UCL Université catholique de Louvain

LOUVAIN School of Management

Louvain School of Management

La cyber-sécurité dans les institutions financières : Comment se prémunir contre le cyber-risque et développer un environnement cyber-résilient ?

Mémoire recherche réalisé par
Stéphane REIS

en vue de l'obtention du titre de
Master 120 crédits en sciences de gestion, à finalité spécialisée (ou à finalité approfondie)

Promoteur(s)
Luc HENRARD

Année académique 2016-2017

Avant-propos et remerciements.

Ce mémoire conclut mes études et ce fut une expérience enrichissante que de le réaliser tant par les connaissances acquises que par la mise en pratique d'une méthodologie de travail particulière.

Je souhaiterais remercier mon promoteur, le professeur Luc Henrard pour m'avoir guidé le long de ce mémoire, mais surtout pour les interviews que je n'aurais jamais eu sans lui. Je souhaiterais également remercier mes professeurs du bachelier en Sciences-Politiques pour l'ouverture d'esprit que j'ai pu gagner en suivant ce cursus, mais également les professeurs de finance à la L.S.M sans qui je n'aurais jamais pu compléter une certaine vision du monde.

Je souhaiterais également remercier les nombreux amis que j'ai pu rencontrer tout au long de ces années à commencer par Kevin Borlée et Jonathan Borlée, qui m'ont supporté financièrement et moralement dans les moments difficiles, mais aussi Alexandre Leclercq pour son soutien indéfectible ces 3 dernières années.

« Débrouillard à jamais », Damso.

1 Table des matières

1 Introduction générale.

1.1 La cyber sécurité dans les institutions financières : vue d'ensemble.

La cyber sécurité est une priorité absolue dans l'industrie financière qui cherche à assurer la sécurité de ses actifs et de ses informations ainsi que l'exécution efficace et fiable des transactions sur les marchés. Dans un monde de plus en plus interconnecté et digitalisé, les chefs d'entreprise se doivent d'être plus conscients des diverses cyber-menaces auxquelles ils sont confrontés. Ils se doivent également d'être proactifs en ce qui concerne la protection de leurs clients, leurs données, leurs réseaux ainsi que leurs opérations contre le vol, l'interruption, la perturbation et la destruction.
Des criminels motivés par le gain financier aux Etats-nations, accusés d'espionnage d'entreprises ou cherchant à déstabiliser les marchés, les cyber-menaces deviennent de plus en plus sophistiquées dans leurs méthodes d'attaque. Cela place la cyber-sécurité au rang des risques qui doivent être gérés activement par les entreprises au même titre que d'autres menaces.

Selon une enquête de PwC (2016), la cyber-criminalité aurait bondi au deuxième rang des crimes économiques les plus signalés et les institutions financières en sont les premières cibles (SecurityScorecard, 2016). En témoigne le cyber-braquage de la banque centrale du Bangladesh qui a été piratée par une équipe de pirates informatiques sophistiqués qui a infiltré le réseau de la banque afin d'y installer un logiciel malveillant. Grâce à ce logiciel, l'équipe de pirates a pu obtenir les identifiants de la banque qui permettent de se connecter au réseau mondial de télécommunication interbancaire (SWIFT). La connexion à ce réseau de communication utilisé par les institutions financières a permis aux pirates de dérober la somme de $80 millions de dollars.

Ceci met en évidence la nécessité de protéger les systèmes et les réseaux de manière systémique et pas seulement de manière individuelle.

Il s'agit, dès lors, pour les entreprises, de prendre en compte à la fois les aspects techniques de la menace aussi bien interne qu'externe à leur organisation ainsi que d'aborder le problème à tous les niveaux managériaux de l'organisation.

1.2 Cyber-risque et Cyber-Sécurité : Définition du problème.

Nous vivons dans un monde interconnecté et cette tendance ne cessera d'augmenter avec notamment l'internet des objets qui devient une réalité. Dans ce contexte, la capacité des institutions financières à fournir des services à leurs clients, à poursuivre leurs activités quotidiennes, à commercer et à être compétitif dépend de leur habileté à exploiter, gérer et traiter l'information afin de créer un environnement cyber-résilient.

McAfee (2014) estime que le coût annuel pour l'économie mondiale s'élève à plus de 400 milliards de dollars. Bien que ces estimations varient selon les sources, l'estimation la plus prudente représente bien plus que le produit intérieur de certains pays du monde (McAfee, 2014).

Il ne s'agit pas d'un problème devant être délégué au seul département IT comme étant un risque à part, l'ingrédient clé pour une gestion efficace des risques opérationnels étant le soutient du top management (Hull, 2012) et l'instauration d'un cadre de gestion du risque de l'entreprise[1] englobant la totalité des intervenants de l'entreprise.

1.3 Objectifs de la recherche.

L'objectif de cette recherche est de contribuer modestement à la théorie de la gestion des risques en dévoilant comment le cyber-risque peut s'insérer dans le cadre plus large de gestion des risques opérationnels définis par Bâle II afin de le modéliser. Le but sera également de faire l'état des lieux de l'approche actuelle du management du cyber-risque

1 Entreprise Risk Management en anglais ou encore ERM.

afin de fournir une taxonomie, une structure et un cadre conceptuel permettant la gestion efficace de celui-ci. Mais aussi évaluer comment ce risque pourrait être mitigé. Le but final étant de proposer un modèle robuste aboutissant à des mesures du risque robustes qui autorisent des comparaisons efficaces permettant ainsi de prendre des décisions informées dans le but d'obtenir une gestion active du cyber-risque.

1.4 Cadre théorique.

Cette recherche se fondera sur le concept de gestion du risque de l'entreprise plus communément connu sous les termes « Entreprise Risk Management » (ERM). Ce cadre conceptuel implique la spécification de l'appétit au risque ou du niveau de tolérance au risque, la création d'une culture forte du management du risque au travers de toute l'organisation et l'implication des cadres supérieurs.
Quant à la modélisation, elle trouvera ses fondements dans le concept de VaR ou « Value at Risk » qui correspond au montant des pertes qui ne devrait être excédé qu'avec une probabilité donnée sur un horizon temporel donné (Hull, 2012). Cette notion est utilisée par les régulateurs des institutions financières et par les institutions financières afin de déterminer le capital économique – le capital requis pour protéger le groupe de l'insolvabilité économique sur une période de un an et qui peut être également utilisée comme une mesure du risque (Henrard, 2009) –. La Var donnera naissance au concept de cyber-Var.

1.4.1 Limite de la recherche.

Le domaine de la cyber-sécurité en général reste très compliqué à saisir de par sa nature polymorphe et par son environnement très dynamique et changeant (Geers, 2011). Ce fût dès lors un défi de construire une recherche qui trouve écho sur le long terme, car la technologie à venir ne sera plus la même que celle d'aujourd'hui notamment avec le big data, le « machine learning » et autres intelligences artificielles. La recherche ne rentrera pas

dans le détail quant à la modélisation du cyber-risque, il s'agira plutôt d'aborder les différentes méthodes pour en dégager des bonnes pratiques.

1.5 Questions de recherche.

Afin de soutenir l'objectif de la recherche et atteindre le résultat escompté, ce mémoire comportera une question principale :

- Comment rendre l'environnement bancaire cyber-résilient ?

Dans le but de répondre à cette question, le chercheur répondra également à trois sous questions :

- Quelle approche managériale pour la gestion du cyber-risque dans l'industrie bancaire ?
- Comment modéliser ce risque ?
- Quels outils et quelles stratégies pour réduire ce risque ?

1.6 Méthodologie de recherche.

Cette recherche adoptera un paradigme pragmatique et se fonde sur les méthodes de la recherche axée sur la conception ou « research design » en anglais (Andersen et Shattuck, 2012 ; Reeves et McKenney, 2013 ; Herrington et Oliver, 2005). Les données seront principalement qualitatives par nature et une logique inductive sera utilisée afin de conduire la recherche.
Les données collectées se fondent sur la littérature académique, sur les rapports de l'industrie, ainsi que sur différentes interviews trouver en utilisant des moteurs de recherche.

Comme expliqué, la recherche se base sur la méthode de la conception ou « design-based research ». Cette méthode permet de balancer entre les conceptions positivistes et interprétatives. Elle possède également l'avantage de tenter de combler les lacunes entre la théorie et la pratique d'où le choix de celle-ci dans le cadre de ce mémoire. En effet, elle

mêle les méthodes d'observations empiriques à la théorie qui régit un certain environnement. Dans ce cas-ci, l'environnement cyber des banques. Elle permet ainsi de répondre à la question de recherche principale qui est : Comment rendre l'environnement bancaire cyber-résilient ?

Cette méthodologie est importante pour comprendre comment, quand et pourquoi la théorie fonctionne ou ne fonctionne pas en pratique et permet aussi de découvrir les relations entre la théorie et la pratique.

1.7 Structure de la recherche.

L'introduction générale met en contexte le sujet avant de définir la problématique de recherche. Elle donne une idée générale à propos de la recherche en incluant notamment les objectifs ainsi que le cadre théorique de la thèse. En lisant l'introduction générale, le lecteur comprendra le plan de recherche et sera ainsi prêt pour le reste de l'étude.

La deuxième partie fera le tour de l'état de l'art afin de construire une revue de littérature solide qui sera confrontée aux interviews menées dans deux banques dans la troisième partie. Elle fera un bref historique de la question portant sur la cyber-sécurité pour finalement définir les différents concepts utilisés pour la réalisation de ce mémoire.

Dans la troisième partie, les données concernant les interviews seront présentées lors d'une analyse descriptive pour finalement être comparées et mettre en lumière les découvertes.

Finalement, la dernière partie conclura la recherche et fournira des éléments pour des recherches futures.

2 Revue de littérature.

2.1 Introduction : Historique de la Cyber-Sécurité (Julian, 2014).

Des vers et des virus aux DDOS[2] et APT[3]. Au cours du dernier quart de siècle, la sophistication, l'impact et l'ampleur des cyber-attaques ont considérablement évolué. Cependant, comme la cyber-criminalité est devenue plus sophistiquée, la sécurité l'est devenue aussi. Cet aperçu historique retrace les étapes importantes de ces 25 dernières années caractérisant la manière dont le paysage de la menace a évolué et celle dont la sécurité s'est développée en réponse (Julian, 2014).

2.1.1 Le premier ver informatique (fin des années 1980 - début des années 1990).

En 1989, Robert Morris crée ce qui est maintenant largement reconnu comme le premier ver informatique. Ce virus auto-propagateur s'est propagé de manière si agressive et rapide qu'il a réussi à fermer la majeure partie d'Internet. Alors que d'autres attaques ultérieures ont gagné beaucoup plus en notoriété, le ver Morris a été un incident historique en ce sens que c'était la première attaque généralisée utilisant le déni de service (DoS). En raison des débuts d'internet à l'époque, l'impact de ce ver était conséquent et dévastateur. Cependant, il a jeté les bases de la sécurité tel que nous la connaissons aujourd'hui (Julian, 2014).

2.1.2 Les premiers virus (années 1990)

À partir de ces années-là, les virus ont continué à faire la une des journaux. Le virus « Melissa » et « ILOVEYOU » ont infecté des dizaines de millions de PC provoquant ainsi l'échec des systèmes de messagerie dans le monde entier. Et cela avec peu d'objectifs stratégiques ou de motivation financière claire. Ces menaces ont conduit au développement de technologies antivirus afin de repérer la signature du virus et de l'empêcher de s'exécuter. Tout aussi importantes, ces menaces ont également joué un rôle important en

[2] DdoS: Denial of Service attack.
[3] APT: Advanced persistent threat.

sensibilisant les utilisateurs d'ordinateurs aux risques liés à la lecture de courriels provenant de sources non fiables et à l'ouverture de leurs pièces jointes. Cette réalisation n'a pas été dans les entreprises, car il est devenu évident que, si les virus devaient se répandre à partir des comptes de courrier électronique de l'entreprise, des questions sur la sécurité et l'intégrité de l'entreprise pourraient être mises en évidence (Julian 2014).

2.1.3 Cartes de crédit sous attaque (fin des années 2000)

À mesure que nous nous sommes installés dans le nouveau millénaire, les choses ont radicalement changé au fur et à mesure que les cyber-attaques sont devenues plus ciblées. Notamment avec les premières brèches de données concernant des numéros de carte de crédit. Entre 2005 et 2007, Albert Gonzalez vole des informations provenant d'au moins 45,7 millions de cartes de paiement utilisées par les clients du détaillant américain TJX, propriétaire de TJ Maxx et TK Maxx au Royaume-Uni. Il s'agissait d'une brèche massive de sécurité sur une échelle qui était auparavant inconnue et a souligné l'impact énorme que de telles infractions peuvent avoir. Cette brèche coûterait à la société quelque 256 millions de dollars (Julian, 2014).

C'est là que les choses sont devenues plus sérieuses. Les données impliquées dans ces infractions ont été réglementées et, par conséquent, les incidents ont nécessité la notification des autorités et des fonds destinés à indemniser les victimes. Les entreprises ont découvert de manière difficile les conséquences désastreuses d'être non protégées et ont commencé à s'armer avec des systèmes de sécurité plus sophistiqués spécialement conçus pour faire face à cette nouvelle réalité (Julian, 2014).

2.1.4 Les attaques ciblées et la menace systémique (de nos jours)

L'évolution rapide de la menace et l'escalade de l'échelle de la violation de données — dont les 40 millions de cartes de crédit volées chez Target[4] — ont façonné le paysage de la cyber-sécurité tel que nous le connaissons aujourd'hui.

Tout d'abord, d'un point de vue technique, cette attaque a été beaucoup plus sophistiquée que l'incident TJX et perpétrée par des criminels qui ont compris que, pour atteindre leurs objectifs, il ne serait pas possible de cibler directement l'entreprise. À l'aide d'un code spécifiquement développé pour les systèmes de point de vente (PoS), l'attaque a attiré les numéros de carte de crédit au moment précis où ils étaient présents dans la mémoire du système et non cryptés (Julian, 2014).

Les retombées de l'attaque ont illustré l'impact qu'une violation de cette échelle pourrait avoir, non seulement pour les clients, mais aussi dans toute l'organisation. En fin de compte, cela a conduit à la démission du PDG lui-même, ce qui révèle le fait que les infractions cybernétiques sont maintenant des problèmes au niveau des comités de direction (Julian, 2014).

La réponse publique est donc devenue une considération critique dans le traitement des incidents liés à la cyber-criminalité. Les entreprises ne peuvent plus adopter une approche ad hoc pour répondre. Il est impératif que tous les niveaux de l'organisation comprennent le risque qu'engendre la cyber-criminalité et engagent toutes les ressources appropriées pour prévenir les infractions, les détecter lorsqu'elles se produisent et répondre de manière appropriée.

[4] Entreprise de grande distribution, deuxième plus gros distributeur discount et cinquième distributeur général aux Etats-Unis.

2.2 Définition et catégorisation du cyber-risques selon la littérature.

Le cyber-risque peut être classifié selon le type d'activité (ex : criminel et non criminel), selon le type d'attaque (ex : logiciel malveillant) ou encore la source (ex : terroriste, criminels et gouvernements). Les attaquent dépendent principalement des activités des criminelles et sont renforcées par ce que Elling et Schnell appellent « the network effect »[5]. C'est ensuite la vulnérabilité de l'organisation qui déterminera si l'attaque sera un succès. Cette vulnérabilité, étant déterminée dans une certaine mesure par la spécificité même des paramètres de l'entreprise ou de l'organisation telle que la technologie, les processus et les personnes, est caractérisée par une composante du risque idiosyncratique entraînant ainsi un risque de préjudice moral pour les assureurs (Eling et Schnell, 2016). De plus comme le souligne Biener et al. (2015), en raison du caractère public de l'investissement en sécurité informatique, les entreprises tendent à investir de manière moindre que ce qui serait désirable économiquement. Finalement en ce qui concerne les conséquences, celles-ci dépendent des motifs de l'attaque (ex : espionnage, sabotage, etc.) et pourraient déboucher sur l'arrêt des services qui dépendent de l'infrastructure IT, sur l'altération de l'intégrité et de la confidentialité de données qui pourraient à leurs tours amener à des pertes monétaires, une perte de réputation ou tout simplement à l'arrêt des activités (CRO Forum, 2014) et éventuellement à des victimes humaines.
Ces différentes catégorisations du risque mettent l'accent sur les activités criminelles, mais il est évident que les activités non criminelles constituent une part importante des éléments constituants du cyber-risque (Eling et Schnell, 2016).

Le terme "cyber" possède deux éléments constitutifs. Il fait appel au concept de réseau de communication ainsi qu'à une dimension virtuelle (Eling et Schnell, 2016). Ces deux caractéristiques distinguent fondamentalement le cyber-risque des autres types de risques (Eling et Schnell, 2016). Premièrement, la nature virtuelle met l'accent sur la nature intangible de ce risque et donc sur la difficulté d'estimer les pertes et deuxièmement le terme réseau fait souvent référence au cyber-espace qu'on appelle communément internet.

[5] Soit la propagation sur tout le réseau (ex: ver)

Bien qu'internet pourrait être considéré comme la première source de cyber-menaces, celui-ci ne constitue pas le seul réseau, en effet le cyber-espace définit tous les réseaux qui sont connectés à un système IT (Eling et Schnell, 2016).).

La plupart des définitions met l'accent sur le concept de réseau (Swiss Re, 2014 ; CRO Forum, 2014 ; Lloyd's, 2015 ; Willis, 2013. Ainsi, Cebula et Young (2010) définissent le cyber-risque comme: « O*perational risks to information and technology assets that have consequences affecting the confidentiality, availability, or integrity of information or information systems* ». Cette définition permet de gérer ce risque dans toute l'organisation et ne caractérise plus ce problème comme étant celui du département IT. Similairement, l'Association[6] nationale des commissaires aux assurances (2013) identifie le vol, la divulgation d'informations sensibles et l'interruption d'activité comme des exemples de cyber-risque. D'autres chercheurs ne s'intéressent qu'à un type particulier de cyber-risque, tel que les brèches de données (Böhme et Kataria, 2006).

Etant donné que les banques s'appuient de plus en plus sur les infrastructures IT, il est à noter que l'exposition à ce risque est réglementée, notamment par BASEL II, comme appartenant au risque opérationnel. Il importe donc de savoir de quelle manière les régulateurs financiers entendent gérer le risque opérationnel afin d'y inclure le cyber-risque opérationnel.

2.3 Définition du risque opérationnel

Comme pour le cyber-risque, il existe de nombreuses façons de définir le risque opérationnel (Hull, 2012). Le risque opérationnel pourrait être considéré comme un risque résiduel, le risque auquel font face les institutions financières et qui n'est ni le risque de crédit, ni le risque de marché (Hull, 2012). Mais cette définition reste trop large : elle inclut les risques associés avec l'entrée dans de nouveaux marchés, le développement de nouveaux produits, de facteurs économiques, etc…(Hull, 2012).

[6] En anglais, The National Association of Insurance Commissioners

Autrement, on peut dire qu'il s'agit, comme son nom l'indique, du risque découlant des opérations. Cette définition devient trop étroite et n'inclut pas les risques tels que les « *rogue trader* » (Hull, 2012). Il est possible de faire la distinction entre les risques internes et les risques externes (Hull, 2012). Les risques internes représentent ce sur quoi la banque à un contrôle. En effet, elle choisit qui elle emploie, quel système IT elle utilise, quels contrôles mettre en place… C'est dans cette continuité que s'inscrit le cyber-risque provenant de contrôles inadéquats et de risques liés aux employés. Les régulateurs bancaires préfèrent inclure plus que juste les risques internes : ils incluent donc à la définition, l'impact d'évènements externes comme les catastrophes naturelles, les risques liés à la régulation et à la politique, les brèches de sécurité et bien d'autres (Hull, 2012).

Tout cela apparaît dans la définition du risque opérationnel du comité de Bâle : « *The risk of loss resulting from inadequate or failed internal processes, people, and systems or from external events.* » Cette définition inclut les risques légaux et exclut les risques stratégiques et risques réputationels (Basel Committee on Banking Supervision, 2011). Ces derniers font référence au risque de pertes issues de dommages à l'image de marque d'une entreprise et qui engendre une perte de confiance de la part des consommateurs (IFC[7] et The MasterCard Foundation, 2016).

D'un point de vue réglementaire, il importe également de mentionner le risque opérationnel tel que défini dans la directive européenne « *Solvency II »* qui passe en revue le régime prudentiel pour les entreprises d'assurance et de réassurance dans l'Union européenne. La directive définit ce risque comme étant : « Risk of a change in value caused by the fact that actual losses, incurred for inadequate or failed internal processes, people and systems, or from external events (including legal risk), differ from the expected losses. » Cette description englobe en son sein la définition du « *business risk* » : « *Unexpected changes to the legal conditions to which insurers are subject, changes in the economic and social environment, as well as changes in business profile and the general business cycle*. »

[7] International Finance Corporation

Enfin le risque opérationnel appartient à la taxonomie plus large du capital économique que l'on doit comprendre comme étant le capital requis pour protéger les institutions financières de l'insolvabilité économique sur une période d'un an et qui représente l'agrégation de tous les risques (Henrard, 2009). Ce capital économique reflète les risques réels compris comme des mouvements inattendus dans la valeur des actifs et des passifs sur l'intervalle de confiance que le management de l'organisation tolère.

2.4 Le risque opérationnel sous Basel II

En 1999, les superviseurs bancaires annoncent un plan pour assigner du capital pour couvrir les risques opérationnels dans la nouvelle réglementation qu'était Basel II (Hull, 2012). A l'époque, ce plan ne faisait pas l'unanimité parmi les praticiens ; cependant les superviseurs persistèrent et il fut instauré. Cependant la perspective de nouvelles exigences en matière de capitaux les a amenés à augmenter considérablement les ressources qu'ils consacrent à la mesure et à la surveillance du risque opérationnel (Hull, 2012).

Le risque opérationnel n'est pas plus difficile à gérer que le risque financier, il se traite simplement différemment via une amélioration des processus et de la qualité des données (Henrard, 2017). En effet pour le risque de crédit et de marché, il existe des instruments financiers tels que les produits dérivés qui permettent mitiger ces risques. Par opposition, le risque opérationnel est le risque lié à l'activité de l'entreprise et dans ce cas-ci, des banques. Il importe donc d'identifier les différents types de risques opérationnels puisque certains nécessitant une assurance (Hull, 2012). En effet il existe toujours le risque d'une perte énorme liée à un évènement qui n'était pas reconnu comme un risque (Hull, 2012) : cela fut le cas avec le cyber-risque qui est désormais inclus dans le risque opérationnel et est désormais géré de la sorte.

Ainsi, les banques font face à une faible probabilité d'une énorme perte engendrée par le risque opérationnel et ce risque n'affecte que la banque qui est concernée (Hull, 2012). Cette déclaration à l'ère du cyber-risque doit être considérée avec caution.

2.4.1 Le cyber-risque : Un risque opérationnel

Le cyber-risque et la cyber fraude sont des éléments qui appartiennent à la catégorie « *event risk* », défini comme un risque unique et ponctuel, tel que la défaillance des systèmes, les erreurs et omissions, la fraude ou les dommages non assurés aux installations et aux équipements (Henrard, 2009). Cet « *event risk* » fait à son tour partie des risques opérationnels. Ainsi, le cyber-risque doit être compris comme une sous-catégorie d'évènements (fraudes internes et externes) appartenant au risque opérationnel bâlois.

Le CRO Forum (2014) définit le Cyber Risque comme étant : « *the risk of doing business in the cyber environment* » ; par déduction personnelle, il s'agirait donc d'un risque opérationnel dans le cyber environnement comme défini dans la section 2.2. Ainsi, cette définition du cyber risque couvre (CRO Forum, 2016) : tous les risques émanant de l'emploi de données électroniques et de leur transmission, les dégâts physiques pouvant être causés par des cyber attaques, les fraudes commises par abus des données, toute responsabilité découlant de l'emploi fautif des données, du stockage et du transfert de ceux-ci, la disponibilité, l'intégrité et la confidentialité des informations électroniques, qu'elles soient liées aux particuliers, aux entreprises ou aux gouvernements.

En utilisant la définition du CRO Forum (2014) et celle de Bâle II on peut définir le cyber-risque formellement comme: « *The risk of loss resulting from inadequate or failed internal processes, people, and systems or from external events in the cyber environment ».*

2.4.2 Qu'est-ce un cyber système ?

Afin de comprendre le risque émanant du cyber espace, nous devons comprendre et prendre en compte l'étendue du sujet. Les risques qui proviennent ou sont dus au cyber-

espace, compris comme l'environnement dans lequel la communication sur les réseaux informatiques se produit, pourraient avoir des implications au-delà son univers (Refsdal, Solhaug et Stølen, 2015). La raison en est que n'importe quel système dépendant du cyber espace peut être vulnérable du fait de cette dépendance. Afin de tenir compte de cette relation, il importe de définir ce qu'est un cyber système : c'est un système qui utilise le cyber espace (Refsdal *et al.,* 2015).

2.4.3 Qu'est-ce la cyber sécurité ?

Alors que la cyber sécurité peut impliquer la sécurité du cyber espace dans son ensemble, la plupart des organisations s'occupe de la protection de leurs propres cyber-systèmes contre les cyber-menaces. Ces deux préoccupations intègrent la définition de la cyber-sécurité de Refsdal, Solhaug et Stølen (2015) qui définissent le concept comme étant la protection d'un cyber-système contre les cyber-menaces, menaces exploitant les failles du cyber-espace.

2.4.4 Définition de la résilience dans le cadre de la cyber-sécurité

La PPD-21[8] (2016) définit la résilience comme la capacité à se préparer, à s'adapter aux conditions changeantes, à résister et à se remettre rapidement de perturbations ou d'interruptions (Homeland Security, 2017). La cyber-résilience se concentre sur les contrôles préventifs, la détection et les contrôles réactifs dans l'environnement IT afin d'évaluer les faiblesses et les facteurs d'amélioration de la posture générale de l'entité en matière de sécurité (Homeland Security, 2017).

[8] Presidential policy directive 21 aux Etats-Unis.

2.4.4.1 Caractéristiques de la cyber-résilience

Il est primordial d'examiner les caractéristiques de la cyber-résilience afin de souligner les différences entre cyber-sécurité et cyber-résilience. Il est à noter que toute approche de la cyber-sécurité pourrait inclure des composants et caractéristiques de la cyber-résilience (Bjôrk *et al.,* 2015). On distingue cinq caractéristiques de la cyber résilience qui sont résumées sur le schéma suivant :

Aspect	**Cyber-Sécurité**	**Cyber-Résilience**
Objectif	Protéger les systèmes IT	Continuité des opérations
Intention	Fail-Safe	Safe-to-fail
Approche	Sécurité de l'extérieur	Sécurité à l'intérieur
Architecture	Protection à couche unique	Protection multicouche
Etendue	Une seule organisation	Réseau d'organisations

Tableau 1 : Caractéristiques comparées de la cyber-sécurité et la cyber-résilience (Bjôrk *et al.,* 2015)

2.4.5 Les six piliers du cyber-risque (Livanis, 2016)

Les dirigeants d'entreprises qui souhaitent développer et implémenter un cadre managérial intégré, devraient d'abord considérer les caractéristiques de ces cyber-risques et leurs relations avec leur organisation. Livanis (2016) propose l'emploi d'une taxonomie composée de six piliers faisant référence aux acteurs du cyber risque, aux buts d'une attaque, aux cibles, aux méthodes, aux actifs soumis aux risques ainsi qu'aux répercutions.

2.4.5.1 Premier Pilier : Les Acteurs

Il s'agit d'identifier la source de risques pour l'organisation. Ainsi les acteurs peuvent être classifiés en deux sous-groupes : les « *insiders* » et les « *outsiders* ».

Les « *insiders* » viennent de l'intérieur même de l'organisation et font référence aux ressources humaines et aux systèmes d'informations et télécommunications. A l'opposé, les « outsiders » proviennent de l'environnement externe où les organisations opèrent.

2.4.5.2 Deuxième Pilier : Buts et Motivations

Ce pilier fait référence aux majeures motivations et buts d'une attaque. On y retrouve le gain financier, la vengeance, la protestation, le gain d'un avantage stratégique sur ses concurrents, la curiosité, la politique ou la religion, ou encore la tentative de trouver un employeur.

2.4.5.3 Troisième Pilier : Les Cibles

Ce sont les cibles des attaques. On y retrouve les organisations publiques, les organisations privées, les employés et les dirigeants des organisations, ainsi que les infrastructures nationales critiques (fournisseurs d'électricité, marchés financiers).

2.4.5.4 Quatrième Pilier : Méthodes d'attaque

Ce pilier inclut les différentes méthodes utilisées pour bénéficier d'accès non autorisés, divulguer, interrompre, utiliser, modifier ou détruire des données ou les systèmes d'informations et de communication des organisations. On parle ici du vol ou de la perte d'appareils électroniques/digitaux, d'attaque malveillante, de l'oubli ou erreur d'un membre du personnel, de la malfonction d'un système ou encore de désastres naturels.

2.4.5.5 Cinquième Piliers : Actifs ciblés

Il est crucial pour les organisations de savoir quels actifs sont les plus précieux et exposés aux cyber-risques. On peut citer les infrastructures informatiques, les actifs intangibles, d'autres informations et la présence online.

2.4.5.6 Sixième Pilier : Les répercussions

Les répercussions du cyber-risque peuvent être financières, légales ou opérationnelles (Kaspersky Lab, 2015). On peut également ajouter à ces dernières l'impact négatif sur la réputation (IBM Corp., 2013). Lorsqu'une organisation comprend les répercussions possibles, l'établissement des coûts engendrés par ces risques peut être plus facile.
Cette taxonomie peut être un cadre de références pour les chercheurs et les praticiens afin d'évaluer, gérer et modéliser le risque. Il s'agit d'un prérequis nécessaire pour un management effectif de ce risque.

2.5 Le problème posé par le manque de données

La disponibilité des données en matière de cyber-risque est assez rare. Ce phénomène est dû au fait que les institutions qui ont été compromises, ne révèlent pas les incidents qui les touchent (Symantec, 2016).

Cependant depuis 2002 aux Etats-Unis, les entités qui subissent une brèche de sécurité, se doivent de reporter les incidents à leurs clients ainsi qu'aux autres parties (NCSL[9], 2016). De même on retrouve en Europe, depuis 2004, l'AESRI[10] (ou ENISA en anglais) qui est une agence dont le rôle est de recueillir et d'analyser les données relatives aux incidents liés à la sécurité en Europe et aux risques émergents. On retrouve également au niveau de la Banque Centrale Européenne un cadre permettant de reporter les cyber-incidents, qui a été mis en

[9] *National Conference of State Legislatures*.
[10] Agence européenne chargée de la sécurité des réseaux et de l'information.

place en 2017. Au Luxembourg la CSSF (Commission de Surveillance du Secteur Financier) a également mis en place un système de rapport pour les institutions sous sa surveillance.

Cette obligation de reporter les brèches permet d'augmenter la disponibilité des données (Eling et Schnell, 2016). Il est également possible de retrouver des données sur les cyber-incidents dans le domaine privé : on peut citer Sas, Fitch et Orx qui sont basées respectivement aux Etats-Unis pour les deux premiers et à Genève pour le dernier.

Même si les données historiques étaient disponibles, celles-ci seraient probablement devenues inutilisables de par la nature dynamique et changeante de l'environnement du cyber (CRO FORUM, 2014).

2.6 La modélisation du cyber risque

2.6.1 Propriétés du cyber-risque

Sans doute à cause du manque de données, il n'existe pas de modèle établi pour le cyber-risque et il n'existe que peu de recherche dans le domaine jusqu'à présent (Eling et Schnell, 2016).

Certains auteurs proposent d'éviter l'emploi de modèles stochastiques classiques, favorisant une approche basée sur la définition de scénarios (Lloyd's, 2015). Rakes, Deane et Rees (2012) suggèrent que pour les évènements à faible probabilité, mais à haute sévérité, il serait plus prudent de se baser sur le jugement d'un expert qui définirait les pires scénarios et leurs probabilités.

Deux des recherches qui modélisent le cyber-risque avec des techniques de modélisation stochastique, sont celles de Mailart et Sornette (2010) et Wheatley *et al.* (2015). Les premiers enquêtent sur les brèches de données personnelles (ex : vol de numéro de carte de crédit, numéro de sécurité sociale…) et constatent que la fréquence de ces incidents a connu une croissance exponentielle de 2001 à 2006. Toutefois, depuis 2006, cette fréquence a atteint un plateau.

De plus, les auteurs constatent que la sévérité par incidence suit une loi de puissance avec une distribution à queue lourde. Bien que les brèches de données personnelles ne

représentent qu'un seul type de cyber-risque, les auteurs soutiennent que cette constatation est représentative d'autres types de cyber-risques provenant d'internet.

Se basant sur les résultats de l'étude précédente, mais avec un ensemble plus large de données actualisées, Wheathley *et al.* (2015) mènent une analyse similaire et constatent que la quantité de brèches par incidence suit une distribution à queue encore plus lourde depuis 2007. Les résultats montrent que les lois gouvernant les propriétés du cyber-risque, soit la fréquence ou la sévérité, sont dynamiques.
De plus, l'environnement très changeant de la technologie requiert une révision continue de l'approche de modélisation (Eling et Schnell, 2016). La qualité des données disponibles limite également les améliorations qui pourraient être faites en matière de modélisation (Eling et Schnell, 2016). C'est le cas des assureurs pour qui les données sur le nombre de brèches ne sont pas suffisantes pour calculer les primes et les réserves (Eling et Schnell, 2016).

2.6.2 Value at Risk

La « *value at risk* » (VaR) est une tentative de fournir un seul nombre qui résume le risque total dans un portefeuille (Hull, 2012). Ce concept a été lancé par J.P. Morgan et est devenu largement utilisé par les managers de fonds, les trésoriers d'entreprise ainsi que les institutions financières. Il s'agit de la mesure que les régulateurs ont choisi d'utiliser pour bon nombre de calculs qu'ils effectuent concernant l'établissement des exigences de fonds propres pour le risque de marché, le risque de crédit ainsi que le risque opérationnel.

2.6.2.1 Définition de la VaR

Pour un portefeuille d'actifs donné, la VaR quantifie la somme qui au maximum peut être perdue avec une probabilité donnée sur un horizon de temps spécifique. La VaR indique la pire perte attendue (*Worst case scénario*) sur un horizon de temps donné à un niveau de confiance donné dans des conditions de marché normales (J.P. Morgan, 2008). Cette valeur

représente la perte correspondant à un percentile faible de distribution. Il s'agit d'un autre nom pour le quantile d'une distribution (Bodie *et al.,* 2014).

La VaR fournit donc un nombre unique résumant l'exposition de l'entreprise au risque de marché et la probabilité d'un mouvement défavorable dans les positions du portefeuille. Elle fournit également un outil prédictif pour empêcher les gestionnaires de portefeuille de dépasser le seuil de tolérance de risque définie par les institutions financières. Elle peut être mesurée au niveau d'un portefeuille, d'un secteur, ou de la classe d'actifs. La VaR n'est qu'une estimation et non une valeur définie de manière unique (J.P. Morgan, 2008).

À la différence du concept d'« *expected shortf*all » dont il est fait mention plus loin, la VaR ne fournit aucune information sur les pertes qui excèdent sa valeur. Elle ne représente pas le *worst-case scenario* (J.P Morgan, 2008). De ce fait il s'agit d'une très mauvaise mesure pour le cyber-risque qui se retrouve en dehors des intervalles de confiance de la VaR de par sa nature « *low frequency / high severity . »*

2.6.2.2 Expected Shortfall

La VaR représente donc une mesure trop optimiste. Une vision plus réaliste de l'exposition aux pires risques se concentrerait plutôt sur la perte attendue, étant donné qu'il s'agit d'un des « *worst-case scenario* » (Bodie *et al.,* 2014). Cette valeur se nomme « *expected shortfall », « expected tail risk* » ou encore T-VaR. Cette mesure possède de meilleures propriétés que la VaR étant donné qu'elle encourage la diversification. A l'inverse elle n'est pas aussi simple à calculer que la VaR et est donc plus difficile à saisir (Hull, 2012).

L' « *expected shortfall* » (ES) représente une mesure cohérente du risque comme définie par Artzner *et al.* (1999). Elle satisfait les quatre axiomes suivants :

- Subadditivité (diversification) : Le risque d'un portefeuille de deux actifs ne devrait pas être plus grand que la somme des risques des actifs pris individuellement.
- Homogénéité : Augmenter la taille du portefeuille en le multipliant par λ devrait augmenter le risque par un multiple de λ *ceteris paribus*.

- Monotonicité : Un risque plus élevé est associé avec des pertes plus élevées et un risque moins élevé est associé avec moins de pertes.
- Transitivité : Ajouter du cash ou actif sans risque devrait réduire le risque.

En dépit de ses faiblesses, la VaR est devenue la mesure du risque la plus populaire pour les régulateurs et les managers du risque (Hull, 2012). Pour cette raison, elle sera donc la mesure du risque sélectionnée dans la présente recherche en utilisant le concept de *cyber value at risk*.

2.6.3 De la VaR à la Cyber-Value at risk

Comme mentionné, la VaR possède l'avantage d'être facile à comprendre et appliquer. Il en va de même pour le concept de *cyber value at risk (*C-VaR). Cette valeur est caractérisée par son applicabilité générique à travers différentes industries, son évolutivité, sa facilité d'interprétation et sa capacité à supporter les décisions de l'exécutif en matière d'investissement et de gestion du risque (World Economic Forum, 2015). En construisant un modèle *cyber value at risk* et en ayant une vue globale sur les actifs de l'organisation qui sont menacés, les institutions financières peuvent également prendre des décisions en ce qui concerne les montants appropriés d'investissement dans les systèmes IT.

La C-VaR permet de répondre aux questions qui concernent les cyber-attaques, telles que (World Economic Forum, 2015) :

- Qui et pourquoi ? : Aborde les types de menace en exécutant un scénario d'attaque en termes d'attractivité de la cible et de motivation pour les cybercriminels.
- Quoi et comment ? : Aborde le type d'attaque utilisée en terme technique et en matière de sophistication.
- Où et quand ? : Aborde la vulnérabilité selon une mesure du niveau de maturité de la résilience.

2.6.3.1 Cyber Value at Risk (C-VaR)

Le concept de C-VaR trouve sa fondation dans la notion de *Value at risk* qui est largement utilisée par l'industrie financière. Elle permet de déclarer : « Nous sommes X pourcent certain que nous ne perdrons pas plus de V dollars sur la période T » (Hull, 2012). Cette valeur pourrait être appliquée avec succès aux risques cybernétiques en tant que concept indirect pour l'exposition au risque digital. Ce modèle – comme celui de la VaR – utilise une approche probabiliste pour estimer des pertes probables dues aux cyber-attaques sur une période donnée.

Similairement à la VaR, la C-VaR requiert que les organisations comprennent les principaux facteurs du cyber-risque requis pour modéliser les risques cybernétiques et la dépendance entre ces facteurs qui peuvent être incorporés dans les modèles de quantification (World Economic Forum, 2015). Pour ce faire, les institutions financières devraient adopter une posture proactive afin d'empêcher les pertes et mettre en place des contrôles de risque (RCSA)[11] (Hull, 2012). Ces contrôles internes et ces évaluations sont importants car ils permettent aux banques et autres institutions financières de mieux comprendre leur exposition aux risques opérationnels et *ipso facto* le cyber-risque (Hull, 2012).

Il existe deux techniques (Henrard, 2009) :

- La réalisation de *workshop* impliquant tout ou une partie du personnel du *business line* qui est testé.
- La réalisation de sondages ou questionnaires complétés indépendamment par les équipes.

Sur base de ces réponses, les managers peuvent déterminer la probabilité et l'impact, si une brèche venait à se produire (Henrard, 2009).

Un modèle C-VaR complet et complexe permettra aux organisations de répondre au problème suivant : compte tenu d'une cyber-attaque réussie, une entreprise perdra au

[11] RCSA : Risk control and self-assessment.

maximum V unité monétaire sur une période de temps T avec par exemple 97,5% de certitude. D'ici 2019, ceci sera exigé par Bâle III.

La C-VaR intègre plusieurs composants qui doivent être évalués par chaque organisation dans le processus de modélisation du cyber-risque. L'applicabilité et l'impact dans chaque modèle de ces composants varieront selon l'industrie et la maturité de la cyber-résilience. Il est important d'analyser également la dépendance entre les composants du modèle car cette dépendance devrait être incorporée dans les modèles de quantification du cyber-risque (World Economic Forum, 2015).

A l'instar de la VaR, le but du C-VaR est de standardiser et unifier différents facteurs dans une seule distribution normale qui permette de quantifier la valeur à risque en cas de cyber-attaque. Les efforts devraient être spécifiques à l'organisation et refléter les pratiques de l'industrie (World Economic Forum, 2015). Une fois la mesure statistique du cyber-risque disponible, celle-ci doit alors servir à développer une stratégie pour toute l'entreprise (World Economic Forum, 2015). Ces composants sont mentionnés dans la section [2.3.7] et bien que prenant une autre forme, ils sont résumés dans le schéma 2 ci-dessous.

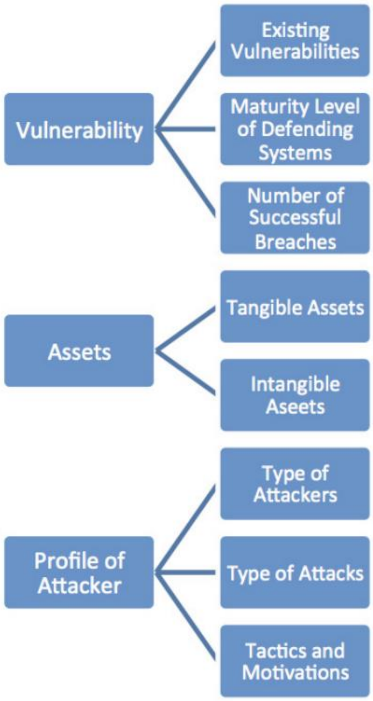

Schéma 2 : Composants de la C-VaR (World Economic Forum, 2015).

2.6.4 Calcul des distributions de pertes agrégées et des exigences de fonds propres pour le risque opérationnel

L'une des tâches les plus difficiles dans la gestion des risques est de fixer le niveau de capital approprié pour couvrir les pertes imprévues dans les banques et autres institutions financières (Scalar Consulting, 2006), tandis que les pertes attendues peuvent être décrites comme les pertes « habituelles » ou encore comme le coût prévisible de faire des affaires (Henrard, 2009).

Les pertes imprévues sont des écarts par rapport à la moyenne qui peuvent mettre en danger la stabilité d'une institution (Henrard, 2009). Les gestionnaires de risque s'inquiètent de ce type de perte, mais également les régulateurs et les superviseurs financiers, de sorte que des normes internationales sont continuellement développées et améliorées pour empêcher les établissements de faire faillite en raison de ces importantes pertes potentielles (Scalar Consulting, 2006). La plus connue et répandue de ces normes est Bâle II de 2004.

Afin d'établir le niveau de capital approprié pour couvrir les pertes imprévues[12] dues aux risques opérationnels (cyber-risques opérationnels), il est impératif d'établir un niveau de confiance adéquat (Scalar Consulting, 2006).

Un niveau de confiance est un concept statistique qui correspond, de façon intuitive, à la probabilité qu'un établissement ne fasse pas faillite ou qu'une des « *business lines* » ne fasse pas banqueroute en raison de pertes extrêmes (Scalar Consulting, 2006).

Il est évident que les banques et autres institutions financières souhaiteraient établir un niveau de confiance proche de 100%. En pratique, cependant, cela n'est pas possible car les distributions de pertes ne sont jamais parfaitement identifiées en utilisant des données historiques incomplètes (Scalar Consulting, 2006). Ce phénomène est renforcé dans le cas du cyber-risque où les données sont encore rares.

Cependant un niveau de confiance de 100% n'est pas désirable car trop coûteux pour les banques. Dans les banques et institutions financières, la gestion se situe habituellement entre 95% et 99%.
Une fois que le niveau de confiance auquel les banques et les assureurs aimeraient couvrir les pertes imprévues est défini, le calcul du montant correspondant au capital requis implique les étapes suivantes :

- Identifier la distribution de fréquence ainsi que celle de la sévérité. – Il importe également d'identifier les montants extrêmes et la fréquence de ces évènements extrêmes (Henrard, 2009). Ceci est d'autant plus vrai avec le cyber-risque.
- Etablir les paramètres de la distribution. Pour la distribution de sévérité, il faut calculer le mode et la queue, et pour la distribution de fréquence, la moyenne. (Henrard, 2009)
- Combiner les deux distributions pour obtenir la distribution des pertes agrégées.

[12] *Unexpected loss* en anglais.

- La « *Operation value at risk* » est obtenue en choisissant le percentile de la distribution à l'intervalle de confiance désiré (Scalar Consulting, 2006).

Les pertes inattendues représentent alors la différence entre la VaR et les pertes attendues comme on peut le constater sur le schéma 3.

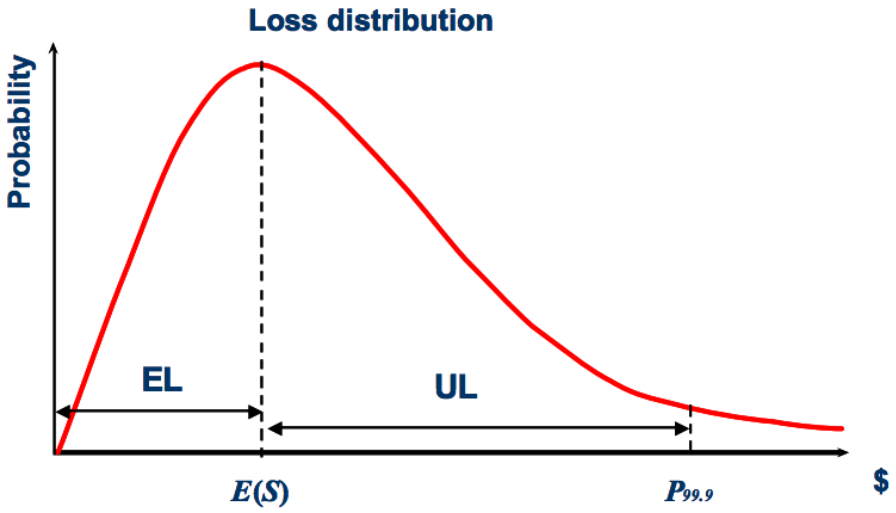

Schéma 3 : Perte attendues (EL), Pertes inattendues (UL) et VaR : l'intervalle de confiance à 99%. (Scalar Consulting, 2006)

Il est à noter que l'on établit habituellement un niveau de capital prudentiel non pour la banque dans son ensemble, mais pour des types spécifiques d'évènements de perte – la fraude interne, la fraude externe, etc. – ou pour les différentes « *business lines* ».

La principale difficulté de la procédure décrite ci-dessus réside dans la troisième étape (Henrard, 2009) qui est l'agrégation des distributions de fréquence et de sévérité obtenues à partir des données. Comme mentionné ci-dessus, les deux distributions ne possèdent pas les mêmes propriétés : la fréquence suit une Loi de poisson discrète et est exprimée en termes de nombres d'évènements par unité de temps, alors que la sévérité est caractérisée par une distribution continue exprimée en unité monétaire (Scalar Consulting, 2006). De ce fait les

deux distributions ne sont pas directement additives ou multiplicatives (Scalar Consulting, 2006).

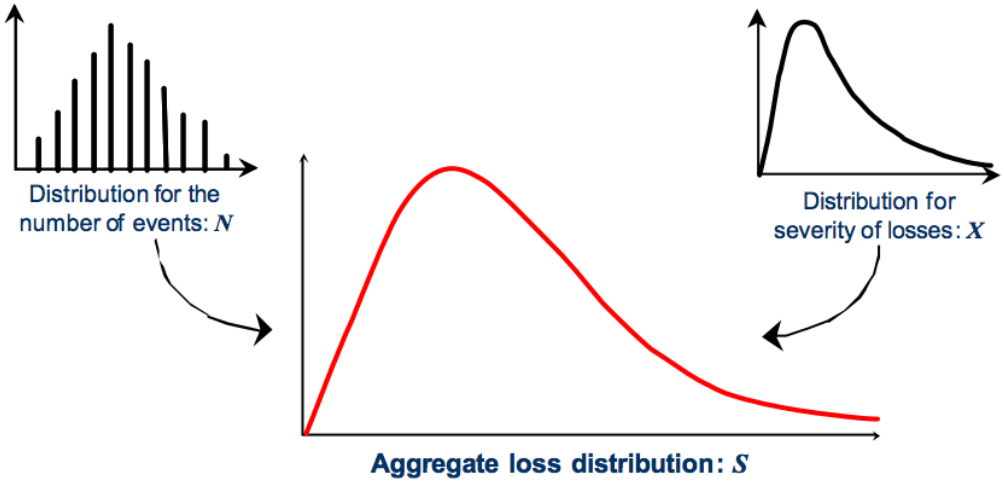

Schéma 4 : Distribution des pertes agrégées (Scalar Consulting, 2006)

Il existe trois approches pour combiner les deux types de distribution : « *closed form* », « *open form* », et finalement l'approche par simulation.

La première méthode implique la résolution de formules analytiques. La solution « *closed form* », la plus directe, consiste à combiner les distributions au moyen d'une opération mathématique principalement théorique. Celle-ci est appelée « convolution » ; cette solution implique la résolution d'intégrales complexes (Scalar Consulting, 2006).

La seconde méthode (« *closed form* ») pour combiner les deux distributions (toujours en forme fermée) ne requiert pas de les traiter directement, mais d'effectuer une certaine transformation qui permette de les manipuler de manière plus efficace. Il s'agit de la transformation de Fourier qu'on opère sur la distribution de la fréquence (Scalar Consulting, 2006). Cette approche implique de traiter des fonctions trigonométriques et des nombres complexes. Puisque la transformation de Fourier est multiplicative, une fois que nous obtenons les distributions transformées, nous pouvons facilement obtenir leur produit ce qui est moins compliqué que la méthode de convolution (Scalar Consulting, 2006).

Obtenir les distributions agrégées peut paraître difficile, surtout pour les petites ou moyennes institutions financières qui ne disposent pas de la logistique ou du capital humain nécessaire.

Contrairement aux solutions mentionnées plus haut et qui impliquent la résolution de formules et d'équations théoriques, la méthode par simulation représente une autre solution de forme ouverte, dans laquelle un algorithme est habilement implémenté et un ordinateur fait le travail (Henrard, 2009). La simulation de Monte Carlo représente l'une de ces méthodes. A l'aide de la simulation, il est produit différents scénarios pour la fréquence et la sévérité des pertes en générant des nombres aléatoires en utilisant chaque type de distributions identifié grâce aux données disponibles sur les pertes (Scalar Consulting, 2006). Le problème de l'agrégation est simple car, pour différents scénarios, chaque perte potentielle est générée selon une simulation qui utilise la distribution de fréquences identifiées à partir des données (Henrard, 2009).

2.6.5 Calcul des distributions des pertes agrégées pour le cyber-risque

Comme pour le risque opérationnel, il est possible de déterminer une distribution pour la fréquence des attaques ainsi qu'une distribution pour leur sévérité. Pour ce faire il importe de décomposer ces distributions en sous-catégories qui dépendent des composants de la C-VaR, mentionnés section [2.3] et [2.5] afin de définir clairement les distributions de probabilités.

Freund et Jones (2014) proposent une décomposition en posant que le risque représente l'exposition aux pertes. A partir de cette définition ils dérivent la définition suivante pour le risque : « La fréquence probable et la sévérité probable des pertes futures ». Les auteurs accordent une grande importance aux termes « fréquence et sévérité » qui sont la base de toutes analyses du risque opérationnel et dans ce cas-ci, du cyber-risque. En effet connaître la sévérité d'une perte sans en connaître la fréquence est peu utile (Freund et Jones, 2014).

De plus l'analyse du risque étant basé sur des données imparfaites et des modèles qui les emploient, la fréquence et la sévérité doivent se fonder sur des probabilités (Freund et Jones, 2014). Et enfin cette analyse du risque est réalisée dans le but d'informer le management afin de prendre des décisions basées sur de futures potentielles pertes (Freund et Jones, 2014).
Avec ces définitions pour point de départ, les deux facteurs déterminants du risque sont comme pour la VaR : la fréquence des pertes et la sévérité des pertes.[13]

2.6.5.1 Fréquence de perte (Loss event frequency - LEF)

Les auteurs définissent les LEF du cyber-risque comme étant la fréquence probable, sur une période de temps donnée où cette perte se matérialisera par l'action d'un acteur (Freund et Jones, 2014). Cette définition est évidente et pourrait être posée plus simplement comme le nombre de fois qu'une perte est susceptible de se produire. Les auteurs insistent cependant sur la nécessité d'avoir un cadre temporel défini pour que la distribution de probabilité puisse avoir une réelle portée. Il importe également de définir clairement les différents types d'évènement et scénarios afin de produire des valeurs probantes en ce qui concerne la fréquence ou la sévérité des pertes (Freund et Jones, 2014).

Cette fréquence des pertes peut être estimée de manière directe ou indirecte en la décomposant en deux sous-facteurs : la fréquence de l'évènement de la menace et la vulnérabilité[14] (Freund et Jones, 2014).

Les chercheurs définissent la TEF comme étant : la fréquence probable, sur une période donnée, qu'une menace agisse et aboutisse à des pertes. La différence entre LEF et TEF réside dans le fait que TEF n'engendre pas nécessairement une perte (Freund et Jones,

[13] Fréquence des pertes: *Loss event frequency (*LEF) et Sévérité des pertes: *Loss Severity* (LS).

[14] Fréquence de l'évènement de la menace : *Threat event frequency* (TEF) (Freund et Jones, 2014).

2014). Similairement à LEF, TEF peut être estimée directement ou en la décomposant également en deux sous-facteurs : la fréquence de contact et la probabilité d'action (Freund et Jones, 2014). La fréquence de contact est la fréquence probable, sur une période donnée, qu'une menace rentre en contact avec des actifs ciblés.
Cette fréquence de contact peut être diminuée en cherchant des moyens de réduire la probabilité/fréquence qu'une menace rentre en contact avec ces actifs (Freund et Jones, 2014). Dans le cas du cyber-risque il peut s'agir de l'implémentation d'un pare-feu qui bloque l'accès au réseau d'un *serveur* ou d'une application.

La probabilité d'action, quant à elle, fait référence à la probabilité qu'une menace agisse sur les actifs ciblés une fois que le contact est établi. Comprendre la probabilité d'action est aussi très utile pour la mise en place de contrôles et moyens de dissuasion. En implémentant des mesures qui affectent l'apparente valeur des actifs ciblés, augmentent l'effort perçu requis pour atteindre les actifs ou augmentent le niveau de risque perçu, il est possible de réduire la probabilité d'action (Freund et Jones, 2014).

La vulnérabilité est définie, quant à elle, comme la probabilité que l'action d'une menace résulte en une perte (Freund et Jones, 2014). Ici, les auteurs ne considèrent pas la vulnérabilité comme une condition de faiblesse qui peut être exploitée, mais mettent en exergue le niveau d'effort à fournir. La vulnérabilité est un pourcentage qui représente la probabilité que l'action d'une menace résulte à une perte (Freund et Jones, 2014). A son tour la vulnérabilité peut être déduite directement ou par sous-segmentation en deux facteurs : la capacité de la menace et la difficulté, référée comme *Threat Capability* (TC)[15].

Ici la définition de la TC parle d'elle-même et englobe les actions malveillantes et l'erreur humaine. Estimer la TC est un des éléments les plus difficiles de l'analyse de risque. En effet, la plupart du temps, l'analyse ne porte pas sur un élément facilement mesurable, comme le

[15] Capacité de la menace: *Threat Capability* (TC).

vent par exemple. Il s'agit ici de mesurer des éléments comme le savoir humain ou l'expérience (Freund et Jones, 2014).

En matière de contrôle, lorsqu'il s'agit d'erreur humaine on pourrait améliorer la TC et réduire la vulnérabilité en proposant des formations, de meilleurs outils, etc. Dans le cas d'une action malveillante, on pourrait réduire la TC en réduisant le temps d'action que la menace possède pour compléter sa tâche en ayant une réaction plus rapide (Freund et Jones, 2014).

2.6.5.2 Sévérité des pertes

Il s'agit de la probable sévérité d'une perte primaire et secondaire résultant d'un évènement causant une perte (Freund et Jones, 2014). Cette définition peut paraître relativement simple, en effet il s'agit de savoir combien on risque de perdre si un évènement se produit. Mais il existe une subtilité qu'il faut relever quant à l'évaluation de la sévérité des pertes : en effet il faut faire la distinction entre les pertes primaires et les pertes secondaires (Freund et Jones, 2014).[16]

Les *Primary loss* (PL) severity sont les pertes qui touchent directement les parties prenantes telles que les managers du risque ou encore l'exécutif. Ce sont les pertes qui se matérialisent directement à la suite d'un évènement (Freund et Jones, 2014).
Les *Secondary risk* (SR) représentent quant à eux l'exposition au risque qui existe du fait de la réaction d'autres parties prenantes à un évènement : ceci englobe les risques légaux, la réputation, etc. Cependant, Bâle II n'inclut pas ces risques dans la définition du risque opérationnel et il convient de les traiter à part. Les facteurs qui régissent les risques secondaires sont la fréquence d'évènements secondaires et la sévérité des pertes secondaires (Freund et Jones, 2014).

[16] *Primary loss* (PL) severity et *Secondary risk* (SR).

La définition de ces sous-facteurs et de leur distribution permet de calculer la C-VaR en utilisant la même méthode que pour les risques opérationnels comme mentionné dans la section [2.5.4].

2.7 L'organisation du management du cyber-risque et la mitigation du risque

Un des aspects importants de la gestion du cyber-risque est que celui-ci n'est pas de la responsabilité du département IT. Sa gestion nécessite un dialogue global entre les différents départements. En effet, il est important pour les institutions financières de développer une approche holistique du management du risque (Hull, 2012).
Cela implique la spécification de l'appétit au risque ou d'un seuil de tolérance au risque, la création d'une culture forte du management du risque au travers toute l'organisation et l'implication du management senior (Hull, 2012). Ce processus fait référence au management du risque de l'entreprise ou « *enterprise risk management* » (ERM). Il s'agit alors d'identifier les meilleurs moyens de mettre à profit l'ERM pour gérer le cyber-risque.
Cependant, l'engagement institutionnel démontré dans la lutte contre les cyber-menaces en ayant une personne responsable de la sécurité est essentiel (Eling et Schnell, 2016). Les firmes possédant un *Chief Information Security Officer* (CISO) ou un poste similaire ont des coûts moyens dus aux brèches beaucoup moins élevées quand une brèche de sécurité se produit, qu'une entreprise sans leadership stratégique en matière de sécurité (Shackelford, 2012).

Le développement du cadre ERM des banques et des institutions financières implique de définir tout d'abord la situation initiale et les buts de la gestion du cyber-risque (Eling et Schnell, 2016). Il s'agit ensuite d'impliquer les gestionnaires du risque ainsi que les équipes IT afin de partager l'information et de définir les responsabilités de chacun pour développer un processus d'évaluation des risques[17]. Ce processus implique l'identification des risques, leurs analyses, leurs évaluations, leurs traitements et finalement leurs suivis et évaluations (The MasterCard Foundation ; IFC, 2016).

[17] Risk Assessment Process.

Pour l'identification des risques, les actifs pertinents et leurs processus doivent être identifiés pour ensuite déterminer les menaces potentielles et leurs sources (Eling et Schnell, 2016). Un premier indicateur potentiel pour l'identification des risques peut être fourni par une auto-évaluation du cyber-risque (Marsh, 2016). Cette auto-évaluation est également nécessaire pour la modélisation du risque qui constitue également un outil de décision pour le management du risque. En effet, ces outils peuvent aider à déterminer l'exposition aux risques et la prise de conscience du risque[18] d'une entreprise et fournir des indications sur les risques non identifiés.

Un outil populaire pour l'analyse du risque est l'analyse de l'impact (cf. RCSA). Premièrement, les coûts directs pour des scénarios particuliers sont calculés et la perte totale attendue d'un incident peut être estimée en considérant la dépendance entre les différents scénarios. Cette analyse pourrait inclure les effets indirects comme les risques liés à la réputation qui ne rentrent pas dans le risque opérationnel de Bâle II. Néanmoins, le manque de données ne permet pas l'estimation correcte des probabilités. De plus, la nature dynamique du cyber-risque rend l'évaluation des données historiques assez difficiles (Eling et Schnell, 2016).

Parmi les différentes techniques possibles pour le management, on retrouve l'évitement, la mitigation, le transfert et la rétention de risque. Mais à l'ère du tout digital, l'évitement paraît être une solution peu crédible. La mitigation du risque semble être plus efficace et est plus répandue comme pratique, avec l'emploi notamment d'instruments qui réduisent la fréquence des pertes (antivirus, pare-feu, etc.) (Elling et Schnell, 2016).

Rakes *et al.* (2012) soulignent que la plupart des entreprises ne disposent pas d'un processus décisionnel efficace pour sélectionner les mesures de sécurité optimales. Ils proposent donc un cadre dans lequel différentes contre-mesures sont comparées sur base de leur aptitude à

[18] Risk awareness.

réduire la cyber-menace. Il est aussi possible de transférer le risque en prenant une assurance (cf. prochaine section).

Comme signalé plus haut, le cyber-risque possède une nature dynamique. Ceci fait que le *monitoring* du cyber-risque est un élément clé du management. Etant donné que les stratégies d'attaques ne cessent de changer, le management du risque se doit d'être amélioré en permanence. De même, une communication approfondie et le partage de l'information sont capitaux pour le cyber-risque et cela afin de renforcer le savoir-faire en matière de sécurité et la sensibilisation dans l'ensemble de l'entreprise (Eling et Schnell, 2016).

Lorsqu'on parle de cyber-risque, il est nécessaire de garder à l'esprit qu'aucun système n'est inviolable. Il convient alors de développer un plan de réponses. Les organisations qui possèdent des plans de réponse aux incidents, ont une capacité à poursuivre leurs opérations journalières bien meilleures que celles qui n'ont pas de plan. Ainsi l'étape finale est de développer un plan qui, d'abord et avant tout, définit qui seront les personnes relais pour les activités internes et externes quand une brèche se déroule (Dunbar, 2012). Il est à noter que lors de l'élaboration du plan, il faut prendre en compte s'il existe une assurance afin que les différentes équipes puissent s'appuyer sur l'expertise de l'assureur en cas de brèche. En effet, certains assureurs offrent une équipe d'experts en cas de crise, des équipes spéciales pour gérer la brèche ainsi qu'une expertise légale (Dunbar, 2012). Ce plan doit représenter également une opportunité d'apprendre en cas de brèches. Enfin, il est à souligner qu'un plan n'a de la valeur que si celui-ci fonctionne d'où la nécessité de le tester.

2.7.1 Le facteur humain au cœur de la gestion du cyber-risque

Bien que certains pirates informatiques cherchent à interrompre les opérations d'une organisation (hacktivistes), la plupart d'entre eux recherche le gain (Cisco, 2008). Le vol d'identité, la vente d'informations techniques ou financières sensibles aux concurrents, l'abus des données confidentielles de clients et l'utilisation abusive du nom d'entreprises ou

de leurs marques de produits sont quelques-unes des façons dont les pirates peuvent profiter d'une brèche sécurité ou de l'obtention de contenu confidentiel (Cisco, 2008).

La menace extérieure reste donc réelle et justifie les préoccupations et les actions des professionnels de la sécurité ainsi que des managers du risque. Mais, la plupart des pertes de données massives provient d'activités internes aux organisations (Cisco, 2008). Cette menace interne est souvent caractérisée par l'action malveillante d'employés, telle que le sabotage, le vol de données ou d'appareils électroniques, ou la publication volontaire de données confidentielles comme ce fût le cas lors du « *Panama papers* ». Cependant cette menace interne ne se limite pas aux employés malveillants, mais concerne tous les employés (Cisco, 2008).

2.7.1.1 L'employé négligent

On peut citer comme sources de menaces internes dues à la négligence des employés : le manque de conscience du risque (Cisco, 2008). Les pertes de données ou brèches sont souvent le résultat de comportements dangereux de la part d'employés qui ne sont pas conscients de la dangerosité de leurs actions – d'où l'intérêt d'avoir une culture du risque forte s'inscrivant dans le management du risque de l'entreprise. Il est également important de mentionner le manque de diligence de la part des employés (Cisco, 2008).

2.7.1.2 L'employé malveillant

Un employé qui est mécontent ou cherche l'appât du gain par des actions illicites impliquant les ressources d'une entreprise, peut également devenir une menace interne. Il ajoute une nouvelle dimension dangereuse dans la prévention des pertes de données (Cisco, 2008).
L'employé mécontent défie en effet la perception commune que les menaces de sécurité significatives proviennent d'en dehors des entreprises (Cisco, 2008). Les salariés avec des intentions malveillantes et motivées par le gain financier, peuvent en effet utiliser leur statut *d'insider* pour causer des pertes encore plus significatives que les attaques externes (Cisco,

2008). Dès qu'il s'agit d'employés malveillants ou de négligence, la solution réside dans la formation, la communication ainsi que la prévention inscrite dans le cadre de la gestion du risque de l'entreprise.

2.7.1.3 Les relations avec les tierces parties

Un des challenges importants de la cyber-sécurité et du cyber-risque est le management des relations avec les tierces parties qui représentent un risque significatif (Freund et Jones, 2014) [Cf. Le cambriolage de la Banque Nationale du Bangladesh via le système de communication SWIFT.] Ce risque est d'autant plus significatif qu'il existe une multitude de relations avec différentes tierces parties et inversement pour ces dernières (Freund et Jones, 2014).

Lorsqu'il s'agit de la relation entre une organisation et les tierces parties, les managers du risque devraient se concentrer sur les points suivants : la valorisation des informations de l'entreprise auxquelles ils ont accès, la connectivité entre le réseau de l'entreprise et celui de la tierce partie, les pratiques managériales de celle-ci, et l'habilité de celle-ci à manager le risque (Freund et Jones, 2014).

2.8 Le marché de l'assurance et les challenges que posent l'assurabilité du cyber-risque

L'assurance de la propriété et de la responsabilité commerciale est disponible dans la plupart des marchés d'assurances dans le monde entier. Cependant, la plupart des polices d'assurance ne couvre que les dégâts sur les actifs tangibles comme les usines de productions et excluent le cyber-risque. De plus, quand bien même le contrat couvrirait le cyber-risque, les termes de celui-ci n'incluent parfois pas, quels types d'évènements jouissent d'une couverture (Lloyd's, 2015).

Cette ambiguïté est source de conflits légaux. En conséquence, les assureurs cherchent à établir les termes des contrats de manière plus explicite (Eling et Schnell, 2016). Pour ce

faire, ils procèdent de deux manières. La première consiste à exclure le cyber-risque des contrats traditionnels et à fournir un contrat distinct pour le cyber-risque et la deuxième consiste à inclure explicitement ce risque, tout en augmentant la prime d'assurance.

En ce qui concerne le marché de la cyber-assurance, il est à noter que celui des Etats-Unis est bien plus développé que l'européen. Ceci est dû au fait que les compagnies doivent déclarer leurs brèches depuis plusieurs années comparativement à l'Europe (Eling et Schnell, 2016). Ces nouvelles régulations ont permis de prendre conscience du cyber-risque et ont contribué à augmenter la demande notamment pour la couverture du risque des tierces parties. Comparativement, le peu de polices d'assurances disponibles en Europe ne couvrent que ce qu'on appelle les *first-party data*, c'est-à-dire les données qui concernent l'entreprise directement. En 2018, l'obligation de reporter des brèches sera également effective dans l'Union Européenne, ce qui pourrait avoir un impact important dans le développement du marché de la cyber-assurance en Europe.

Biener *et al.* (2015), dans leurs recherches, discutent du cyber-risque en allant plus loin que la question des critères d'assurabilité et soulignent trois problèmes majeurs que pose la question de l'assurabilité du cyber-risque.

- L'indépendance et la prédictibilité des pertes ne sont pas données ainsi la mutualisation (entre assureurs) ne pourrait pas fonctionner de manière appropriée.
- L'asymétrie de l'information : Les entreprises ayant subi une cyber-attaque sont plus prônes à souscrire à une assurance (Schackelford, 2012) résultant ainsi en une sélection adverse. Mais les assureurs ont mis en place des contre-mesures (ex : *Screening*, questionnaires, audit, etc.). Et finalement le risque moral (*moral hazard*) : Le changement d'attitude face aux risques après souscription à une police d'assurance. Ici aussi, l'emploi de *screening* et le partage du risque sont employés pour pallier à ce risque (Eling et Schnell, 2016).
- Le troisième problème incombant au développement d'un marché de l'assurance du cyber est que le plus souvent les polices d'assurance ne couvrent qu'une petite partie

des pertes ou excluent certains évènements (ex : les pertes auto-imposées, l'accès à des sites non sécurisés, etc.)

Dans ces conditions, les scénarios extrêmes (faible probabilité, haute sévérité) ne peuvent pas être couverts par les polices d'assurance existantes (Eling et Schnell, 2016). Au vu du large nombre d'exclusions et de la nature dynamique du cyber risque, il règne une incertitude à propos des risques couverts par les cyber-assurances.
Lorsqu'il s'agit d'assurance, on retrouve également le problème de la définition d'une terminologie commune, permettant une comparaison d'offres aisée (Eling et Schnell, 2016). De manière générale, les polices disponibles ne couvrent que les petits risques et non les cas extrêmes qui pourraient conduire à d'énormes pertes.

Le marché de la cyber assurance en est à ses balbutiements, mais à mesure que le développement du marché se poursuit, les « *pools* » de risques deviendront plus importants et plus de données seront disponibles. De plus, de nouveaux acteurs dans le domaine de la collection de données rentrent dans les marchés, engendrant une disponibilité accrue de données (Eling et Schnell, 2016). Ceci augmentera la compétition et poussera les prix à la baisse. Cela mènera également vers une terminologie et une standardisation des contrats.

3 Le cas de la BGL et de la BIL : Analyse des données, discussion, découverte.

3.1 Introduction

Dans ce chapitre, le chercheur décrira tout d'abord ce que les répondants ont mentionné lors d'interview à questions ouvertes. Il s'agira d'abord de présenter les données d'un point de vue général, pour finalement analyser les réponses au questionnaire en se basant sur la revue de littérature afin d'affirmer ou d'infirmer les propositions faites au premier chapitre. Par la suite, sont dégagées les conclusions et recommandations, fournissant des suggestions pour de prochaines recherches. Les interviews ont été menées à Luxembourg, à la Banque Internationale au Luxembourg et à la BGL BNP Paribas respectivement le 01/06/2017 et le 08/06/2017.

3.2 Analyse descriptive

3.2.1 Le cas de la Banque Internationale à Luxembourg (BIL)

3.2.1.1 Taxonomie commune

Au niveau de la BIL, la mise en place d'une taxonomie commune est assez récente, le terme cybersécurité étant la terminologie du moment. En témoigne la cyber-attaque d'une ampleur sans précédent menée par une équipe d'hackers ayant programmé le ransomware « *wanna cry* ».

Le besoin d'une taxonomie commune est apparu il y a plus ou moins deux ans lorsque le besoin d'une évaluation de la maturité en matière de cybersécurité s'est fait ressentir dans la banque, notamment avec la montée en puissance des cyber-attaques. Cette taxonomie commune est nécessaire pour l'évaluation de la maturité de la banque et a été réalisée par une société d'audit qui accompagne la banque. Elle est également essentielle afin de communiquer, d'éduquer et sensibiliser les différents collaborateurs, mais également dans la phase de « *change management* ».

Au sein de la banque lorsqu'on parlait de « fraude au président », de malware, de ransomware, les employés avaient tendance à regrouper le tout dans une même catégorie sans faire de distinction. Aujourd'hui, cela change et demain ce ne sera plus le cas, d'où les termes : « *change management* », c'est-à-dire l'acceptation par le personnel de terminologies qu'ils entendent désormais dans la banque et qui sont harmonisées. Pour ce faire, la banque communique activement sur le sujet via Intranet notamment dans le cas de « *wanna cry* », où la banque expliquait les raisons et méthodes des hackers et du ransomware et donnait ses recommandations. Il ne s'agit en effet que d'informations via Intranet, mais cela permet d'avoir un bon retour quant à la sensibilisation et l'« *awareness* ». Ce processus d'information a graduellement réduit les erreurs dans la banque et ainsi renforcé la culture du risque.

3.2.1.2 Culture du risque, implication du « top » management et des autres départements

Au niveau de la culture du risque, et plus précisément du cyber-risque, il n'y a pas d'implication à proprement parler des autres départements que celui de l' « *information security* » dans la lutte contre le cyber-risque. Ainsi, les autres départements participent à des séances d'informations qui leur permettent de réaliser moins d'erreurs. On peut cependant citer les départements de communication interne et externe. Le premier joue un rôle important dans la sensibilisation, via la communication interne. Elle est utilisée pour réaliser l' « *awareness* ». Cette communication est réalisée a priori et non a posteriori en communiquant de manière interne sur un évènement en expliquant ce qui s'est passé, comment mitiger ce risque et les procédures à suivre pour éviter d'autres problèmes. Elle s'occupe donc de paraphraser, reformuler et vulgariser ce que le département sécurité de l'information (qui inclut le cyber-risque) désire communiquer car il s'agit d'un métier au jargon technique. Au niveau externe, la communication est un outil qui permet de mitiger notamment les conséquences sur la réputation.

Quant au mangement senior, la mission cybersécurité de la banque a commencé également il y a deux ans et elle implique les membres du comité de direction. La BIL organise des

STIRCO, c'est-à-dire un comité de direction du projet qui a lieu tous les trois mois et qui fait l'état des lieux des avancements et émet de nouvelles recommandations. Dans ce comité, on retrouve deux membres du comité de direction qui sont directement impliqués et qui reprennent ce qui se dit et se décide dans les STIRCO directement au niveau du comité de direction de la Banque.
De plus, ils sont formés également sur la question de la « fraude au président » : on leur demande également de sensibiliser en interne leurs collaborateurs. Cependant, il pourrait arriver qu'un manager, proche de la pension par exemple, ne se sente pas concerné directement et délègue cette responsabilité signifiant ainsi une implication à un niveau plus bas du management.

3.2.1.3 Le facteur humain : L'employé négligent et mal intentionné

En ce qui concerne le facteur humain, pour prévenir la négligence des employés, le rôle du top management est également essentiel : en effet, ce sont les « *senior managers* » qui sont chargés de transmettre les bonnes pratiques et d'induire une culture du risque forte. Cette transmission se fait donc par le top de la structure. En complément, il existe des campagnes au sein de la banque qui permettent aux différents collaborateurs de se former, de se sensibiliser et de développer leur « *awareness* ». Ce type de campagne de sensibilisation est annuelle et s'inscrit dans le cadre des pratiques ISO 27001.

Un nouveau collaborateur est également sensibilisé dès son arrivée. Il lui sera décrit ce qu'est le travail dans un environnement bancaire, le secret bancaire, ce qu'il peut ou ne peut pas faire et le familiariser avec les différentes classifications d'informations. Par exemple, certains documents peuvent être publics, restreints, confidentiels ou secrets (la différence entre les deux derniers étant la contenance de données clients pour le dernier. La banque organise régulièrement des quizz obligatoires sur Intranet. L'institution n'attend pas un retour de 100% vis-à-vis de ces tests, mais un retour de 70 à 75% représente une bonne moyenne.

Quant aux employés qui seraient malveillants, ils existent des outils IT en plus de la sensibilisation, plutôt destinée aux employés négligents. Ces outils sont contraignants et cette contrainte est mise en place au niveau de la gestion des entrées et sorties de données dans la banque. La banque est définie par un périmètre clos sur lequel il peut y avoir plusieurs portes d'entrée physique ou cyber. Ainsi, autoriser les employés à surfer sur le net peut être une porte. Comme outils de contrainte, on peut citer l'interdiction de téléchargements, l'interdiction de transmettre des formulaires via la création de formulaires en ligne, sauf exception (par exemple pour le site des impôts). L'emploi de webmail ou de toute autre boîte mail personnelle est également interdit ; en effet celui-ci peut être un moyen de sortir de l'information (pour rappel, les *Panama papers)*. Ce genre de communication est bloqué par des filtres et il s'agit de procédures automatisées de contrôle du web. Au niveau des mails au sein de la banque, on retrouve plus ou moins les mêmes contrôles à la différence qu'il existe un risque de conflit avec le département *Compliance* car les analyses dynamiques de mails sont considérées trop intrusives. Les employés acceptent cependant lors de la signature de leur contrat que soient conduites des analyses de pièces jointes si celles-ci sortent de la banque. Sont exempts les mails estampillés « privé » auquel cas l'attachement de pièces jointes est interdit.

Il persiste cependant une faille : il reste possible d'envoyer des informations contenues dans le corps du mail si celui-ci fait moins qu'un certain volume et si celui-ci ne contient pas de caractères prévisibles, tels que des références client. En effet le « *free text »* reste compliqué à détecter d'où la difficulté de repérer des noms par exemple.

A Luxembourg, il existe également le Computer Incident Response Center Luxembourg (CIRCL), qui est une organisation labélisée gouvernementale dans laquelle les entreprises et les organisations basées à Luxembourg peuvent contribuer. Cette organisation possède une plateforme qui s'appelle MISP et dont le but est la prévention. Par exemple si au Luxembourg il y a un incident du type DdoS, le CIRCLE préviendra les banques. C'est une agence qui réalise de l'analyse de haut niveau, fournit le service gratuitement et réalise une analyse proactive du territoire luxembourgeois.

3.2.1.4 Organisation du management du cyber-risque

A la BIL, comme dans beaucoup d'entreprises au Luxembourg, la sécurité de l'information fait partie du département du risque. Il s'agit d'un principe de neutralité qui différencie la partie « *IT security* » et la partie « *Information Security* » qui comprend les informations tant physiques que digitales. L' « *Information Security* » comprend la cyber sécurité qui ne se préoccupe que du digital.

Thierry Lopez (le CRO) a une vue moins complète que le responsable de la sécurité de l'information en tant que telle, mais possède une meilleure vue sur l'aspect opérationnel de ce risque.

Sont comprises dans la sécurité de l'information, une partie des règles de la gouvernance, les politiques de sécurité de la banque, et une partie contrôle à deux niveaux qui sont sur un même pied d'égalité.

Le premier niveau est opérationnel IT et concerne grande partie toutes les données qui se trouve sur les systèmes d'informations, mais également sur supports papiers, mais il n'y a pas d'automatisation des contrôles sur papier.

Le deuxième contrôle concerne les accès, que ce soit pour les employés internes à la banque ou avec les sous-traitants qui ont accès aux systèmes de la BIL.

Ensuite, on retrouve une partie « *Business continuity* » qui fait partie du management du risque et se chevauche avec la sécurité de l'information et la cyber sécurité, comme nous pouvons le voir sur le schéma ci-dessous.

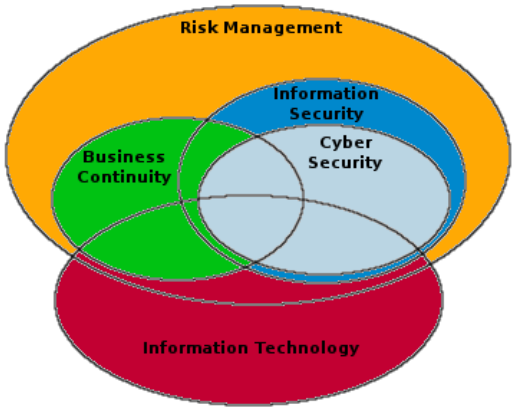

Schéma 5 : Organisation du management du cyber-risque.

Au niveau de la cyber sécurité la banque utilisons les matrices *Responsible, Accountable, Consulted, Informed* (RACI) qui définissent le rôle et les responsabilités d'un projet. *Informed* signifie recevoir l'information, mais ne rien en faire. *Consulted* veut dire qu'on demande un avis. *Accountable* est la personne qui implémente et remonte le résultat de son implémentation à celui qui est responsable. Le responsable de la cyber sécurité à la BIL est le CISO, tandis que l'ITSO est *accountable*. Un ensemble de politiques et de règles est défini par une personne qui n'a pas la connaissance, par exemple, l'expérience technique sur la configuration d'un firewall. C'est donc l'ITSO qui est vraiment dans la partie technique qui prend le relais en proposant des solutions, cependant l'aspect cyber-sécurité reste couvert par un ensemble d'acteurs.

3.2.1.5 Gestion des tierces parties

La banque regroupe sous le terme de tierces parties, la notion *d'outsourcing* et les prestations de services qui peuvent être réalisées dans la banque-même ou à l'extérieur de celle-ci, mais par un prestataire externe.

Pour la gestion des tierces parties, la banque a établi une double classification. La première est basée sur les coûts financiers annuels et la deuxième sur base de l'impact sur la sécurité. Chaque prestataire se voit attribuer un grade selon que celui-ci a accès ou non à des

informations sensibles que ce soit sur papier ou sur un support digital. L'aspect sécuritaire prime sur l'aspect financier. En effet, un jardinier qui accède au bureau du directeur, bien que peu coûteux, sera surveillé beaucoup plus parce qu'il peut potentiellement tomber sur des données très sensibles.

Une fois cette classification effectuée, la banque déclenche une procédure de *due diligence*. Cette procédure se fait de plusieurs manières, soit en mettant en ligne un formulaire à destination des tierces parties, soit en lui remettant directement un formulaire papier. Ce questionnaire reprend plusieurs questions du type : « Comment gérer vous les accès chez vous ? Vos locaux sont-ils protégés par des badges ? ».

Il s'agit d'une liste de 140 questions à remplir qui a été adaptée pour les prestataires de services tels que les petits prestataires (les traiteurs, etc.).

Cette « *due diligence »* permet donc d'établir la maturité des tierces parties en matière de sécurité de l'information, de confidentialité et de bonnes pratiques managériales. La banque attend donc que les tierces parties possèdent une maturité optimale sur la gestion des accès sur les serveurs chez eux, qu'ils procèdent à des vérifications mensuelles, etc.

3.2.1.6 La mitigation du cyber-risque et les assurances

Concernant les investissements en infrastructures hardware et software, la banque possède deux budgets. Il s'agit tout d'abord du budget prévisionnel récurrent. Ce budget est basé sur les besoins en IT et est connu à l'avance. Le deuxième budget consiste, lui, en un exercice annuel qui identifie les besoins-projets qui émanent des autres métiers.

Le budget de la cybersécurité faisait partie de ce deuxième budget. Il y avait une infrastructure vieillissante sur certains points et le département de la sécurité de l'information, bien que n'ayant jamais eu de problème, estimait qu'il fallait investir et a demandé un budget qui devait être validé par le comité de direction.

Quant à l'assurance, elle jouit d'un contrat spécifique en parallèle chez le même fournisseur. Ces contrats seraient sous-évalués de par la nature nouvelle de ce type d'attaque. En effet, les assureurs manquent de données et vivent également en j-1. Le contrat est spécifique

pour des raisons de taxonomies, il s'agit d'avoir des termes communs entre l'assureur, la banque et les informaticiens. Il y a la nécessité d'évoluer ensemble. Au départ, l'assureur possède une idée de contrat et le soumet afin que la taxonomie soit revue par la banque pour qu'il n'y ait pas de litiges. Il s'agit là d'un moyen d'évoluer sur un terrain neutre. Pour la part de la Banque, la couverture correspond aux attentes de la banque ainsi qu'à celles de l'assureur par rapport aux soucis que la banque a déjà pu avoir, d'où l'intérêt encore une fois, d'un contrat spécifique qui évite des problèmes d'interprétation.

3.2.1.7 La modélisation du cyber-risque

La banque ne modélise pas à proprement parler le risque opérationnel. En effet, la BIL est soumise aux règles de Bâle III et de fait, elle applique une approche standardisée pour le calcul de son capital régulatoire. Bien qu'utilisant l'approche stochastique et scénaristique, la banque se base surtout sur la deuxième approche afin de cartographier ses risques car elle s'est rendu compte qu'en ne se fondant que sur de la théorie, il y avait encore des incidents.
Cette approche scénaristique permet à la banque d'affiner et de créer certaines politiques spécifiques sur la cryptographie ou même sur le simple emploi d'un IPad.

Quant à la propriété « *low frequency / high severity* » du cyber-risque, la banque se base sur une méthodologie où elle part d'une échelle qui cherche à voir si un incident est déjà arrivé dans le monde, à Luxembourg puis enfin à la BIL afin de lui assigner une gradation entre 1 et 4. A partir de là, elle crée une matrice à 16 cases avec un impact et la probabilité, afin d'attribuer une note globale à un incident.

Pour la création des scénarios, la banque a fait appel à des experts sur le projet cyber sécurité de manière proactive et ce pendant 4 à 5 ans minimum. Le but étant d'avoir des scénarios concrets qui collent avec ce qui se fait en Europe et au Luxembourg. On peut également citer les experts qui sont dans l'équipe du CISO ainsi que dans le département IT.

Ces derniers ne créent pas de scénario, mais font la veille réactive chaque matin, le but étant de voir les tendances actuelles et éventuellement ce qui pourrait impacter la banque.

En matière de révision de l'approche de modélisation, la banque organise un comité de sécurité qui a lieu tous les deux mois, qui peut être lié à des projets qui sont demandés par les différents métiers de la banque. Par la suite, un dossier d'analyse est préparé sur base de la méthodologie (cf. plus haut) afin d'être présenté au comité de sécurité représenté par les différents départements selon qu'ils aient un rôle à jouer dans les projets. Le comité décide collégialement s'il y a lieu de progresser dans le dossier ou non. Cette veille permet de corriger les petites défaillances au fur et à mesure et n'est pas infaillible.

A cause du manque de données sur le cyber-risque puisque ces dernières sont historiques, la banque considère qu'il y aura toujours un décalage par rapport aux attaques qu'elle peut subir. La banque considère donc que rechercher des données pour les collecter ne sert à rien et préfère se baser sur l'avis d'experts qui émettent des scénarios. Elle se base également sur ce qui se passe au Luxembourg et sur le fait de savoir si une cyber-attaque au Luxembourg par exemple pourrait avoir un impact sur la banque. Si tel est le cas alors, l'incident est rajouté à la base de données de la banque.
Il y a également un outil externe sur place, Il s'agit de Monarch, une société qui fait de l'analyse de risques, en y entrant des *inputs* afin de voir les risques auxquelles la banque est soumise.

De plus, les mentalités ont bien évolué par rapport à l'époque où toute information était bonne à conserver afin d'obtenir un avantage sur un concurrent. Mais la nature systémique des attaques a forcé les banques à comprendre qu'il n'y a pas d'intérêt à retenir de l'information et que cela n'apportait pas forcément un avantage compétitif dans un contexte d'interconnectivité. D'où une collaboration accrue aujourd'hui.

3.2.2 Le cas BGL BNP PARIBAS

3.2.2.1 Taxonomie commune

Dans le cas de la BGL BNP Paribas, il n'existe pas de taxonomie commune à proprement parler. En effet la banque se base sur les évènements bâlois, qui définissent différents phénomènes types en termes de risques opérationnels. On retrouve la fraude interne et la fraude externe, dans lesquelles on peut inclure le cyber-risque[19]. La banque est donc dans les catégories bâloises plutôt que dans une classe spécifique nommée cyber-risque.

De plus, les incidents potentiels sont modélisés « *bottom-up* ». La direction ne donne pas de directive sur la manière d'analyser les scénarios majeurs. Chaque métier se doit d'analyser et comprendre ses différents processus et de les modéliser sur cette forme-là. Il s'agit donc pour eux de scénariser leurs risques potentiels. On y retrouve la cyber-fraude dans la classe d'évènements « fraude externe ».

3.2.2.2 Culture du risque et implication du « top » management et des autres départements

Au sein de la BGL, les membres du comité de direction sont responsables de la gestion du risque opérationnel dans leur entité ; il s'agit d'un premier niveau de défense qui permet la création d'une culture du risque forte qui implique effectivement le management « *senior*. » Cette implication se traduit par la mise en place de contrôles permanents qui identifient et cartographient les différents risques et qui assignent un contrôle pour chaque risque modélisé.

Selon qu'il s'agisse d'un risque majeur ou mineur, des contrôles plus ou moins stricts sont mis en place et c'est la responsabilité du responsable de métier qui doit gérer tous les risques opérationnels, cyber-risque inclus.

[19] On retrouve dans la fraude externe 80 à 90 % des évènements du type cyber-risque.

La fonction IT possède évidemment un grand rôle à jouer : ils ont des contrôleurs permanents qui cartographient leurs risques et qui mettent en place les contrôles nécessaires. De manière générale, chaque manager est responsable pour son entité et tous les managers sont impliqués ; il n'y en a pas un qui l'est plus particulièrement qu'un autre dans le premier niveau de défense.

Il existe également un deuxième niveau de défense qui est à charge des métiers du risque, qui interviennent dans cette deuxième ligne de défense en contrôlant les dispositifs sous-jacents et en se posant la question de leur suffisance quant à la sécurité.

Finalement, le troisième niveau de défense est nommé par la banque « inspection générale ». L'ensemble des deux premiers niveaux représente ce la banque appelle le dispositif de contrôle permanent : il s'agit du dispositif journalier, et on retrouve dans le troisième une vérification périodique qui contrôle aussi bien le premier niveau que le deuxième niveau.

3.2.2.3 Le facteur humain : l'employé négligent ou mal intentionné

Dans le cas des employés qui pourraient être négligents, plusieurs éléments ont été mis en place par la banque.

Le premier type de formation est générique et destiné à l'ensemble des employés : chaque employé reçoit une charte informatique lorsqu'il commence à travailler dans la banque. Il s'agit d'une charte de bonnes pratiques qui contient des règles relativement simples concernant le secret bancaire et professionnel, ainsi que l'emploi des réseaux sociaux qui peut être une source d'informations pour la criminalité.
Le deuxième type de formation porte sur ce que la banque appelle les « opérationnels » : il s'agit des personnes qui travaillent par exemple sur la plateforme SWIFT. Ce sont également les personnes qui traitent les informations qui concernent le développement des modèles et

qui ont des accès administrateurs. Ces personnes reçoivent des formations spécifiques dédiées à la fonction les rendant ainsi attentifs aux risques qui leur incombent. Sous peu, des formations spécifiques aux risques IT et cyber-risque à destination du management seront mises en place.

En ce qui concerne le risque des employés mal intentionnés, il convient de rappeler que l'évaluation des risques se fait « *bottom-up* » et qu'il faut donc intégrer la notion d'employés mal intentionnés comme un scénario avec une cartographie des risques liés et des contrôles. Il y a également des alertes dans le cas de sortie en masse de données : ce sont des contrôles par software mis en place par l'IT.

3.2.2.4 Organisation du management du cyber-risque

Comme mentionné précédemment, chaque métier doit évaluer le risque lié à ses processus et à la fraude qui y est liée. Chaque responsable de métier est responsable de ses *process*, ainsi que des faiblesses et défaillances dans son dispositif. Mais il est évident que l'IT reste responsables de la partie technique des attaques.

3.2.2.5 Gestion des tierces parties

Lorsque la banque travaille avec des tierces parties (ici en matière IT), elle possède de très fortes préférences pour tout ce qui est professionnel du secteur financier (PSF) parce qu'ils sont également très réglementés. Cela permet ainsi à la banque de connaître son vis-à-vis et de savoir que celui-ci est tout autant réglementé.

Ensuite, la banque établit des contrats de confidentialité avec les tierces parties qu'elle emploie, ce qui remet la responsabilité sur le « *tierce provider* ». Ces contrats sont relativement contraignants avec des clauses sur la confidentialité. Ces clauses permettent de s'assurer que les données ne seront utilisées que pour la mission qui est assignée, mais que les données seront également détruites après la mission.

Finalement, les accès que les tierces parties ont dans la banque sont limités au maximum. Un externe verra son accès à la banque le plus restreint possible. Il y a également des questionnaires qui sont remis, mais il s'agit d'une procédure globale qui touche autant le cyber que ce qui n'est pas cyber. Cela dépend de l'intensité des relations que la banque entretient avec la tierce partie. Ces questionnaires permettent d'évaluer les dispositifs de contrôle et selon les projets, la banque se réserve même le droit d'aller faire des audits chez les tierces parties.

3.2.2.6 Mitigation du risque et les assurances

Au niveau des infrastructures (Anti-virus, pare-feu, infrastructure matérielle) le budget est un exercice banque. Chaque métier a la responsabilité d'établir son budget. Dans le cas par exemple de tout ce qui est purement informatique tel que les pare-feux, il s'agit effectivement d'un budget que l'IT élabore en cours d'année pour l'année suivante comme le font les autres métiers qui élaborent leur budget. Celui-ci est ensuite soumis au conseil d'administration avant d'être challengé et puis validé. Il n'y a donc pas de budget IT par métiers, le budget de l'IT est refacturé selon les différents métiers. Au niveau de la banque, on retrouve des « *profits center* » et des « *costs center* » dont l'IT fait partie.

Au niveau des assurances la banque ne possède pas une police d'assurance spécifique pour le cyber-risque, il est inclus dans la police actuelle.

3.2.2.7 Modélisation du cyber-risque

Pour modéliser le cyber-risque, la banque emploie l'approche scénaristique. Quant au problème lié à la propriété de queue lourde du cyber-risque, la banque identifie des incidents potentiels qui sont des incidents pour lesquels elle développe d'abord des scénarios. Par la suite, chacun de ces scénarios se voit attribuer un « *likely-case* » avec fréquence et impact et sur certains scénarios un « *worst-case* » avec un impact sur le

« *worst-case* ». Ensuite, une remodélisation stochastique est effectuée. Cette modélisation est indépendante. En effet, le « *worst-case* » et le « *likely-case* » sont modélisés de façons indépendantes et agrégées sur un principe de « *weighted average loss* ».

Pour la définition des scénarios et pour chaque incident potentiel, on retrouve autour de la table tous les experts nécessaires. Dans le cas du cyber-risque, il y a toujours une personne du département IT présente, mais aussi des personnes du département juridique afin de calculer l'impact possible, depuis des amendes jusqu'aux condamnations juridiques.
Ces scénarios vont véritablement dans le détail et dans le cas du cyber-risque, la banque essaie de scénariser des évènements très réalistes. Concernant l'emploi d'experts externes, la banque fait appel à des experts, mais au sein du groupe (à Paris par exemple si c'est nécessaire sur certains scénarios).

Quant à la révision et la nature dynamique du cyber-risque, la méthodologie à la BGL prévoit que les scénarios soient revus chaque année. Ils doivent être remis en question afin de prendre en compte les nouveaux risques qui apparaissent. Il y a également un challenge au niveau du groupe, c'est-à-dire que si une filiale du groupe déroule un nouveau scénario, il s'agira pour la banque de l'analyser, de le comparer à sa propre cartographie du risque et de prendre les mesures adéquates si nécessaire. La procédure de révision annuelle est inhérente à tous les risques opérationnels (cyber inclus).

En matière de modélisation, celle-ci ne se fait pas sur base d'informations externes, empiriques, mais sur base de scénarios. Mais il est évident que ces scénarios incluent des réflexions sur l'impact que des événements, comme celui de la banque du Bangladesh, pourraient avoir sur la banque. Mais les modèles ne sont pas paramétrés par des données empiriques.

Dans la prochaine section, le chercheur répondra aux questions de départ qui cherchent à déterminer quelle approche managériale adopter pour gérer au mieux le cyber-risque, comment le modéliser dans un contexte de rareté des données, et finalement comment

réduire ce risque alors que la technologie et la nature du cyber-risque ne cessent de changer de par son dynamisme.

3.3 Analyses et comparaisons des données

3.3.1 Gestion du cyber-risque

3.3.1.1 Taxonomie

On retrouve à la BIL une taxonomie commune qui dépasse la définition de Bâle en matière de risques opérationnels. Elle a été mise en place car le contexte des cyber-attaques galopantes a créé le besoin d'évaluer la maturité des banques. De plus avoir un même vocabulaire lorsqu'il s'agit de cyber-sécurité, facilite la communication qui est un élément essentiel en cas d'attaques ou même pour sensibiliser les employés et développer leur conscience en matière de sécurité de l'information.

A l'inverse de la BIL, la BGL n'a établi aucune taxonomie propre à l'entreprise. La banque se base exclusivement sur la définition Bâle II du risque opérationnel qui ne comporte pas de partie cyber-sécurité à proprement parler. On retrouve notamment la cyber-sécurité parmi la fraude interne ou la fraude externe. Ce manque de taxonomie est sans doute dû au fonctionnement de la banque, c'est-à-dire « *bottom-up* » (voir supra).

3.3.1.2 Le rôle du top management

A la BIL et de manière générale, il n'y a pas d'implication des autres départements dans la gestion du cyber-risque. Inversement à la BGL chaque responsable de métier est chargé de cartographier ses processus et est impliqué dans la gestion du cyber-risque dans son entité. Cette différence s'explique sans doute par le fait que dans le cas de la BIL, la cyber-sécurité a fait l'objet d'un projet particulier avec la création d'une taxonomie afin d'être traitée en tant que risque singulier alors qu'à la BGL celle-ci est incluse dans les évènements bâlois en tant que risque opérationnel que les managers sont chargés de cartographier.

Au niveau du comité de direction, on retrouve dans les deux banques l'implication des membres du comité. A la BIL ces derniers suivent des formations axées cyber depuis deux ans maintenant, alors qu'à la BGL ce type de formation est neuf A la BIL, on retrouve également leurs implications au niveau d'un comité de projet sur la cyber-sécurité. Tout ce qui se dit dans ces comités est communiqué au niveau du comité de direction de la banque. N'ayant pas de projet cyber-sécurité en tant que tel et travaillant « *bottom-up* », l'implication des membres du comité de direction se traduit sous formes de contrôles à la BGL (cf. supra).

Il reste évident que les départements IT des deux entités jouent un rôle majeur dans la lutte contre les cyber-menaces.

3.3.1.3 Gestion des employés en matière de cyber-risque

3.3.1.3.1 Les employés « négligents »

Dans les deux banques les nouveaux employés reçoivent une formation qui porte sur l'environnement bancaire, mais également sur le secret bancaire, l'emploi des réseaux sociaux et la confidentialité : il s'agit d'une formation générique.
A la BIL, le management senior et le département communication sont chargés de communiquer sur le risque afin de développer une conscience à propos de ce risque et ainsi construire une culture du risque solide. A la BGL on retrouve en plus de la formation générique, une formation plus poussée pour les opérationnels qui traitent des informations sensibles. Il y a également une formation spécifique IT, mais il s'agit d'une nouveauté à l'inverse de la BIL où une telle formation a été mise en place depuis un certain temps.

3.3.1.3.2 Les employés malveillants

En ce qui concerne les employés dont les intentions seraient malveillantes, les deux banques ont mis en place une série d'outils afin de lutter contre l'extraction de données en masse par

exemple. Pour la plupart il s'agit d'outils du type software qui ne sont pas infaillibles, mais permettent un niveau de sécurité supérieur.

3.3.1.4 Le rapport avec les tierces parties

A la BIL, la gestion des tierces parties se fait sur base de la maturité en matière de sécurité de l'information des prestataires externes. Cette évaluation se fait sur base de questionnaires, une procédure nommée « *due diligence* » et la banque attend des tierces parties qu'elles possèdent une maturité optimale sur la gestion des accès. La BGL quant à elle va encore plus loin, en effet elle évalue également la maturité des prestataires externes en remettant des questionnaires, mais il s'agit d'une procédure standard. La BGL préfère travailler avec des prestataires qui sont des professionnels du secteur financier car ces prestataires sont également fortement réglementés. De plus la banque se réserve le droit de réaliser des audits afin de s'assurer du sérieux des tierces parties avec qui elle travaille.

3.3.2 La modélisation du cyber-risque

3.3.2.1 Approche stochastique ou scénaristique ?

Bien que les deux banques emploient l'approche stochastique, elles favorisent cependant une approche scénaristique pour cartographier leurs risques. A la BIL, cette approche à l'avantage de permettre de rester proche de la réalité en matière de risque. Il en va de même à la BGL puisque les processus opérationnels sont cartographiés par chaque métier et ceci sans utiliser des données historiques, utiles à l'emploi de la stochastique.
Les deux banques partent d'incidents qu'elles cartographient avec une probabilité ainsi que l'impact de l'incident. L'approche scénaristique est donc favorisée à l'approche stochastique de par le manque de données historiques, mais aussi et surtout par le fait que cette approche permette de se rendre compte de la réalité des deux banques au niveau des processus.

3.3.2.2 Propriété à queue lourde du cyber-risque

Afin de traiter la propriété « *low frequency, high severity* » du cyber-risque, les deux banques identifient des incidents potentiels et les scénarios possibles afin d'attribuer des probabilités à ces incidents ainsi que leurs impacts. A la BIL ceci se fait sous forme de matrice où une note globale est attribuée à un incident. C'est aussi le cas à la BGL à la différence, qu'ici on attribue à un incident un « *likely case* » et parfois un « *worst case* » qui sont agrégés afin d'obtenir une moyenne pondérée des pertes.

3.3.2.3 Définition des scénarios.

Afin de définir les différents scénarios, les deux banques font appels à des experts. Cependant, la BIL fait appel à des experts extérieurs à la banque, tels que des auditeurs externes afin de monter les différents scénarios. Il faut également rappeler que la cyber sécurité a fait et fait encore l'objet d'un projet à part, au sein de la BIL et que la participation des experts s'est faite de manière proactive durant 4 à 5 ans.
Quant à la BGL, elle fait quasi exclusivement appel à des experts en son sein. On retrouve dans les équipes des personnes du département IT à l'inverse de la BIL où ceux-ci ne participent apparemment pas à la création de scénarios, mais seulement à une veille stratégique. Ils collaborent avec des personnes du département juridique qui étudient les impacts possibles, tels que des condamnations juridiques.
Cette différence est sans doute due à la taille des deux groupes. En effet la BGL dispose d'experts disséminés partout dans le monde de par la taille de son groupe et peut donc faire appel à un expert de Paris afin de traiter un problème à Luxembourg.

3.3.2.4 Nature dynamique du cyber-risque et changements de technologie

Il est évident que la cyber sécurité nécessite une révision et une veille qui permettent de se tenir à jour. Les deux banques revoient à des intervalles différents leurs méthodologies ainsi que la cartographie de leurs risques (cf. 3.2.1.7 et 3.2.2.7).

3.3.2.5 Le manque de données historiques

Ainsi, les deux banques favorisent l'approche scénaristique qui permet de rester plus proche de la réalité qu'une modélisation stochastique basée sur des données historiques. Celles-ci ont en effet le défaut d'être en décalage avec le présent. De plus, les banques communiquent de plus en plus en matière de cyber sécurité car elles se sont rendues compte qu'il n'y a pas d'avantage compétitif à retenir de l'information en matière de cyber-sécurité. Mais il reste bien évident que des incidents du type cyber déclenchent dans les deux banques une réflexion nouvelle sur leurs processus et les données historiques ne sont donc plus d'aucune utilité.

3.3.3 Outils pour la réduction de ce risque et mitigation

Comme mentionné, les deux banques investissent dans des systèmes software et hardware afin de prévenir toute fuite de données ou intrusions. Ces investissements font l'objet d'un budget récurent à la BIL, mais aussi d'un budget annuel par projet et par métier. La BGL quant à elle fonctionne plus ou moins sur le même principe ; chaque métier est responsable de son budget, y compris le département IT qui a son propre budget, mais qui refacture les besoins en IT aux différents métiers. Il n'y a donc pas de budget IT par métier comme c'est le cas à la BIL. Dans les deux banques, ces budgets sont soumis à l'approbation du comité de direction selon des modes de fonctionnement différents.

Au niveau des assurances, les deux banques jouissent d'une couverture qui correspond à leurs attentes. Cependant, la cyber-sécurité fait l'objet d'une police à part à la BIL dans un souci de clarté en termes de taxonomie et d'interprétation. C'est le cas inverse à la BGL du fait sans doute de l'emploi d'une définition bâloise des évènements cyber-risques.

3.4 Discussion et découverte : Caractéristique de l'environnement bancaire cyber-résilient

3.4.1 Approche managériale holistique

3.4.1.1 Culture du risque et le rôle du top management

Dans chacune des banques, le senior management est impliqué dans la gestion du cyber-risque ce qui contribue à créer, comme le souligne Hull (2012), une culture du risque forte qui s'inscrit dans l'« *entreprise risk management* » (ERM) des deux banques. Bien que cette implication puisse prendre diverses formes (Cf. Section 3), elle contribue effectivement à la BIL comme à la BGL à induire par différents moyens, tels que la mise en place de contrôles, une culture du risque qui permet de comprendre les enjeux de la cyber-sécurité.

Hull (2012) accentue également l'importance de développer une approche holistique qui implique tous les départements dans la gestion du risque et donc du cyber-risque. Dans les deux banques, cette implication des différents départements prend l'aspect de formations à la cyber-sécurité durant lesquelles les employés sont formés afin d'éviter les risques liés au cyber. Mais les employés eux-mêmes ne sont pas directement concernés dans la lutte contre la cyber-menace. Il importe cependant de communiquer intensivement sur le sujet : cela semble être beaucoup plus le cas à la BIL où une taxonomie commune a été développée, à l'inverse de la BGL.

Bien qu'une approche holistique soit nécessaire, Eling et Schnell (2016) soulignent également l'intérêt d'un engagement institutionnel de la part d'une équipe spécifiquement dédiée à la sécurité informatique, ce qu'on peut retrouver dans les deux banques.

Finalement, le développement d'un cadre ERM implique de définir la situation initiale et les buts de la gestion du cyber-risque (Eling et Schnell, 2016). Pour ce faire, les managers ont mis en place à la BIL et à la BGL des scénarios qui permettent de modéliser ce risque, mais aussi d'identifier les actifs pertinents, leurs processus pour ensuite déterminer les menaces

potentielles et leurs sources afin de développer un processus d'évaluation des risques. On retrouve tout cela dans les trois types de contrôles à la BGL et dans le STIRCO à la BIL.

3.4.1.2 Le facteur humain

Comme mentionné plus haut, la menace extérieure reste réelle. Cependant comme le souligne la société spécialisée dans le domaine de la sécurité CISCO (2008), la plupart des pertes de données provient d'activités internes aux organisations. Il importe dès lors de prendre en compte le facteur humain dans les aspects managériaux du cyber-risque. Ce facteur humain est géré par la formation aux risques ainsi que la sensibilisation dans le cas d'employés peu diligents et par la mise en place d'outils hardware et software pour faire face aux actions d'employés malveillants. Dès lors que l'on parle d'employé malveillant ou de négligence, la solution réside dans la formation, la communication ainsi que la prévention inscrite dans le cadre de la gestion du risque de l'entreprise.

3.4.1.3 Tierces parties

Selon Freund et Jones (2014) la relation aux tierces parties représente un risque significatif pour la gestion du cyber-risque. Et c'est notamment le cas à dans les deux banques interviewées où l'accès aux informations pour les externes est fortement limité et où la maturité des tierces parties sont évalués à l'aide de moyens divers, en analysant leurs pratiques managériales, ainsi que la certification des tierces parties (BGL), etc.

3.4.2 La modélisation du cyber-risque : La scénarisation comme aide à la prise de décision

Par manque de données et de par la nature à faible fréquence/haute sévérité du cyber-risque, certains auteurs dont Lloyd's (2015), préconisent l'emploi d'une approche scénaristique fondée sur le jugement d'experts. Dans les deux banques interviewées, c'est cette approche qui était privilégiée afin de pallier à la nature changeante de ce risque, aux

changements de technologie (Eling et Schnell, 2016), mais également au manque de données ou leurs non-validités du fait de leurs décalages dans le temps.

La scénarisation ne sert pas seulement à modéliser le risque ; elle sert également à la prise de décision. En effet cette scénarisation se fait sur base d'une cartographie des processus et des risques que ceux-ci engendrent, permettant ainsi d'identifier les actifs à risques, de prendre des décisions de manière plus informée tant pour l'approche managériale [3.4.1] que pour la réduction du risque [3.4.2] et pour le contrôle permanent de ces risques.

Une fois ces scénarisation et modélisation réalisées, le calcul des distributions agrégées et de la VaR ou C-VaR se fait sous les mêmes modalités que pour le risque opérationnel étant donné que le cyber-risque rejoint les définitions bâloises.

3.4.3 La réduction du risque : Evitement, mitigation, transfert et rétention

Comme fait mention section [2.7] pour réduire le cyber risque, l'évitement à l'ère du tout digital n'est pas possible (Eling et Schnell, 2016). Il reste alors pour les banques la mitigation, le transfert et la rétention du cyber-risque.

Pour les deux banques interviewées la mitigation du risque passe par la mise en place d'outils managériaux. Le management éduque les employés et met en place des outils qui préviennent d'éventuelles fuites de données. Cette mitigation du risque doit s'accompagner du transfert de ce risque par la souscription à une police d'assurance qui soutient la mitigation par la prise en compte de l'expertise d'assureurs (Eling et Schnell, 2016).

Ces polices d'assurances peuvent faire l'objet d'une police particulière à part, comme c'est le cas à la BIL afin d'établir les termes du contrat de manière plus explicite (Eling et Schnell, 2016). On peut y retrouver une taxonomie développée de concert par l'entreprise et l'assrueur. A la BGL, cette police est incluse explicitement dans la police actuelle avec une prime supérieure ce qui est sans doute due au manque de taxonomie.

Malgré le développement moindre du marché de la cyber-assurance en Europe, les banques jouissent d'une couverture adaptée à leurs besoins. Il reste que selon la BIL, ces polices sont sous-évaluées du fait de l'asymétrie d'informations (Schackelford, 2012) et du manque de reports de brèche.

4 Conclusions et futures recherches

4.1 Conclusions

La cyber-sécurité et les risques qu'elles engendrent sont des problèmes qui touchent toutes les industries et le secteur bancaire. Les institutions financières n'échappent pas à ce problème qui est global, de par l'inter-connectivité des systèmes informatiques ainsi que par la globalisation de nos économies. Cette dimension internationale requiert une coopération renforcée entre états et entreprises afin d'endiguer un problème dont la nature n'a de cesse d'évoluer, le rendant ainsi quasi impossible à solutionner complètement.
Dans ce contexte il importe d'établir un environnement cyber-résilient en mettant en place les outils managériaux qui permettent de gérer ce risque en le mitigeant, le transférant et éventuellement en retenant une part de ce risque. Pour ce faire il importe de pouvoir modéliser le cyber-risque afin de soutenir les décisions managériales et de fournir les outils adéquats afin de soutenir le management.

Afin de répondre aux impératifs d'un environnement cyber-résilient, il importe de répondre aux questions suivantes :

- Quelle approche managériale est complémentaire à la gestion du cyber-risque dans l'industrie bancaire ?
- Comment modéliser ce risque ?
- Quels outils et quelles stratégies sont nécessaires pour réduire ce risque ?

Des entretiens ont donc été réalisés à la Banque Internationale à Luxembourg ainsi qu'à la BGL BNP Paribas. Ces interviews [20]confrontées à la revue de littérature permettent de tirer les conclusions qui suivent.

4.1.1 Approche managériale

Il existe à chaque étape du management du risque des outils et pratiques qui nécessitent une adaptation pour le cyber-risque. Une approche holistique reste nécessaire afin de saisir le problème. Cette approche nécessite une taxonomie commune qui permet à l'entreprise entière de communiquer sur des bases similaires.

Le cyber-risque bien qu'étant le sujet principal de préoccupation du département IT, doit faire l'objet d'une attention particulière de tous les collaborateurs ainsi que du management senior. Ce dernier est le premier responsable en cas de problèmes, mais aussi le premier communicant des bonnes pratiques en matière de cyber-risque. Pour ce faire, les banques et institutions financières se doivent de communiquer avec leurs employés, les clients ainsi que les fournisseurs et tierces parties sur le cyber-risque. Cette communication est plus efficace lorsqu'elle est réalisée de manière *top-down*.

Tout cela permet d'avoir un cadre de gestion du risque de l'entreprise qui promeut des bonnes pratiques en matière de gestion du risque, de communication et qui ultimement permet d'obtenir un environnement plus résilient face à la cybercriminalité.

4.1.2 Modélisation

L'approche stochastique ne permet pas de se rendre compte de la réalité du terrain. Il est dès lors suggéré de favoriser une approche scénaristique qui permet de mieux saisir la fréquence ainsi que l'impact des évènements du type cyber-risque. L'emploi d'experts permet de mieux saisir la portée des scénarios sur plusieurs aspects, dont la réputation pour n'en citer qu'un.

[20] Annexe 1 et annexe 2.

De plus cette approche permet d'éviter l'écueil que représente le manque de données historiques, leur décalage dans le temps, ainsi que la propriété faible fréquence/haute sévérité du cyber-risque.

La modélisation adéquate permet de soutenir les décisions managériales tant sur le plan de l'approche à prendre que sur les investissements à réaliser en matière de software ou hardware.

4.1.3 Réduction du risque et assurance

La réduction du cyber-risque passe par l'emploi de pratiques managériales propices à l'endiguement de ce risque [4.1.1]. Ces pratiques trouvent leurs sources notamment dans la prise de décision informée qui découle d'une modélisation adéquate, de la communication entre les différents départements et au sein d'un groupe, ainsi que du contrôle et de la révision permanente des risques liés au cyber.
Lorsqu'il s'agit de réduire ce risque, on peut également citer l'emploi de software et hardware qui permettent de limiter et non de supprimer le risque lié aux menaces externes ou aux employés malveillants. Ici la cartographie des risques et la scénarisation jouent un rôle extrêmement important.

Le marché de l'assurance du cyber bien qu'étant moins développé qu'aux Etats-Unis, n'est pas en reste en Europe. Lorsqu'il s'agit de contrats négociés de concert avec l'assureur, les couvertures correspondent aux attentes des banques, mais les couvertures sont actuellement sous-évaluées.

4.2 Recherches futures

Cette recherche analyse les bonnes pratiques afin d'obtenir un environnement cyber-résilient. Beaucoup plus pourrait être réalisé en étudiant le comportement et la perception des consommateurs face aux risques dans les entreprises commerciales et de détails, en mettant l'accent sur le fatalisme latent dont font preuve les personnes face au cyber-risque. Il pourrait être intéressant d'identifier les éléments qui favorisent cette perception et permettre ainsi d'améliorer la conscience en matière de cyber-risque. Il pourrait également être intéressant de comparer la perception du risque et l'aversion au risque dans le domaine de la cyber-sécurité avec d'autres domaines d'assurances.

Il importe également d'analyser le lien entre les nouvelles technologies comme le *Big data*, le *deep learning* et le cyber-risque car ces technologies sont prometteuses et devraient permettre aux métiers de la risque et de l'information d'être plus précis et rapide avec un traitement de données jamais égalé auparavant.

4.3 Auto-Evaluation

L'auto-évaluation suit une analyse SWOT.

S : La recherche donne un aperçu des bonnes pratiques managériales dans le domaine de la gestion du cyber-risque dans le secteur bancaire et dans les institutions financières. Les interviews réalisées dans les banques ont permis de renforcer les intuitions développées lors de la réalisation de la revue de littérature.

W : La recherche se base sur deux interviews ce qui ne permet pas d'inférer les résultats de manière définitive. Néanmoins, la recherche permet d'avoir un aperçu pour d'éventuelles études futures. En matière de modélisation, la recherche manque de démonstrations mathématiques. Cela est dû à une faiblesse de la part du chercheur en matière de modélisation et d'emploi d'outils statistiques. La recherche n'avait pas une portée

quantitative, mais l'emploi de statistiques aurait pu compléter l'argumentation du chercheur.

O : Le sujet est d'actualité et évoluera encore. En effet, l'apparition de nouvelles technologies permettra de saisir le cyber-risque de façon nouvelle, et cela engendra de nouvelles recherches dans le domaine.

T : Le manque de littérature dans le domaine du cyber-risque dans l'industrie bancaire. On retrouve énormément de données sur les différentes bases de données, mais celles-ci ne s'appliquent pas forcément au domaine bancaire et financier.

5 Bibliographie

Articles de périodiques électroniques :

Biener, C., Eling, M., & Wirfs, J. H. (2015). Insurability of cyber risk: an empirical analysis. *The Geneva Papers on Risk and Insurance Issues and Practice*, *40*(1), 131-158.

Cebula, J. L., & Young, L. R. (2010). *A taxonomy of operational cyber security risks* (No. CMU/SEI-2010-TN-028). CARNEGIE-MELLON UNIV PITTSBURGH PA SOFTWARE ENGINEERING INST.

Eling, M., & Schnell, W. (2016). What do we know about cyber risk and cyber risk insurance?. *The Journal of Risk Finance*, *17*(5).

Maillart, T., & Sornette, D. (2010). Heavy-tailed distribution of cyber-risks. *The European Physical Journal B-Condensed Matter and Complex Systems*, *75*(3), 357-364.

Shackelford, S. J. (2012). Should your firm invest in cyber risk insurance?. *Business Horizons*, *55*(4), 349-356.

Rakes, T. R., Deane, J. K., & Rees, L. P. (2012). IT security planning under uncertainty for high-impact events. *Omega*, *40*(1), 79-88.

Wheatley, S., Maillart, T., & Sornette, D. (2016). The extreme risk of personal data breaches and the erosion of privacy. *The European Physical Journal B*, *89*(1), 7.

Monographie :

Creswell, J. W. (2013). *Research design: Qualitative, quantitative, and mixed methods approaches*. Sage publications.

Freund, J., & Jones, J. (2014). *Measuring and managing information risk: A FAIR approach*. Butterworth-Heinemann.

Hull, J. (2012). *Risk management and financial institutions* (Vol. 733). John Wiley & Sons.

Jones, S., Wahba, K., & Van der Heijden, B. (2008). *How to write your MBA thesis*. Meyer & Meyer Verlag.

Refsdal, A., Solhaug, B., & Stølen, K. (2015). Cyber-risk management. In *Cyber-Risk Management* (pp. 29-47). Springer International Publishing.

Documents non-publiés ou à diffusion limitée :

Allianz. (2015). *A Guide to Cyber Risk, Managing the Impact of Increasing Interconectivity*.

Böhme, R., & Kataria, G. (2006, June). *Models and Measures for Correlation in Cyber-Insurance*. In *WEIS*.

Cebula, J. L., & Young, L. R. (2010). *A taxonomy of operational cyber security risks* (No. CMU/SEI-2010-TN-028). CARNEGIE-MELLON UNIV PITTSBURGH PA SOFTWARE ENGINEERING INST.

Cisco. (2008), *Data leakage worldwide: The high cost of insider threats*.

CRO Forum. (2014), *Cyber resilience - the cyber risk challenge and the role of insurance*.

Dunbar T. (2012), *The first steps to managing cyber-risk*.

Henrard L. (2009), *Risk management of financial institution*.

International Finance Corporation, & The MasterCard Foundation. (2016),

Lloyd's. (2015), *A quick guide to cyber risk*.

Lloyd's. (2015), *Business blackout – the insurance implications of a cyber-attack on the US power grid*.

Marsh. (2016), *Marsh launches new cyber risk assessment solutions*.

National Association of Insurance Comissioners (NAIC). (2013), *Cyber risk*.

PwC. (2016), *Turnaround and transformation in cybersecurity*.

Scalar Consulting. (2006), *Pratical calculation of expected and unexpected losses in operational risk by simulation*.

SecurityScoreCard R&D Department. (2016), *2016 Financial Industry Cybersecurity Report*.

Symantec. (2016), *Internet security threat report*.

World Economic Forum. (2015), *Partening for Cyber Resilience: Towards the Quantification of Cyber threats*.