terminaux par exemple, « attaque réussie »).

Figure 7. Note : Adapté de « Heinrich et Bird, la malédiction des pyramides, un problème de géométrie ? », Mortureux, Y. (2013). Consulté sur https://www.foncsi.org/fr/blog/nouvelle-tribune-interpretation-pyramide/image/image_view_fullscreen

Selon le Guide Belge de la Cybersécurité, « *il règne encore beaucoup d'incertitude quant à "ce qu'il faut faire" et "comment le faire", quand il s'agit de gérer les risques émanant des cyber-menaces. En règle générale, davantage d'initiatives sont prises dans des entreprises internationales de taille plus importante, alors que les entreprises moyennes ou familiales sont tout autant exposées à ces menaces. Et même dans les plus grandes entreprises, les initiatives en matière de sécurité de l'information ne font souvent pas l'objet d'un engagement fort de la part du plus haut niveau de l'entreprise. Nous sommes cependant convaincus que la sécurité de l'information devrait être à l'ordre du jour dans toutes les organisations - indépendamment de leur taille, de la complexité ou de la nature de leurs activités – et s'adresser à chaque individu qui les compose* » (ICC et al., 2016 : 6).

Cette dernière source montre également qu'il serait une erreur d'envisager la sécurité informatique seulement d'un point de vue technologique, mais qu'une véritable culture d'entreprise devrait être mise en place. En effet, d'après « l'Enquête Mondiale sur la Sécurité de l'Information 2012 », « *35% des incidents sont dus à une erreur humaine, plutôt qu'à une attaque délibérée. Et si l'on s'intéresse aux 65% restants, plus de la moitié de ces attaques délibérées auraient échoué si les individus impliqués avaient traité l'information de manière plus sécurisée* » (CPVP, 2012 : cité par ICC et al., 2016 : 12). Une autre source[14](IBM, 2016) parle même de 60 % « d'insiders » comme vecteurs des attaques, que cela soit par inadvertance ou par malveillance (2015) !

[14] Je pense, pour ma part, ces chiffres surévalués. Les limites méthodologiques habituelles ainsi que de possibles effets de composition de l'année 2015 sont à garder à l'esprit.

D'après le « Guide Belge de la Cybersécurité » (ICC et al., 2016), trois bénéfices importants sont à attendre d'une vision allant au-delà du simple aspect technologique : tout d'abord, (1°) une meilleure prise de décision, stratégiquement, grâce à la connaissance de l'exposition aux risques, ensuite (2°) financièrement, grâce à une réduction des pertes, et enfin (3°) opérationnellement, grâce à l'existence de plans adéquats pour l'entreprise[15]. Cette culture d'entreprise devrait inclure la cybersécurité comme une partie faisant partie d'un tout, interagissant et étant « *alignée sur les objectifs stratégiques, les politiques de l'organisation, la gestion du risque, les exigences de conformité et la mesure des performances* » (ICC et al., 2016 : 12).

Il s'agit donc d'un changement de paradigme à opérer, entre la situation actuelle, qui considère la sécurité comme un domaine à part (voire comme un département, au même titre que les départements marketing, finance, etc), et une situation où la sécurité accompagne véritablement chaque action et se trouve au centre des processus, afin de calquer le *Secure by Design* sur le fonctionnement même de l'entreprise.

4.1.2 Les pratiques à adopter

Tout d'abord, l'élément charnière d'un changement des mentalités, mais également et surtout d'un changement des pratiques et habitudes concernant l'utilisation des outils informatiques de l'entreprise est la formation. En effet, celle-ci vise à sensibiliser et faire adopter le *Security Awareness* à au sein de l'entreprise. Le « Security Awareness », concept récent[16], se définit comme « *[la] conscientis(ation) sur l'importance de la sécurité afin de sensibiliser (les parties prenantes) aux divers risques, de leur permettre d'adopter une attitude préventive et (de) réagir de manière adéquate* » (Securitas, s.d.).

Avant d'aborder la formation, je pense primordial de viser un engagement de tous concernant la sécurité[17]. Le respect des mesures de sécurités de la part des employés (« compliance », en anglais) est une condition *sine qua non* d'un système de sécurité résilient. Pour ce faire, une

[15] Ces plans, tels que le Plan de Continuité de l'activité (PCA) seront abordés dans la partie « gestion de crise » et font partie du deuxième volet d'intervention mis en place par l'entreprise.
[16] Il a été difficile de trouver une définition académique du concept, étant donné que les articles intéressants sur le sujet sont payants (malgré l'abonnement de l'université à ces mêmes bases de données). Je choisis donc la définition proposée par une entreprise dans le secteur.
[17] La transposition de l'aspect pratique de cet engagement dans la réalité, pouvant faire intervenir des questions de l'ordre de la théorie des jeux (chaque employé ayant un intérêt propre, et n'allant pas dans la même direction que les autres acteurs, etc) n'est pas abordé dans ce mémoire.

charte, c'est-à-dire une politique de la sécurité cyber propre à l'entreprise peut être rédigée et signée de tous. Celle-ci peut être utile à de nombreux niveaux.
En effet, d'après le « Guide Belge de la Cybersécurité » une charte a pour but de :

- « … s'assurer que la vision de l'entreprise en matière de sécurité est traduite dans la pratique ».
- « rendre visible les engagements en matière de sécurité [et] faire croitre la sensibilisation à la sécurité ».
- « offrir un cadre de référence en matière de politique de sécurité » (ICC et al., 2016 : 14).

Cette charte sert par conséquent de point de départ concernant l'engagement, mais également et surtout la responsabilisation de tous en matière de politique de sécurité. Celle-ci peut être étendue aux partenaires ayant des liens étroits avec l'entreprise (fournisseurs de longue date, etc), puisque le comportement de ceux-ci peut également avoir un impact en terme de sécurité, de la même façon que les internes de l'entreprise (utilisation d'appareils privés non sécurisés, ouverture de lien suspect, etc).

Le cœur du sujet, c'est-à-dire la formation, doit être délivrée de manière continue, en parallèle avec le développement du paysage des risques cyber, qui est, par définition, toujours mouvant. Elle doit être mise à jour régulièrement et est adaptable en fonction du domaine propre à l'entreprise. Elle a pour but d'augmenter la sécurité et d'éviter la mise en place de comportements non souhaitables de la part d'employés et de faire de ceux-ci « *(le) plus grand atout sécuritaire (de l'entreprise)* » (ICC et al., 2016 : 16). Celle-ci devrait enseigner les domaines suivants, en répondant aux questions (non exhaustives) : « *Comment communiquer en toute sécurité et de manière responsable ? Comment utiliser les médias sociaux de manière judicieuse ? Comment transférer les fichiers numériques de manière sécurisée ? Comment utiliser son mot de passe de façon appropriée ? Comment éviter la perte d'informations importantes ? Qui avertir lorsque vous constatez un incident de sécurité potentiel ? Comment ne pas se faire piéger et divulguer des informations à des tiers malveillants* ? etc » (ICC et al., 2016 : 24).

Ces questions, d'apparence évidentes, sont pourtant pleinement d'actualité et touchent les entreprises avec une probabilité moyenne à relativement élevée. Considérons par exemple les « Ransomware » ou encore « logiciel de rançon », évalué à « likely » (probable), deuxième degré de probabilité le plus élevé et à l'impact fort, (voir « Radar des risques », page 34). Ou

encore l'ingénierie sociale (phishing, c'est-à-dire une tentative d'usurpation d'identité via un courriel), évalué à « très probable » et à l'impact moyen. Ces risques ne sont pas à négliger ou à balayer d'un revers de main, au risque d'en être victime.

Ci-dessous, un tableau[18], non exhaustif, du cadre de la formation à inculquer aux membres du personnel :

Menace ou domaine	Caractéristiques	Formation
Ransomware	Virus verrouillant l'ordinateur	✓ Reconnaitre les emails frauduleux ✓ Ne pas cliquer sur les emails douteux ✓ Effectuer des sauvegardes régulièrement
Phishing (hameçonnage)	Usurpation d'identité afin d'obtenir des données sensibles à l'entreprise	✓ Reconnaitre les adresses correctes, être attentif aux petites modifications ✓ Reconnaitre les situations douteuses
Utilisation d'appareils particuliers (Bring Your Own Device, BYOD)	Apport d'appareils privés au sein de l'entreprise, augmente l'exposition aux risques	✓ Politique claire concernant ce qui est autorisé ou pas ✓ Mots de passe robustes ✓ Appareils mis à jour
Données sensibles	Les données sensibles sont des données internes à l'entreprise, parfois vitales pour son bon fonctionnement	✓ Être capable de distinguer les données sensibles des données non sensibles

[18] Les références, telles que "Safe on web » (site internet officiel : https://www.safeonweb.be/) ou encore « CERT » (site internet officiel : https://www.cert.be/fr) ont été utilisées afin de réaliser ce tableau, ainsi que le Guide Belge de la cybersécurité (ICC et al., 2016).

Accès privilégié	Un accès privilégié permet d'avoir accès, de modifier le document (ajout de parties, suppression, etc).	✓ Personnes ayant accès à des données privilégiées doivent être mises au fait que ces accès ne peuvent être partagés ✓ Règles, bonnes pratiques et mesures de protections des accès privilégiés[19]
Incident cyber	Utilisation d'un plan d'incident (Incident contact list)	✓ Apprendre qui avertir en premier ✓ Mettre les premières mesures en place ✓ Savoir quelle(s) information(s) transmettre
Utilisation des réseaux sociaux		✓ Veiller à une utilisation sure des réseaux sociaux, sans divulgation de données sensibles
Mots de passe	Un mot de passe veille à l'accès réglementé à un domaine	✓ Directives concernant l'utilisation de mots de passe sûrs, personnels, et changés régulièrement.
Simulation de crise	Attaque informatique réussie	✓ Où trouver les plans de continuité ?[20]

[19] Commentaire de Monsieur Gelissen Frédéric
[20] Commentaire de Monsieur Gelissen Frédéric

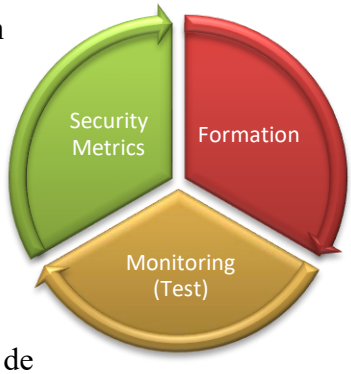
		✓ Respecter les priorités[21] ✓ Actions à faire ou ne pas faire ✓ Utilisation correcte de la liste de contact ✓ Respect des plans de communication

Plusieurs domaines sont à détailler concernant ce tableau. En effet, les membres de l'entreprise doivent être mis au fait des actes malveillants (ingénierie sociale), savoir reconnaitre les variations mineures dans les adresses mail ou les sites web, afin de ne pas cliquer sur un lien malveillant, et infecter l'entreprise. Des comportements sains également en matière de sécurité doivent être adoptés concernant la sécurité des appareils privés, apportés sur le lieu de travail, afin qu'ils ne soient pas un vecteur, une porte d'entrée aux attaques et à la déstabilisation des systèmes de l'entreprise.

Une attention particulière doit être portée également concernant les accès privilégiés. Des données sensibles pourraient être mises dans les mauvaises mains si une politique ainsi que des indications claires à ce sujet n'ont pas été prodiguées. En effet, fait étonnant, l'actualité semble s'écrire au même moment que la rédaction de ce mémoire. Ainsi, comme le rapporte le journal le Monde (2019), Facebook, pourtant très grande entreprise mondialement connue, semble avoir conservé des millions de mots de passe de manière non sûre, de sorte que n'importe quel employé ayant accès au système interne de l'entreprise pouvait avoir accès aux mots de passe de millions de clients (gestion des accès privilégiés) ! Même si ce fait expose plutôt une erreur informatique, ces faits sont tout de même interpellants. Un plan de contact en cas d'incident (similaire au « incident contact list » (SANS, s.d.), [Voir Figure C Annexe]) sous forme de formulaire de contact doit être prodigué, avec comme adresse les responsables sécurité ainsi que les coordonnées (si l'entreprise a choisi de recourir à une aide extérieure) d'entreprises fournisseurs de sécurité informatique (aide au recouvrement de données, délimitation de l'impact, etc).

[21] Commentaire de Monsieur Gelissen Frédéric

Le volet de la formation peut être complété par une phase d'évaluation (test) de l'apprentissage des bonnes procédures. Cette phase peut faire partie d'un processus de *monitoring*, défini comme l' « *ensemble de techniques permettant d'analyser, de contrôler, de surveiller* » (CNRTL, s.d.) le bon apprentissage des acquis. Ainsi, des simulations d'attaques inopinées (sans avertissement du personnel) pourrait être lancées afin d'observer le comportement des membres du personnel et vérifier, par exemple le respect de l'utilisation de la liste de contact en cas d'incident, ainsi que les premières mesures effectuées par le personnel. Dans le même état d'esprit, des faux mails, simulant des tentatives de phishing peuvent être envoyés afin de voir si des erreurs sont commises par les employés. Le but de ces tests n'est pas de punir, mais de conscientiser les employés aux bonnes pratiques à adopter en matière de sécurité de l'entreprise au quotidien, et utiliser les résultats de ces « tests discrets » comme contenu pour les prochaines sessions de formation. Le « Centre de la Cybersécurité Belge (Centre for Cyber Security Belgium)[22] » appelle également à une revue périodique de l'état de la sécurité via un audit, un contrôle, ou un questionnaire d'évaluation (Centre for Cyber Security Belgium, 2019). Dans ce cadre, il semble utile de mettre en place des outils quantitatifs (Security Awareness Metrics) afin de pouvoir évaluer le degré d'évolution des employés [Voir Figure D Annexe pour des exemples].



Afin de piloter les mesures engagées par la formation, un outil managérial, le « Gap Analysis », ou encore l'analyse des écarts, se charge de piloter le décalage entre la situation actuelle (mesures organisationnelles, opérationnelles et techniques déjà en place [Centre for Cyber Security Belgium, s.d.]) et la situation future (mesures supplémentaires) et veille à l'implémentation des mesures. Il peut se représenter sous forme de tableau (le contenu est à titre d'exemple) :

[22] Organisme officiel.

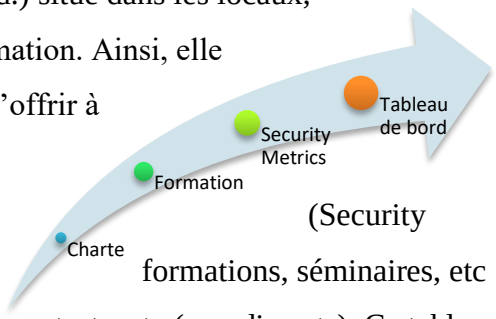
Mesures déjà en place : Où en sommes-nous ?	Mesures supplémentaires : Où voulons-nous aller ?	Leviers actionnables	Monitoring (contrôle)
Affiche d'éléments de base concernant la sécurité : ne pas cliquer sur des liens suspects. Actuellement, plus ou moins 35% erreurs concernant l'ingénierie sociale[23]	Arriver à des erreurs au test Phishing inférieures à 5 %	Formation concernant le Phishing	Phishing test
Simples conseils concernant les mots de passe	Mots de passe robustes, changés régulièrement	Directives concernant les mots de passe	Contrôle des mots de passe
Pas d'attention portée à la sécurité des objets apportés sur le lieu de travail (BYOD)	Objets apportés sécurisés, mis à jour, analyse anti-malware effectuée régulièrement, etc.	Formation concernant les BYOD	Vérifications des appareils
Gestion des accès privilégiés (personnes ayant accès à des données sensibles) défaillante	Gestion des accès privilégiés claire et définie	Formation aux accès privilégiés pour les personnes (employés) se chargeant des données sensibles	Contrôle et vérification des accès ainsi que du respect de la politique de l'entreprise dans ce domaine

Ce tableau, non exhaustif, décline les mesures supplémentaires à mettre en place en vue d'atteindre un objectif fixé et décrit les leviers actionnables ainsi que les procédures de

[23] Il s'agit d'une moyenne (CPVP, 2012 : cité par ICC et al., 2016 : 12).

contrôle pour réaliser ces objectifs. Il est propre à chaque entreprise et doit, bien entendu, être mis à jour régulièrement.

En plus de mettre au point une charte, prémisse visant à l'engagement de tous concernant la sécurité de l'information, l'entreprise peut compléter cette approche par l'affichage, sur un tableau de bord (Centre for Cyber Security Belgium, s.d.) situé dans les locaux, des avancées concernant l'état de la sécurité de l'information. Ainsi, elle expose l'évolution de l'état de la sécurité dans un but d'offrir à la sécurité toute la visibilité qu'elle se doit d'avoir. Ce tableau de bord inclut le score général obtenu aux tests (Security Metrics) ainsi qu'un agenda des prochaines formations, séminaires, etc ou dates prévues pour des questionnaires, audit, tests, etc (non discrets). Ce tableau doit bien entendu être mis à jour régulièrement. Ainsi, ce serait l'aboutissement d'un processus, par définition toujours à compléter parallèlement au développement du paysage informatique, d'un engagement (charte), d'une formation, et de la présentation des résultats.



Cette formation (voir tableau page 23), de manière générale, veille à la réduction au maximum des risques occasionnés par le facteur humain, d'origine non intentionnelle. Cependant, il existe aussi des risques à caractère malveillant (cf. supra) de la part « d'insider », c'est-à-dire de personnes ayant accès aux systèmes informatiques de l'entreprise. Concernant ces personnes, il est bien entendu évident qu'une formation à la sécurité informatique n'aura pas d'impact sur leurs actes, c'est pourquoi il serait logique, de la part de l'entreprise, d'envisager des contrôles sur les personnes ayant un accès privilégié aux données sensibles.

Mais ce n'est pas tout : ce tableau pourrait donner l'impression qu'il faille envisager la formation cyber point par point, réglant ainsi la majorité des problèmes. La formation à la sécurité devrait être dispensée comme un tout, selon une approche holistique, en inculquant la sécurité comme une tâche quotidienne accompagnant la majorité des activités. Cette formation devrait être mise à jour en fonction des « innovations » concernant les menaces, alimentée par un retour de la veille technologique et du Risk management.

4.2 Volet gestion des risques

4.2.1 Introduction

Tout d'abord, de quoi parle-t-on lorsque l'on aborde les risques liés à la toile ? L'OCDE, l'Organisation de Coopération et de Développement Economiques, fait référence aux incertitudes liées au développement, à l'utilisation, aux managements des outils informatiques[24]. Le risque cyber est également un facteur qui peut bouleverser, perturber, voire faire infléchir la trajectoire désirée concernant les objectifs fixés par l'entreprise, qu'ils soient opérationnels, financiers, sociaux, etc. En caricaturant un peu le trait, le risque peut être vu comme un « agent perturbateur » affectant l'entreprise dans son quotidien.

Le Management des risques liés à l'informatique est d'ailleurs la pierre angulaire de la définition de la bonne gouvernance (ENS, 2014), définie en 2008 par une norme (ISO 38500). La norme, réalisée par l'ISO (Organisation Internationale de Normalisation, vise à établir un système de normalisation mondiale) « *établit des définitions, des principes et un modèle de bonne gouvernance informatique d'entreprise […] (et) énonce six principes* » (ISO, s.d.) :

- Responsabilité
- Stratégie
- Acquisition
- Exécution
- Conformité
- Comportement humain

Dans le même domaine, une autre norme (ISO/IEC 27005 : 2018), plus récente (2018), énonce des « *lignes directrices relatives à la gestion des risques en sécurité de l'information (…) (et) est applicable à tous types d'organismes (…) (ayant) l'intention de gérer des risques susceptibles de compromettre la sécurité des informations de l'organisme* » (ISO, 2018).

[24] "Risk is the effect of uncertainties on objectives. "Digital security risk" is the expression used to describe a category of risk related to the use, development and management of the digital environment in the course of any activity. This risk can result from the combination of threats and vulnerabilities in the digital environment. They can undermine the achievement of economic and social objectives by disrupting the confidentiality, integrity and availability of the activities and/or the environment. Digital security risk is dynamic in nature. It includes aspects related to the digital and physical environments, the people involved in the activity and the organisational processes supporting it" (OCDE, 2015 : 30).

Un management des risques est absolument nécessaire au sein d'une stratégie de gestion de risques cyber. Dans le cas de la PME française attaquée par un logiciel de rançon, décrit par le reportage de France 2[25](France 2, 2017), les conséquences de l'attaque ont été importantes, et ce, dans plusieurs domaines : la comptabilité, les données clients, les fournisseurs, tout était stocké et géré sur internet. L'entreprise a tout perdu, du jour au lendemain, à cause d'une probable négligence de la part d'un employé ou des responsables de l'entreprise.

Toute une terminologie du risque ainsi que des nuances intéressantes sont précisées dans cette même source (OCDE, 2015). Ainsi, trois concepts[26] semblent importants à préciser afin de cerner la galaxie du risque avec acuité : les menaces, les vulnérabilités, et les incidents. Les menaces sont considérées en général comme extérieures à l'activité, tandis que les vulnérabilités sont considérées comme internes. Les incidents peuvent être internes ou externes, puisqu'ils peuvent émaner d'une négligence d'un employé ou être le fait d'une cause extérieure. Les menaces ainsi que les incidents peuvent être intentionnels ou non intentionnels. Dans ce cadre, le risque, résultant d'un évènement[27] arrive au croisement des menaces et vulnérabilités (« menaces + vulnérabilités = risque », c'est-à-dire que le risque est une combinaison entre en général un fait extérieur – une menace – et une faiblesse au niveau de la protection du système ou un manque de culture de sécurité de l'entreprise en interne). Toute la tâche du management du risque consiste donc à « *faire une distinction claire entre les causes et les conséquences et à considérer les premières (menaces, vulnérabilités et incidents) afin de manager les seconds (risques)*» (OCDE, 2015 : 32), et consiste également en un ensemble de procédures d'actions coordonnées au sein d'une entreprise (OCDE, 2015).

Tout d'abord, un état sur l'avancement de l'entreprise par rapport à sa « maturité cyber » doit être faite. A l'instar des indices précédemment énoncés ci-dessus, l'entreprise doit se positionner sur une échelle de sensibilisation aux risques cyber, suivant le précepte bien connu « connais-toi toi-même » de Platon, énoncé il y a plus de 2000 ans. Pour reprendre la terminologie utilisée ci-dessus, cette analyse veille à explorer les vulnérabilités afin de plus tard réduire l'occurrence d'incidents (non intentionnels). Il s'agit d'une analyse similaire à l'analyse SWOT, dans le domaine du marketing, concernant les forces et les faiblesses de

[25] Envoyé spécial. Cyberattaques : les braqueurs de l'ombre - 14 décembre 2017 (France 2). Pour rappel, cette société avait été infectée par un Ransomware, virus bloquant l'ensemble des terminaux de l'entreprise. Le moyen de contamination le plus fréquent est l'ouverture d'un contenu infecté par un virus.
[26] Cette terminologie n'est pas universelle, et, selon cette même source, d'autres mots peuvent être utilisés pour désigner les mêmes concepts. Elle ne doit pas servir de prescription inflexible.
[27] Toujours selon cette même source, un évènement qui bouleverse une activité est souvent appelé un incident (OCDE, 2015).

l'entreprise, à l'exception qu'il s'agit ici de forces et faiblesses de son système de défense (de manière générale) cyber.

Les catégories (« Immature », « Developing », etc) sont définies en fonction de divers facteurs [Voir Figure C Annexe]. Le positionnement est une première étape, une condition *sine qua non* pour construire un système de management des risques. Connaitre ses propres forces et faiblesses (i.e. vulnérabilités) permet d'ajuster au mieux sa stratégie de défense, remédier aux points faibles, construire un système plus résilient.

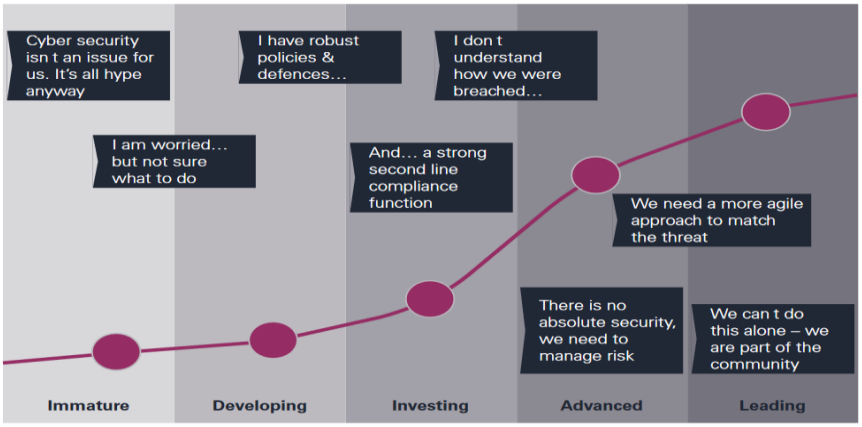


Figure 8. Note : reproduit à partir de « Building Cyber Resilience in Asset Management », KPMG. (2018). Consulté sur https://assets.kpmg/content/dam/kpmg/bm/pdf/2018/07/building-cyber-resilience-in-asset-management.pdf

4.2.2 Approche de gestion des risques par l'OCDE[28]

Conformément à la définition qu'elle donne du management des risques (« *(celui-ci) consiste également en un ensemble de procédures d'actions coordonnées* » [OCDE, 2015 : 34] au sein d'une entreprise), l'OCDE propose l'organigramme suivant :

[28] J'ai choisi différents outils (Risk Matrix, radar des risques) afin de proposer une évaluation des risques. Ces outils ne sont pas préconisés par l'OCDE et, bien entendu, d'autres outils peuvent être utilisés ainsi qu'une terminologie similaire.

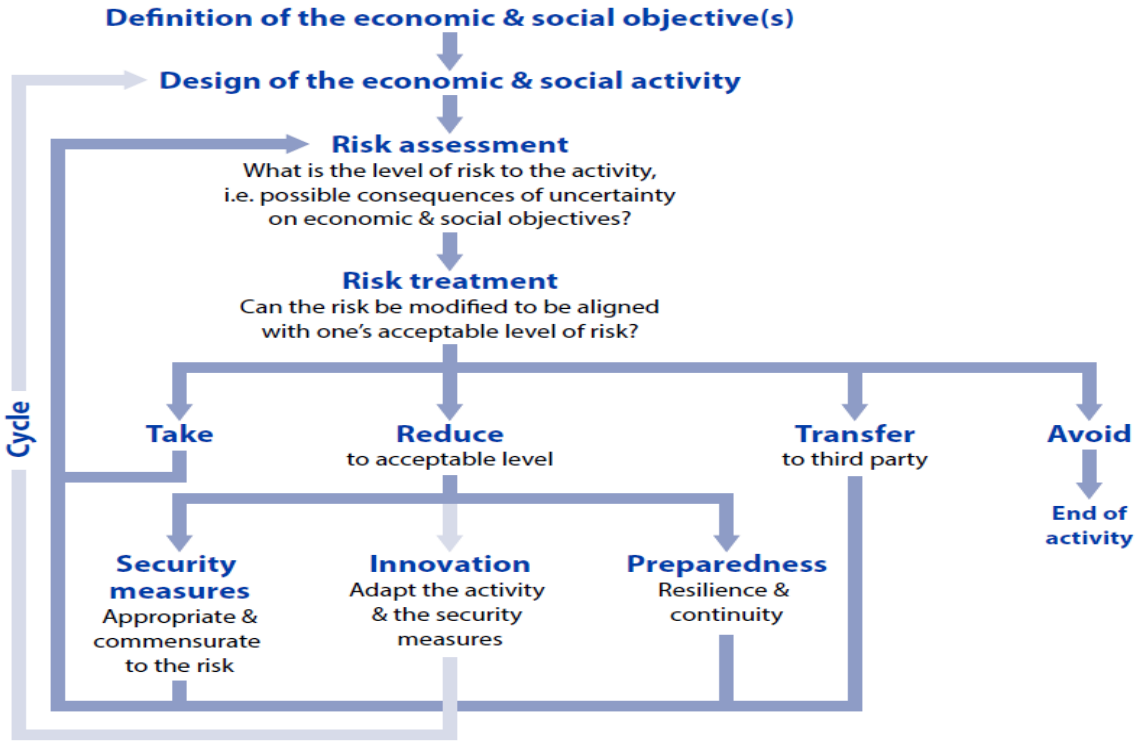


Figure 9. Note : reproduit à partir de « Digital Security Risk Management for Economic and Social Prosperity, OECD Recommendation and Companion Document », OCDE. (2015). Consulté sur https://read.oecd-ilibrary.org/science-and-technology/digital-security-risk-management-for-economic-and-social-prosperity_9789264245471-en#page1

Au niveau de l'évaluation des risques, première étape dans la gestion de celui-ci (cf. supra), plusieurs outils peuvent être utilisés afin d'établir une cartographie des risques au sein de l'entreprise. Celle-ci doit répondre à la question : quels sont les risques, concrètement, auxquels l'entreprise est soumise ? Quelle est la probabilité de ceux-ci ? Quel est leur importance s'ils venaient à se matérialiser ? Quel impact ? Ces risques sont bien sûr liés au domaine d'activité propre à l'entreprise et en fonction des données les plus sensibles de l'entreprise, il n'existe pas de « canevas » générique applicable à toutes les entreprises (« *there is no "silver bullet" solution for cyber security* » [Allianz, 2015 : 4]).

Ainsi, l'entreprise peut mettre en place une matrice des risques (« risk matrix »), outil désormais connu dans de nombreux domaines. Ces risques mélangent l'aspect

Likelihood \ Impact	Negligible	Minor	Moderate	Significant	Severe
Very Likely	Low Med	Medium	Med Hi	High	High
Likely	Low	Low Med	Medium	Med Hi	High
Possible	Low	Low Med	Medium	Med Hi	Med Hi
Unlikely	Low	Low Med	Low Med	Medium	Med Hi
Very Unlikely	Low	Low	Low Med	Medium	Medium

Figure 10. Note : reproduit à partir de « Beyond the risk Matrix », ARMS reliability. (2017). Consulté sur https://www.thereliabilityblog.com/2017/09/13/beyond-the-risk-matrix/

interne et externe du risque (il y a des risques auxquels l'entreprise est exposée qui sont des menaces provenant de tiers, mais également des menaces internes – bien que les menaces soient en général considérées comme externes par l'OCDE – provenant d'employés qui font preuve d'inadvertance ou de malveillance, comme on peut le constater sur le radar des risques, page 34) Cet outil a une finalité qualitative (apposer une échelle de valeur sur les risques, i.e. « élevés », « faibles », etc) grâce à une évaluation des risques de la part de l'entreprise (i.e. un nombre sur une échelle de 1 à 10, qui est ensuite retranscrit en valeurs). Ce tableau caractérise les risques en fonction de leur impact et leur probabilité d'occurrence. Seront considérés comme négligeables les risques à impact très faible et à la probabilité quasi nulle. Suivant le principe d'allocation des ressources, il est même envisageable de ne pas se protéger contre les risques considérés comme mineurs (ce qui correspond au simple « Take » du schéma des risques proposé par l'OCDE). Plus le risque se déplacera vers la droite et en haut du tableau, plus une attention ainsi que des moyens particuliers devront lui être accordés.

Pour ce faire, un « radar » général des menaces extérieures et intérieures est à utiliser dans l'identification des risques au niveau management. Selon la source « Building Cyber Resilience In Asset Management », un radar de la cybersécurité est proposé afin d'avoir une vue générale sur les menaces, ventilé selon les différents acteurs à l'origine des menaces[29]. Il s'agit des menaces en fonction de leur degré de risque et leur probabilité d'occurrence, données agrégées par KPMC[30], un réseau d'audit à l'international, en fonction des évènements qui se sont produits.

[29] Notons que selon ce même rapport, les « insiders » (membres de l'entreprise) peuvent représenter une menace ! Un autre rapport (IBM, 2016) parle même de 60 % (2015) d'attaques provenant des internes à l'entreprise. Des effets de composition de l'année 2015 sont certainement d'application.
[30] Un autre rapport venant d'ENISA (European Union Agency For Network And Information Security, 2018) met en avant des risques informatiques similaires. Je maintiens ce graphique pour des questions de représentation.

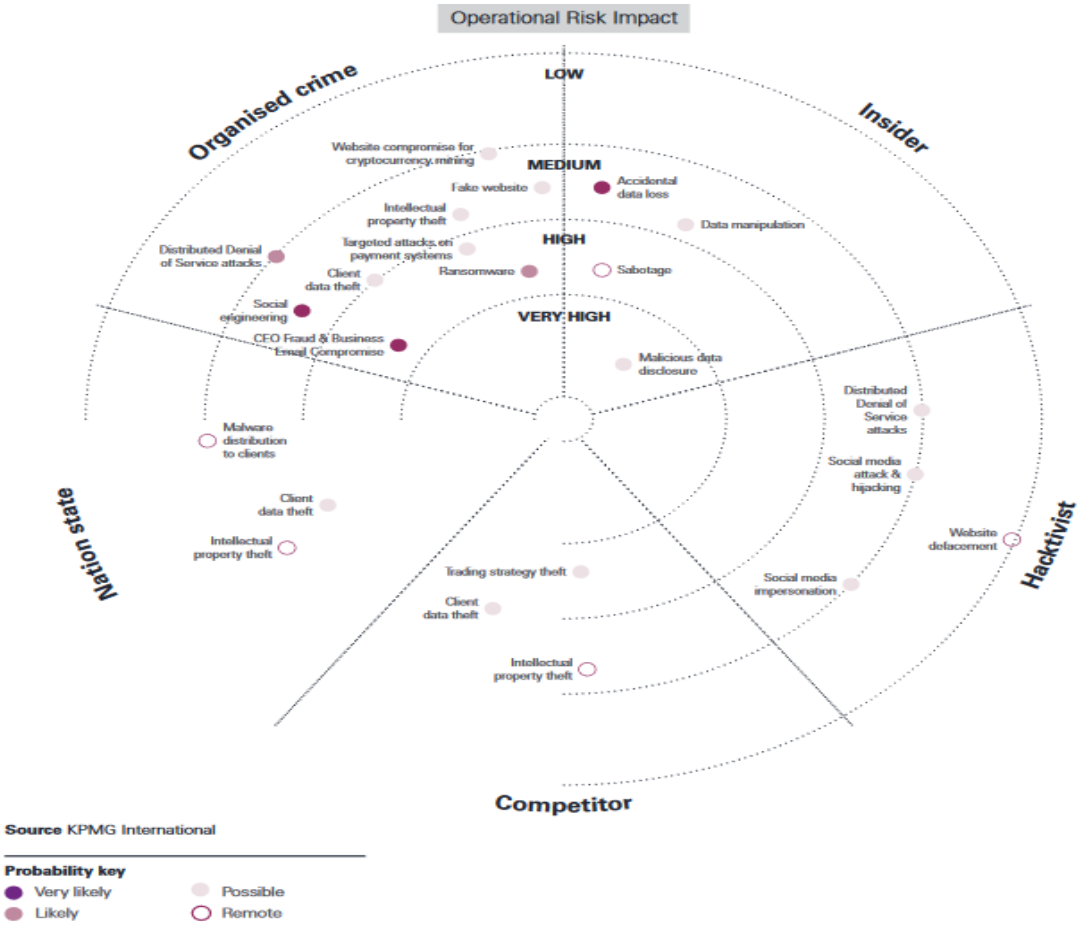


Figure 11. Note : reproduit à partir de « Building Cyber Resilience in Asset Management », KPMG. (2018). Consulté sur https://assets.kpmg/content/dam/kpmg/bm/pdf/2018/07/building-cyber-resilience-in-asset-management.pdf

Ainsi, si l'entreprise a listé comme faisant partie des menaces le vol de propriété intellectuelle, mais qu'elle constate, selon plusieurs sources, que la probabilité de ce risque est relativement faible, il lui revient de décider de se protéger ou pas contre cette vulnérabilité, sachant que la protection contre les menaces extérieures est un domaine, comme un autre, dans lequel le choix de l'allocation des ressources se pose. En effet (ICC et al., 2015), il est important de rester concentré sur l'essentiel, afin que cette protection soit efficace.

Après l'évaluation des risques (« Risk assessement ») vient le traitement de celui-ci : pouvons-nous modifier le niveau du risque, de sorte à le rendre acceptable ? Quatre chemins s'offrent à nous afin de « traiter » le risque (voir schéma OCDE page 32). Aux extrémités, prendre ou rejeter le risque sont deux options qui sont à considérer. Lorsque celui-ci est particulièrement mitigé ou très faible, l'option de la prise de risque « simple » peut être envisagée (« Take »), c'est-à-dire prendre un risque sans mesure compensatoire. A l'inverse, éviter purement le risque entraine la fin de l'activité (« Avoid »). C'est également un cas rare, dans lequel aucune solution ne peut être trouvée, et que les enjeux sont trop importants que

pour continuer l'activité. Entre ces deux formes binaires, se trouvent la réduction des risques et le transfert à une partie tierce, telle que les assurances cyber, domaine qui va se développer fortement et de manière concomitante à la gestion des risques cyber.

C'est sur le volet de la réduction des risques que se joue la grande partie du travail de l'entreprise. Il s'articule en trois parties, mélangeant la gestion technique et humaine du risque, se découpant en (1°) des mesures de sécurité (que cela soit au niveau informatique mais également au niveau formation de la sécurité du personnel : voir point 4.1 concernant la prévention et culture d'entreprise…), en (2°) « Innovation », c'est-à-dire en une veille technologique et réglementaire et enfin en (3°) un volet « d'état d'alerte » (Preparedness), avec pour composantes générales la résilience et la continuité, définis par les différents plan (plan de continuité d'activé ou PCA), domaine propre à la gestion des crises (voir page 40).

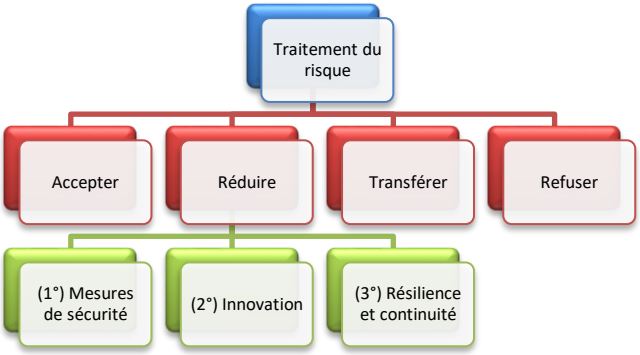


Figure 12. Note : reproduit à partir de « Digital Security Risk Management for Economic and Social Prosperity, OECD Recommendation and Companion Document », OCDE. (2015). Consulté sur https://read.oecd-ilibrary.org/science-and-technology/digital-security-risk-management-for-economic-and-social-prosperity_9789264245471-en#page1

4.2.3 Approche de gestion des risques par le « Centre de Cybersécurité Belge »

Cette approche élégante a l'avantage d'être simple et est constituée de seulement 6 étapes. Elle vise à protéger l'information de l'entreprise, « *bien précieux pour toute organisation* » (Centre for Cyber Security Belgium, s.d.). Elle repose en partie sur la troisième section du « Règlement Général sur la Protection des Données » (RGPD) réalisé par l'Union Européenne et entré en vigueur en mai 2018 (Union Européenne, 2016) :

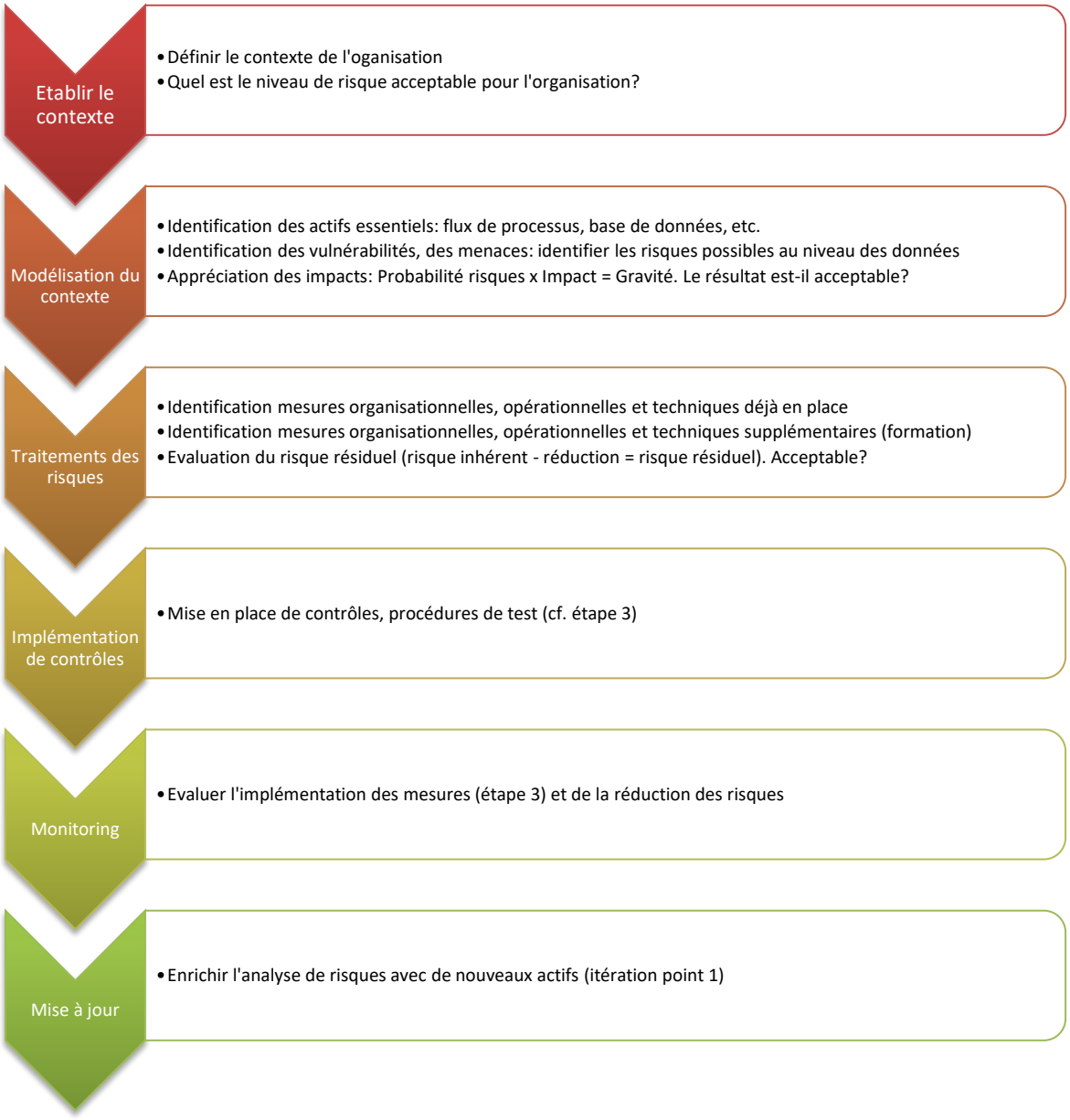


Figure 13. Note : Adapté de « Protégez vos biens les plus précieux », Centre for Cyber Security Belgium. (s.d.). Consulté sur https://cyberguide.ccb.belgium.be/fr/protegez-vos-biens-plus

Ce schéma débute par l'identification du contexte, de la situation de l'entreprise par la définition du risque général acceptable. Il se poursuit par l'identification des actifs essentiels (i.e. données sensibles) ainsi qu'une analyse de la gravité d'un impact donné. Concernant

cette étape, des outils similaires à ceux proposés ci-dessus (approche OCDE) peuvent être utilisés, comme par exemple la matrice des risques. La troisième étape quant à elle concerne le traitement des risques, sujet qui a fait l'objet du point 4.2.2. Ensuite, la mise en place de contrôles concernant les mesures introduites à l'étape 3 est proposée. Vient après cela l'étape de « Monitoring », c'est-à-dire les processus de surveillance en vue d'évaluer les mesures introduites à l'étape 3 afin d'obtenir un risque résiduel le plus faible possible. Concernant ces trois dernières étapes (de 3 à 5) un outil propre au domaine du mangement, le « Gap Analysis » semble assez approprié afin de piloter de manière opérationnelle les mesures engagées. Pour rappel, celui-ci vise à montrer l'écart entre la situation actuelle et la situation souhaitée (voir page 27).

Enfin, la dernière étape concerne la veille technologique, à savoir l'observation de nouvelles menaces et / ou apparition d'un nouveau contexte, dans le but d'offrir une formation (des mesures) la plus adéquate possible.

4.3 Veille technologique et réglementaire

La veille technologique consiste en une observation de l'évolution du cadre des risques informatiques liés à l'utilisation d'internet à des fins professionnelles. Elle est importante, puisqu'il s'agit d'une actualisation en permanence des risques auxquels l'entreprise est soumise. Il s'agit d'une mesure à réaliser afin d'être conscient de la vulnérabilité de l'outil informatique aux « innovations » en matière de menaces cyber. Elle s'effectue par des personnes ayant des connaissances informatiques. Elle est similaire à d'autres veilles que l'entreprise peut mettre en place, par exemple dans le domaine du marketing, ou l'idée de « veille environnementale » est désormais chose courante.

Bien entendu, pragmatiquement, toute entreprise ne pourra mettre en place une veille technologique avec des membres permanents, pour des raisons de coûts évidentes, étant donné les difficultés que certaines entreprises rencontrent déjà dans le développement de leur activité principale. Les solutions à trouver pour pallier ce problème se trouvent - entre autres - au niveau politique (par exemple un organisme actif créé par l'état venant en aide et informant les entreprises des menaces actuelles, en gardant en tête que l'exhaustivité est chose impossible et que des menaces inconnues peuvent apparaitre). On peut imaginer aussi une collaboration entre entreprises sur les menaces actuelles afin de rationaliser les coûts de prospection des données.

Similairement à l'observation des innovations sur le terrain des risques, une veille réglementaire devra être mise en place incessamment sous peu, étant donné « l'avalanche » (Institut des actuaires, 2017 : 16) de textes réglementaires à venir. En effet, il est prévisible que les juridictions nationales et européennes viennent encadrer les pratiques au niveau de la gestion de tout ce qui touche de près ou de loin aux données personnelles mais également au domaine cyber. Par ailleurs, il existe désormais, depuis mai 2018, une obligation de *reporting* aux autorités nationales compétentes en cas de brèche informatique touchant aux données personnelles (Voir point 5.3.3). Cette veille est nécessaire afin d'être aux normes au niveau européen, afin de ne pas être sujet à des sanctions qui seront très certainement d'application en cas de manquements. Ci-contre, un tableau recensant les principales réglementations européennes déjà en place. Pour rappel, une directive énonce les principes à respecter, et laisse le choix aux gouvernements de les appliquer. A l'inverse, un règlement s'applique totalement et est un « *acte législatif contraignant (…) il doit être mis en œuvre dans son intégralité* [31]» (UE, s.d.).

Réglementation déjà en place au niveau européen :

- Directive 2013/40/UE « Cybercrime »
- Directive 2015/2366 « Service de paiements II »
- Directive 2016/943 « Secret des affaires »
- Directive 2016/1148 « NIS » (Network and Information Security), à transposer en droit national en 2018
- Règlement 2014/910 « Identification électronique et services de confiance »
- Règlement 2016/679 RGPD « Protection des données personnelles « (applicable au 25/05/2018)

Figure 14. Note : Adapté de « Emergence du besoin en cyber assurance », Institut des actuaires. (2017). Consulté sur https://www.institutdesactuaires.com/global/gene/link.php?doc_id=12313&fg=1

4.4 Solutions logicielles

En développement, des solutions logicielles apparaissent sur le marché. Celles-ci consistent à proposer une aide à l'entreprise afin de réaliser les étapes énoncées dans ce chapitre (à l'exception de la formation du personnel, culture d'entreprise, etc), à savoir l'analyse de risques en fonction d'une situation de l'entreprise prédéfinie, le traitement de ceux-ci, l'implémentation, etc.

[31] La définition a été mise au singulier.

Au Luxembourg, une méthode développée par CASES, appelé MONARC (pour Method for an Optimised Analysis of Risks) est une initiative gouvernementale afin d'aider les petites entreprises dans la gestion des risques cyber. Il comporte une analyse de risque de type « matrice de risques », une création de rapport automatique, des objectifs à définir, etc.

- https://www.monarc.lu/

En France, une méthode appelée EBIOS risk manager, développé par l'ANSSI (Agence nationale de la Sécurité des systèmes d'informations), organisme officiel, vise également à un traitement du risque cyber suivant les principales étapes énoncées dans ce chapitre.

- https://www.ssi.gouv.fr/administration/management-du-risque/la-methode-ebios-risk-manager/

En dépit de l'appellation « Solutions », il semble que ces logiciels servent, à l'heure actuelle, plus d'outils offrant une aide aux entreprises. En effet, dans le cas du MONARC, et d'après la vidéo de présentation, l'insertion des données dans la matrice de risques présuppose au préalable sa réalisation[32]. De plus, il est difficile de connaitre pour l'instant les limites inhérentes aux programmes ainsi que de savoir dans quelle mesure et « jusqu'où » ces programmes peuvent se substituer à une complète analyse des risques de la part de l'entreprise. Ce qui parait pour l'instant évident, c'est que ceux-ci ne remplacent pas les étapes de formation et de conscientisation du personnel, énoncées dans le chapitre 4.

Cependant, un œil est à garder sur ces logiciels et concernant leur futur développement. Un aspect prometteur réside dans la collecte des risques et autres données des entreprises, celles-ci pouvant ensuite servir à une identification relativement précise des menaces secteur par secteur. Dans ce cadre, ces logiciels serviraient d'aide mais également de centralisation des données quant aux menaces récentes ainsi que les mesures mises en place pour les contrer, répondant ainsi à la nécessaire collaboration des entreprises, aspect soulevé dans le point 4.3 concernant la veille technologique. Etant d'origine étatique, les inquiétudes concernant les données collectées par ces programmes se feraient moins pressantes. Des questions concernant la délimitation juridique de ces programmes suite à une attaque réussie envers une entreprise ayant utilisé lesdits outils restent tout à fait ouvertes.

[32] Voir la vidéo d'introduction à la méthode MONARC, site internet : https://www.monarc.lu/

5 Gestions des crises[33]

5.1 Introduction

Une crise est définie comme étant une « *période troublée que traverse un pays, une société ; troubles qui affectent un secteur d'activité, le fonctionnement d'une institution, etc.* » (CNRTL, s.d.). Appliquée à l'entreprise, une crise est un évènement qui vient perturber le fonctionnement normal de celle-ci. Elle s'en retrouve affectée dans son outil de production, dans sa réputation, dans sa relation avec ses fournisseurs. Une crise est par définition unique et se distingue par plusieurs paramètres communs à chaque crise : « *l'ampleur, l'urgence, l'incertitude, [la gestion du] temps, la multiplication des intervenants, internes et externes, etc*. » (Laurent Combalbert et Eric Delbecque, 2012 : 38). Ces paramètres sont critiques en temps de crise. Une crise peut également avoir un effet multiplicateur, et entrainer une crise interne, comme dans le cas de Sony Pictures[34]. Le préjudice subi par cette dernière a été très vaste, du préjudice commercial au préjudice réputationnel, causant des dégâts à ses fournisseurs lorsque des documents stratégiques de ces derniers ont été divulgués (Jean Marc Lehu, 2018).

La gestion de crises cyber n'est pas réellement différente de la gestion de crises normale dans les procédures à mettre en place au niveau du management[35], mais certaines nuances sont à observer. En effet, lors de la gestion d'une crise cyber (c'est-à-dire post-impact) les facteurs temporels, les facteurs de coût, ainsi que le facteur réputationnel sont critiques. Le fait d'exposer quasiment l'ensemble des informations de l'entreprise sur internet (que cela soit grâce au Cloud computing ou autre) exacerbe le périmètre de la crise, périmètre relativement

[33] Je n'aborde pas dans ce mémoire la « gestion des incidents » définie par l'ITIL, référence dans le domaine informatique. Celle-ci aborde le caractère managérial informatique et technique des incidents, alors que je me concentre sur l'aspect managérial de la gestion des problèmes pouvant survenir en cas de crise, en faisant intervenir plusieurs outils, tels que des plans ou une cellule d'intervention. Une crise est un état général défavorable, alors qu'un incident est un évènement défavorable. Ainsi, un incident est nécessairement présent lors d'une crise, alors qu'un incident seul peut ne pas entrainer de crise (« *Les incidents majeurs peuvent signifier une situation de crise* » [Dauvin, 2018]). Dans ce chapitre seront donc présupposés des incidents importants ayant abouti, et non des incidents pour lesquels une simple et légère intervention est requise, ne requérant pas de plans ou outils managériaux pour y faire face. Pour pousser la délimitation encore plus loin, Lexsi (propriété d'Orange), un des plus grands CERT privé d'Europe (Computer Emergency Response Team), énonce que « *la gestion des incidents est un contributeur technique de la gestion des crises* ». (Lexsi, 2016)

[34] La Cyberattaque ayant touché Sony Pictures en 2012 entraina une crise interne, par la révélation de centaines de milliers de documents, où l'on apprit la recherche d'emploi du dirigeant de l'entreprise, qui montrait pourtant une volonté jusqu'au-boutiste dans la défense de son entreprise, ainsi que les propos à connotation raciste de sa co-présidente.

[35] Voir Annexe pour un bref comparatif.

restreint lorsqu'il s'agit d'une crise classique, c'est-à-dire lorsqu'elle touche par exemple la qualité des produits venant d'un fournisseur. La gestion des crises, à l'ère cyber, devient de plus en plus indispensable et devra, je pense, être appliquée à toutes entreprises, et pas seulement les plus grandes. En effet, le risque cyber s'applique à toutes entreprises ayant des activités sur la toile, et la manière de gérer un évènement défavorable qui survient est cruciale : elle peut révéler la force de l'entreprise, dans le cas où celle-ci se montre particulièrement structurée, résiliente, ou au contraire mettre l'entreprise dans une position très délicate. J'imagine possible, à l'avenir, de voir des entreprises rentables plonger en faillite pour négligence de gestion des risques cyber.

La gestion des crises agrège en réalité les domaines précédemment étudiés dans ce mémoire. En effet, il n'est pas étonnant que cela en soit ainsi, étant donné que la gestion des crises forme une boucle incluant l'ensemble des étapes qu'une entreprise sensibilisée aux enjeux cyber met en place. Si, d'après la source « La gestion des crises » (Laurent Combalbert et Eric Delbecque, 2012) celle-ci doit être prise selon une approche holistique, c'est-à-dire selon un cycle entier («*il faut […] la manager comme un tout organique* » [Laurent Combalbert et Eric Delbecque, 2012 : 44]) alors elle est ressemblante au management des risques pris sous la même approche[36].

Ce qui rend la gestion des crises plus complexe qu'il n'y parait, est que certains facteurs sont implicites (i.e. sous-jacents) et découlent de la bonne exécution de certaines étapes au préalable. Ainsi, par exemple, la gestion du temps découle de la bonne réalisation de l'ensemble des étapes, et, malgré qu'elle soit activement recherchée, ne s'offre pas directement aux personnes qui souhaitent la maitriser.

L'analyse de la cyberattaque ayant touché Sony Pictures est particulièrement éclairante concernant la gestion des crises. Un article académique lui est d'ailleurs consacré (Jean Marc Lehu, 2018). En effet, d'après l'avis de l'auteur même, cette attaque est « *d'une puissance encore jamais égalée à ce jour. De par sa violence, son ampleur et ses conséquences en termes de désorganisation fonctionnelle de l'entreprise, cette cyberattaque demeure exemplaire et riche d'enseignements, pour mieux appréhender le danger global et les conséquences potentielles auxquelles les entreprises concernées peuvent être confrontées (M. Stohl, 2006 ; J. Kizza, 2017) […] Au-delà de son ampleur jamais rencontrée auparavant, la*

[36] Je renverrai dans ce chapitre le lecteur aux endroits où j'ai traité de la question du management des risques, afin de ne pas alourdir la lecture et éviter les doublons. Un bref rappel est cependant proposé.

crise à laquelle le studio Sony Pictures a été confronté en 2014 est d'autant plus intéressante, qu'elle comporte de nombreuses facettes qui, dans une situation de crise classique, constitueraient autant de crises différentes possibles. Mais dans le cas de Sony Pictures, toutes ces facettes se sont trouvées agrégées dans une même crise, la rendant beaucoup plus complexe à gérer » (Jean Marc Lehu, 2018 : 44 - 46).

Tout d'abord, la gestion du temps, critique dans la gestion de crise, semble avoir fait défaut. En effet, il a fallu trois mois à l'entreprise pour circonscrire la menace, ce qui, comparé aux données fournies par le rapport « Hiscox Cyber Readiness report 2018 » (voir supra) semble extrêmement long, et le processus d'identification n'a été initié qu'une fois le second volet de l'attaque subi (Jean Marc Lehu, 2018). Sony Pictures semble avoir donc réagi de manière assez naïve et n'imaginait pas de suite à la première attaque. Ensuite, la gestion de l'information de crise, autre pilier sur lequel repose un *bon management* des crises s'est révélé assez médiocre[37](Jean Marc Lehu, 2018). A la place de cela, c'est bien plutôt l'impréparation qui régna. Finalement, l'auteur de l'article conclut que « *cette crise demeure cependant plus largement significative de la mauvaise évaluation des besoins en termes de cyberdéfense et révélatrice du fait que les principes de base de gestion du risque sont encore souvent ignorés, voire négligés à cause d'une myopie consciente ou non de certains managers. Cette cyberattaque est sans doute illustrative d'un cygne noir qu'il est toujours difficile d'envisager (A. Ignatius, 2015). Mais comme à chaque cas (sur)médiatisés, elle aura au moins eu l'intérêt d'attirer l'attention des managers sur le problème (…)* » (Jean Marc Lehu, 2018 : 49).

5.2 Le cycle de la gestion de crises[38]

La gestion de crises, en général, s'articule autour de plusieurs étapes, formant un cycle, une boucle de réaction que l'on oppose à un « fait générateur » : tout d'abord (1°), la première étape, qui est d'une importance cruciale, « éviter les crises », englobe une gestion technique du risque, mais pas seulement[39]. En effet, pour rappel, une cartographie des risques (tâche

[37] « Lorsque l'entreprise qui subit une crise dispose d'un plan d'urgence, d'une cellule de crise entrainée et activable dès les premières minutes de la crise, de grilles de lecture pour déterminer le fondement de la crise et évaluer les conséquences, de scenarii pour guider ses premières réactions…, elle ne s'assure pas de sortir indemne de la crise. Mais elle se donne les moyens de gérer l'information de crise avec moindre surprise, plus grande efficience et dans le meilleur des cas, réelle efficacité (A. Boin et A. McConnell, 2007). » (Jean Marc Lehu, 2018 : 48).

[38] En management, la gestion des crises forme très souvent une boucle, qui se fait en plusieurs étapes : 1° Prévention (éviter la crise) 2° Préparation 3°Contenir et résoudre 4° Retour d'expérience (Deloitte, 2018).

[39] Je renvoie pour cela au chapitre « gestion des risques » ainsi que celui concernant la formation du personnel.

propre au management des risques, voir chapitre 4) actuels est réalisée, afin d'être au courant des menaces qui pèsent sur l'entreprise. Mais la gestion des risques ne s'arrête pas là. Elle doit être complétée par une formation du personnel, afin que celui-ci soit le meilleur défenseur de la sécurité de l'entreprise. En effet, et pour rappel, la sécurité doit être une affaire de tous, et le facteur humain « *[doit être] au cœur de la conduite des crises, [qui est] avant tout une affaire de comportement et d'état d'esprit, […] une capacité d'adaptation accrue à une situation toujours plus incertaine et aléatoire* » (Laurent Combalbert, 2012 : 42). Une formation continue doit être prodiguée afin de sensibiliser tous les acteurs à l'importance du sujet. Cette formation ne doit pas être exclusivement utilisée à des fins de « conscientisation » du personnel, mais devrait bien entendu inclure également un volet de gestion technique, relativement basique, afin de transformer tout acteur en bouclier contre la menace extérieure, et ne doit pas se borner à l'utilisation de l'information de l'entreprise, mais également être étendu à la gestion des données de leur vie privée (ICC et al., 2016). En effet, il existe de nombreuses mesures à inculquer afin d'éviter les menaces évitables[40] (voir chapitre 4)

Ensuite (2°), le volet « préparation aux crises », étape importante, entre en jeu : il s'agit également de former chaque membre du personnel à adopter le comportement le plus adéquat en cas d'incident cyber (voir « Incident contact list » mais également le plan de communication interne, point 5.3.3). Faisant partie de cette seconde étape se trouve également une « boite à outils », tels que certains plans d'action, de communication, ou encore de continuité de l'activité. Ces plans sont un véritable atout et constituent une organisation en amont de la crise (avant l'impact). Il n'existe pas de « plans génériques », disponibles à chaque entreprise, mais ceux-ci doivent être réalisés par chaque entreprise, en fonction de son domaine d'activité[41]. Enfin, élément non moins important du volet de la formation du personnel est la mise en place de simulation et de debriefing. En effet, ces exercices, qui devraient être « non conventionnels » (Laurent Combalbert, 2012 : 47), devraient préparer le

[40] Pour rappel, à titre d'exemple : « Comment communiquer en toute sécurité et de manière responsable ? Comment utiliser les médias sociaux de manière judicieuse ? Comment transférer les fichiers numériques de manière sécurisée ? Comment utiliser son mot de passe de façon appropriée ? Comment éviter la perte d'informations importantes ? Comment s'assurer que seules les bonnes personnes puissent accéder à vos données ? Comment se protéger des virus et autres logiciels malveillants (malware) ? Qui avertir lorsque vous constatez un incident de sécurité potentiel Comment ne pas se faire piéger et divulguer des informations à des tiers malveillants ? » (ICC et al., 2016 : 24).

[41] J'aborderai ces plans plus en détails lors de la partie « boite à outils » de ce chapitre.

personnel à faire face à une vraie attaque, en inculquant les bons gestes à adopter, incluant un debriefing, une analyse rétrospective des actions entreprises, difficultés rencontrées, etc.

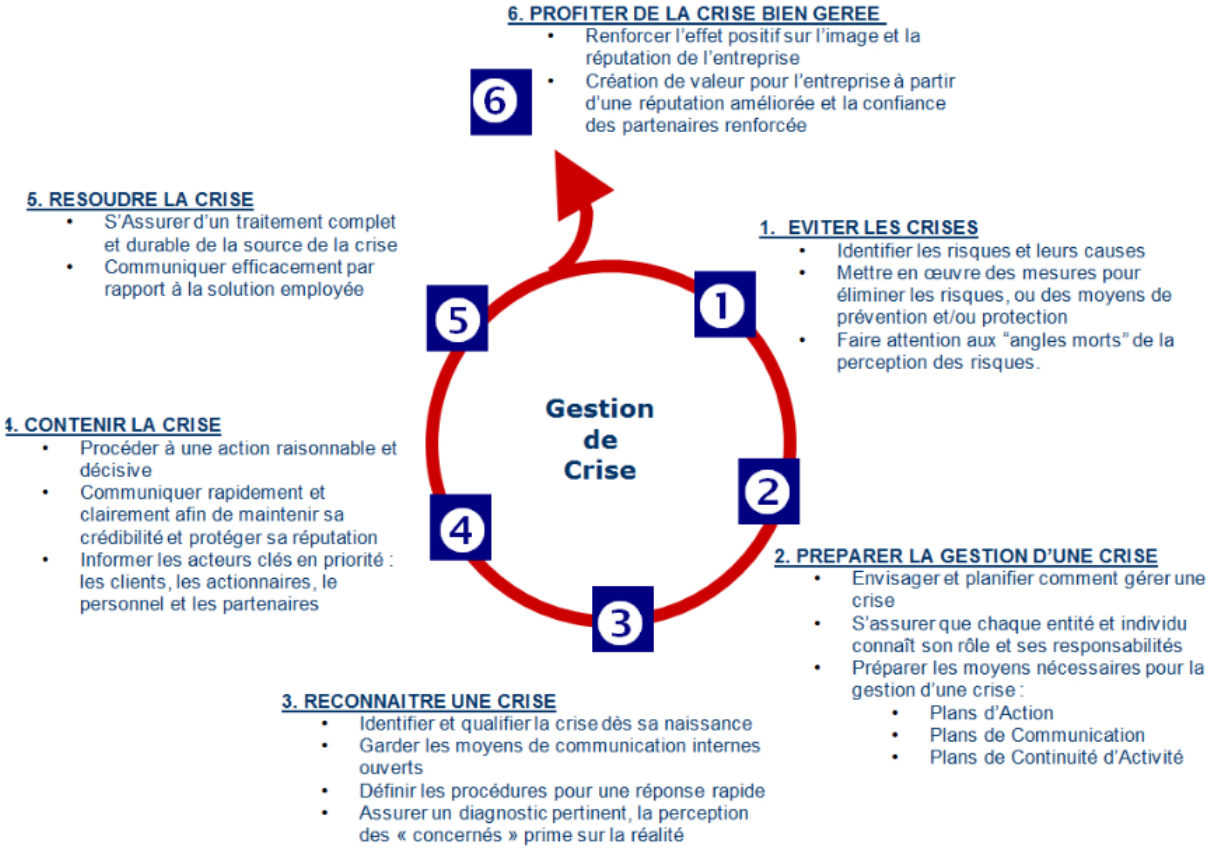


Figure 15. Note : reproduit à partir de « Gestion de crise en agroalimentaire : quels sont les bons réflexes ? », Menard, A. (s.d.). Message posté sur https://reussirenagroalimentaire.wordpress.com/2012/07/10/gestion-de-crise-agroalimentaire-quels-sont-les-bons-reflexes/

Ensuite (3°), selon ce schéma[42], la troisième étape est dédiée à la « reconnaissance d'une crise », étape, parmi d'autres, qui a crucialement fait défaut dans le cas de la gestion de crises faite par Sony Pictures. En effet, comme mentionné ci-dessus, « […] *le processus d'identification n'a été initié qu'une fois le second volet de l'attaque a été subi* »(Jean Marc Lehu, 2018 : 48), faisant perdre un temps précieux à l'entreprise, facteur qui a très certainement multiplié les dégâts occasionnés par la crise. Désemparée, l'entreprise Sony Pictures n'avait pas prévu de moyens de communication alternatifs, et a dû recourir au tout « non numérique[43] », situation qui prévalait au début du 20ème siècle ! Parmi cette étape, le

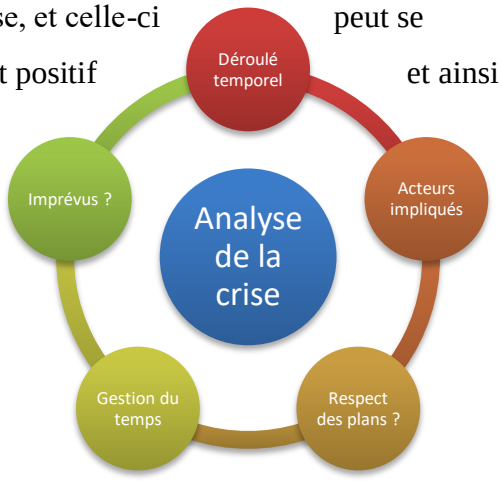
[42] Bien que la source n'émane malheureusement pas d'une source scientifique, c'est le schéma le plus clair que j'ai pu trouver jusqu'à présent concernant les étapes de gestion des crises. Une adaptation au domaine cyber est réalisée dans les paragraphes de cette section. Il est similaire à d'autres schémas de gestion de crise que l'on peut trouver dans la littérature. 1° Prévention (éviter la crise) 2° Préparation 3°Contenir et résoudre 4° Retour d'expérience (Deloitte, 2018).

[43] « *(…) la destruction partielle du système d'information et le risque non encore identifié imposèrent la mise en place d'urgence d'une messagerie électronique parallèle temporaire, et de demander à l'ensemble des employés un nouveau mode de travail « non-numérique ». Le système de comptabilité n'étant plus opérationnel, le*

facteur concernant l'identification et la qualification de la crise dès son apparition est crucial. Cette étape est propre à chaque entreprise, en fonction de son domaine, mais la définition générale de « crise », mentionnée ci-dessus, est commune à chacune. Une crise est un évènement capable de bouleverser, d'impacter fortement l'entreprise, que cela soit au niveau de sa réputation, de sa production, de sa relation avec ses fournisseurs, etc[44].

L'étape suivante (4°), « contenir la crise » concerne une intervention au niveau informatique afin de contenir la crise, mais implique surtout la gestion de l'information de crise (voir plans de communication, point 5.3.3). En effet, communiquer de manière claire à tous les intervenants est une étape non négligeable afin d'éviter un possible impact sur la valorisation de titres, s'il s'agit d'une entreprise cotée. Il serait dommageable qu'une crise commise par un impact externe (i.e. une attaque) entraine une autre crise de confiance avec les parties prenantes de la société, impactant le déroulement à moyen terme de ses activités. C'est pourquoi il est primordial, selon moi, de ne pas atténuer ou embellir l'attaque que l'entreprise a subie. Cependant, d'après l'article dédié à l'analyse de l'attaque subite par Sony Pictures, la gestion de l'information de crises découlerait majoritairement du respect de nombreuses étapes, comme par exemple d'un « *plan d'urgence, […] d'une cellule de crises, […] de grilles de lectures […]* (Jean Marc Lehu, 2018 : 48). L'étape suivante (5°) concerne majoritairement une intervention informatique, couplée d'une communication adaptée par rapport à la solution envisagée[45].

Enfin, la dernière étape (6°) concerne le retour sur expérience. Une gestion de crise bien effectuée peut révéler une véritable force de l'entreprise, et celle-ci peut se « saisir » de cet évènement pour le transformer en effet positif et ainsi sortir de la crise avec un véritable « effet de résilience ». En effet, bien que chaque crise soit dommageable à court terme, étant donné la perturbation induite par celle-ci, l'entreprise peut faire de cette faiblesse une force, et transformer ce bouleversement en un effet réputationnel à long terme.



paiement des fournisseurs, des prestataires et des employés dut être réinventé avec des supports physiques oubliés (…) » (Jean-Marc Lehu, 2018 : 46 – 47).

[44] Bien que cela semble relativement évident, l'exemple de Sony Pictures, pourtant entreprise d'une certaine taille, prouve qu'il reste une relativement grande « myopie » à l'égard des menaces cyber qui pèsent sur les entreprises.

[45] Selon ce schéma.

L'entreprise peut, une fois la crise passée, conduire une analyse de celle-ci afin d'en comprendre les différentes étapes, les acteurs impliqués, de comprendre le déroulement temporel de celle-ci… Cette analyse doit s'abstenir de chercher des coupables idéals, mais bien plutôt s'interroger sur « *(la) culture globale et (les) modèles quotidiens de fonctionnement, […] incarnés par une grande quantité de personnes* » (Laurent Combalbert et Eric Delbecque, 2012 : 113). Cette analyse pouvant par la suite être enseignée et ajoutée à la formation du personnel, bouclant ainsi le cercle entamé. Cette même source (Laurent Combalbert et Eric Delbecque, 2012) pointe la nécessité d'effectuer cette analyse afin de contrer l'oubli, fruit des préoccupations opérationnelles du quotidien.

Un facteur fondamental et sous-jacent qui découle (notamment) de la bonne réalisation de l'ensemble des étapes mentionnées ci-dessus, facteur qui est implicite et non directement visible, est la gestion du temps. En effet, cet aspect est crucial afin de non seulement circonscrire l'attaque, mais également de limiter le périmètre des dégâts occasionnés. Dans le cas de Sony Pictures, pour rappel, il a fallu trois mois pour identifier la menace (Jean Marc Lehu, 2018). La gestion du temps, du début jusqu'à la fin de la crise permet aussi de limiter le dégât réputationnel de l'entreprise et impacter de manière réduite la poursuite de ses activités.

5.3 Plans et outils

Indispensable à une bonne préparation en amont des crises se trouve toute une « boite à outils » dont dispose une entreprise afin d'anticiper les incidents. Ces outils sont sous forme de plans, sorte de « guides » qui aideront l'entreprise à faire face au mieux à la crise, et manageant le déroulement des opérations, des *process*, pour faire en sorte que la poursuite de l'activité se fasse dans les meilleurs délais, et à coût restreint.

Schématiquement, l'ensemble des outils qui vont être détaillés dans la section suivante se présentent comme suivant :

Cependant, selon la Cyber Security Coalition (2015), l'ensemble de ces trois outils peuvent être réunis au sein d'un seul, appelé « plan de réponse aux incidents ». Concrètement, il devrait inclure différentes étapes, au croisement de plusieurs domaines, dont le management des risques précédemment étudié :

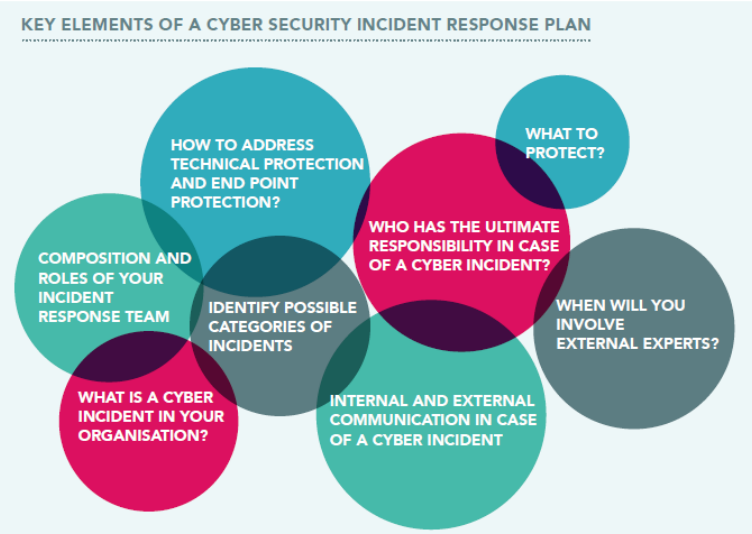


Figure 16. Note : reproduit à partir de « Cyber security incident management guide », Cyber Security Coalition (2015). Consulté sur https://www.cybersecuritycoalition.be/content/uploads/cybersecurity-incident-management-guide-EN.pdf

Ainsi, ce plan repose sur l'identification des risques, domaine propre au management des risques, mais également une analyse des vulnérabilités de l'entreprise, afin de définir les domaines les plus sensibles et critiques à la poursuite des activités. Il précise également toutes les étapes à respecter, muni des plans de communication et de continuité des activités. Il devrait inclure précisément les rôles de chacun ainsi que les différents scenarii élaborés auparavant. Toujours selon cette même source, ce plan n'est pas statique et doit être mis à jour (Cyber Security Coalition, 2015).

5.3.1 Plan de continuité des activités (PCA)

Tout comme son nom l'indique, le plan de continuité des activités vise à proposer la poursuite des activités dans un environnement dégradé et soumis à une dynamique défavorable. En

effet, une crise peut « *contraindre fortement, voire stopper complètement l'exercice d'une entreprise* » (Cyber Security Coalition, 2015 : 67). Le PCA identifie *ex-ante* des scenarii afin d'y opposer des réponses aux crises, et propose un mode alternatif en cas d'indisponibilité des ressources impactées (Alain Coursaget et Laurent Haas, 2014). Dans ce cadre, il est donc absolument indispensable de prévoir une « sortie par le haut » de la crise et de fournir une possibilité à l'entreprise de poursuivre ses activités.

Toujours selon la même source (Laurent Combalbert et Eric Delbecque, 2012), le plan de continuité des activités « *répondrait à deux objectifs* » : (1°) tout d'abord, assurer un « *service minimum* » et par là cibler les activités critiques à la réalisation de certaines tâches indispensables au niveau par exemple des processus de production. Assurer ce service permettrait d'ailleurs de « *pallier les effets de la crise* » (Laurent Combalbert et Eric Delbecque, 2012 : 68). Ensuite (2°), il serait un outil intéressant, propre au domaine de la « théorie du signal », c'est-à-dire servirait d'outil de communication « *afin de rassurer l'opinion publique et les actionnaires d'un groupe qui voient en cela un signe de professionnalisme* » (Laurent Combalbert et Eric Delbecque, 2012 : 68). Etant donné le caractère évolutif des activités de l'entreprises au niveau technologique, ce plan n'est pas exempt d'une mise à jour.

De manière détaillée, le plan de continuité d'activité se présente comme suivant (Alain Coursaget et Laurent Haas, 2014 ; 18) :

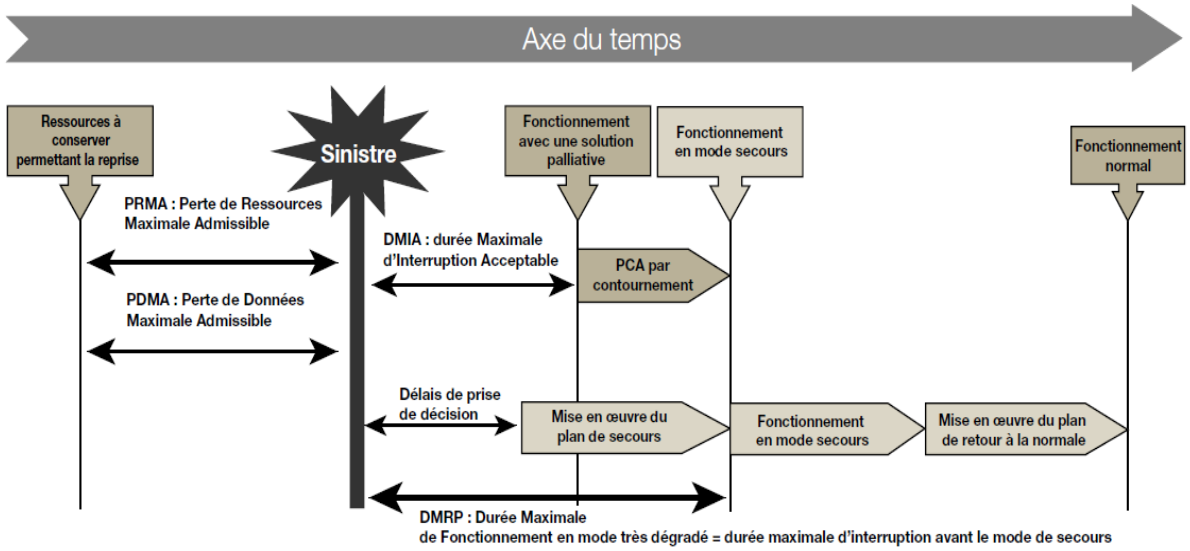


Figure 17. Note : reproduit à partir de « Le plan de continuité d'activité (PCA) : Approche méthodologique, Coursaget, A. et Hass, L. (2018). Consulté sur https://www.cairn.info/revue-securite-et-strategie-2014-3-page-13.htm

Ce plan vise à exposer, à partir d'une situation de sinistre, un certain « écart de dispersion » acceptable quant à la perte de données ou la durée maximale autorisée avant la mise en œuvre « *d'une solution palliative* » (Alain Coursaget et Laurent Haas, 2014 ; 18). Il organise le déroulement des évènements jusqu'à le recouvrement de la situation normale avant crise.

5.3.2 Cellule de crise

Parmi les acteurs nécessaires à l'ensemble du processus de gestion des crises, la « cellule de crise » occupe une place prépondérante, mais pas exclusive, afin de ne pas imiter les égarements cités ci-dessus, à savoir que la gestion des crises serait uniquement le fait d'un ou plusieurs acteurs précis. Effectivement, la « *mise en place d'une telle cellule, vise, en effet, à contenir les effets négatifs d'une situation dégradée en solutionnant les problèmes auxquels fait face l'entreprise […] (celle-ci) repose sur des moyens humains et techniques ainsi que des procédures précises de gestion des évènements […] elle n'est pas l'unique moyen de gestion du risque* » (Laurent Combalbert et Eric Delbecque, 2012 : 53). Bien qu'assignée à cet effet, cette équipe ne couvre donc pas, à elle seule, de manière auto-suffisante, la gestion du risque au sein de l'entreprise et sa composition devrait être adaptable en fonction des situations (Laurent Combalbert et Eric Delbecque, 2012). Cette cellule ne doit pas être une entité « ad hoc », et doit être bien préparée afin de ne pas entrainer un « déni de crise » (Stéphanie Ruelle, 2012 : 39), impactant l'étape 3 du schéma. Cette cellule est nécessairement présente lors de l'étape 1 ou 2 du schéma, par son caractère « préparatoire ». Son mode de fonctionnement, adaptable, ne se borne pas à ces premières étapes, mais s'étend à l'ensemble du processus de gestion des crises.

Cependant, un mode de fonctionnement général peut être identifié : en effet, toujours selon cette même source, elle devrait fonctionner en mode « REAC », c'est-à-dire faire preuve de Réactivité, Efficience, Adaptabilité et Cohésion (Laurent Combalbert et Eric Delbecque, 2012 : 54 – 55). La réactivité fait intervenir majoritairement un facteur *temps*, un intervalle maximum toléré par l'entreprise après incident. C'est l'entreprise, en fonction de ses moyens et de son domaine d'action, qui doit fixer cet intervalle de tolérance maximum. L'efficience, concept qui fait intervenir la gestion des ressources en fonction d'un objectif recherché, fait référence aux « *outils disponibles et en se passant des moyens inopérants* [propres à une situation dégradée] ». Ensuite, l'adaptabilité devrait être une qualité inhérente à une cellule de crise fonctionnelle, permettant au groupe de s'adapter aux paramètres propres de chaque

situation, les amenant à « *faire preuve d'une intelligence des situations* ». Enfin, la cohésion signifie que bâtir le groupe « *autour d'une confiance mutuelle est une nécessité, […] (et) chaque membre de la cellule doit accepter le jugement constructif de ses pairs pour faire progresser l'ensemble de l'équipe dans la résolution du problème* ». Ces quatre qualités, pour fonctionner de manière optimale, devraient être sous-tendues par des exercices et simulations réguliers.

Mais ceci n'est pas tout : la cellule de crise se doit de bien connaitre la dynamique des crises, à savoir que notre mode de pensée normal en entreprise, le mode « analytico-déductible », mode de pensée inculqué par l'éducation mais également favorisé par les entreprises lorsque chaque domaine est séparé en département et qu'une (sur)spécialisation est requise, ce mode de pensée se trouve suranné en période de situation dégradée. En effet, la crise induit des « *conséquences interactives* » (Laurent Combalbert et Eric Delbecque, 2012 : 43), c'est-à-dire que celles-ci s'influencent mutuellement et « (qu') *agir isolément sur une des origines ou une des conséquences la crise ne sert pas à grand-chose […] il faut au contraire la manager comme un tout organique* » (Laurent Combalbert et Eric Delbecque, 2012 : 44).

La composition de la cellule de crise se décline en fonction de la structure de l'entreprise. Le rôle, la responsabilité ainsi que les compétences de chacun sont définis dans le cas d'une grande structure [Voir Figure E Annexe].

Concernant le budget alloué à la mise en place d'une cellule de crise, les petites entreprises n'ayant pas les moyens d'y consacrer une part substantielle de leur chiffre d'affaire devraient néanmoins mettre en place une « structure minimale », telle que définie ci-après (Cuber Security Coalition, 2015 : 12).

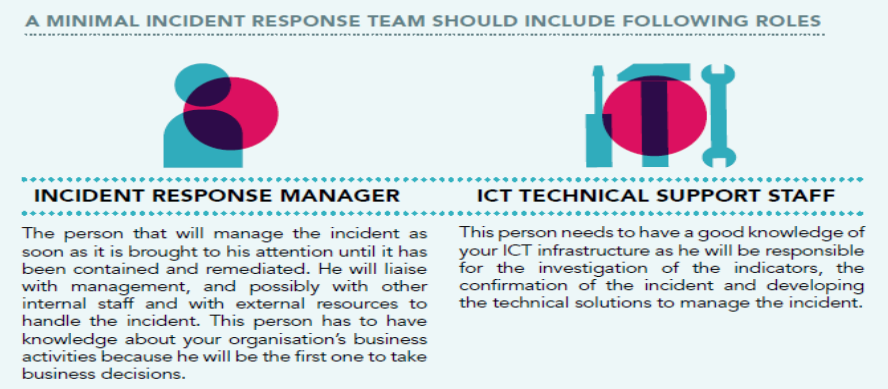


Figure 18. Note : reproduit à partir de « Cyber security incident management guide », Cyber Security Coalition (2015). Consulté sur https://www.cybersecuritycoalition.be/content/uploads/cybersecurity-incident-management-guide-EN.pdf

Autre acteur possible pour les entreprises, est le recours à « *des fournisseurs de services spécialisés dans la maîtrise et la remédiation d'incidents de sécurité* » (ICC et al., 2016 : 21), mais qui, eux aussi, ne remplacent pas, bien entendu, la gestion totale des menaces cyber qui

pèsent sur l'entreprise et ne peuvent servir de palliatif à la nécessaire conscientisation des entreprises aux risques. Ici aussi, la préparation est de mise : une liste de fournisseurs externes de services devrait être envisagée.

5.3.3 Plan de communication

En temps de crise, et alors que les évènements peuvent s'enchainer plus rapidement que prévu et que le stress, l'imprévu, viennent bouleverser l'organisation interne de l'entreprise, il est nécessaire de gérer l'information et la communication, « *outil indispensable à la gestion d'une situation dégradée et donc à la protection d'une organisation* » (Laurent Combalbert et Eric Delbecque, 2012 : 65). A ce titre, nous l'avons vu, le cas de la crise au sein de Sony Pictures et le défaut de préparation représentent un contre-exemple à ne pas suivre, lorsque « *l'impréparation et la surprise furent telles pour Sony Pictures que la gestion releva davantage d'une réaction improvisée et itérative, générant parfois l'incohérence* » (Jean Marc Lehu, 2018 : 48). En effet, l'entreprise qui a produit le film « The Interview » envoya des signaux assez ambigus concernant sa volonté de diffusion du film, passant d'une position à l'autre.

Dans ce cadre, le plan de communication vise précisément à « *maitriser les flux d'informations générés par l'entreprise en temps de crise* » (Laurent Combalbert et Eric Delbecque, 2012 : 65). Comme énoncé ci-dessus concernant l'étape 4 du schéma de gestion de crise, il est nécessaire de ne pas atténuer ou embellir les informations de l'attaque, et que la « *sincérité du discours et son authenticité sont les meilleurs moyens pour réussir cet exercice difficile* » (Laurent Combalbert et Eric Delbecque, 2012 : 65).

Schématiquement, le plan de communication devrait s'articuler en 2 volets différents :

Plan de communication	Caractéristiques
Plan de communication externe	• Vise à délivrer les informations concernant les actions que l'entreprise va prendre, informations qui concernent l'entreprise et les acteurs externes. • « *Vise tous les acteurs qui ne sont pas membres de l'entreprise* » (Laurent Combalbert et Eric Delbecque, 2012, 66), i.e. les médias. • Ce plan doit être adapté en fonction du récepteur du message[46]. • Ce plan informe les collaborateurs « *afin qu'ils puissent relayer les bonnes informations* » (Laurent Combalbert et Eric Delbecque, 2012 : 66) • L'information doit être fiable, pertinente, claire. • Ce plan nécessite une préparation et « *ne peut s'improviser* » (Laurent Combalbert et Eric Delbecque, 2012 : 67).
Plan de communication interne	➢ Cible les personnes internes à l'entreprise ➢ Délivre les informations concernant les actions qui vont être entreprises ➢ Veille à fournir des informations cohérentes, qui précédent le mode d'action à adopter en fonction de la situation dégradée[47]. ➢ Ici aussi, l'information se doit d'être fiable, pertinente, claire.

Ces deux plans sont à adapter en fonction de la taille de l'entreprise et ne dictent pas les démarches à suivre de manière rigide. En effet, les plans de communication externes par exemple ne seront pas les mêmes pour une petite PME que pour une grande entreprise dans la

[46] De plus, il est par exemple possible « *d'envisager une stratégie de communication pour chacun des scenarii listés dans le plan de crise* ». (Laurent Combalbert et Eric Delbecque, 2012, 66)
[47] En effet, selon le scénario rencontré, les employés doivent adopter leur comportement dans la vie de tous les jours au sein de l'entreprise. Par exemple, en cas d'indisponibilité d'un outil suite à un incident cyber, un mode alternatif doit être proposé.

priorité de l'information à fournir aux membres externes de l'entreprise. Ainsi, alors que la PME informera ses proches collaborateurs (externes) et n'aura que rarement contact avec les médias, la situation sera tout autre dans le cas d'une grande entreprise, pour qui le contact avec médias devra être entrepris assez rapidement et sera d'une importance élevée.

Depuis mai 2018, l'entreprise a l'obligation[48] de notifier une fuite de données à l'autorité compétente en la matière :

Notification	Caractéristiques
RÈGLEMENT (UE) 2016/679, Article 33 (Union Européenne, 2016) : • **https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32016R0679**	Notification à l'autorité compétente : • En Belgique, Autorité de Protection des Données (APD) :https://www.autoriteprotectiondonnees.be/formulaire-notification-de-fuites-de-donnees • Délai de 72 heures, ou évocation des motifs en cas de non-respect • Par le responsable du traitement des données
RÈGLEMENT (UE) 2016/679, Article 34 (Union Européenne, 2016)	Notification à la personne concernée d'une violation de ses données personnelles : • Dans les meilleurs délais • Par le responsable du traitement des données

[48] Sauf si elle n'entraine pas de risques pour les « *droits et libertés des personnes physiques* » (Union Européenne, 2016 : 52)

5.4 Conclusion de la section

Au risque de se répéter, il est devenu absolument indispensable d'envisager une gestion des crises à l'heure de la digitalisation des sociétés, et ce, indépendamment de la taille de l'entreprise. De très nombreuses sociétés semblent assez loin d'afficher un degré de conscientisation suffisant afin d'anticiper les dangers à venir. Au-delà de l'aspect technique, l'aspect humain semble également déterminant, car, la gestion de crise, « *loin d'être un amoncellement de procédures rigides à suivre mécaniquement* » (Laurent Combalbert, 2012 : 42), est avant tout réalisée par des hommes et des femmes dont il est nécessaire de guider le fonctionnement, d'en comprendre les ressorts psychologiques, etc (Laurent Combalbert, 2012). Non moins indispensable est la faculté d'adaptation des membres de l'entreprise, étant donné le caractère unique de la crise. De cette faculté d'adaptation, de la formation du personnel, des plans de gestion de crises découlera la bonne réussite de gestion des crises, cruciale en termes de réputation, de continuité d'activité, et, au final, de survie de l'entreprise. Cet exercice semble plus complexe qu'il n'y parait, de par sa préparation minutieuse, et une des clés du succès est la communication et la coordination permanente entre les membres et collaborateurs de l'entreprise. Ce chapitre a montré les grandes étapes ainsi que les acteurs et les outils à disposition des entreprises afin de faire face, au mieux, à la menace cyber déclenchant une crise.

6 Externaliser la gestion des risques à une partie tierce

Les assurances cyber représentent un marché avec un fort potentiel de croissance et vont très certainement se développer de manière concomitante à la gestion des risques cyber au sein des entreprises. En effet, selon plusieurs sources (Statista, 2019), le marché de l'assurance cyber connait une tendance haussière ces dernières années, en pourcentage d'entreprises envisageant d'acquérir une assurance, mais également en valeur. A ce titre, il semble toutefois que le

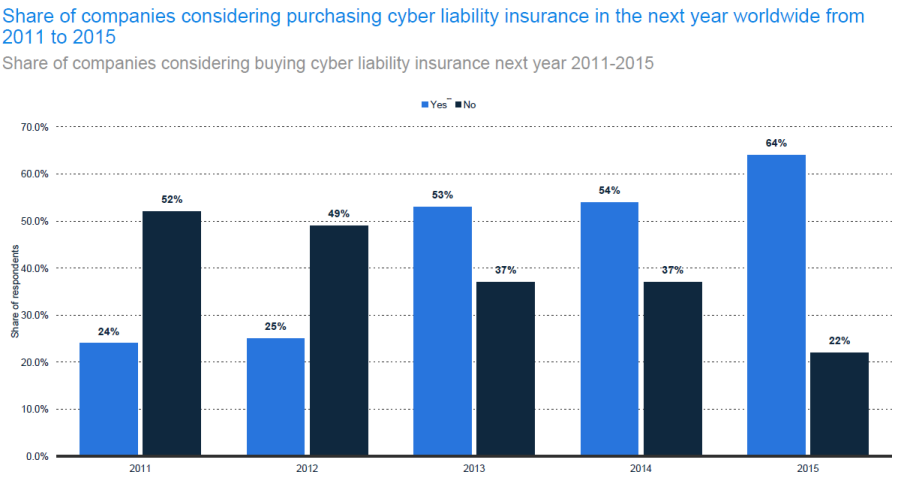


Figure 19. Note : reproduit à partir de « Cyber Insurance », Statista. (2019). Consulté sur *https://proxy.unamur.be:2391/study/27800/cyber-insurance-statista-dossier/*

marché américain capte la très grande majorité (90%) des assurances cyber [Voir Figure G Annexe]. L'Europe, à la traine, n'affiche qu'un maigre 4% quant à la conclusion d'un contrat d'assurance. La raison est (en partie) certainement imputable à la réglementation, mise en place en 2003 aux États-Unis et complétée par des lois fédérales avec sanctions en cas de manquements (SCOR, 2017).

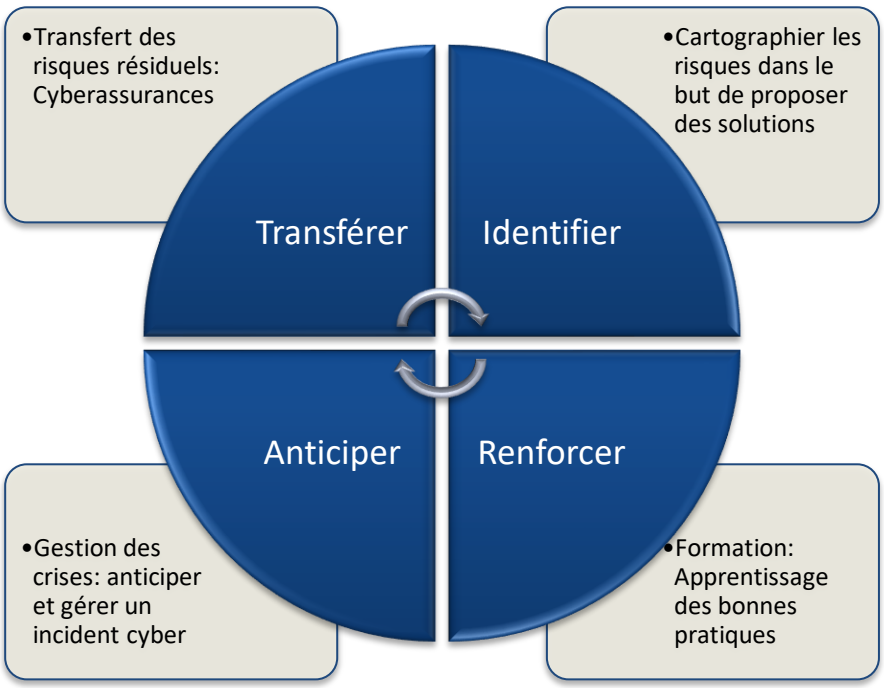
Les cyber assurances « *propos(ent) une gamme de produits permettant d'assurer les biens immatériels des entreprises comme leur patrimoine informationnel, essence même de leurs activités métiers* » (CLUSIF, 2018 : 6). Il n'existe pas, à l'heure actuelle, de consensus concernant le périmètre des assurances cyber (CLUSIF, 2018). En effet, ce domaine fait face à des plusieurs difficultés : tout d'abord, celle des entreprises, qui ont du mal à « *évaluer leurs besoins d'assurance* » (Didier Parsoire, 2015 : 65). Aspect intéressant soulevé par cette même source, la gestion des risques par les entreprises, de manière générale, ne serait pas encore optimale, c'est-à-dire serait encore perçue comme une problématique relevant d'un département (le département finance s'occupe de finance, le département marketing de marketing) et déteindrait sur la capacité à évaluer leur besoin en assurance (Didier Parsoire, 2015). Ensuite, celle des assurances elles-mêmes qui rencontrent des problèmes quant à la tarification de leur offre, dû à « *un manque de données historiques sur les sinistres et incidents, renforcé par la réticence des entreprises à partager l'information* » (Didier Parsoire, 2015 : 65). Citant l'ENISA (European Network Information Security Agency), une autre source énonce la difficulté concernant le caractère assez évolutif de la technologie, « *l'absence de réassureurs et d'assureurs de dernier recours* » (Frédérick Douzet et Sébastien Héon, 2013 : 50), et le problème de chevauchement avec les assurances existantes (Frédérick Douzet et Sébastien Héon, 2013).

Ces difficultés ne vont cependant pas empêcher l'émergence d'assurances cyber, que cela soit consécutif à un manque identifié par les entreprises concernant leur protection cyber ou sous le coup de réglementation arrivant en Europe (cf supra, point 4.3). Dans l'état actuel des choses, il semble raisonnable pour la petite entreprise de ne pas souscrire à une assurance cyber pour des raisons de coût, mais de mettre en place une gestion des risques, l'assurance ne « *substitu(ant) (pas) une gestion optimisée des risques* » (Dider Parsoire, 2015 : 65), externaliser les risques à une partie tierce ne peut se faire que de manière complémentaire à l'implémentation d'étapes de gestion des risques cyber. Concernant une grande entreprise, il est également difficile de répondre à la question de l'assurance, à savoir que la réduction supplémentaire des risques (transfert) valle les coûts occasionnés par la souscription à une

police d'assurance, faute d'outils quantitatifs précis. Il existe cependant des articles tentant de répondre, via une modélisation mathématique, à la question de la prise d'une assurance cyber[49]. Le développement du contexte actuel, en revanche, présage une généralisation, dans un futur plus ou moins proche, de l'utilisation d'assurance cyber comme stratégie complémentaire au traitement des risques.

7 Modèle de cybersécurité

Identifier, Renforcer, Anticiper, Transférer : IRAT



Sur base des dimensions identifiées précedemment dans ce mémoire, un modèle, abrégé IRAT, peut être proposé. Il se compose de 4 étapes essentielles (même si la dernière reste, dans l'état actuel, une source d'interrogation) qui visent à fournir un cadre d'analyse et de réponses aux risques cyber. Tout d'abord, une identification des risques propres à l'entreprise doit être effectuée. Sur base de ce constat, une proposition de renforcement est proposée : il

[49] "We build a model to capture the impact of secondary loss in structuring the use of cyber insurance and then combine the backward analysis of myriad breach scenarios to derive the overall optimal decision to purchase cyber insurance. We demonstrate that the optimal purchase decision depends on the mix of the types of cyber breaches that a firm faces. Numerical experiments corroborate market observation of limited use of cyber insurance after 20 years from when these products became available." (Tridib Bandyopadhyay and Vijay Mookerjee, 2017 : 1).

s'agit mettre en place les politiques et processus nécessaires à la bonne gestion des risques[50] et de former les membres de l'entreprise aux bonnes pratiques. Le troisième volet repose sur l'anticipation d'un incident et la gestion de celui-ci via des outils préparés en amont. Enfin, la dernière étape, qui est le transfert à un organisme tiers (assurance) va faire l'objet d'une attention croissante dans les années à venir. A l'heure actuelle, la nécessité de prendre une assurance spécifique, dédiée aux risques cyber résiduels ne fait pas l'objet d'un consensus dans la littérature.

8 Limites de ce mémoire

Ce mémoire s'inscrit dans une démarche de gestion des risques cyber au niveau managérial. Il n'aborde donc pas l'aspect du management de l'informatique du sujet, revers de la médaille de la réaction des entreprises face à la menace. Pour être tout à fait complet, il aurait fallu que celui-ci soit axé sur les deux faces de la médaille : tout d'abord, avec le côté management (les plans et outils, tels que définis dans ce mémoire), mais également les procédures à mettre en place au niveau informatique afin de circonscrire celle-ci, ainsi qu'éventuellement l'articulation entre ces deux choses. Ce deuxième côté, manquant, aurait pu compléter la première approche, ainsi qu'éventuellement la préciser et / ou la corriger.

Ensuite, la portée de ce travail est par définition générale : les catégories abordées (prévention, formation, gestion des risques, gestion des crises, etc) ne peuvent être vues que de manière « superficielle », étant donné qu'il existe des livres de plusieurs centaines de pages rien que sur la gestion des crises (par exemple). Ce choix méthodologique permet donc d'aborder les nombreux domaines nécessaires à la gestion des risques, mais de manière assez générale.

La deuxième partie de limites, qui sont cependant hors de ma méthodologie, est le caractère très évolutif du sujet, qui pourrait faire varier les outils proposés et en diminuer la pertinence, ainsi que la construction du sujet même. En effet, « *dans le contexte actuel d'absence de données et de statistiques significatives, le cyber risque demeure un risque très difficile à cerner, en particulier de par son caractère cumulatif et universel* » (APREF, 2016 : 6).

[50] Selon une rectification de Monsieur Gelissen Frédéric.

Cependant, un point d'attention a été porté concernant le fait de mettre à jour les outils, par définition toujours incomplets au vu de l'évolution du paysage numérique.

9 Conclusion

La menace cyber va véritablement être un des plus grands défis du 21ème siècle. De nombreux commentateurs déclarent par ailleurs qu'il ne s'agit pas de savoir si des cyberattaques vont se produire, mais « quand » elles vont se produire.

A travers l'historique des attaques, l'état des lieux des risques informatiques, ainsi que l'analyse des coûts engendrés par les brèches informatiques, j'ai tenté de montrer toute l'ampleur de ce phénomène et de sensibiliser le lecteur aux enjeux qui, certainement, prendront une importance croissante au fil du temps. La force d'une entreprise réside également dans son adaptation au paysage technologique, dans son accompagnement vis-à-vis des avancées et des progrès dans l'échange de l'information, même si ces domaines ne font pas partie du business habituel de l'entreprise.

C'est pourquoi, j'ai proposé, tout au long de ce mémoire, certains outils afin d'anticiper ce risque et de faire face au bouleversement occasionné par les avancées technologiques. Ces outils ont vocation à être adaptés, améliorés, complétés, et mis à jour, dans le même état d'esprit que (par exemple) l'évaluation des risques cyber existants à un instant « T » par l'entreprise. Face à la menace, une formation doit être prodiguée aux membres de l'entreprise, afin que ceux-ci contribuent, par leurs actions, à la protection des biens précieux de celle-ci. Conscient qu'une protection parfaite n'existe pas, j'ai proposé également un volet de gestion des crises, afin de faire face au mieux à l'adversité. Même si certaines entreprises, malgré la bonne sensibilisation du personnel aux enjeux et une bonne gestion des risques sont victimes d'un incident cyber, il reste en leur pouvoir de gérer convenablement les crises en amont, afin de limiter l'impact et d'envoyer des signaux forts concernant le fonctionnement de celle-ci.

J'ai tenté également de proposer, tout au long de la rédaction de ce mémoire, un recueil de la littérature existante sur le sujet, et gardé une fenêtre ouverte sur le futur développement du domaine par la présentation de solutions logicielles, non encore parfaitement abouties, ainsi que l'état des lieux de la réglementation, rejoignant le même état d'esprit que le thème de ce mémoire.

10 Bibliographie

10.1 Bibliographie de la littérature

- Agence du numérique. (2018). *Baromètre 2018 de maturité numérique des entreprises wallonnes*. Consulté sur https://content.digitalwallonia.be/post/20181212203954/Barometre_entreprises_2018_Digital_Wallonia.pdf
- Agence nationale de la sécurité des systèmes d'informations, ANSSI. (2018). La méthode Ebios Risk Manager. Consulté sur https://www.ssi.gouv.fr/administration/management-du-risque/la-methode-ebios-risk-manager/
- Allianz Global Corporate and Speciality, Allianz. (2015). *A Guide to Cyber Risk*. Consulté sur https://www.agcs.allianz.com/content/dam/onemarketing/agcs/agcs/reports/AGCS-Cyberrisk-report.pdf
- Amalberti, R. (2015). Sortir de l'impasse. *Tribune de la sécurité industrielle, 2015* (03), 1 – 4, https://www.foncsi.org/fr/publications/tribunes-securite-industrielle/sortir-impasse/tribune-2015-03[51]
- ARMS reliability. (2017). Beyond the risk Matrix. Consulté sur https://www.thereliabilityblog.com/2017/09/13/beyond-the-risk-matrix/
- Arpagian, N. (2016). *La Cybersécurité* (2e éd.). France : Presses Universitaires de France - PUF
- Association des professionnels de la réassurance en France, Apref. (2016). *Etude sur les « cyber risques » et leur (ré)assurabilité*. Consulté sur https://www.apref.org/sites/default/files/espacedocumentaire/note_apref_cyber_risque.pdf
- Bandyopadhyay, T et Mookerjee V. (2017). A model to analyze the challenge of using cyber insurance. *Information systems frontiers*, 1 – 25, https://doi.org/10.1007/s10796-017-9737-3[52]
- Cases Monarc. (s.d.). Introduction. Consulté sur https://www.monarc.lu/
- Centre for Cyber Security Belgium. (2019). Consulté sur https://www.cert.be/fr

[51] Il s'agit d'une tribune.

[52] Références du volume et numéro non disponibles.

- Centre for Cyber Security Belgium. (2016). Consulté sur https://www.safeonweb.be/
- Centre for Cyber Security Belgium. (s.d.). Evaluez vos actions. Consulté sur https://cyberguide.ccb.belgium.be/fr/evaluez-vos-actions
- Centre for Cyber Security Belgium. (s.d.). Protégez vos biens les plus précieux, https://cyberguide.ccb.belgium.be/fr/protegez-vos-biens-plus
- Centre National de Ressources Textuelles et Lexicales, CNRTL. (2012). Consulté sur http://www.cnrtl.fr/definition/monitoring
- Club de la sécurité de l'information français, CLUSIF. (2018). *Assurance des risques cyber, guide pratique*. Consulté sur https://clusif.fr/publications/assurance-risques-cyber-guide-pratique/
- Coursaget, A. et Haas, L. (2018). Le plan de continuité d'activité (PCA) : Approche méthodologique. *Sécurité et stratégie, 2014/3* (18), 13 – 20, https://www.cairn.info/revue-securite-et-strategie-2014-3-page-13.htm
- Combalbert, L. (2012). L'agilité des organisations dans la gestion des crises. *Sécurité et stratégie, 2012/3* (10), 42 – 48, https://www.cairn.info/revue-securite-et-strategie-2012-3-page-42.htm
- Combalbert, L et Delbecque E. (2012). *La gestion de crises* (1e éd.). France : Presses Universitaires de France - PUF
- Dauvin, E. (2018-2019). ELBEM102 : Gestion de la qualité [Présentation PDF]. Disponible sur : https://webcampus.unamur.be/my/
- De Laubier, C. (10 mars 2019). Le commerce électronique doit être régulé. Consulté sur https://www.lemonde.fr/economie/article/2019/03/10/le-commerce-electronique-doit-etre-regule_5434094_3234.html
- Deloitte. (2018). *La gestion de crise des entreprises résilientes*. Consulté sur https://www.deloitte-france.fr/formulaire/telechargement/la-gestion-de-crise-des-entreprises-resilientes
- Douzet, F et Héon S. (2013). L'analyse du risque cyber, emblématique d'un dialogue nécessaire. *Sécurité et stratégie, 2013/3* (14), 44 – 52, https://www.cairn.info/revue-securite-et-strategie-2013-3-page-44.htm
- ENISA, European Union Agency For Network And Information Security. (2019). *ECSM 2018 Deployment Report*. Consulté sur https://www.enisa.europa.eu/publications/ecsm-2018-deployment-report

- Esquema Nacional de Seguridad, ENS. (2014). *MAGERIT – version 3.0 Methodology for Information Systems Risk Analysis and Management*. Consulté sur https://docplayer.net/533733-Magerit-version-3-0-methodology-for-information-systems-risk-analysis-and-management-book-i-the-method.html
- European Union Agency For Network and Information Security, ENISA. *ENISA Threat Landscape Report 2018*. Consulté sur https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2018
- Cyber Security Coalition (2015). *Cyber security incident management guide*. Consulté sur https://www.cybersecuritycoalition.be/content/uploads/cybersecurity-incident-management-guide-EN.pdf
- France 2. (14 décembre 2017). Cyberattaques : les braqueurs de l'ombre. Consulté sur https://www.youtube.com/watch?v=JrFoFBNfv7A
- Garnier, J. (5 mars 2019). Quand les algorithmes révolutionnent le secteur de la beauté. Consulté sur https://www.lemonde.fr/economie/article/2019/03/05/les-maths-nouvelle-equation-du-secteur-de-la-beaute_5431396_3234.html
- Gemalto. (s.d.). Breach Level Index. Consulté sur https://breachlevelindex.com/data-breach-risk-assessment-calculator
- Hiscox Ltd. (2017). *The Hiscox Cyber Readiness Report 2017*. Consulté sur https://www.hiscox.co.uk/cyber-readiness-report/docs/cyber-readiness-report-2017.pdf
- Hiscox Ltd. (2018). *2018 Hiscox Cyber Readiness Report*. Consulté sur https://www.hiscox.com/sites/default/files/content/2018-Hiscox-Cyber-Readiness-Report.pdf
- IBM. (2016). *Reviewing a year of serious data breaches major attacks and new vulnerabilities*. Consulté sur https://www.ibm.com/downloads/cas/GN0D7O4N[53]
- ICC et al. (2016). *Guide Belge de la Cybersécurité*. Consulté sur https://www.vbo-feb.be/globalassets/publicaties/belgische-gids-voor-cyberveiligheid/cybersecurityfr.pdf
- Institut des actuaires. (2017). *Emergence du besoin en cyber assurance*. Consulté sur https://www.institutdesactuaires.com/global/gene/link.php?doc_id=12313&fg=1

[53] Pour des raisons non connues, cette source n'est plus disponible au moment de la réalisation de la bibliographie

- KPMG. (2018). *Building Cyber Resilience in Asset Management*. Consulté sur https://assets.kpmg/content/dam/kpmg/bm/pdf/2018/07/building-cyber-resilience-in-asset-management.pdf
- Lehu, J.M. (2018). Cyberattaque : la gestion du risque est-elle encore possible ?. *La revue des sciences de gestion, 2018/3-4* (291-292), 41 – 50, https://www.cairn.info/revue-des-sciences-de-gestion-2018-3-page-41.htm?contenu=resume
- McAfee. (2018). *Economic Impact of Cybercrime – not Slowing Down*. Consulté sur https://csis-prod.s3.amazonaws.com/s3fs-public/publication/economic-impact-cybercrime.pdf
- Menard, A. (s.d.). Gestion de crise en agroalimentaire : quels sont les bons réflexes ? Message posté sur https://reussirenagroalimentaire.wordpress.com/2012/07/10/gestion-de-crise-agroalimentaire-quels-sont-les-bons-reflexes/
- New York University, NYU. (Avril 2019). Index of Cybersecurity. Consulté sur http://cybersecurityindex.org/
- OCDE. (2015). *Digital Security Risk Management for Economic and Social Prosperity, OECD Recommendation and Companion Document*. Consulté sur https://read.oecd-ilibrary.org/science-and-technology/digital-security-risk-management-for-economic-and-social-prosperity_9789264245471-en#page1
- Organisation internationale de normalisation, ISO. (2018). Avant-propos. Consulté sur https://www.iso.org/obp/ui/#iso:std:iso-iec:27005:ed-3:v1:fr
- Organisation internationale de normalisation, ISO. (2008). Nouvelle norme ISO/CEI pour la gouvernance des technologies de l'information par l'entreprise. Consulté sur https://www.iso.org/fr/news/2008/06/Ref1135.html
- Organisation internationale de normalisation, ISO. (2018). Technologies de l'information -- Techniques de sécurité -- Gestion des risques liés à la sécurité de l'information. Consulté sur https://www.iso.org/fr/standard/75281.html
- Outil de consultation du Dictionnaire de l'Académie Française. (s.d.). Crise. Consulté sur https://academie.atilf.fr/9/consulter/crise?page=1
- Parsoire, D. (2015). *Cyberassurance : offres et solutions*. Consulté sur https://www.apref.org/sites/default/files/espacedocumentaire/2015-05-27_risques_-_101_parsoire.pdf

- Ponemon Institute LLC. (2017). *2017 Global Cyber Risk Transfer Comparison Report*. Consulté sur https://www.aon.com/forms/2017/2017-global-cyber-risk-transfer-comparison-report.jsp
- Roos, B. (12 janvier 2016). Gestion de crise SSI. Consulté sur https://www.lexsi.com/securityhub/gestion-de-crise-ssi/
- Ruelle, S. (2012). Continuité d'activité et gestion de crise : de la technique à l'humain. *Sécurité et stratégie, 2012/3* (10), 43 – 40, https://www.cairn.info/revue-securite-et-strategie-2012-3-page-32.htm
- SCOR. (2017). *Couverture du cyber risque, extrait de la revue d'économie financière n°126*. Consulté sur https://www.scor.com/sites/default/files/lacouvertureducyberrisque_fr.pdf
- Secureworks. (s.d.). Counter Threat Unit (CTU) Research Team. Consulté sur https://www.secureworks.com.au/about/counter-threat-unit
- SRC. (2018). *Technical service cybersecurity*. Consulté sur https://www.srcinc.com/pdf/Technical-Services-Cybersecurity.pdf
- Statista. (2019). *Cyber Insurance*. Consulté sur https://proxy.unamur.be:2391/study/27800/cyber-insurance-statista-dossier/[54]
- Union Européenne, UE. (2016). *Journal officiel de l'Union Européenne, Parlement Européen. RÈGLEMENT (UE) 2016/679 DU PARLEMENT EUROPÉEN ET DU CONSEIL*. Consulté sur https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32016R0679
- Union Européenne, UE. (s.d.). Règlements, directives et autres actes législatifs. Consulté sur https://europa.eu/european-union/eu-law/legal-acts_fr
- Union Européenne, UE. (2016). *Règlement (UE) 2016/679 du parlement européen et du conseil, RGPD, Règlement Général sur la Protection des Données*. Consulté sur http://www.ipcf.be/uploads/documents/Verordening_FR_inhoud.pdf
- Untersinger, M. (29 Janvier 2019). Quelle est la bonne équation pour pacifier le cyberespace ?. Consulté sur https://www.lemonde.fr/pixels/article/2019/01/29/course-aux-cyberarmes-logiciels-destructeurs-dormants-le-difficile-apaisement-du-cyberespace_5416003_4408996.html

[54] Il s'agit d'un dossier compilé.

❖ Ventre, D. (2016). De l'utilité des indices de cybersécurité. *Sécurité et stratégie*, *2016/2* (22), 5 – 11, https://www.cairn.info/revue-securite-et-strategie-2016-2-page-5.htm

10.2 Bibliographie des figures

Figure 1 : New York University, NYU. (Avril 2019). Index of Cybersecurity. Consulté sur http://cybersecurityindex.org/

Figure 2 : Hiscox Ltd. (2018). *2018 Hiscox Cyber Readiness Report*. Consulté sur https://www.hiscox.com/sites/default/files/content/2018-Hiscox-Cyber-Readiness-Report.pdf

Figure 3 : Hiscox Ltd. (2018). *2018 Hiscox Cyber Readiness Report*. Consulté sur https://www.hiscox.com/sites/default/files/content/2018-Hiscox-Cyber-Readiness-Report.pdf

Figure 4 : Association des professionnels de la réassurance en France, Apref. (2016). *Etude sur les « cyber risques » et leur (ré)assurabilité*. Consulté sur https://www.apref.org/sites/default/files/espacedocumentaire/note_apref_cyber_risque.pdf

Figure 5 : Hiscox Ltd. (2018). *2018 Hiscox Cyber Readiness Report*. Consulté sur https://www.hiscox.com/sites/default/files/content/2018-Hiscox-Cyber-Readiness-Report.pdf

Figure 6 : Hiscox Ltd. (2018). *2018 Hiscox Cyber Readiness Report*. Consulté sur https://www.hiscox.com/sites/default/files/content/2018-Hiscox-Cyber-Readiness-Report.pdf

Figure 7 : Mortureux, Y. (2013). *Heinrich et Bird, la malédiction des pyramides, Un problème de géométrie ?*. Consulté sur https://www.foncsi.org/fr/blog/nouvelle-tribune-interpretation-pyramide/image/image_view_fullscreen

Figure 8 : KPMG. (2018). *Building Cyber Resilience in Asset Management*. Consulté sur https://assets.kpmg/content/dam/kpmg/bm/pdf/2018/07/building-cyber-resilience-in-asset-management.pdf

Figure 9 : OCDE. (2015). *Digital Security Risk Management for Economic and Social Prosperity, OECD Recommendation and Companion Document*. Consulté sur https://read.oecd-ilibrary.org/science-and-technology/digital-security-risk-management-for-economic-and-social-prosperity_9789264245471-en#page1

Figure 10 : ARMS reliability. (2017). Beyond the risk Matrix. Consulté sur https://www.thereliabilityblog.com/2017/09/13/beyond-the-risk-matrix/

Figure 11 : KPMG. (2018). *Building Cyber Resilience in Asset Management*. Consulté sur https://assets.kpmg/content/dam/kpmg/bm/pdf/2018/07/building-cyber-resilience-in-asset-management.pdf

Figure 12 : OCDE. (2015). *Digital Security Risk Management for Economic and Social Prosperity, OECD Recommendation and Companion Document*. Consulté sur https://read.oecd-ilibrary.org/science-and-technology/digital-security-risk-management-for-economic-and-social-prosperity_9789264245471-en#page1

Figure 13 : Centre for Cyber Security Belgium. (s.d.). Protéger vos biens les plus précieux, https://cyberguide.ccb.belgium.be/fr/protegez-vos-biens-plus

Figure 14 : Institut des actuaires. (2017). *Emergence du besoin en cyber assurance*. Consulté sur https://www.institutdesactuaires.com/global/gene/link.php?doc_id=12313&fg=1

Figure 15 : Menard, A. (s.d.). Gestion de crise en agroalimentaire : quels sont les bons réflexes ? Message posté sur https://reussirenagroalimentaire.wordpress.com/2012/07/10/gestion-de-crise-agroalimentaire-quels-sont-les-bons-reflexes/

Figure 16 : Cyber Security Coalition. (2015). *Cyber security incident management guide*. Consulté sur https://www.cybersecuritycoalition.be/content/uploads/cybersecurity-incident-management-guide-EN.pdf

Figure 17 : Coursaget, A. et Haas, L. (2018). Le plan de continuité d'activité (PCA) : Approche méthodologique. *Sécurité et stratégie, 2014/3* (18), 13 – 20, https://www.cairn.info/revue-securite-et-strategie-2014-3-page-13.htm

Figure 18 : Cyber Security Coalition. (2015). *Cyber security incident management guide*. Consulté sur https://www.cybersecuritycoalition.be/content/uploads/cybersecurity-incident-management-guide-EN.pdf

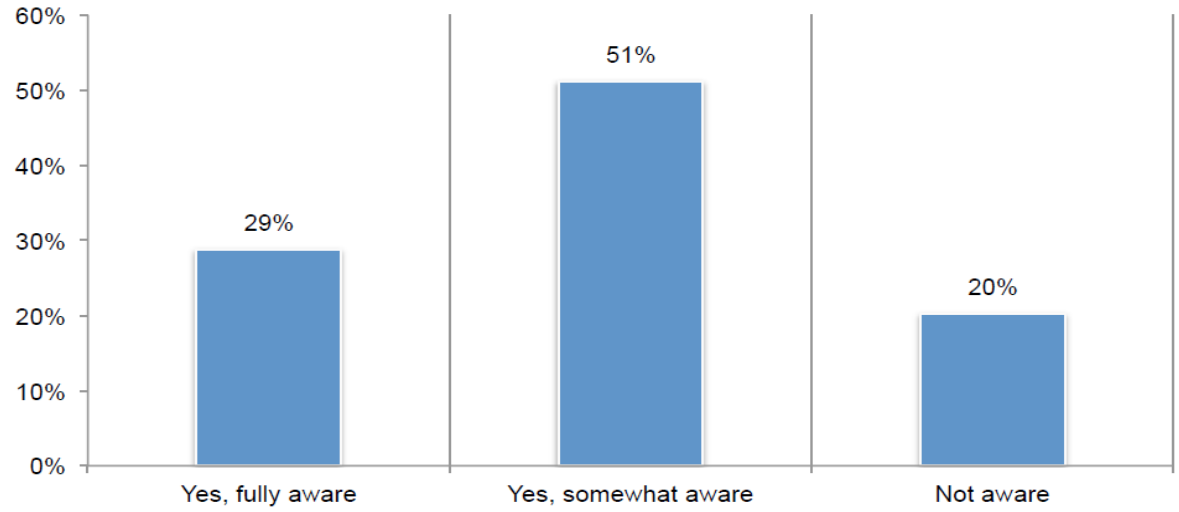
Figure 19 : Statista. (2019). *Cyber Insurance*. Consulté sur https://proxy.unamur.be:2391/study/27800/cyber-insurance-statista-dossier/

11 Annexe

11.1 Figure

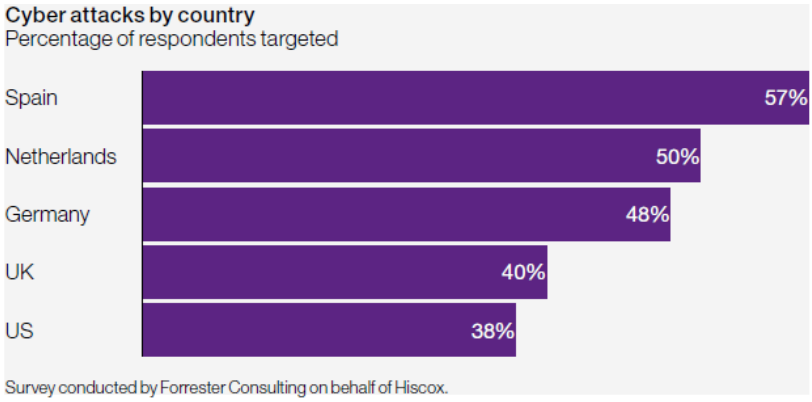
Figure A :

Figure 8. Awareness of the economic and legal consequences from an international data breach or security exploit



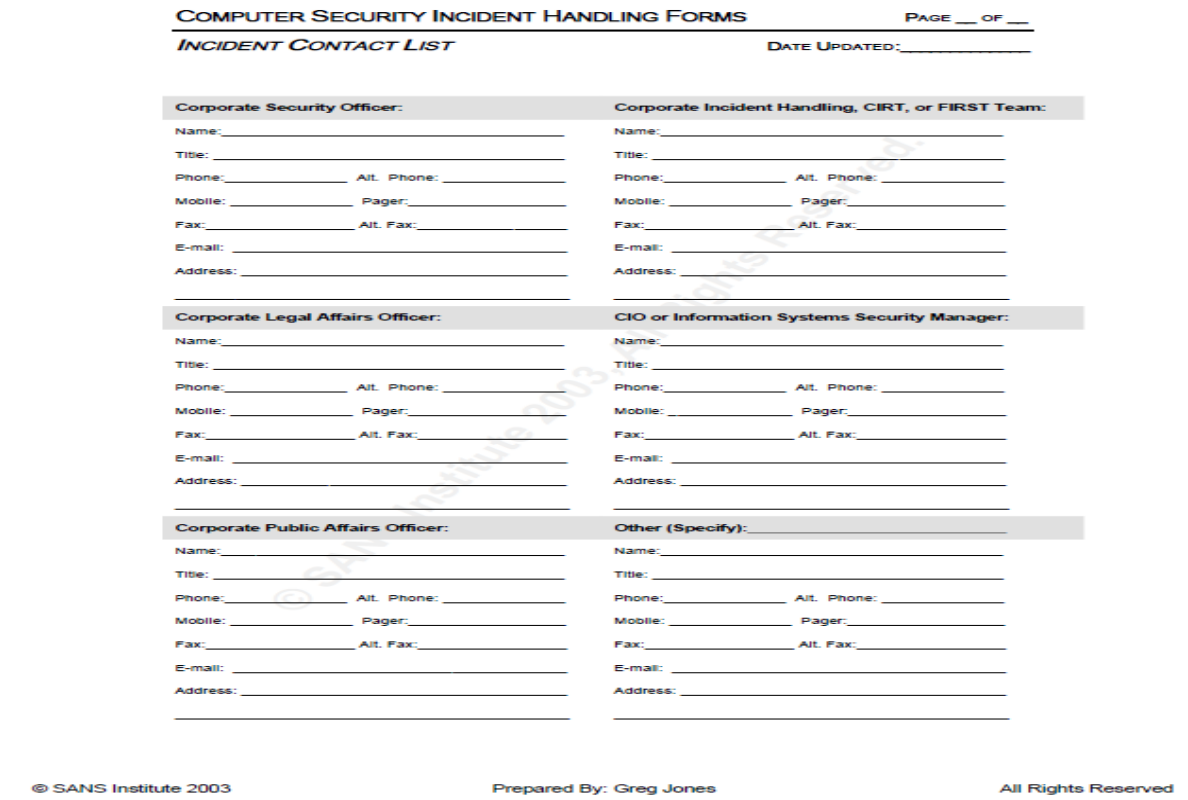
Source : Ponemon Institute LLC. (2017). *2017 Global Cyber Risk Transfer Comparison Report*. Consulté sur https://www.aon.com/forms/2017/2017-global-cyber-risk-transfer-comparison-report.jsp

Figure B :



Source : Hiscox Ltd. (2018). *2018 Hiscox Cyber Readiness Report*. Consulté sur https://www.hiscox.com/sites/default/files/content/2018-Hiscox-Cyber-Readiness-Report.pdf

Figure C :



COMPUTER SECURITY INCIDENT HANDLING FORMS PAGE __ OF __

INCIDENT CONTACT LIST DATE UPDATED:_____

Corporate Security Officer:
Name:_____
Title: _____
Phone:_____ Alt. Phone: _____
Mobile: _____ Pager:_____
Fax:_____ Alt. Fax:_____
E-mail: _____
Address: _____
_____

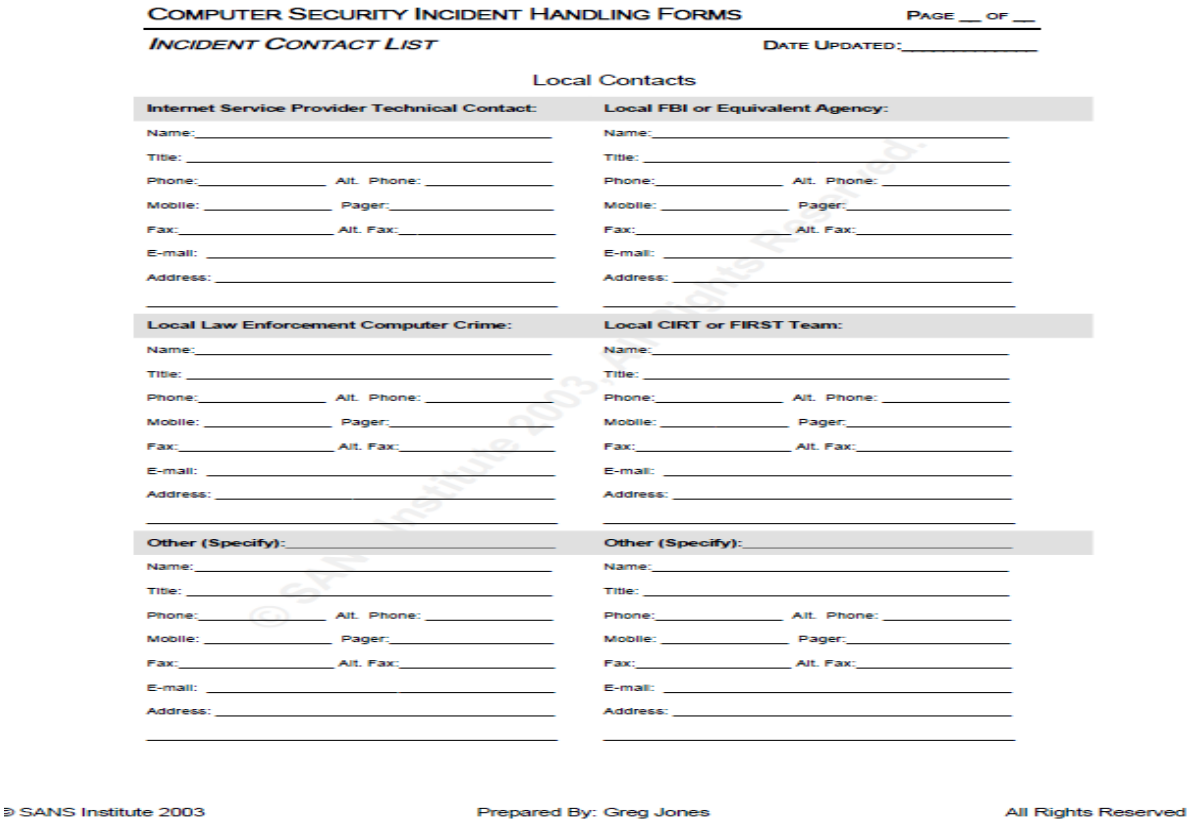
Corporate Incident Handling, CIRT, or FIRST Team:
Name:_____
Title: _____
Phone:_____ Alt. Phone: _____
Mobile: _____ Pager:_____
Fax:_____ Alt. Fax:_____
E-mail: _____
Address: _____
_____

Corporate Legal Affairs Officer:
Name:_____
Title: _____
Phone:_____ Alt. Phone: _____
Mobile: _____ Pager:_____
Fax:_____ Alt. Fax:_____
E-mail: _____
Address: _____
_____

CIO or Information Systems Security Manager:
Name:_____
Title: _____
Phone:_____ Alt. Phone: _____
Mobile: _____ Pager:_____
Fax:_____ Alt. Fax:_____
E-mail: _____
Address: _____
_____

Corporate Public Affairs Officer:
Name:_____
Title: _____
Phone:_____ Alt. Phone: _____
Mobile: _____ Pager:_____
Fax:_____ Alt. Fax:_____
E-mail: _____
Address: _____
_____

Other (Specify):_____
Name:_____
Title: _____
Phone:_____ Alt. Phone: _____
Mobile: _____ Pager:_____
Fax:_____ Alt. Fax:_____
E-mail: _____
Address: _____
_____



COMPUTER SECURITY INCIDENT HANDLING FORMS PAGE __ OF __

INCIDENT CONTACT LIST DATE UPDATED:_____

Local Contacts

Internet Service Provider Technical Contact:
Name:_____
Title: _____
Phone:_____ Alt. Phone: _____
Mobile: _____ Pager:_____
Fax:_____ Alt. Fax:_____
E-mail: _____
Address: _____
_____

Local FBI or Equivalent Agency:
Name:_____
Title: _____
Phone:_____ Alt. Phone: _____
Mobile: _____ Pager:_____
Fax:_____ Alt. Fax:_____
E-mail: _____
Address: _____
_____

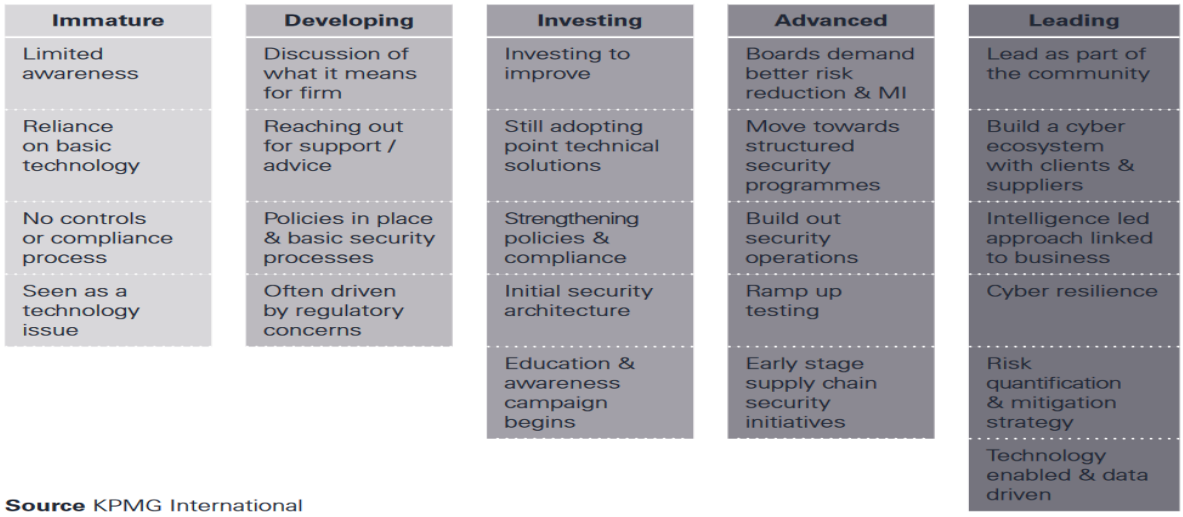
Local Law Enforcement Computer Crime:
Name:_____
Title: _____
Phone:_____ Alt. Phone: _____
Mobile: _____ Pager:_____
Fax:_____ Alt. Fax:_____
E-mail: _____
Address: _____
_____

Local CIRT or FIRST Team:
Name:_____
Title: _____
Phone:_____ Alt. Phone: _____
Mobile: _____ Pager:_____
Fax:_____ Alt. Fax:_____
E-mail: _____
Address: _____
_____

Other (Specify):_____
Name:_____
Title: _____
Phone:_____ Alt. Phone: _____
Mobile: _____ Pager:_____
Fax:_____ Alt. Fax:_____
E-mail: _____
Address: _____
_____

Other (Specify):_____
Name:_____
Title: _____
Phone:_____ Alt. Phone: _____
Mobile: _____ Pager:_____
Fax:_____ Alt. Fax:_____
E-mail: _____
Address: _____
_____

Source : SANS Institute. (2003). *Computer Security Incident Handling Form*. Consulté sur https://www.sans.org/media/score/incident-forms/IH-Contacts.pdf



Source : KPMG. (2018). *Building Cyber Resilience in Asset Management*. Consulté sur https://assets.kpmg/content/dam/kpmg/bm/pdf/2018/07/building-cyber-resilience-in-asset-management.pdf

Figure D :

Metric Name	What Is Measured?	How Is It Measured?	When Is It Measured?	Who Measures?	Details
Phishing Awareness	Number of people who fall victim to a phishing simulation. The definition of falling victim is clicking on the link or opening an attachment.	Phishing assessment	Monthly	Security Team	These attacks replicate the very same ones cyber attackers are using. The goal is to measure who falls victim to such attacks. This number should decrease over time as behaviors change.
Phishing Reporting	Number of people who detect and report a phishing email (regardless of whether it's an assessment or real attack).	Phishing assessment	Monthly	Security Team	Uses the above methodology, but instead of tracking who falls victim, it tracks who identifies the attacks and reports them. This number should increase over time. This is developing the Human Sensor.
Phishing Repeat Offenders	Number of workforce that repeatedly fall victim to phishing simulations. These individuals are not changing behavior and represent a high risk.	Phishing assessment	Monthly	Security Awareness Team	These individuals represent a high risk to an organization and must be addressed. This can include an escalation in training and consequences, being moved to a different job role or department, or being managed in some other way.
Facility Physical Security	Number of employees who understand, follow, and enforce your policies for restricted or protected access to facilities.	Test how many employees are wearing their badges or stopping those who are not.	Monthly or weekly	Information Security or Physical Security	For many organizations, physical security is a major control in reducing risk, especially when dealing with secured facilities. This metric will test and measure people's understanding and enforcement of this control.
Updated Devices	Percentage of devices that are updated and current.	When employees connect to an internal server or use an external service such as browsercheck.qualys.com	Monthly	Security or Technology Team	Measure whether people are keeping their devices updated and current, especially when concerning BYOD (Bring Your Own Device).
Lost/Stolen Devices	Number of devices (laptops, smartphones, tablets) that were lost or stolen. What percentage of those devices were encrypted?	Reports to security team or by physical asset audits	Monthly	Security Team or Asset Management	Employees should be trained in maintaining physical security of their devices. In addition, if your organization has policies on the use of encryption for devices, this measures whether employees are following them.
Secure Desktop	Number of employees who are securing their desk environment before leaving, as per organizational policy.	Nightly walkthrough	Monthly or weekly	Information Security or Physical Security Team	Security team does a walkthrough of organizational facilities, checking each desktop or separate work environment, and looking to ensure individuals are following organizational desktop policy.
Passwords	Number of employees using strong passwords.	Password brute forcing	Monthly or quarterly	Security Team	Security gains authorized access to system password database (such as AD or Unix server) and attempts to brute force or crack password hashes.

Source : SANS Institute. (s.d.). Security Awereness. Consulté sur https://www.sans.org/security-awareness-training/resources/security-awareness-planning-toolkit

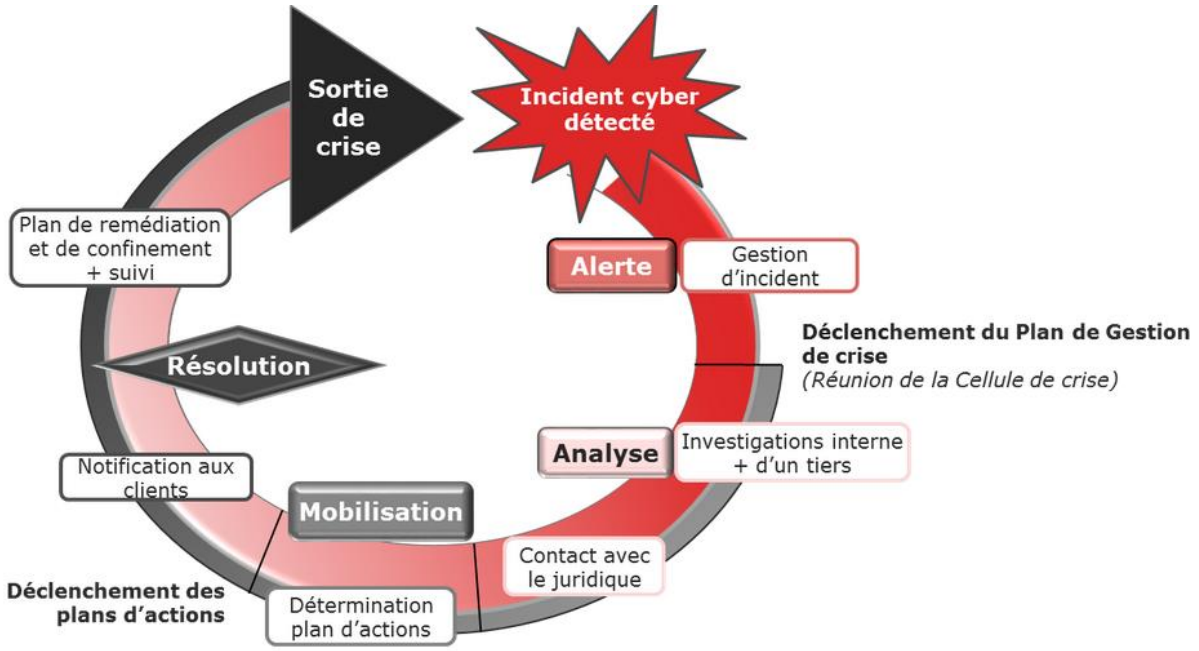
Figure E :

SKILLS	RESPONSIBILITIES	ROLES
Incident management	Manage the cyber security incident from the moment of its detection until its closure.	Cyber security Incident response manager
Business decision capability	Assessing the business impact and act upon it. Engage the right resources. Take decisions on how to proceed e.g. decide if the internet connection of a compromised system can be shut down and when is the most appropriate time. Decide when to start clean-up activities. Decide whether to file a complaint or not.	Management
Network management capabilities	Technical know-how on the organisation's network (firewall, proxies, IPS, routers, switches,…). Analyse, block or restrict the data flow in and out of your network. IT operations Information security and business continuity	ICT technical support staff
Workstation and server administrator capabilities (admin rights)	Analyse and manage compromised workstations and servers.	ICT technical support staff
Legal advice	Assess the contractual and judicial impact of an incident.Guarantee that incident response activities stay within legal, regulatory and the organisation's policy boundaries. Filing a complaint.	Legal department/company lawyer
Communication skills	Communicate in an appropriate way to all concerned stakeholder groups. Answer customer, shareholders, press questions right away.	Communications or Public Relations department
Forensic skills	Gather and analyse evidence in an appropriate way i.e. in a way that the evidence is acceptable by a court of law	ICT technical support staff
Physical security	Handle the aspects of the incident that are linked to • the physical access to the premises • the physical protection of the cyber infrastructure.	Security Officer
Crisis management	Crisis management	Crisis manager

Source : Cyber Security Coalition. (2015). *Cyber security incident management guide*. Consulté sur https://www.cybersecuritycoalition.be/content/uploads/cybersecurity-incident-management-guide-EN.pdf

Comparatif gestion de crise en SSI (1°) et gestion de crise normale (2°) :

(1°)



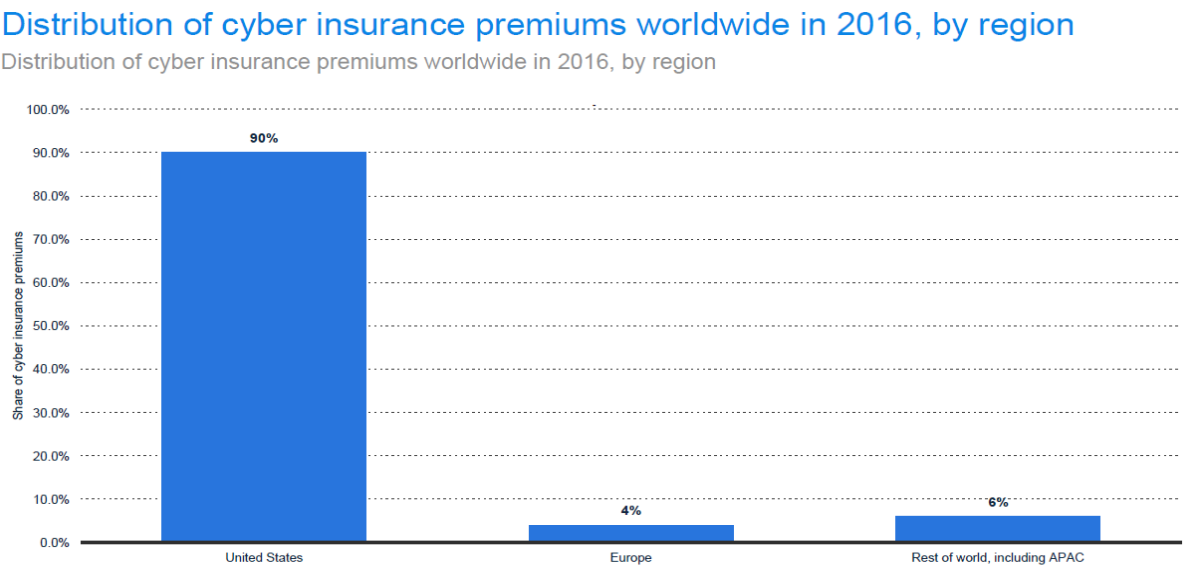
(2°)

Comparatif : il est à remarquer qu'au niveau des procédures, l'étape 3,4,5,6 se trouvent également dans le premier schéma, qui débute avec le déclenchement du plan de gestion de crise. Le schéma n°2 est plus complet, car il englobe la préparation en amont de la crise, bien que le schéma n°1 la mentionne implicitement, par l'existence de plan préparés.

Source (1°) : Roos, B. (2016). Gestion de crise SSI. Consulté sur https://www.lexsi.com/securityhub/gestion-de-crise-ssi/

Source (2°) : Menard, A. (s.d.). Gestion de crise en agroalimentaire : quels sont les bons réflexes ? Message posté sur https://reussirenagroalimentaire.wordpress.com/2012/07/10/gestion-de-crise-agroalimentaire-quels-sont-les-bons-reflexes/

Figure G :



Source : Statista. (2019). *Cyber Insurance*. Consulté sur https://proxy.unamur.be:2391/study/27800/cyber-insurance-statista-dossier/

11.2 Revue du mémoire par un professionnel de la cybersécurité

J'ai eu l'opportunité de présenter mon mémoire à un professionnel, Frédéric Gelissen, faisant partie d'une entreprise proposant des services de consultance en matière de cybersécurité, afin d'avoir une expertise externe sur ce sujet. Celui-ci occupe le poste de « Governance leader – gérant associé » au sein de Procsima - group.

En soulignant la qualité, d'après lui, de ce travail, il m'a fait part de commentaires ponctuels, annotations qu'il a effectuées sur le document. Parmi les choses qui sont plus structurelles (hors commentaires particuliers sur un point précis), il a énoncé, au début du point concernant les bonnes pratiques à adopter, le nécessaire engagement des dirigeants, ainsi que du « middle management » à acquérir avant de s'attaquer à l'implication des employés, par ailleurs tout à fait nécessaire. L'engagement, dans ce cadre, devrait être pensé plus selon une approche « top-down » ; c'est-à-dire s'assurer de l'engagement des preneurs de décisions, avant celui des employés. C'est un point que j'avais également lu dans la littérature mais n'avais pas développé.

Un autre élément digne d'attention est la remarque concernant la précision à apporter par rapport aux rôles ainsi qu'aux personnes assignées à la gestion des risques. Ainsi, le CISO (Chief Information Security Officer) est responsable de la sécurité des systèmes, le Risk Manager s'occupe de la gestion des risques et de son registre, le Continuity Manager a pour rôle de gérer les plans de continuité, etc. C'est effectivement une remarque que je m'étais faite également lors de la rédaction du mémoire, mais je n'avais pu trouver de source détaillée à ce sujet provenant de rapports ou de la littérature.

En creusant davantage la délimitation entre la gestion des crises et celle des incidents, Monsieur Frédéric Gelissen m'a signalé également, bien que la gestion des incidents ne fasse pas partie de mon mémoire, que ceux-ci peuvent servir d'indicateurs concernant la vulnérabilité d'une entreprise. Ainsi, dans le cas où leur nombre est élevé, cela signifie que les procédures de protection contre les risques sont à revoir.

Dans la partie des cyber assurances, Monsieur Frédéric Gelissen m'a fait part du fait que les assurances faisaient désormais appel à un auditeur externe concernant la mise en place de mesures de gestion des risques. Ainsi, cette intervention permet de tarifer les primes d'assurance, abolissant le problème de tarification de leur offre.