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 ? (Annexes)

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

6 Annexes

6.1 Annexe 1 : Interview à la BIL.

(En gras le répondant.)

Du côté de la BIL, comme dans beaucoup d'entreprises au Luxembourg, la sécurité de l'information fait partie du risque. Quelques fois, on nous demande et on se demande pourquoi ce n'est pas rattaché à l'IT.

Cela s'explique par le principe de neutralité il y a la partie IT security d'un côté et l'Information security rattaché au risque de l'autre. Ceci pour pas les mélanger et à la limite pour ne pas être jugé partie.

C'est le cas à la BIL, l'information security est bien rattachée au risque dont Thierry Lopez et Pierre Malevez qui est dans le comité de direction de la banque font partie. Thierry vient juste après et moi au niveau de l'information security. Chez Thierry on va retrouver aussi bien la sécurité de l'information que les autres risques comme le risque opérationnel, le risque de crédit, le risque modèle y compris la partie sécurité de l'information. Mais Thierry a une vue moins complète sur l'information security, un peu plus sur la partie risque opérationnel. Son dada je dirais c'est un peu l'ensemble des risques. Maintenant sur l'information security, c'est un peu à part. Ça se voit quand on a des discussions avec les autres managers, il y a des fois des terminologies et des choses utilisées que moi je ne comprendrais pas et réciproquement.

L'information security est très proche niveau structure et organisation de la norme ISO 27001. On retrouve en effet dans l'information security une partie gestion de la gouvernance, les politiques en place, la politique de sécurité de la banque, donc les définitions de tous ces éléments-là pour la partie gouvernance.

Ensuite, on trouve une partie contrôle, généralement on parle de contrôle de deuxième niveau. Le premier niveau lui sera plus opérationnel IT parce que tout ce qui est information va en grande partie concerner ce qui est en rapport avec le système d'information également ce qui est sur partie papier, mais bon on ne va pas automatiser un contrôle IT là-dessus.

~~L~~e contrôle de deuxième niveau sur la partie informatique concerne mon département, on y retrouve une partie contrôle de tous les accès, que ce soit les employés internes à la banque ou avec les sous-traitants avec qui on travaille qui ont accès à notre système d'information ou les employés qui ont accès à des informations à l'extérieur (ex : Deloitte, PwC, etc…) avec qui on est amené à échanger pas mal d'informations (des documents, etc...) Donc il s'agit également de gérer leurs accès.

Ensuite, on retrouve la partie business continuity. Imaginons qu'une partie de l'immeuble s'effondre et que cela impacte 7 services différents, la question est alors de savoir comment on va reprendre le relais, en se demandant si on a un site de secours quelque part, s'il y a des normes à respecter sur ce qu'il vient de se passer, de combien de postes on dispose sous x temps. On a défini plusieurs périmètres que l'on peut retrouver sous forme d'un schéma. On a défini une zone IT security, au-dessus de ce périmètre on retrouve la partie cyber-security. Autour de ça, on va avoir la partie information security, dont notre département est en charge. Donc, les sujets dont nous traitons vont toucher autant la cyber-security que la partie IT security mais pas hiérarchiquement, c'est-à-dire que ce n'est pas moi qui vais diriger la partie IT-Security, par contre on va s'assurer qu'effectivement les contrôles effectués correspondent aux règles que nous définissons. On est vraiment presque sur une relation de prestation de services, c'est-à-dire que l'IT preste un service pour tous les métiers de la banque. Et en termes de métiers de la banque, on définit un cadre et tout ce qui est presté niveau IT doit être contrôlé et défini.

1. Au sein de votre organisation, existe-t-il une taxonomie commune entre les différents départements en matière de cyber-risque ?

On essaie de la mettre en place, tout justement je disais la cyber-security c'est vraiment la terminologie du moment.

C'est apparu il y a deux ans où les big four ont commencé à dire : « tiens on ferait bien une mission de consultance sur la partie cyber-security et évaluer votre maturité… ». On a joué le jeu il y a deux ans avec tout justement un des big four pour évaluer notre niveau de maturité, voir ce qu'on aimerait atteindre par rapport à des normes qui existent au niveau

de tout ce qui est NIST et ainsi de suite, ce qui peut se faire au niveau Européen et ailleurs pour se situer et voir où on avait des « gaps » pour voir ce qu'on pouvait faire rapidement c'est-à-dire des petits « quick win » et monter après à un niveau de maturité non pas optimal parce-que ça serait un peu la cerise sur le gâteau, mais atteindre déjà un niveau de maturité que nous estimons acceptable. Pour ce faire, on travaille avec un big four et justement ça en fait partie. On a des parties communication, change management, awareness qui vont aller dans ce sens-là (définition d'une taxonomie commune).

Hier, quand on parlait aux gens de « fraude au président », de malware, de virus, de ransomware les gens mettaient tout dans un même sac et chacun l'interprétait à sa manière, demain ça ne sera plus le cas, aujourd'hui c'est en train de changer. C'est pour ça que je parlais de « change management », c'est-à-dire l'acceptation des gens par rapport à des terminologies qu'ils vont entendre maintenant dans la banque et qu'ils vont tenter d'harmoniser. Pour ce faire, on fait des communications sur intranet. Il y avait « wannacry » il y a deux semaines, le dimanche matin on travaillait sur un article qu'on s'apprêtait à publier avec les premiers chiffres, le pourquoi, le comment ça se propage, comment ça s'appelle, ce qu'il y a à faire, ne pas faire, vérifier, etc…

Il ne s'agit que d'une news intranet, mais celle-ci a porté ses fruits parce que le matin, quand tous les employés sont arrivés, ils avaient un message avant même de s'identifier qui disait : « attention, on a potentiellement un souci, veuillez consulter l'intranet vous aurez plus d'infos ».

Et on a eu un bon taux de return là-dessus en sollicitant les gens, donc on est plus sur la partie sensibilisation et awareness qui fait qu'à force de mettre des articles tous les mois par exemple ou de manière ad hoc quand il y a un incident, on va commencer à inculquer des termes qui vont revenir au fur et à mesure et maintenant on a de moins en moins d'erreurs. Donc on essaie d'harmoniser ça.

2. Au niveau de la culture du risque, quel rôle joue le management senior et toutes les équipes sont-elles impliquées dans le management de ce risque ?

Le département communication interne peut être impliqué voire éventuellement celui de la communication externe. On est sur un cas extrême que nous n'avons pas eu, je dis bien que nous n'avons pas eu.

Imaginons qu'effectivement un ransomware pullule chez nous en interne et qu'il rend nos données indisponibles pendant 24h, ça va aussi poser problème sur notre site internet E-banking, on pourrait être amener à ce moment-là à communiquer vers l'extérieur sur le site internet et ailleurs, par exemple les médias locaux et communiquer vers la clientèle ou les prospects en disant : « écoutez, on a un souci, on se met off pendant 24h et on revient vers vous demain ».

C'est un exemple de communication externe. Au niveau de la communication interne, celle-ci est utilisée pour de l'awareness, cette communication est faite a priori et non posteriori en disant par exemple : « Voilà ce qui s'est passé chez nous, est-ce qu'on est touchés ou non, comment faire pour mitiger ce risque, qu'est-ce qu'on vous demande de faire ou de ne pas faire ». C'est l'exemple de la communication interne qui va reformuler, paraphraser ou enjoliver ce que notre département veut communiquer car il est vrai qu'étant la tête dans le guidon comme beaucoup soit de technicien ou de personnes vraiment dans leurs métiers, on a tendance à utiliser notre terminologie qui n'est pas forcément vulgarisable pour tout le monde donc la com' joue ce rôle, donc nous travaillons avec eux, mais ce n'est pas tous les jours que nous publions.

Au niveau du top management, notre mission cyber-security qui a commencé il y a deux ans, on implique le top management dedans. On a un STIRCO, c'est-à-dire un comité de direction du projet qui a lieu tous les 3 mois et qui fait l'état des lieux. Et dans ce comité, on a effectivement deux membres du comité de direction qui sont directement impliqués et qui reprennent ce qui se dit et se décide dans ces CIRCO au niveau du comité de direction de la banque. Par exemple si on a un comité de direction le lundi suivant, les informations et les décisions du STIRCO sont communiquées à ce moment-là donc ils ont une information.

Après on a déjà commencé des campagnes de sensibilisation en interne en disant ce qu'on attend d'eux par rapport à des fraudes aux présidents et ainsi de suite, on leur dit qu'ils doivent sensibiliser leurs collaborateurs. On a donc commencé ça, mais je ne te cache pas qu'un manager qui a 55 ans et qui pense déjà pension qui dans le top management se sentira déjà moins impliqué et va rapidement déléguer ça, mais ça veut dire que niveau implication top-management on sera déjà à un niveau plus bas.

3. Selon les experts, le facteur humain est souvent cité comme étant la source première de brèche. Quels outils avez-vous mis en place en termes de communication de formation ou de sensibilisation ?

On a commencé par le top management par des formations de deux heures dans lesquelles on leur a dit : « c'est vous qui allez devoir transmettre la « bonne parole » à vos collaborateurs et aussi leur demander de participer aux sessions d'awareness disponibles sur intranet ». Donc nous sommes partis par le haut. Par le passé par exemple, nous avions réalisé une campagne de pishing volontaire où 60 personnes avaient participé et certaines de ces personnes s'en souvenaient et m'ont dit qu'il n'avait pas gagné l'Ipad mis en jeu. C'est normal, il s'agissait d'une campagne de pishing.
On a demandé à quelqu'un d'externe de le faire par « black box », c'est-à-dire qu'il a monté un mail list de l'extérieur en se basant les informations disponibles sur LinkedIn, Facebook, etc… et celui-ci a réussi à obtenir 800 mails sur 1800 employés ce qui n'est pas mal du tout, et cela en moins d'une semaine. On a cassé volontairement la gestion d'incident en interne, c'est-à-dire qu'on a empêché les premières personnes qui réagissaient bien en appelant le centre de contact ou directement dans mes équipes pour dire : « on a peut-être quelque chose qui se passe du style pishing, ou spam bien ciblé ». Donc nous n'avons pas été plus loin là où normalement on déclenche une cellule de crise qui va déjà prendre des premières décisions et qui va bloquer ce genre de chose en moins d'une heure. Ici on a laissé « courir » sur une semaine et on a eu un taux de return assez important de gens qui avaient cliqué sur le lien frauduleux. Prochainement on réalisera des quizz via intranet et on a demandé aux managers de jouer le jeu et de demander à

leurs collaborateurs de participer, car en termes d'ISO 27001 nous sommes censés faire des campagnes de sensibilisation de manière annuelle et quand un nouvel arrivant commence à travailler chez nous, il en va de même, il faut le sensibiliser en lui montrant c'est quoi de travailler dans le milieu bancaire, c'est quoi le secret bancaire, ce qu'il peut faire ne pas faire, lui montrer les différentes classifications d'informations, par exemple un document peut-être : publique, restreint, confidentiel, enfin différents niveaux. Cela (sensibilisation) est fait à l'arrivée et de manière annuelle.

Prochainement nous allons réaliser un quizz de 8 questions et on oblige les gens à répondre, ils ont un délai de 2 mois et ça prend 5 minutes, c'est fait sur un ton amusant et pour informer les gens.

Quand je dis que c'est obligatoire, on leur dit qu'ils doivent le faire, on relance pour ceux qui ne le font pas, mais maintenant on y va pas le « couteau sur la gorge » en disant : « il nous faut 100% de répondant », si on a 70, 75 % de participation c'est déjà pas mal.

4. La question précédente concernait le cas d'employés bien intentionnés, mais qui pourraient être négligents. Quels outils avez-vous mis en place en ce qui concerne les employés qui auraient de mauvaises intentions ?

De manière contraignante, on va avoir des outils IT en plus de la sensibilisation qui comme souligné fonctionnent pour quelqu'un qui n'a pas de mauvaises intentions. Maintenant quelqu'un qui veut sortir volontairement quelque chose, c'est plus compliqué donc il faut y aller par la contrainte. Donc la contrainte est mise en place au niveau de la gestion des entrées et sorties de données dans la banque.

On est vraiment sur un périmètre clos sur lequel il peut y avoir plusieurs portes d'entrée par exemple le fait d'autoriser les employés à surfer sur le net peut être une porte. Tout ce qui est poster un formulaire quelque part sur internet n'est pas possible sauf exception (site des impôts par exemple). Tu ne peux pas par exemple aller sur clubic.com pour télécharger quelque chose ou remplir un formulaire et y attacher une pièce jointe, les gens n'ont pas accès au webmail. Par exemple pour le panama papers, c'était le cas. L'employé a ouvert une fenêtre gmail en parallèle, il ne s'est même pas envoyé de mail, il a juste créé

un brouillon dans lequel il a mis une ou plusieurs pièces jointes et il a récupéré le brouillon une fois chez lui.

Nous empêchons ce genre de communication par des filtres, on bloque des catégories de site, etc… Il s'agit de l'automatisation de contrôle sur le web. Au niveau des mails (BIL), c'est à peu près pareil. Mais là, on risque de rentrer en conflit avec le département compliance parce que ça reste intrusif. C'est-à-dire que si on fait de l'analyse dynamique sur les mails, c'est intrusif. Les employés acceptent dans leur contrat de travail qu'on fasse des analyses de pièces jointes, etc… qui sortent de la banque sauf si c'est estampillé « privé », mais à ce moment-là on n'autorise pas de pièce jointe. Mais la personne pourrait coller des informations sensibles sur son mail (tant qu'on reste en dessous de 50Ko). Et en interne, on possède des répertoires partagés par service, par projet. Dans l'exemple du Panama Papers (ou Experta, filiale de la BIL a été exposé), il y a eu la création d'un file service spécifique pour que nous puissions faire notre analyse d'un point de vue sécurité de l'information pour la compliance fasse son analyse ainsi que le département risque, mais plus au niveau du risque de réputation.

Nous avons donc eu un file service qui était classé confidentiel ou secret. La différence étant la contenance de données clients ou pas, si on a des données clients on dira que le fichier est classé secret, si on est sur du stratégique celui-ci sera confidentiel. En l'occurrence le panama, on ne gérait pas nos listes de clients dedans, il s'agissait donc de confidentiel. Un file service confidentiel ne peut pas être accessible par un externe, il a accès à du public du restreint. Donc finalement, on essaie de cloisonner en interne, dans le périmètre du réseau interne, on le verrouille au niveau des portes d'entrée et de sortie, mais ce n'est pas infaillible. Je t'ai par exemple dit que si tu sors 500 mails de 49ko (490 lignes de clients avec des choses dedans), ça fait quand même beaucoup d'information. C'est là notre limite. Même en faire de l'analyse dynamique sur un nom de client est difficile, autant un identifiant peut être repéré facilement par sa « patern », mais un nom client représente du free texte et reste difficile à identifier même avec de l'analyse dynamique. A Luxembourg, il existe le CIRCLE (Computer Incident Response Center Luxembourg), il s'agit d'une organisation gouvernementale où chacun peut devenir contributeur et il possède une plateforme qui s'appelle le MISP et dont le but est la

prévention. Par exemple : Si à Luxembourg, il y a un incident disons du type DdoS, et on ne sait pas encore où et comment, le CIRCLE va prévenir en disant : « attention méfiez-vous ou mettez en place vos contre-mesures ».

Par contre, le CIRCLE fait de l'analyse haut-niveau, ils ont infiltré un botnet underground et ils sont en mesure de dire : « tiens BGL, BNP Paribas, c'est un nom qui va déclencher une alerte parce qu'il est en train de circuler au Etats-Unis sur un groupe Warez qui a remarqué que les Token Luxtrust peuvent être une source de faille ». C'est gratuit, et ils font de l'analyse proactive sur l'exposition du territoire Luxembourgeois.

Je suis en poste depuis deux ans et j'ai déjà eu l'occasion d'être sollicité par le CIRCLE qui vous appelle et vous dit : « tiens un fichier labellisé confidentiel a été uploadé sur telle plateforme. » Par exemple, virustotal qui permet de voir si un fichier est infecté et le CIRCLE appelle et envoie le fichier en crypté pour procéder à des vérifications.

Là il s'agissait d'un template d'entrée en relation qui était vide. Quelqu'un a eu peur et l'a envoyé chez virustotal pour vérifier qu'il s'agissait d'un fichier intègre, et ce fichier s'est retrouvé aux Etats-Unis et ça a mis moins de deux heures avant qu'on reçoive l'appel. Nous avons également de la veille, nous avons un service que nous payons pour autre chose, par exemple quelqu'un qui fait un doublon de notre site pour faire sa propre campagne de pishing sur base de notre image. Nous possédons grâce à eux les moyens de faire fermer un site en moins de deux heures partout dans le monde.

5. Au sein de votre organisation existe-t-il une personne/ ou une équipe responsable de la gestion ce risque en dehors du CISO/CTO ?

Oui, parce que la cyber-security…. Nous utilisons les matrices RACI (Responsible, Accountable, Consulted, Informed) qui définissent les rôles et responsabilités d'un projet. Informé tu reçois l'information, mais tu n'en fais rien, Consulté : on te demande ton avis, Accountable : c'est toi qui fait l'implémentation du truc et tu remontes les résultats de ton implémentation à celui qui est responsable. Celui qui est responsable de ça aujourd'hui, c'est le CISO. Par contre celui qui accountable c'est l'IT security, ITSO qui est accountable. C'est là où je te disais que je définis un ensemble de politiques et de règles, mais je n'ai

pas la connaissance, la compétence technique sur la configuration d'un firewall. Donc là c'est l'ITSO qui prend le relais, qui est vraiment dans la partie technique de la security qui va te dire : « la meilleure solution du moment c'est ça et on met en place ça comme ça, est-ce que ça vous va ? ». Ça reste un ensemble d'acteurs qui fait que l'aspect cyber-security est couvert et là-dessus t'as ce que j'appelle la « cerise sur le gâteau » : la partie assurance qui dans l'operational risk.

6. Comme nous avons pu le constater avec le cas de la banque du Bangladesh, la question de la gestion des tierces parties s'avère être d'une grande importance. Comment gérez-vous la relation avec les tierces parties en matière de données auxquelles ils ont accès (Valeur des données), de connectivité entre les réseaux ? Quels sont les points auxquels vous accordez beaucoup d'importance lorsqu'il s'agit de leurs pratiques managériales ?

Pour les « third party », il y a une notion d'outsourcing et une notion de prestation de services qui peut être faite ailleurs comme chez nous, mais par un prestataire externe. Nous regroupons ces deux catégories dans la case « third party ». Pour les tierces parties, nous possédons une double classification, la première est basée sur les coûts financiers annuels. Si tu as un prestataire IT et que tu délègues toute la gestion de ton parc informatique, de ta sécurité, de la maintenance des patchs, etc… ça revient extrêmement cher. A contrario, le jardinier qui vient une fois par mois faire les jardins ne coûtera pas grand-chose et il sera catégorisé par exemple en D alors que ton prestataire informatique lui sera en A.

Ça c'est pour l'impact financier. A côté, t'as l'impact sécurité, tu peux réagir à peu près de la même manière en te demandant s'il accède ou pas à des systèmes d'informations, est-ce qu'il y accède de l'intérieur ou depuis l'extérieur. L'aspect sécurité prime sur l'aspect financier. Par exemple : le jardinier qui arrose les plantes dans le bureau du directeur, bien qu'il ne coûte pas cher, celui-ci sera classé en S1 parce qu'il peut potentiellement tomber sur des données très sensibles.

Une fois cette classification effectuée, nous déclenchons une procédure de due diligence. Ça peut se faire de plusieurs manières soit en mettant en ligne un formulaire à destination

des tierces parties où on lui demande par exemple : « Comment gérez-vous les accès chez vous ? est-ce que vous avez des machines où les gens doivent s'identifier ou pas, est-ce vos locaux sont protégés par des badges… etc. » Ils ont donc une liste de +- 140 questions à remplir. Je ne te cache pas que la première fois que tu la donnes à quelqu'un qui est boulanger par exemple, ils ne comprennent pas pourquoi autant de questions. Nous avons donc adapté ce questionnaire pour ce genre de tierce partie. Cette due diligence permet d'évaluer la maturité de ton prestataire. Par rapport au métier ou au business qu'on aura avec lui, est-il mature ? Quelqu'un à qui tu confies des données stratégiques, il ne faudrait pas que ces données-là tombent entre de mauvaises mains, donc finalement celui qui va gérer ces données-là, il faut qu'il possède une notion de confidentialité et ainsi de suite… On attend donc de lui qu'il possède une maturité optimale sur la gestion des accès sur les serveurs chez eux, qu'ils aient des vérifications tous les mois par exemple : des administrateurs sur leurs bases de données qui sont en mesure d'aller sur leurs bases de données à partir du moment où elles ne seraient pas cryptées, ça dépend en fait du profil de la tierce partie. Avant on donnait tout maintenant on mitige un peu ça.

Je soulève la question de la modélisation dont les questions suivantes font partie.

1. Quelle approche employez-vous en matière de modélisation du cyber-risque ? Employez-vous une approche stochastique ou une approche basée sur la définition de scénarios ou un mix des deux ?

Un mix des deux parce qu'on est sur le théorique versus le pratique. Il y a deux ans, on s'est bien rendu compte qu'en mettant sur papier que des idées théoriques, on était encore en parallèle de ce qui pouvait nous arriver comme incidents. On a des incidents très souvent (comme tout le monde) et on a affiné et ajusté pour remonter ou même créer certaines politiques spécifiques sur la cryptographie ou même comment utiliser un iPad par rapport à du concret. Je m'explique, il y a deux mois de ça on s'est rendu compte que sur iPad professionnel aujourd'hui il y avait encore la possibilité d'envoyer des documents via Airdrop.

2. Dans le cas de l'approche stochastique, il est à noter que la sévérité suit une loi de puissance à queue lourde, comment traitez-vous ce problème ?

On a une méthodologie définie sur base d'une norme allemande qui ne se base pas sur du high level/low car c'était trop simple.
Les gens auront tendance à aller sur du médium quand il voit du high pour ne pas être embêtés clairement. On est parti d'une échelle où on essaie de voir si c'est déjà arrivé dans le monde, est-ce que c'est déjà arrivé au Luxembourg, est-ce que c'est déjà arrivé à la BIL, ça s'est reproduit à la BIL. Il n'y a donc plus de note médiane, mais plutôt une gradation de 1 à 4.
A partir de là, on crée une matrice qui dit : « si on a une probabilité qui est à deux et un impact qui est à 3, on sera sur un risque qui est à 3 ». C'est une matrice à 16 cases qui est basée sur la proba/impact pour le risque global. Ça on le fait sur le risque brut, ensuite le risque résiduel, une fois que les contre-mesures sont en place et puis tu as un risque incompressible derrière qui est un risque brut, ex : centrale nucléaire pas loin. On établit dans cette étape une liste des risques possibles, ici on en a défini 46 au départ. On va voir l'applicabilité de chaque menace par rapport au projet ou au sujet que nous sommes en train de traiter. Exemple : Si on parle de papier tu excluras déjà tout ce qui concerne les serveurs, etc… Et il te restera que 7 menaces sur du papier et on vérifiera pour chacun le risque brut, le risque résiduel et incompressible sur base des probabilités propre à chez nous ce qui nous permet d'avoir la même échelle de comparaison. Une telle échelle permet de parler le même langage.

3. Dans le 2ème et 3ème cas et étant donné la nature low frequency/ high severity du cyber-risque, employez-vous un expert spécifique (IT) pour la définition de ces scénarios ?

Il y'en a dans l'équipe CISO, dans l'équipe IT. Leurs tâches ne consistent pas à réaliser des scénarios, par contre ils font de la veille tous les matins. Pour voir les tendances et voir éventuellement ce qui pourrait nous impacter. Je dirais que c'est plutôt du réactif. Par contre de manière proactive, cette mission cyber-security, on a une bonne quantité d'experts dessus sur 4-5 ans minimum. Le but étant d'avoir des scénarios concrets qui

collent avec ce qui se fait en Europe et au Luxembourg. Il s'agit vraiment d'experts qui travaillent qui testent nos infrastructures IT.

4. La nature dynamique de la fréquence et de la sévérité, ainsi que l'environnement changeant de la technologie nécessitent une révision continue de l'approche de modélisation, comment ces problèmes sont traités ?

On a un comité de sécurité qui a lieu tous les deux mois qui peut être lié à des projets qui sont demandés par des métiers dans la banque. Ex : on veut créer une nouvelle fonctionnalité E-banking, on va être impliqué car au niveau de l'information security, il peut y avoir des informations du type extrait de compte qui va être généré en pdf et se demander quel risque il y a là-dessus. Par la suite on prépare un dossier d'analyse sur base de la méthodologie (cf. plus haut), on présente un dossier au comité de sécurité dans lequel il y a x représentants de la compliance, audit, etc… Et ils décident collégialement si oui ou non on peut avancer sur tel ou tel sujet. Il s'agit du côté facile du projet, par contre lorsqu'on identifie un « wanna cry », on vérifie dans quelle mesure on peut être impacté, on va drafter quelque chose qui va circuler au niveau du comité de sécurité au départ (mais il y a deux membres du comité de direction dedans aussi). En disant : « voilà déjà l'impact potentiel chez nous, voilà l'état des lieux aujourd'hui, voilà comment on peut améliorer la situation, etc… ». Là-dessus le comité de direction décide de monter une cellule de crise ou non et réadapter les procédures derrière. En cas de problème, revoir la matrice PDC.

Cette veille permet de corriger les petites défaillances que tu vois au fur et à mesure, ce n'est pas sans erreur, tu vas corriger 7 situations sur 10. Et les trois vont être corrigées par un audit interne ou externe qui va identifier les problèmes restants. C'est un process qui est déclaré dans les politiques comme quoi il est fait, ce process est fait dans la pratique, mais ça couvre 70 à 80 % des cas, on n'arrivera jamais à 100% là-dessus.

Je pense qu'on est sur un ensemble de mesures, si tu cumules awareness, veille IT, nouveau élément d'infrastructure, et que chacun est à 70, 80%, ton niveau global sera aussi à 70,80 %.

5. Le cyber-risque étant assez récent et l'obligation de reporter les brèches en Europe n'étant en place que pour 2018, comment palliez-vous au manque de données (si c'est le cas) ?

Le problème de ce qui est cyber-risque, quand tu es dans une entreprise bancaire, industrielle, bref secondaire ou tertiaire, c'est que tu es dans du réactif sauf si t'es dans une société de service qui fait de la reg-team ou de la veille technologique dont c'est le métier. Donc manque de données tu seras toujours en décalage (j-1) par rapport aux attaques que tu peux avoir. C'est là où tu es obligé, quand tu es dans du tertiaire de t'encadrer et de faire des missions de manière continue. On bosse beaucoup avec des externes et aller chercher de la donnée pour aller chercher de la donnée ça ne sert à rien, on est plus sur ce qui est déjà arrivé à telle ou telle banque au Luxembourg, à ce moment-là on se demande si on est concerné, si oui on rajoute ça à notre knowledge base. Il existe aussi des outils sur la place à Luxembourg. Il y a monarque qui permet de faire de l'analyse de risque, on rentre des inputs et l'outil nous donne les risques auxquels on pourrait être soumis.
Il y a également un changement de mentalité entre les banques qui ont compris qu'il n'y a pas d'intérêt à retenir de l'information pour la retenir. C'est aussi lié à la nouvelle génération et au fait que les banques, en tout cas à Luxembourg, ont des segments bien définis. Et il y a des groupes de travail en commun ou des échanges se font. Et c'est important surtout d'un point de vue réactif, si on n'a pas cet effet de masse on s'enterre.

1. En matière de mitigation du risque, il est nécessaire de posséder des infrastructures robustes (Antivirus, pare-feu, infrastructure matérielle). Comment établissez-vous les budgets en la matière ? (Relation entre département IT/CISO/CTO avec le département financier)

Il y a deux types de budgets. Le budget prévisionnel récurrent : on sait par exemple qu'on a 4000 ordinateurs à dispositions. Nos 4000 ordinateurs sont facturés par nos prestataires IT (chiffre au hasard) 300€ par mois chacun. A ce moment-là tu es capable de dire qu'au

niveau IT, Infra, il te faudra X euros. Là-dessus, il y a un exercice annuel qui identifie les besoins projets qui émanèrent des autres métiers (finance, wealth management, IT, etc.). Il y a un challenging des projets, c'est-à-dire prioritaires ou pas, stratégiques ou pas, avec un impact transversal sur toute la banque ou juste sur un silo qui vont déterminer un budget qui est validé au niveau du board de direction.
La cyber-sécurity était un projet comme ça au départ, c'est-à-dire on a une infrastructure IT répondante ou vieillissante sur certains points, on n'a jamais eu de problème, mais par contre on estime qu'on n'est pas assez protégés niveau Ddos par exemple et on demande une enveloppe qu'on a ou pas.

2. En Europe le marché des assurances cyber-risque n'est pas encore bien développé comparativement à celui des Etats-Unis, possédez-vous une assurance en matière de cyber-risque ?

Il existe un contrat spécifique en parallèle chez le même fournisseur. Je pense que ces polices sont sous-évaluées. Parce qu'ils vivent aussi en J-1 et ils n'ont pas encore les backlogs nécessaires pour fournir un prix à la juste valeur. Le contrat est spécifique pour des raisons de taxonomies, il faut qu'on parle de la même chose. L'assureur n'a pas le même vocabulaire que le banquier et le banquier n'a pas le même vocabulaire que l'informaticien et il fallait trouver un terrain neutre. Je dirais qu'on a évolué ensemble, l'assureur a une idée de contrat et il aimerait que la taxonomie soit revue par la banque pour qu'ils puissent parler de la même chose.

3. Jouissez-vous d'une couverture assez large ou celle-ci est très limitée ? (Contrat standard ou sur mesure)

C'est une couverture qui correspond à nos attentes et à leurs attentes par rapport aux problèmes que nous avons déjà eu. Il s'agit de l'interprétation.

6.2 Annexe 2 : Interview à la BGL BNP PARIBAS.

(En gras le répondant)

Je souhaiterais faire une introduction sur la façon dont on fonctionne ici et la façon également dont on est réglementé. Le cyber-risque pour nous est clairement un risque opérationnel selon les règles bâloises. On est donc clairement dans cette catégorie qu'est le risque opérationnel. Selon les règles bâloises en termes de risque opérationnel on a différents « event type » qui sont la fraude interne et la fraude externe. Les dommages aux bâtiments par exemple, aux actifs de façon plus générale comme « event class Bâle ». Il y a 7 sept classes d'incidents, de type d'incident selon les règles bâloises en termes de risque opérationnel. Nous sommes en tant que groupe BNP Paribas, donc là je ne parle pas simplement de la BGL, mais de BNP Paribas, on est une institution qui calcule le capital réglementaire pour le risque opérationnel sur base de l'AMA. Donc nous avons nos propres modèles, cela est fait au niveau du groupe et non localement. Je parle de cela car pour ce faire, on se base sur ces « events type » bâlois ou il n'y a pas de classe cyber-risque, mais on retrouve dans la fraude externe 80 à 90 % des events du type cyber-risque. Mais la fraude externe en tant que telle recouvre un ensemble plus large que le cyber-risque qui peut se retrouver également dans la fraude interne. Donc nous sommes plutôt sur les catégories bâloises qu'une classe spécifique cyber-risque.

Dans le calcul de notre capital réglementaire, je disais donc que nous sommes en AMA, et nous décrivons donc pour l'ensemble du groupe des incidents potentiels. Au niveau du dispositif de contrôle interne de la banque, qui repose notamment sur une cartographie des risques, on va cartographier les process de la banque. Et derrière ces process, il y a des risques et les plus gros risques sont scénarisés et donc on a sur l'ensemble des process de la banque différents scénarios qu'on appelle les incidents potentiels qui eux vont être modélisés derrière pour calculer le capital nécessaire pour le risque opérationnel et donc là-dedans on retrouve chaque métier et fonction qui modélise ses incidents potentiels et on aura des « likely case », des « worst-case » que nous modéliserons.

Toute cette introduction est pour préciser qu'à la date d'aujourd'hui on est sur les évènements bâlois et de deux que nous sommes sur les incidents potentiels qui sont modélisés « bottom-up ». Et donc aujourd'hui, nous n'avons pas une taxonomie top-down du type cyber-risque. Chaque métier doit regarder s'ils ont un cyber-risque et le modéliser sur cette forme-là. Il s'agit plutôt de dire : « regarder vos process, scénariser vos risques potentiels que vous avez » et puis on regarde pour les incidents potentiels au niveau de la banque et plus précisément au niveau de la fraude externe et on retrouvera certainement des incidents potentiels qui sont liés à de la cyber-fraude.

1. Au sein de votre organisation, existe-t-il une taxonomie commune entre les différents départements en matière de cyber-risque ?

Voir l'introduction.

Le répondant a donné les éléments de réponses dans l'introduction.

2. Au niveau de la culture du risque, quel rôle joue le management senior et toutes les équipes sont-elles impliquées dans le management de ce risque ?

La réponse est deux fois oui. On a ce qu'on appelle le premier niveau de défense en termes de gestion du risque opérationnel. Le premier responsable, c'est le responsable du métier donc le management est responsable, chez nous c'est au niveau du comité de direction : les membres du comité de direction de cette banque sont responsables de la gestion du risque opérationnel dans leur entité. Pour cela ils ont, au sein de leur propre métier, ce qu'on appelle le premier niveau de défense. Donc ils mettent en place un contrôle permanent qui font tout justement la cartographie des risques, qui identifient les différents risques, qui mettent les contrôles derrières pour chaque risque modélisé. Selon que ce soit un risque majeur ou mineur, on fait plus ou moins de contrôle derrière et c'est la responsabilité de chaque responsable de métier et de nouveau là on ne fait pas la différence entre le cyber et le reste. Evidemment, pour tout ce qui est cyber la fonction IT a un rôle extrêmement important et ils ont également des contrôleurs permanents qui

cartographie leurs risques et qui mettent en place les contrôles nécessaires et donc oui les managers sont responsables, chaque manager est responsable pour son entité et donc tous les managers sont impliqués. Il n'y en a pas un plus particulièrement qui est impliqué dans le premier niveau.

C'est plutôt dans le deuxième niveau de défense, là c'est typiquement les métiers du risque qui intervient dans cette deuxième ligne de défense en contrôlant les dispositifs en dessous et se demandera s'ils sont suffisants par exemple, sont-ils déroulés selon la méthodologie du groupe et ainsi de suite. Et il y a également un troisième niveau de défense qui s'appelle l'inspection générale. Et l'ensemble des deux premiers niveaux représentent ce qu'on appelle le dispositif de contrôle permanent, c'est-à-dire qu'il s'agit du dispositif journalier après on a encore le contrôle périodique qui vient contrôler aussi bien le premier niveau que le second niveau pour voir si ça fonctionne bien.

3. Selon les experts, le facteur humain est souvent cité comme étant la source première de brèche. Quels outils avez-vous mis en place en termes de communication de formation ou de sensibilisation ?

Il y a plusieurs éléments qui sont en places. D'un, on a des formations génériques pour l'ensemble des employés et nous avons d'ailleurs une charte informatique que chaque employé reçoit lorsqu'il commence à travailler. Il s'agit d'une charte des bonnes pratiques qui contiennent des choses relativement simples comme par exemple le fait de dire qu'il y a le secret bancaire et professionnel et qu'il ne faut donc pas mettre certaines choses sur les « social network » parce que souvent la criminalité va chercher des informations dessus, il s'agit donc d'un élément générique (premier type de formation). Le deuxième type de formation porte sur des opérationnels, ceux qui travaillent par exemple sur la plateforme swift, c'est également les informations qui développent les modèles et qui ont des accès administrateurs et ainsi de suite… Ces personnes reçoivent des formations spécifiques dédiées à la fonction, les rendant ainsi attentifs aux risques. Et puis quelques choses sur lequel on travaille et qui n'est pas encore en place, ce sont des formations spécifiques aux risques IT et cyber-risque à destination du management.

4. La question précédente concernait le cas d'employés bien intentionnés, mais qui pourraient être négligents. Quels outils avez-vous mis en place en ce qui concerne les employés qui auraient de mauvaises intentions ?

Je reviens sur la façon dont on gère ce risque, c'est-à-dire « bottom-up », il faut donc regarder différents scénarios. On a différents contrôles et aujourd'hui on a cartographié comme je l'ai dit certains risques et derrière ces risques on a mis certains contrôles. Après il faut regarder quels types de risque on a. Je ne peux que partir d'un exemple pour répondre à cette question. Prenons le vol de donnée au niveau de la banque, qui est un incident potentiel qui est cartographié, il s'agit de l'incident du type « vol de données client, flux ou autres », une fois que ce risque est cartographié on a un ensemble de contrôles derrière par exemple des contrôles indépendants qui tournent au niveau de l'IT qui identifie par exemple des retraits de données en masse et qui remonte des alertes concernant le retrait de données en masse. On en (outils qui permettent le reporting) a parfois besoin pour les reportings. Il y a également des alertes si des fichiers importants pour la banque sortent. Il s'agit ici de contrôle par software mis en place par l'IT.

5. Au sein de votre organisation existe-t-il une personne/ ou une équipe responsable de la gestion ce risque en dehors du CISO/CTO ?

Tout le monde parce que comme je l'ai dit, l'IT est responsable des attaques, mais tout le monde est responsable de la fraude. Chaque responsable de métier est responsable de ces process, des faiblesses et défaillances dans son dispositif.

6. Comme nous avons pu le constater avec le cas de la banque du Bangladesh, la question de la gestion des tierces parties s'avère être d'une grande importance. Comment gérez-vous la relation avec les tierces parties en matière de données auxquelles ils ont accès (Valeur des données), de connectivité entre les réseaux ? Quelles sont les points auxquelles vous accordez beaucoup d'importance lorsqu'il s'agit de leurs pratiques managériales ?

Il y a différentes choses, mais il faudrait également regarder avec le département IT. Ici je donne les réponses les plus génériques. Première chose lorsqu'on travaille avec des tierces personnes (ici en IT), on a de très fortes préférences pour tout ce qui est professionnel du secteur financier parce qu'ils sont également très réglementés. On va travailler ici avec ce qu'on appelle les PSF (au Luxembourg) qui sont très fortement réglementés, ce qui nous permet de connaître notre vis-à-vis et de savoir qu'il est réglementé également. Ensuite, on a des contrats de confidentialité avec eux qui de toute façon remet la responsabilité sur ce tiers provider. Il y a également des contrats relativement contraignants avec des clauses sur la confidentialité, des clauses qui 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.

Les accès qu'ils ont chez nous sont également limités le plus possible, on va s'assurer qu'un externe qui vient chez nous n'ait que les accès les plus limités. 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. Mais cela dépend de l'intensité de nos relations. Mais oui, nous remettons des questionnaires qui permettent d'évaluer les dispositifs de contrôle et selon les projets, on se réserve même le droit d'aller faire des audits chez eux.

1. Quelle approche employez-vous en matière de modélisation du cyber-risque ? Employez-vous une approche stochastique ou une approche basée sur la définition de scénarios ou un mix des deux ?

Scénario. (Réponse à l'introduction).

2. Dans le cas de l'approche stochastique, il est à noter que la sévérité suit une loi de puissance à queue lourde, comment traitez-vous ce problème ?

J'ai choisi de quand même poser cette question car j'estimais que même dans l'approche scénaristique il y a emploi des statistiques.

Je ne rentre pas dans les détails. Les incidents potentiels sont des incidents où on développe d'abord des scénarios, ensuite sur ces scénarios on met effectivement un « likely case » avec fréquence et impact et (pas toujours, mais sur certains) on peut mettre un « worst-case » avec un impact sur le « worst-case ». Et après c'est remodélisé de façon stochastique effectivement, et même indépendant. On a…, J'ai vu quelque part que tu fais mention du « fat-tail », on n'a pas vraiment des modèles très compliqués. Ça reste des modèles simples où en fait le « worst-case » et le « likely-case » sont modélisés de façons indépendantes et après tout simplement ajoutées, agrégé sur un principe de « weighted average » loss.

3. Dans le 2ème et 3ème cas et étant donné la nature low frequency/ high severity du cyber-risque, employez-vous un expert spécifique (IT) pour la définition de ces scénarios ?

Oui. Un expert, ça dépend. Un expert interne ou externe. Pour chaque IP (incidents potentiels), on va toujours avoir autour de la table tous les experts nécessaires. Par exemple dans le cas du cyber, il y aura toujours quelqu'un de l'IT autour de la table. Il y aura également quelqu'un de notre département juridique autour de la table pour calculer l'impact possible qui peut aller d'amendes à des condamnations juridiques. Donc on a les scénarios qui vont vraiment dans le détail et dans le cas du cyber-risque, on essaie de scénariser quelque chose de très, très réaliste. Et à ma connaissance jusqu'à présent, si la question porte plus sur des experts externes, on fait plutôt appel à des experts au niveau du groupe (A Paris par exemple) si c'est nécessaire sur certains scénarios.

4. La nature dynamique de la fréquence et de la sévérité, ainsi que l'environnement changeant de la technologie nécessite une révision continue de l'approche de modélisation, comment ces problèmes sont traités ?

Déjà les gros incidents potentiels, typiquement les cybers chez nous ; la méthodologie prévoit qu'ils soient revus chaque année. Les scénarios doivent être remis en question chaque année. S'il y a des nouveaux risques qui apparaissent, on est également « challenger » au niveau du groupe. Par exemple, si en Belgique ou en Italie, ils ont déroulé un nouveau scénario, il s'agit pour nous de le regarder, de le comparer à notre cartographie des risques et de prendre les mesures nécessaires. Etant donné que nous sommes en AMA, les cycles de révisions sont annuels pas seulement pour le cyber-risque pour tous les risques opérationnels.

5. Le cyber-risque étant assez récent et l'obligation de reporter les brèches en Europe n'étant en place que pour 2018, comment palliez-vous au manque de données (si c'est le cas).

Le cyber-risque chez nous n'est pas modélisé sur base d'informations externes, empiriques je dirais, mais vraiment sur base de scénarios. Et après dans les scénarios, on reprend les cas typiquement comme celui de la banque du Bangladesh qui déclenche chez nous une réflexion à savoir si cela peut arriver chez nous, est-ce que tel ou tel incident aura un impact chez nous. Mais nous ne reprenons pas de données empiriques pour paramétriser nos modèles.

6. Lors du calcul de la distribution agrégée, décomposez-vous la fréquence et la sévérité en sous-facteurs ou ceux-ci sont évalués directement ?

Sur les scénarios on fait effectivement la distinction entre « worst-case » et « likely-case » pour faire une moyenne.

1. En matière de mitigation du risque, il est nécessaire de posséder des infrastructures robustes (Antivirus, pare-feu, infrastructure matérielle). Comment établissez-vous les budgets en la matière ? (Relation entre département IT/CISO/CTO avec le département financier)

Le budget est un exercice banque. Chacun a sa responsabilité clairement définit là-dedans pour tout ce qui est pure informatique tel que les pare-feux, il s'agit effectivement d'un budget IT que l'IT élabore en cours d'année pour l'année suivante comme les autres métiers qui élaborent leurs budgets qui passent également au conseil d'administration avant d'être challengé et puis validé.

Il y a donc un budget récurrent, et des budgets IT par métiers ? **Non, en fait tout ce qui est IT, c'est le budget de l'IT qui est refacturé aux différents métiers, là on rentre dans les détails du budget. Au niveau de la structure, on a des « profits center » et des « costs center ». L'IT est un « cost-center » qui a un budget « run » et un budget « change ». Le premier concerne les opérations « day-to-day » et le deuxième le développement de nouveau software par exemple.**

2. En Europe, le marché des assurances cyber-risque n'est pas encore bien développé comparativement à celui des Etats-Unis, possédez-vous une assurance en matière de cyber-risque ?

A ma connaissance, on n'a pas de contrat spécifique cyber-risque. Evidemment, on a des assurances et à ma connaissance, ce risque-là est inclut dans la police actuelle.

3. Possédez-vous une police spécifique pour le cyber-risque, ou le cyber-risque fait l'objet d'une close spécifique dans les contrats actuels ?

Le répondant donne des éléments de réponses dans les questions précédentes.

4. Jouissez-vous d'une couverture assez large ou celle-ci est très limitée ? (Contrat standard ou sur mesure) **JOKER.**