Comment les banques se sont prémunies contre les vols et fuites de données bancaires ?

Travail de Bachelor réalisé en vue de l'obtention du Bachelor HES

par :

Sejo Bajrektarevic

Conseiller au travail de Bachelor :

Emmanuel Fragnière, Professeur HES

Lieu, date de dépôt

Haute École de Gestion de Genève (HEG-GE)

Filière Economie d'entreprise

Déclaration

Ce travail de Bachelor est réalisé dans le cadre de l'examen final de la Haute école de gestion de Genève, en vue de l'obtention du titre de Bachelor en économie d'entreprise, orientation « Banque et Finance ». L'étudiant accepte, le cas échéant, la clause de confidentialité. L'utilisation des conclusions et recommandations formulées dans le travail de Bachelor, sans préjuger de leur valeur, n'engage ni la responsabilité de l'auteur, ni celle du conseiller au travail de Bachelor, du juré et de la HEG.

« J'atteste avoir réalisé seul le présent travail, sans avoir utilisé des sources autres que celles citées dans la bibliographie. »

Fait à Genève, le 16 août 2013

Sejo Bajrektarevic

Remerciements

Je tiens à remercier:

Monsieur Emmanuel Fragnière, qui m'a aidé dans mon travail. J'ai apprécié les conseils qu'il m'a donnés et sa disponibilité pour mes questions.

Les différents sondés qui ont accepté de participer à mon travail, en m'accordant de leur temps.

Monsieur Jean-Pierre Meynard qui a pris le temps de lire mon travail et m'aider à l'améliorer.

Les amis que j'ai rencontrés durant ces 3 années à l'HEG, avec qui j'ai passé de bons moments.

Pour finir, ma famille qui m'a beaucoup soutenu durant toute ma formation.

Sommaire

Le but de cette étude était de mieux comprendre le problème de vol de données bancaires. Les affaires, qui ont été rendues publiques, ont surtout parlé des données volées, sans évoquer les raisons qui pouvaient inciter une personne à commettre ce genre de méfait et des méthodes utilisées par les banques, pour se prémunir contre des pertes de données.

Cette étude a été réalisée avec l'aide de douze personnes, qui exercent ou qui ont exercé dans le domaine. Sans leurs informations et leurs conseils, je n'aurais pas pu réaliser mon travail.

Les informations récoltées ont fait l'objet d'une analyse et ont débouché sur des recommandations. Le résultat obtenu a permis de mieux connaître les outils utilisés par les banques pour protéger ses données, mais également des cas qui n'ont pas été rendus publics ou encore les efforts entrepris par la FINMA et l'Association Suisse des Banquiers (ASB).

Table des matières

Liste des Tableaux

Liste des Figures

1. Problématique

Ce travail vise 3 objectifs :

- Mieux comprendre les attaques que peuvent rencontrer les banques.
- Les raisons qui peuvent inciter des personnes à voler des informations
- Les moyens qui existent pour se prémunir contre les pertes.

Les banques en Suisse ont subi plusieurs cas de vol de données bancaires ces dernières années. Les noms de plusieurs clients se sont retrouvés aux mains de plusieurs états, qui ont utilisé ces données pour trouver des clients qui n'auraient pas déclaré de l'argent dans leur pays. Malgré ces affaires, l'image des banques en Suisse n'a pas connu d'impact négatif important, ni même sur la confiance des clients vis-à-vis des banques.

2. Introduction

Le secteur bancaire suisse occupe une place importante en Suisse. Il doit notamment son succès à la qualité de ses services, qui est régulièrement citée comme un des meilleurs au monde. Les banques offrent aux clients une relation privilégiée, leur permettant d'avoir un suivi de dossier de qualité, des produits et stratégies de placements qui répondent à leurs attentes, une discrétion absolue des clients grâce au secret bancaire et une forte implication dans la lutte contre le blanchiment d'argent et le financement du terrorisme.

Mais ce qui fait la renommée du secteur bancaire suisse est le Private Banking. Il a profité d'un accroissement de la demande de conseils, la forte croissance des titres financiers, l'augmentation de produits financiers et la complexité de placement, au cours de ces 25 dernières années. Aujourd'hui, les avoirs sous-gestion en Suisse représentent 27 % du Private Banking transfrontalier, estimés à plus de 5300 milliards dont 2700 milliards représentent la clientèle à l'étranger.

Entre 2002 et 2012, le produit intérieur brut suisse a connu une croissance de 2.7% annuel. Toutes les branches économiques ont contribué au développement, le secteur financier a une part importante dans ces bons résultats, avec une croissance d'environ 8 % annuel durant la période 2002 à 2007. Mais en 2008, le secteur financier va subir une grave crise des liquidités. La cause se trouve aux Etats-Unis avec la baisse du marché immobilier. Cela a entrainé la faillite de plusieurs établissements bancaires et l'intervention des états pour sauver les banques. Les banques suisses ont aussi été impactées par la crise. Aux troisièmes trimestres 2007, la banque Crédit Suisse a subi une dépréciation de ses actifs estimée 2.5 milliards de dollars et la banque UBS de 11 milliards de dollars. La confédération viendra en aide à ces dernières en rachetant des titres toxiques. Malgré la crise, les banques ont continué à recruter du personnel. En effet, en 2007, elles comptent 119'500 employés environ et en 2012, 122'900 personnes y travaillent, représentant 6% de la main-d'œuvre Suisse.

Tableau 1

Secteur Financier en chiffre(1)

	2002	**2007**	**2012**
Création de valeur, en % du PIB	10,1 %	12,4 %	10,3**%**
Produit intérieur brut du secteur financier (en million de francs)	45'302	66'903	59'958
Produit intérieur brut (PIB) Suisse (en million de francs)	446'786	540'800	592'992
Activités des services financiers	118'000	119'500	122'900

Source : Département fédéral des finances DFF, *Place financière Suisse, Chiffre Clé,* Berne, mars 2013, P.1-2

Tableau 2

Secteur Financier en chiffre(2)

2011 hors assurance	**Valeur absolue (en milliards CHF)**	**Part de valeur ajouté**
Valeur ajoutée totale du secteur bancaire	35.0	6.2%
Banque de détail	13.5	2.4%
Gestion de fortune	14.7	2.6%
Gestion d'avoirs	4.1	0.7%
Banque d'investissement	2.7	0.5%

Source : SWISSBANKING, *L'importance de la place financière suisse,* Juillet 2012, P.1-2

2.1 La protection des données en Suisse

Les banques suisses sont connues pour la protection de la sphère privée de ses clients, grâce notamment à son secret bancaire, qui oblige les banquiers à ne révéler aucune information sur des clients de la banque, sauf en cas de procédure pénale. La

protection de la sphère privée et les données des clients sont régies par la loi. Un banquier peut être puni par une peine privative de 3 ans de prison et une amende allant jusqu'à 250'000 francs pour des informations révélées sur un client.

2.2 Les vols de données bancaires :

Les vols de données bancaires peu se définir par le vol d'informations permettant l'identification d'une personne, telle que son nom, prénom, adresse, le numéro de compte, les avoirs détenus et d'autres données la concernant.

Les vols de données bancaires font partie de la famille des risques opérationnels et peuvent être défini comme : *« le risque de pertes pouvant résulter de procédures internes inadéquates ou non appliquées, des personnes, des systèmes ou d'évènements externes »*[1]*.* Mais cette définition n'inclut pas les risques stratégiques et la réputation.

Le comité de Bâle a regroupé le risque opérationnel en 7 catégories :

- Fraude interne : Transaction non autorisée, vol, corruption, abus de confiance
- Fraude externe : Attaque informatique, usurpation d'identité, falsification de chèques
- Poste de travail : Harcèlement, grève, non-respect des règles de sécurité et de santé
- Client, produits et pratiques commerciales : non-respect du secret professionnel, offre de produit non adapté au profil du client
- Dommages aux actifs corporels : incendie, vandalisme
- Interruption d'activité et dysfonctionnement des systèmes : panne d'électricité, dysfonctionnement des appareils informatiques, incapacité de communiquer
- Exécution, livraison et gestion des processus : négligence, mauvaise saisie, perte de documents, mauvaise prestation avec partenaires commerciaux.

Au niveau du comité de Bâle, les vols de données bancaires sont considérés comme une fraude.

[1] FINMA, *Circ.-FINMA 08/21 « Risques opérationnels – banques »,*Berne, 2008, P.3

2.3 Historique des affaires

Le vol de données bancaires n'est pas une pratique très courante dans le milieu bancaire. En effet, très peu de cas ont été médiatisés dans l'histoire. Il a fallu attendre la dernière crise financière pour voir une augmentation du nombre de vols de données en Suisse.

La première affaire qui va secouer la place financière suisse concerne l'Affaire Birkenfeld en 2007. Bien qu'il n'y ait pas eu de vols de données bancaires dans cette affaire, elle sera l'élément déclencheur qui mettra les banques suisses dans une position délicate. Au début des années 2000, Monsieur Bradley Birkenfeld est recruté par UBS et apporte avec lui un portefeuille de clients, dont un dénommé Monsieur Olnicoff, qui est soupçonné de frauder les autorités fiscales américaines. Monsieur Birkenfeld va aider Monsieur Olnicoff à dissimuler 200 millions de dollars aux autorités fiscales des États-Unis pour une économie d'impôt d'environ 7 millions de dollars. En 2005, il démissionne de son poste à la suite d'un litige qui l'oppose à son employeur. En 2007, il prend contact avec les autorités fiscales américaines et dénonce les pratiques de la banque, qui a instauré un système permettant d'aider les contribuables américains à frauder le fisc. La banque UBS est condamnée à une amende de 780 millions de dollars et la menace de retrait de sa licence aux États-Unis. Sous-pression, la banque livrera une liste de 300 comptes. De là, les tensions entre la Suisse et les États-Unis, puis plus tard avec les pays voisins vont s'accroître. Monsieur Birkenfeld fera 30 mois de prison et recevra 104 millions de dollars.

La véritable affaire de vols de données a lieu durant l'été 2008, où la banque HSBC subit un vol de données par le biais d'un de ses informaticiens Monsieur Hervé Falciani, qui se serait introduit dans des serveurs, dont il n'avait pas l'autorisation d'accès. Dénoncé par un collègue, il passera devant le juge fédéral, puis sera relâché avant de s'expatrier en France. Il se fera arrêter par la justice française et saisir son ordinateur sur demande de la Suisse. Une enquête sera ouverte en France pour blanchiment et les données seront remises au ministre Français Éric Woerth. Ce sont plus de 15'000 noms de clients qui seront volés et transmis à différents États.

Julius Baer sera victime, à trois reprises, de vols de données bancaires. D'abord en 2008, Rudolf Elmer, un employé qui sera licencié après 20 ans de service, récupère de nombreuses pages de documents confidentiels, où il présente des extraits sur le site internet de « Wikileaks ». En 2011, il remet à Julien Asenge (fondateur du site internet

de « Wikileaks ») deux disques contenant des informations sur près de 2000 clients de la banque qui auraient fraudé le fisc de leur pays. Cette affaire a permis de mettre en lumière la pratique du Trust et Monsieur Rudolf Elmer a obtenu une peine de 240 jours-amendes à 30 francs ainsi qu'une période de sursis de 2 ans. Ensuite 2010, un disque contenant des informations sur 200 clients sera vendu à Land, en Allemagne. La banque versera 50 millions d'euros à l'Allemagne pour arrêter les investigations contre ses clients. Pour finir en 2012, avec un autre disque volé et remis, à nouveau, à Land en Allemagne.

En janvier 2010, Crédit Suisse a subi un cas similaire à Julius Baer, avec un disque de données vendu pour environ 2.5 millions, à l'Allemagne, contenant environ 1'500 noms.

En mars 2010, UBS subira un vol de données. Cependant, contrairement aux autres cas, les données seront volées par un employé, en prenant des photos avec son téléphone portable. Ces informations volées étaient considérées comme plus que complètes et seront vendues à un Land en Allemagne.

Les États ne sont pas les seuls intéressés par des données bancaires. Par exemple, une employée de la banque Vaudoise aurait transmis des relevés de compte à un détective privé, qui était aussi un ancien employé de la banque. En 2004, c'est un employé de Pictet, déçu de sa situation, qui vol des données de la banque. Avec l'aide de 4 complices, il tentera de faire du chantage à la banque, réclamant 42 millions d'euros. Il y a aussi les nombreux espions américains, sous couverture diplomatique, qui ont essayé d'entrer en Suisse en 2008. Ou encore les douaniers français qui ont surveillé l'entrée du parking de la banque Pictet aux Acacias, en 2013.

Mais toutes ces pratiques ne sont pas récentes. En effet, dans un travail de mémoire, réalisé par Monsieur Thomas Chappot et dirigé par le professeur Sébastien Guex, nous apprenons que dans les années 30, des représentants allemands de l'autorité fiscale rémunéraient des banquiers suisses pour livrer des noms de fraudeurs. A l'époque, avec l'arrivée au pouvoir d'Hitler, les pratiques ont continué, mais la méthode était bien différente. Des représentants nazis obtenaient, sous la contrainte, la procuration d'un client. Ils pouvaient alors accéder à des informations sur les clients, en se rendant au guichet de la banque, parfois avec les clients[2].

[2] CHAPPOT, Thomas, l'*espionnage bancaire* (1930-1935). Travail de mémoire, Faculté des lettres, Section d'histoire, Université de Lausanne, 2010

Les banques ne sont pas les seules à subir des attaques. En effet, les clients subissent des attaques de *Phising*, une des nouvelles tendances des pirates. En prétendant être la banque, les pirates envoient un courrier électronique à des clients et leur exigent de donner les coordonnées de leurs cartes de crédit. Ces données acquises peuvent, soit être exploitées par le pirate, ou bien revendues à des escrocs ou usurpateurs d'identité.

Cette augmentation est aussi observée par le cabinet d'audit KPMG, dans une publication sortie en 2013, Le «*KPMG Forensic Fraud Barometer*»[3]. En 2012, la Suisse est le pays qui subit le plus de pertes de données dans le monde, très loin devant le Japon, ou encore les États-Unis ayant subi seulement 4 % des vols. 65 % des infractions les plus subies par les 30 plus grandes entreprises Suisses sont des vols de données internes. Dans ces infractions, les banques subissent environ 30 % des vols. Mais le nombre de cas de vols de données a diminué ces dernières années. Ce qui est surprenant, c'est que plus d'un tiers des fraudes sont commises par des managers.

2.4 Impact de données volées

Comme le montre l'étude de KPMG, la Suisse est une cible privilégiée pour la fuite de données. Si pour d'autres secteurs, les informations volées concernent des secrets de fabrications ou d'informations technologiques, pour les banques, les informations qui sont le plus souvent volées concernent des données clients.

Ainsi, la livraison par la banque UBS de 4500 noms à l'autorité fiscale des États-Unis aurait incité 33'000 contribuables à régulariser leur situation et récupérer une recette de 5 milliards de dollars. Les résultats sont les mêmes pour les Lands allemands, qui ont acheté pour quelques millions d'euros, ont conduit à des perquisitions auprès de 200 fraudeurs et des contribuables qui se sont autodénoncés. La recette fiscale est estimée à 670 millions d'euros.

[3] KPMG, *Fraude: les managers causent les plus grands dommages,* 2013, http://www.kpmg.com/ch/fr/mediareleases/2013/pages/forensic-fraud-barometer-2013.aspx (consulté le 05.05.2013)

Tableau 3

Récapitulatif

Cas	Année	Cas	Résultat
UBS Birkenfeld	2007	Fraude d'un client	-Dénonciation des pratiques de la banque -Livraison de plus de 4'500 clients américains -40 mois d'emprisonnement + prime de 104 millions dollars pour Monsieur Birkenfeld -Dénonciation spontané de plus de 33'000 clients -Recette fiscale récupérée estimée à 5 milliard de dollars -Nouvelle demande de noms.
HSBC	2008	Vol de données clients par un informaticien	-Liste de 15'000 clients volé -3000 noms de fraudeurs potentiels en mai des autorités françaises -livraison de 2'000 noms aux autorités fiscales de la Belgique, par la France -Recette fiscale récupérée estimée à 1.2 milliards d'euros -Arrestation de Monsieur Hervé Falciani
Crédit Suisse	2010	Vol de données et vendus à un Land Allemand	-Vente de cd contenant 1'500 noms de contribuables allemands -Avoir estimé d'environ 1.9 milliard d'euros. -Paiement de 2.5 millions d'euros pour l'acquisition du cd - Arrestation de l'employé -Arrestation et suicide de l'initiateur de la vente.
UBS	2010	Vol de données par photographie et vente un Land Allemand	-Noms de 750 fondations livrées -Avoir estimé d'environ 3.5 milliard d'euros.
Julius Baer	2008-2011, 2010 et 2012	Vol de données et transmises au site internet de « Wikileaks » Vol de données et vendues aux autorités allemandes	-2000 noms remis à Wikileaks -Médiatisation du Trust -Peine de 240 jours-amendes à 30 francs et 2 de sursis pour Monsieur Rudolf Elmer -200 noms de clients dérobés -Versement de Julius Baer de 50 millions pour arrêter les investigations. -Cas 2012 pas détaillé

2.5 Profil des voleurs

Concernant les vols réalisés en interne, les affaires présentées précédemment ont permis de relever qu'il y a trois motifs qui incitaient aux vols de données.

Le premier point relevé montre que le fraudeur avait des problèmes privés et/ou personnels. Cela peut venir d'une non-promotion pour un poste, une augmentation refusée, un différend avec la hiérarchie. Dans l'une des affaires avec la Banque Julius Baer, Monsieur Rudolf Elmer a été licencié après avoir travaillé 20 ans dans la banque.

Le deuxième point relevé montre que la personnalité du fraudeur pouvait avoir une influence sur les vols de données. Certains voleurs sont motivés à vendre des informations confidentielles, avec les importantes sommes versées par des personnes externes. On peut voir avec la banque UBS et Monsieur Bradley Birkenfeld qui a dévoilé des informations pour être considérer comme un lanceur d'alerte et être rémunéré pour son action. Ou bien les Lands allemands qui acceptent de rémunérer avec d'importante somme d'argent pour l'obtention de disques contenant des données clients avec les banques UBS, Crédit Suisse et Julius Baer.

Le troisième point relevé montre qu'il existant des opportunités de voler des informations. Cela peut venir de mesures de sécurité absente, problème dans l'organisation avec une mauvaise définition des rôles ou encore les collaborateurs n'ont pas été assez bien formés sur certaines règles de travail. Dans Monsieur Rudolf Elmer avait pu imprimer un nombre important de documents confidentiels sans que qu'il ne soit gêné dans son vol. Dans l'affaire HSBC et Monsieur Hervé Falciani, La banque avait pu détecter l'intrusion de Monsieur Falciani à des informations qui lui étaient interdites. Mais la banque n'a pas réalisé une enquête efficace car il a pu quitter la Suisse avec les disques volé avant qu'elle constate l'acte que Monsieur Falciani a réalisé.

Il existe plusieurs éléments qui permettent de détecter une personne qui serait tenté de commettre un vol de données. Un des premiers signes qui peut être perçu par les autres collaborateurs c'est le comportement au travail de la personne comme avec cette liste non-exhaustive présentée ci-dessous :

- Stress
- Fatigue
- Silencieux
- Discret
- Difficulté à communiquer
- Difficulté à travailler en équipe
- Problème avec son supérieur ou ses collègues
- Frustré
- …

Cela a également une répercussion dans le travail de la personne et sa vie privée. Par exemple :

- Opacité dans son travail
- Horaires de travail important (tard, ne prend pas congé et travail depuis l'extérieur)
- Problèmes financiers
- Non-respect des règles
- …

3. Méthodologie appliquée

Il est difficile de trouver des informations sur le vol de données bancaires. Cela est dû au nombre limité de cas rendus publics. De plus, les livres traitant de la gestion du risque n'offrent pas beaucoup d'informations sur le sujet. Enfin, les banques ne publient pas beaucoup d'informations sur le site internet. La meilleure solution pour obtenir des informations sur le sujet était d'aller les chercher directement auprès de professionnels de la branche, par le biais d'entretien semi-directif.

3.1 Entretien semi-directif

La méthode d'entretien privilégiée pour ce travail est l'entretien semi-directif. C'est une méthode couramment utilisée auprès d'un échantillon de sondés, pour récolter des données qualitatives. Il présente de nombreux points intéressants. Tout d'abord, une grille d'entretien est réalisée sur des idées retenues avant l'élaboration de l'entretien. Ensuite, les entretiens avec les sondés sont réalisés en face à face, cela permet à l'intervieweur de récupérer des informations sur le non verbal et sur l'environnement dans lequel l'entretien a été réalisé. En plus, l'intervieweur dirige l'entretien pour obtenir une réponse pour chaque idée recherchée. Contrairement à un entretien directif, l'entretien semi-directif doit laisser aux sondés la possibilité d'exprimer leur avis, leur ressenti ou des expériences connues, qui sont une véritable valeur ajoutée à une enquête.

3.2 Mise en place du sondage

Il existe 5 étapes pour la réalisation d'un sondage :

1. La première étape consiste à rechercher de la documentation sur le sujet. Pour mon travail, il s'agissait d'avoir un maximum d'informations sur les pertes de données bancaires et les méthodes de protections.
2. Dans la deuxième étape, il s'agit d'établir un questionnaire qualitatif qui doit permettre obtenir les informations souhaités. Il doit permettre d'ouvrir la discussion sur un sujet et éviter de mettre mal à l'aise le sondé sur une question gênante. Pour ce travail, six questions ont été élaborées et validées par Monsieur Fragnière.
3. La troisième étape consiste à trouver les personnes qui seront capables de nous fournir des informations sur le sujet. Il faut avoir un échantillon suffisant, pour avoir des informations pertinentes et en tirer une analyse, mais aussi pas trop important, car il devient alors trop compliqué à travailler. Dans mon cas,

mon échantillon est composé de 12 personnes qui travaillent ou ont travaillé dans le milieu bancaire.

4. La quatrième étape concerne le déroulement de l'entretien. Il s'agit de prendre contact avec les sondés, expliquer le but du travail, donner le temps de répondre au questionnaire, fixer la date et le lieu de l'entretien. Dans mon cas, les interviews ont été réalisées dans un lieu proposé par les sondés.
5. La cinquième étape du sondage consiste à retranscrire les réponses des sondés et faire l'analyse des résultats.

3.3 Grille d'entretien

Le questionnaire est composé de six questions orientées sur le thème de la protection de données sensibles au sein des banques. Les questions posées et les réponses recherchées sont présentées ci-dessous :

Q.1 Pourriez-vous me présenter brièvement les étapes principales de votre carrière? (Quelle formation avez-vous suivie?)

Cette question permet de connaitre le parcours professionnel et les connaissances qu'il a acquises au cours de sa carrière. De plus, cela permettra de voir si leurs compétences et connaissances proviennent surtout du milieu bancaire ou bien de leur formation ou encore de leurs précédents emplois.

Q.2 Pourriez-vous décrire vos fonctions principales?

Cette question permet de mieux connaître le travail du sondé. Cela donne également un aperçu des tâches les plus importantes ainsi que les manières de les traiter.

Q.3 Avez-vous été confronté à des tentatives de vols de données au cours de votre carrière? (en interne/externe, à l'étranger) (quels sont les moyens possibles que vous connaissez?)

Cette question permet au sondé de raconter une histoire antérieure qu'il a vécue ou qui lui a été racontée. Elle permet aussi d'avoir un aperçu des méthodes de vols les plus courantes que subissent les banques.

Q.4 Comment intervenez-vous lorsqu'une tentative de vol est sur le point de s'y produire?

Cette question permet de savoir quels sont les acteurs de la banque et comment ils interviennent lors d'une tentative de vol ou fuite de données.

Q.5 Quelles sont les tendances dans le milieu bancaire pour se prémunir contre les vols et fuites de données? (Qu'en pensez-vous?) (Quels sont les différents outils et *méthodes utilisées?)*

Cette question permet de connaître les moyens des banques pour faire face à des vols de données. Voire, les avantages et inconvénients de ces méthodes.

Q.6 Pensez-vous qu'il faudrait redéfinir les rôles des différents intervenants pour une meilleure sécurité des données?

Les différentes affaires, qui ont secoué la place bancaire suisse, ont montré que le risque humain était très important. L'affaire HSBC a montré que la fuite venait d'un collaborateur du service informatique. Cette question permet d'obtenir l'avis du sondé sur la manière dont les rôles sont réparties mais également de proposer leur solution pour améliorer la protection des données.

Chacune des questions a été posée de la même façon. Si le sondé n'avait pas compris la question ou bien il avait besoin d'avoir des précisions, je reformulais et donnais les mêmes compléments d'information aux sondés. Je n'ai pas transmis le questionnaire aux personnes avant l'interview, à l'exception d'une personne qui voulait savoir s'il était en mesure de répondre aux questions.

3.4 Elaboration de l'échantillon

L'échantillon est composé de douze personnes évoluant dans le milieu bancaire. Étant donné que le sujet des vols de données bancaires est un sujet sensible dans le milieu, aucun nom des sondés, ni d'établissement ne seront mentionnés. Pour la sélection des douze sondés, Monsieur Fragnière m'a remis le nom de contacts qui pourraient m'aider à débuter mon travail. Après chaque entretien, j'essayais d'obtenir du sondé, une de ses connaissances, qui pourrait me donner des informations sur le sujet.

3.5 Retranscription des entretiens

La retranscription est une partie longue et difficile à réaliser. Dans le cadre de mon travail, aucune interview n'était enregistrée. L'utilisation d'un dictaphone pourrait en effet amener un malaise aux sondés, qui pourraient, par conséquent, faire attention aux mots qu'ils emploient. De plus, ne pas enregistrer les interviews m'obligeait à être plus concentré et attentif durant les entretiens, car je savais qu'il n'y en aurait pas deux avec la même personne. Le résultat de la retranscription était envoyé à chaque sondé. Il s'agissait d'avoir leur avis sur la retranscription et si elle correspondait et ne dénaturait pas les propos du sondé. La plupart des sondés n'ont pas apporté beaucoup de changements, par rapport aux premières versions. Les changements apportés étaient par exemple *« L'affaire avec Monsieur Falciani… », au lieu de « L'affaire Falciani »*.

4. Analyse des informations recueillies

Pour faire mon analyse, j'ai procédé selon les étapes suivantes :

- Dans la première étape, j'ai fait une lecture complète de toutes les retranscriptions. A la fin, j'ai fait un petit résumé des informations générales qui sont ressorties. Cela m'a permis de voir les pistes que je allais étudier.
- Dans la deuxième étape, j'ai fait une deuxième lecture par question. Je soulignais et prenais des notes sur une feuille vierge, des mots clés. Cela m'a permis de sortir les opinions des sondés.
- Dans la troisième étape, j'ai complété mon analyse des étapes précédentes avec les recommandations faites des sondés. Certains m'ont conseillé de lire un article sur l'affaire de la banque vaudoise ou bien de regarder la révision partielle de la circulaire de la FINMA sur les risques opérationnels.
- Dans la quatrième étape, j'ai cherché à analyser l'environnement et l'atmosphère dans lequel l'entretien s'était déroulé.
- Dans la cinquième étape, j'ai ajouté les avis des personnes interrogées, sous la forme de citation. Toutes les retranscriptions des entretiens sont disponibles, en annexe 1, de ce dossier.

4.1 Lieu et déroulement d'un entretien

Quand nous fixions un rendez-vous avec le sondé, je lui laissais le choix du lieu de l'entretien. Étant donné que le vol de données peut être interprété comme un sujet sensible, j'ai pensé que les personnes auraient évité les lieux publics, et privilégié les locaux où ils travaillent. Je réalise que j'avais de gros « à priori » sur les personnes travaillant dans les banques, car plusieurs des interviewés m'ont proposé l'entretien dans un lieu public, avec peu de personnes autour, pour ne pas être dérangés par le bruit pendant l'entretien. Les autres sondés m'ont proposé de réaliser l'interview dans leurs locaux, où ils avaient réservé une salle spécialement pour l'occasion.

Quels que soient les établissements visités, j'ai d'abord dû me présenter à la réception en expliquant la raison de ma visite. Si pour les banques, il suffisait que je m'annonce à la réception, lorsque je suis entré dans le bâtiment d'un cabinet d'audit, j'ai dû remplir une fiche avec mon nom, prénom, adresse, numéro de téléphone, la raison de ma présence, l'heure à laquelle je suis arrivé et sorti ainsi que le numéro de badge pour le visiteur. Ces protections supplémentaires peuvent s'expliquer par les documents qui se

trouvent dans leurs locaux. Les cabinets d'audit s'engagent, par le biais de la signature de leurs collaborateurs, à des poursuites pénales, si les états financiers d'entreprises ne sont pas conformes ou s'ils perdent un rapport.

Les salles étaient aménagées au strict minimum. Il y avait une grande table, plusieurs chaises, une corbeille, une petite table qui avait un téléphone dessus. Je n'avais pas réalisé, avant qu'un sondé ne m'en fasse la remarque, qu'il n'y avait pas de bloc note et de stylo qui étaient disponible. On peut constater que la protection des données contre une personne ne travaillant pas dans les locaux débute dès l'entrée et se poursuit jusqu'à la sortie. En effet, à aucun moment je n'ai été laissé sans « surveillance ». Cette manière de faire évite aux collaborateurs d'utiliser leur bureau ou espace de travail et donc que des informations sensibles soient exposées aux visiteurs.

Avant de commencer l'interview, nous avons parlé de divers sujets durant 5-10 minutes, en faisant notamment la présentation plus en détail de mon travail. Durant cet échange, les sondés m'ont demandé si j'étais déjà venu dans les locaux ou bien si j'avais des contacts dans la banque.

A la fin de l'entretien, plusieurs sondés pensaient devoir répondre à des questions « sensible » comme par exemple, révéler l'organisation dans leur service ou bien une procédure interne et ils ont ensuite donné des informations supplémentaires. Par exemple, un sondé a dessiné un schéma sur la protection informatique d'une banque. Il a expliqué, qu'il était possible de lire sur les sept pages suivantes, ce que nous avions écrit sur un bloc-notes. Un autre sondé m'a donné des explications supplémentaires, par email, sur des éléments qu'il avait oublié durant l'interview. Un exemple donné concerne les informaticiens et les consultants qui peuvent encore avoir beaucoup d'accès dans certains établissements bancaires. Il y a également des sondés qui ont expliqué que les collaborateurs non-résident suisse ou qui n'ont pas une discrétion forte, étaient considérés comme moins fiable. Pour ce dernier point, ils m'ont demandé de ne pas le mettre dans leur retranscription, car ce genre de propos étaient très souvent mal interprété, par écrit.

Lors des 2 premières questions posées, les sondés étaient très ouverts et acceptaient volontiers de parler des formations et des postes occupés.

Lorsque j'ai demandé, s'ils avaient été confrontés à un cas de vol de données (question 3), j'ai pu observer un silence, auprès de certains sondés, avant de me répondre qu'ils n'ont pas connu de tentative. J'ai eu l'impression qu'ils ne voulaient pas me raconter leur expérience, parce que nous ne nous connaissions pas et ils ignoraient comment leurs réponses seraient utilisées. Lorsque je leur ai demandé, s'ils

connaissaient une méthode ou un scénario possible, il prenait souvent l'exemple des affaires de la banque HSBC ou bien de la banque Julius Baer. Il y a eu des sondés qui n'ont pas connu de tentative de vol de données, mais spontanément, ils ont parlé d'un cas qui leur a été raconté ou donnaient l'exemple d'un scénario qui pourrait se produire. Les personnes interrogées qui ont été confrontées à une tentative de vol de données, ont donné une meilleure description du cas et des impressions ressenties (Un sondé relatait un cas d'instruction de paiement falsifiée. Sa banque avait reçu un fax pour une demande de virement. La méthode était étrange car cela n'était pas dans les habitudes du client d'utiliser un fax et a pris contact avec le client, pour avoir confirmation de la véracité de la demande de virement).

Ces sondés ont aussi directement expliqué comment la banque était intervenue et ils ont expliqué les différentes étapes de l'intervention.

A la question 4, quelques sondés ont décrit la manière dont la banque est intervenue, mais ils ont reconnu, que pour eux et la banque, il était difficile d'intervenir à temps.

A la question 5, personnes, les sondés ont énuméré quelques outils et méthodes utilisés dans la banque avec une description, sans donner leur avis sur ces moyens de protection.

A la question 6, j'ai observé que les sondés se sont sentis concernés. Ils n'ont pas hésité à donner leur avis sur le sujet et à expliquer quelles étaient les causes de ces vols. Plusieurs sondés ont émis leurs recommandations pour améliorer la protection des données.

4.2 Formations et études

Les études suivies par la majorité des sondés sont une formation universitaire. Les autres sondés ont fait une maturité ou bien un apprentissage bancaire. Tous les interviewés ont complété leurs connaissances avec des formations supplémentaires en interne ou externe.

Les sondés, ayant terminés une formation universitaire, ont suivi des formations continues dans une spécialisation qui était liée au métier futur. Cependant, un sondé a fait deux masters dans des domaines qui ne le destinaient pas à poursuivre un parcours dans le domaine bancaire.

Les sondés, n'ayant pas fait d'études universitaires, ont suivi le programme de formation de la banque. Ils se sont tous accordés pour dire que ces établissements bancaires offrent d'excellentes formations.

Citations recueillies

Sondé numéro 3: *« La banque offre d'excellentes formations qui sont à la pointe sur les métiers de la banque. »*

Sondé numéro 6: *« Elles offrent d'excellentes formations pour les jeunes et la possibilité de voir différents métiers. »*

4.3 Carrière professionnelle

Les personnes interrogés ont toutes ont travaillé dans différents établissements et exercés différentes fonctions.

Les sondés qui ont exercé la fonction d'auditeur, gestionnaire du risque et ceux qui ne travaillent plus dans un établissement bancaire étaient plus ouvert à la discussion, en donnant davantage de précisions sur des éléments, par exemple :

- le sondé numéro 5 m'avait remis un dossier de l'ASB, qui concerne la protection des données.
- le sondé numéro 11 m'a donné des informations supplémentaires, par email, sur les points qui doivent être améliorées dans certaines banques.
- Le sondé numéro 12 a dessiné un schéma présentant le système informatique d'un banque.

4.4 Types de vols de données bancaires

A la question 3 : *« Avez-vous été confronté à un vol de donnée au cours de votre carrières ? »,* nous apprenons que :

- Quatre sondés ont été confrontés à un risque de vol de données ou perte de données.
- Deux sondés ont appris l'histoire d'risque de vol de données ou perte de données, sans y être confronté.
- Six sondés n'ont jamais été confrontés à un risque de vol de données ou perte de données.

Plusieurs personnes interrogées ont expliqué que leur banque prenait aux sérieux le risque de vols de données bancaires, car leur réputation en serait impactée.

Citations recueillis

Sondé numéro 6 : « Les banques préfèrent éviter qu'on ébruite un vol commis, la réputation de la banque en sera affectée. »

Sondé numéro 2 : *« La banque prend très au sérieux la menace des données bancaires, c'est l'image de la banque qui peut être touchée. »*

Tous les sondés avait au moins deux définitions des vols de données bancaires :

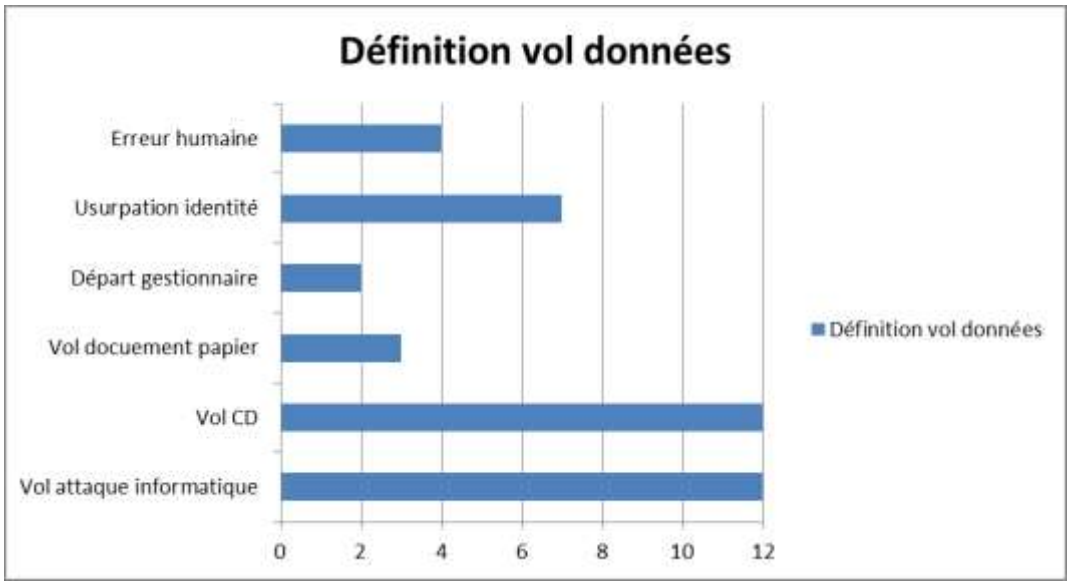
- La première définition donnée concerne les vols commis par un collaborateur, qui enregistre un disque de données avec des informations concernant des clients.
- La deuxième définition donnée concerne les vols commis par une personne extérieure à la banque. Il s'agit d'espions, de pirates informatique et d'autres, qui vont s'introduire dans le système pour récupérer des informations sur des clients.

Certains sondés ont aussi ajouté d'autres définitions des vols donnés :

- 3 sondés ont mentionné les vols de documents papiers.
- 2 sondés ont mentionné les vols de clients par un gestionnaire.
- 4 sondés ont mentionné la négligence.
- 7 sondés ont mentionné l'usurpation et le vol d'identité.

Concernant la dernière définition, les personnes interrogés ont eu des hésitations, ils ne savaient pas si elle pouvait être considérer comme une fraude ou bien un vol de données, car les coordonnées des clients sont utilisées pour obtenir un gain.

Figure 1



Ces différentes définitions du vol de données présentées par les personnes interrogées peuvent être regroupées en trois catégories

- Vol de donnés simple : Le vol d'informations.
- Echange de banque : Le client veut garder son gestionnaire et change de banque
- Vol et monétisation frauduleuse : Le vol de coordonnées bancaires qui sont revendues à des fraudeurs

Quelques citations recueillis

Sondé numéro 11 : *« Il existe pour moi deux types de données bancaires. Il y a les données qui ont été médiatisées par Monsieur Falciani, établir un CD contenant des données sensibles de clients, qu'on essaye de transmettre en échange d'argent. Et il y a le deuxième type qui est plutôt « emprunter » des données. C'est-à-dire, qu'il y a un gestionnaire qui quitte son établissement bancaire pour aller chez le concurrent ou bien se mettre à son propre compte et qui veut récupérer le portefeuille client qu'il a géré. »*

Sondé numéro 5 : « Des données perdues par négligence peuvent être monnayées par une personne externe. »

Sondé numéro 3: « Une fraude ou un vol c'est pareil, la banque sera impactée. »

Les sondés ont accepté de raconter une histoire sur un vol de données bancaires. Les sondés qui n'ont jamais été confronté à un vol de données ont souhaité donner un exemple qui pourrait se produire. Les cas sont présentés ci-dessous :

Pertes données par usurpation d'identité et extorsion d'informations confidentielles:

Ce genre d'attaque consiste à soutirer des informations des clients d'une banque pour en tirer avantage. Cette menace est réalisée par une personne de l'extérieur à la banque. Le procédé de la menace est présenté avec deux cas :

Le voleur va créer une fausse demande de virement bancaire par écrit. Le voleur va faire des recherches sur internet pour récupérer des images des documents bancaires et la copie des signatures de certaines personnes importantes. En réalisant le montage, l'usurpateur peut se faire passer pour n'importe qui avec un document qui pourrait paraître comme un original de la banque. L'usurpateur va ensuite envoyer le document par fax à des banques et va essayer de récupérer de l'argent avec la fausse demande de virement.

Le collaborateur qui était chargé du dossier avait remarqué que cette méthode de procédé n'était pas dans les habitudes du client ou de la banque. L'employé a eu la bonne réaction en prenant contact avec la personne qui a émis le fax pour avoir des explications. Il a constaté que la personne n'avait jamais envoyé cette demande à la banque. Le collaborateur a averti sa hiérarchie et signalé le cas au gestionnaire du risque qui va établir une enquête. Le sondé numéro 2 explique que le gestionnaire du risque va aussi avertir les autres banques du cas, en utilisant la messagerie Swift.

La deuxième méthode consiste à récolter des informations sur une personne. Le fraudeur va se rendre au guichet d'une banque prétextant qu'il souhaite effectué un virement sur le compte de x, car il sait que la victime a un compte dans la banque.

Dans ce genre de situation, les collaborateurs sont formés pour ne révéler aucune information sur des clients. Le cas est signalé au gestionnaire du risque et les autres banques sont averties par messagerie.

Pertes de données liées à un vol d'un collaborateur :

La perte liée à un vol d'un collaborateur consiste à soutirer des informations confidentielles et sensibles de la banque. Le collaborateur va très souvent chercher à monnayer ces informations avec des personnes qui pourront les exploiter. Les sondés ont tous parlé du cas médiatique de l'affaire HSBC, où un informaticien a volé un CD contenant la liste de plusieurs milliers de clients de la banque, qu'il a voulu vendre à différents états. Les sondés ont aussi mentionné les affaires Pictet et la banque Cantonal Vaudoise présentées en introduction de dossier.

Le deuxième exemple donné consiste à voler des informations en les imprimant. Le voleur va imprimer deux exemplaires d'une liste de client. Il justifie la première impression comme étant nécessaire à son travail. Tandis que la seconde est remise à un autre service qui avait aussi demandé cette liste. Dans ce genre de cas, le voleur a profité d'une faille dans l'organisation pour commettre son méfait.

Le troisième exemple raconté par plusieurs sondés et qui les préoccupe est le vol commis avec Smartphone. Avec l'évolution de la technologie, le téléphone portable est devenu un « couteau suisse ». Mais ses nombreuses fonctions sont aussi une menace pour les banques, parce que n'importe quelle personne peut prendre des photos avec son téléphone portable sans laisser de trace au bureau.

L'intervention survient très souvent après que les vols soient commis. Un élément qui est ressorti de plusieurs sondés est qu'il existe deux méthodes d'intervention :

- La première méthode consiste à déceler un comportement étrange d'un collaborateur. Un collaborateur peut avoir un changement d'humeur lié à sa situation dans la banque. Dans ce genre de cas, ce sont ses collègues qui peuvent réagir en signalant cela au supérieur hiérarchique. Une enquête sera alors réalisée pour chercher à comprendre la cause du mal-être de l'employé. Il est très important que l'enquête soit rapide, pour éviter de laisser la situation se détériorer. Un entretien avec la personne sera réalisé pour chercher à comprendre sa situation et savoir comment la banque peut l'aider et intervenir au mieux. Après l'enquête et l'entretien, un rapport est établi et des actions sont prises. Les mesures peuvent être un changement de poste, modification dans son travail, limitation des accès, voire une mise à pied.
- La deuxième méthode consiste à réagir aux vols qui se sont produits. Les différents sondés expliquent qu'il est difficile et qu'il y a peu de choses que la

banque puisse faire. Différentes personnes interviennent dans l'enquête pour connaître quel type d'information a été volé. Le sondé numéro 5 a donné des éléments de réponse d'un point de vue de l'audit externe. La banque est dans l'obligation d'aviser et d'expliquer le cas à la FINMA et aussi son auditeur. La FINMA va ensuite mandater l'audit pour effectuer un audit et va exiger un rapport sur :

- Savoir ce qui s'est passé et comment. Il s'agit de savoir si c'est un cas déjà connu ou un nouveau qui ne s'est pas encore produit dans un établissement.
- Savoir pourquoi cela s'est produit. La FINMA veut savoir s'il y a un moyen d'éviter ce genre de situation à l'avenir.
- Est-ce qu'il y a un moyen de corriger l'erreur produise.

Selon le rapport établi par le cabinet d'audit. La FINMA peut :

- Demander un plan de remédiation à la banque
- Infliger une amende
- Obliger la banque à avertir ses clients que leurs données ne se trouvent plus en sécurité dans les serveurs de la banque et qu'elles se trouvent à l'étranger.

Le cabinet d'audit va réaliser l'état de la situation et va transmettre le rapport à la FINMA.

Le quatrième exemple donné s'agit d'un collaborateur, qui interceptait le courrier des clients, qui allait recevoir une nouvelle carte de débit ou bien une carte de crédit. Les cartes volées étaient alors utilisées pour les besoins personnels du collaborateur.
La banque a reçu de nombreux d'appels de clients qui n'avaient pas reçu leurs cartes et leur mot de passe. Une enquête a été réalisée et la banque a observé des changements d'habitude auprès d'un employé. En effet, il effectuait des achats pour plusieurs nouveaux produits comme par exemple une nouvelle voiture ou une montre.

Pertes de données liées à une erreur humaine :

Les pertes de données ne sont pas uniquement des attaques externes ou des voleurs. Elles sont très souvent l'origine d'un collaborateur qui a commis une erreur sans intention de nuire à l'établissement. Les causes de ces erreurs sont très souvent l'oubli, la négligence et la paresse. Ce genre de cas peut se produire avec une banque travaillant avec des intervenants externes:

Le sondé numéro 5 a présenté le cas suivant: *« Deux collaborateurs travaillant pour la même banque mais dans des bureaux différents (Genève et New York), qui doivent collaborer pour un travail ou projet. Les deux parties doivent échanger des données sensibles et font des échanges via e-mail. Le problème c'est que la donnée qui était sécurisée dans les serveurs de la succursale à Genève se retrouve aussi dans les serveurs de New York. La banque se retrouve avec des données qui ne sont plus sécurisées dans leurs locaux et ignore le risque que subir ces informations. »*

Un autre exemple avec l'e-mail peut se produire lorsqu'un collaborateur envoie des documents à plusieurs personnes en reprenant le destinataire d'un précédent message envoyé. Malheureusement, il transmet ainsi ces informations à une personne qui n'était pas destinée à les recevoir.

Dans les deux exemples donnés, l'intervention est similaire à la deuxième méthode appliquée concernant les vols de données bancaires.

Perte de données externalisées :

Au cours des différents entretiens, un sondé a raconté le cas d'une banque qui avait externalisé son parc informatique. La société mandatée avait décidé de changer entièrement son parc informatique. Toutefois, elle n'a pas réalisé correctement son travail sur la protection des données, car les anciens disques durs, où étaient stockées les informations importantes, n'ont pas été effacés. La banque s'était retrouvée avec un risque important que quelqu'un récupère ces informations.

Il n'y a pas eu de conséquences négatives pour la banque. L'entreprise sous-traitante aurait dû cependant signaler à la banque qu'un changement de son parc informatique sera réalisé. La banque aurait dû établir une enquête pour savoir :

- Quelles sont les données externalisées
- Quels sont les outils changés et ceux qui sont débarrassés
- Comment le sous-traitant a-t-il protégé ses informations
- Comment le sous-traitant a-t-il supprimé les données sur l'ancien support

Le sous-traitant aurait dû détruire les disques durs, pour ne pas pouvoir récupérer les informations contenues.

Utilisation d'accès non autorisé :

Ce type de vol est réalisé par un collaborateur qui exploite des accès qui ne lui sont pas autorisés. Un collaborateur qui travaille à la hotline, a profité pour se connecter sur le poste de travail d'un collaborateur, pour accéder au fichier de ressources humaines à des usages personnels.

La banque a pu intervenir rapidement grâce à une procédure de dénonciation mise en place.

Le départ d'un gestionnaire avec un portefeuille client :

Un gestionnaire de fortune est responsable de la gestion des avoirs de plusieurs clients. Son portefeuille peut se décomposer en deux parties. La première partie est constituée de clients que la banque a mandatés. La deuxième est composée de clients à amener à la banque. Lorsque le gestionnaire quitte la banque, il va vouloir récupérer ce portefeuille de clients, soit pour travailler à son compte ou bien l'utiliser comme atout pour postuler dans une banque concurrente. Pour réussir à récupérer ses clients, la personne va préparer son départ. Il va profiter de la relation de confiance qu'il a nouée avec ses clients et la qualité de son travail pour tenter de les « fidéliser ».

Le cas d'un gestionnaire partant avec le portefeuille qu'il a géré, exige une approche différente. Étant donné que le portefeuille client n'appartient pas à la banque ni au gestionnaire, ce sont les clients qui décident s'ils souhaitent continuer avec la banque ou bien s'ils veulent que leurs avoirs soient gérés par le gestionnaire. C'est pourquoi la banque agit en trois étapes:

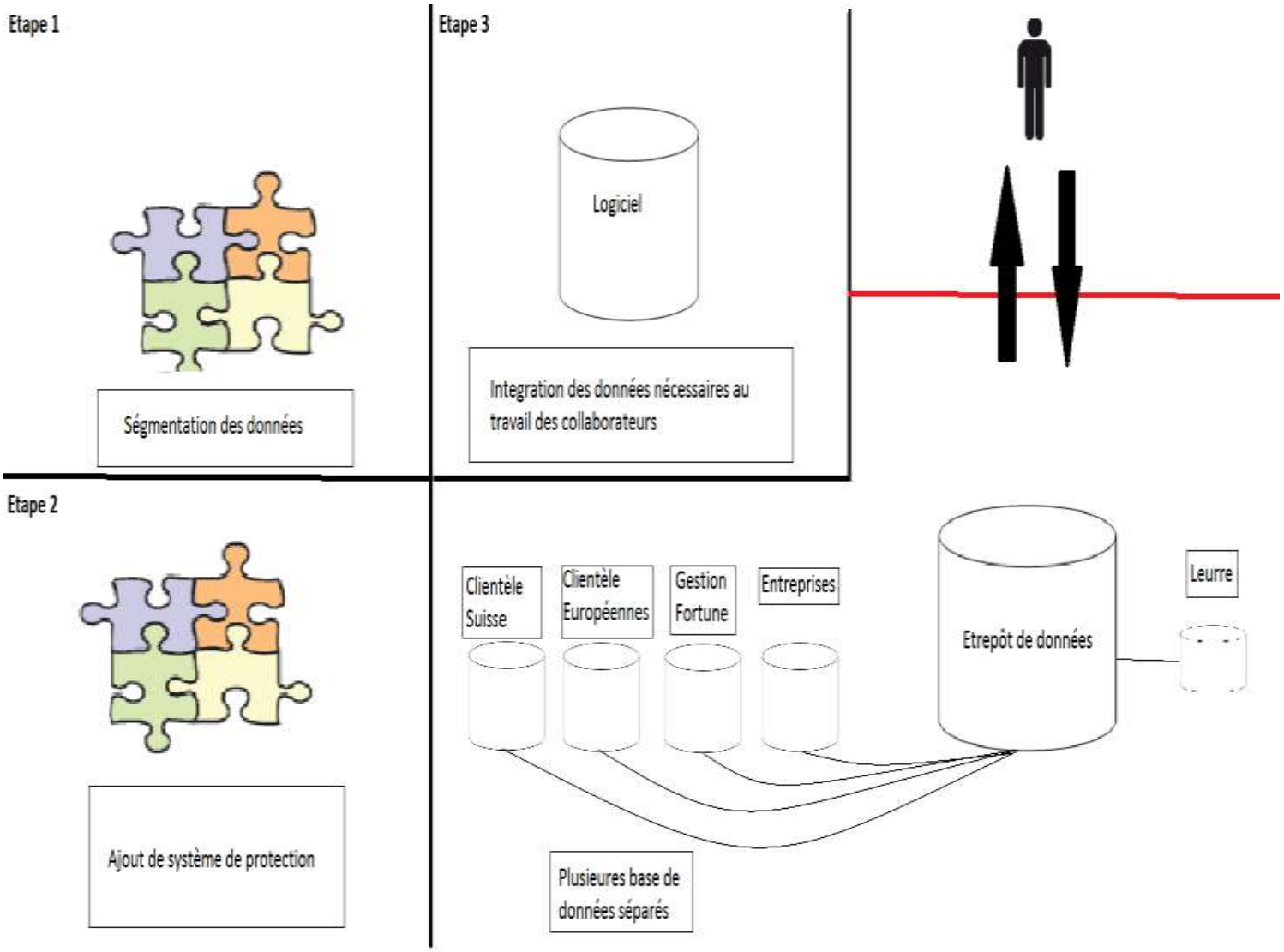
- La première étape consiste à offrir une qualité de service de grande qualité. Cela passe par un suivi du client avec une mise à jour régulière du dossier, être à l'écoute des besoins du client, des conseils avisés. Il s'agit de garder le client pour ne pas qu'il aille chez un concurrent
- La deuxième étape consiste à mettre deux conseillers au service du client, où le premier est le gestionnaire principal/accrédité et le deuxième est le remplaçant ou l'assistant. Les deux ont toujours des contacts réguliers avec le client. De plus, le supérieur du gestionnaire doit aussi connaître les clients du gestionnaire et créer des liens avec lui. Il s'agit de montrer l'implication de la banque sur le suivi du client en montrant que si le gestionnaire quitte l'établissement, son remplaçant offrira la même qualité de service.
- La troisième étape consiste à préparer le départ du gestionnaire efficacement. La banque va retirer la gestion du portefeuille au conseiller pour le mettre à l'écart et pour que son remplaçant puisse créer des liens. Le conseiller sera toujours un employé de la banque, mais il n'exercera pas de fonction. Il est possible qu'à la signature du contrat, le collaborateur ait accepté une clause de non-concurrence, l'empêchant par exemple de « récupérer » ses clients.

Attaque informatique :

L'attaque informatique a été mentionnée par tous les sondés sans que les sondés le développent. Un pirate informatique va tenter de s'introduire dans une des bases de données pour récupérer des informations, en utilisant des malicielles. La menace peut aussi venir d'un collaborateur qui tente de s'introduire dans des serveurs qui ne lui sont pas autorisés.

Figure 2

Schéma de protection d'une banque



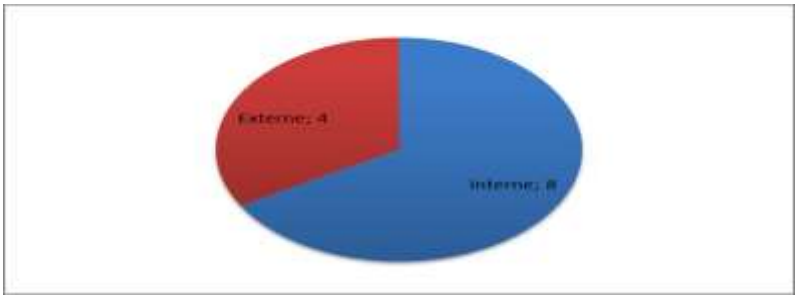
- Dans l'étape 1, la banque possède différentes données (financières, clients, collaborateurs,…) qui vont être segmentées et attribuées à différents services. Le but est d'éviter qu'une personne ait une concentration importante d'informations (un gestionnaire responsable de la clientèle suisse ne pourra pas accéder à la clientèle asiatique).
- Dans l'étape 2, des outils de protections sont ajoutés sur ces données pour éviter une utilisation frauduleuse (Par exemple, insertion de deux codes où un va servir à limiter les accès et le deuxième à interdire les copiés-collés et impressions, ainsi que l'ajout d'un Water Mark contrôler les transmissions)
- Dans l'étape 3, ces données sont affichées sur le logiciel de la banque. Chaque collaborateur a une clé de cryptage lui permettant d'accéder aux informations nécessaires à son travail (un conseiller ne pourra pas passer des ordres et faire la réconciliation)
- Dans l'étape 4, ces données sont stockées sur différents serveurs qui sont regroupées dans un entrepôt de données. Des programmes de sécurité sont installés comme des pare-feu. Les données sont surveillées et des alertes sont lancées, quand des éléments non autorisés tentent de se connecter :
  - Clé USB
  - Programme .EXE
  - Des messages
  - Flux importants

Si un collaborateur veut accéder à des informations qu'il ne peut pas voir, il se verra refuser l'accès et les organes de surveillance seront avertis du mouvement.

Contre les attaques externes, les pirates doivent passer les différents systèmes de sécurité comme l'antivirus, pare-feu et autres mesures. S'il réussit à trouver une faille dans les programmes de protection et à accéder aux bases données, il accédera à un leurre. Il s'agit d'une fausse base de données, avec de fausses informations qui servent d'appât pour les pirates.

Figure 3

Origine de la menace



Sur les 12 exemples donnés, nous pouvons voir que la menace provient le plus souvent à l'intérieur de la banque. Les sondés expliquent qu'ils n'imaginent pas qu'un collaborateur puisse commettre ce genre vol. Un sondé estime que les banques ont sous-estimé le vol interne, car les collaborateurs connaissent mieux leur travail que leur manager ou les fonctions de surveillances et ils peuvent voir les défauts dans une organisation. Les exemples donnés ont aussi démontré qu'il pouvait exister des lacunes dans l'organisation de la banque, avec une absence ou un manque de contrôle sur des éléments de l'organisation.

Citation recueillies

Sondé numéro 8 : *« Il m'est arrivé d'avoir des tentatives d'extorsion ou des usurpations pour voler des données, mais c'était des petites tentatives sans succès. »*

Sondé numéro 8 : *« on ne s'attend pas à ce qu'un collaborateur puisse commettre un vol. Mais il existe des pistes, par exemple, les personnes qui commettent des fraudes ou vols internes sont très souvent frustrées ou bien qui ont un problème avec leur supérieur hiérarchique. »*

Sondé numéro 5 : *« Les banques investissent beaucoup dans la sécurité pour se protéger contre une attaque venue de l'extérieur avec par exemple des firewalls et autres outils de sécurité, mais moins d'effort son réaliser pour les attaques venant en interne. »*

Sondé numéro 9 : *« un collaborateur qui veut voler des données, il réussira, car il aura trouvé une défaillance dans l'organisation de la banque. »*

Parmi les exemples mentionnés, tous les cas concernent un collaborateur de bas niveau hiérarchique. Ces cas n'obtiennent pas les mêmes résultats que la publication de KPMG, car aucune des histoires n'a mis en situation un manager. Selon les informations recueillies auprès des sondés, leurs exemples contredisent ce dossier et nous pourrions en déduire qu'un collaborateur avec un degré de responsabilité plus élevé et une rémunération plus importante serait moins tentée de commettre un vol. Toutefois, deux sondés avaient mentionné, durant leur interviews, que les managers avaient les moyens de commettre un vol ou fraude, en donnant des ordres à leurs collaborateurs d'exécuter des opérations et il pouvait les faire valider auprès de la hiérarchie.

PWC a également publié un rapport sur les crimes économiques réalisés en Suisse. Le cabinet c'est intéressé sur les fonctions hiérarchies de des fraudeurs. Nous apprenons qu'en 2009 :

- 20% des fraudes internes sont réalisées par des top manager, en 2009
- 50% des fraudes internes sont réalisées des middle management, en 2009
- 30% des fraudes internes sont réalisées par des employés, en 2009

En 2011, il y a eu d'important changement :

- 20% des fraudes internes sont réalisées par des top manager, en 2011
- 10% des fraudes internes sont réalisées des middle management, en 2011
- 70% des fraudes internes sont réalisées par des employés, en 2011

Nous émettons le postulat suivant : des sondés devaient avoir entendu ou connus un cas, au cours de leur carrière concernant un manager qui aurait commis un vol de données. Plusieurs raisons pourraient expliquer qu'ils aient préféré parler des collaborateurs au bas niveau de la hiérarchie :
La première raison, certaines personnes interrogées avaient donné le nom des établissements où ils avaient travaillé. Ils voulaient peut-être éviter qu'une personne puisse faire un rapprochement entre la banque et l'histoire, parce que les sondés ignoraient comment je pouvais traiter les données.
La deuxième raison, a été mentionnée avec certains sondés, les banques préfèrent éviter de rendre publique des affaires de fraudes ou de vol de données car cela peut ternir la réputation de la banque. Mais l'impact est « moins grave » quand cela concerne un collaborateur en bas de la hiérarchie

L’intervention est toujours compliquée et se réalise bien souvent après que le vol ait été commis. Un raison mentionné par les sondés est que ces personnes ne se sont pas fait remarquer dans leur travail et ont pu échapper aux systèmes de contrôles.
Le plus souvent se sont les collègues du voleur qui vont signaler à leur hiérarchie, qu'ils ont pu observer un changement dans la personnalité ou l’exécution de tâches étranges.
Les systèmes de contrôles peuvent aussi détecter un risque potentiel, en surveillant le travail des collaborateurs et essayer de détecter un élément étrange comme les mouvements effectués, les comptes clients consultés. Mais cette surveillance a aussi ses limites, les fonctions de surveillances ne peuvent pas surveiller toutes les actions effectuées par les collaborateurs, mais elles choisiront un échantillon de personne sur lequel des contrôles seront effectués. De plus, un collaborateur peut prendre des photos avec son Smartphone et revendre ces données sans laisser une trace dans le système.
L’enquête était relativement courte, une semaine suffisait pour avoir tous les éléments et réfléchir aux mesures à prendre si nécessaire. Il s’agit aussi d’éviter que la situation ne se détériore.

Chaque cas a permis de mettre en évidence des défaillances qui pouvaient y avoir dans l’organisation et pouvoir y remédier. Le sondé numéro 2 expliquait, durant l’entretien, que les banques profitaient des affaires du passé pour améliorer leur protection. Un autre sondé avait parlé, après l’interview, que ces affaires ont aussi un impact négatif sur les collaborateurs. Lorsque les dirigeants d’une banque ont connaissance d’un vol de données ou d’une fraude, de nouvelles mesures sont mises en place pour éviter qu’un nouveau cas se produise. Une augmentation des moyens de surveillances, combinée à de nouvelles contraintes (interdiction de connecter une clé USB) réduisent la liberté des collaborateurs, mais peut aussi créer une atmosphère tendue.

4.5 Méthode de protection

Si les moyens d'interventions ont plusieurs similitudes pour les exemples énoncés, les banques ont plusieurs méthodes pour se protéger contre la menace de pertes de données.

Segmentations et limitations d'accès (mentionnées par 12 sondés) :

La segmentation et limitation d'accès est une des méthodes les plus utilisées et où les banques prêtent une attention particulière. Si ces mesures étaient déjà mises en place bien avant les différentes affaires sur les vols de données bancaires, les banques renouvellent d'effort pour éviter que des collaborateurs se retrouvent avec une trop forte concentration d'informations.

La segmentation consiste à attribuer les outils et les accès informatiques nécessaires aux collaborateurs pour leur permettre d'effectuer leur travail. Pour plusieurs sondés, la segmentation doit être définie pour pouvoir répondre à ces deux questions :

- Quelle est la fonction du collaborateur ?
- Quelles sont les informations dont il a besoin pour travailler ?

Bien sûr, les sondés ont expliqué qu'il y avait d'autres critères qui devaient être utilisés par exemple, l'expérience des collaborateurs ou bien la structure de la banque.

Après, avoir défini le poste et les informations nécessaires aux employés, la banque doit réaliser une deuxième segmentation sur les informations, qui est déterminée selon des critères de la banque.

Citations recueillies

Sondé numéro 2 : *« Un plombier a sa propre boîte à outils, il n'est pas censé s'occuper du tableau électrique même s'il sait comment le réparer. Dans la banque c'est pareil un collaborateur travaillant dans le trafic des paiements ne doit pas avoir accès aux fonctions des sécurités informatiques. »*

Sondée numéro 6 : *« Si les collaborateurs possèdent plusieurs accès concernant un ou plusieurs client la qualité du service sera moins bonne et la surveillance ingérable. »*

Mais toutes les banques n'ont pas les mêmes moyens pour faire une segmentation et la taille de la banque doit être prise en compte. Il est possible qu'un collaborateur puisse avoir des accès plus important dans le cadre de son travail.

Citations recueillies

Sondé numéro 7 : *« Les grandes banques ont un effectif et des moyens suffisants pour faire une segmentation efficace. Mais les petites moyennes banques n'ont pas ces capacités financières et en terme d'effectifs. Certains collaborateurs peuvent avoir plus de responsabilités. »*

Sondé numéro 7 : *« Dans les petites structures, il peut arriver qu'un collaborateur, dans le cadre de son travail, ait besoins de faire une extraction importante d'informations (exemple dans la base de données de la clientèle : suisse, francophone,…). Il est possible de lui ouvrir les accès temporairement à ces données. Ce genre de situation, la personne doit avoir l'autorisation de la hiérarchie et pour que le travail soit effectué correctement, le Security Officer de la banque doit être présent pour surveiller le travail du collaborateur. »*

Des contrôles sont effectués pour vérifier que des personnes ne se retrouvent pas avec des accès non-attribués.

Citation recueillie

Sondé numéro 11 : *« Lorsque j'étais auditeur, j'étais amené à effectuer un contrôle des accès des différents employés. Pour chaque employé, un pointage était effectué. Si nous constations qu'un collaborateur avait des accès trop importants pour sa fonction, nous demandions des explications. Certains accès étaient justifiés, mais il est arrivé que certains employés ne soient même pas au courant qu'ils accès à certains outils. »*

Traçabilité (mentionnée par 11 sondés) :

La traçabilité consiste à enregistrer les différents mouvements effectués sur le poste de travail du collaborateur. Dans les établissements bancaires, le poste de travail de l'employé est surveillé. La banque connaît tout sur le travail du collaborateur:

- Les pages internet visitées
- Les données client consultées
- Les programmes utilisés
- Les appareils externes utilisés, comme clés USB,
- Les documents imprimés
- Les tentatives d'accès à des informations non autorisées.
- ...

Toutes les informations sont enregistrées. La traçabilité doit permettre de détecter un comportement suspect d'un collaborateur pour pouvoir intervenir rapidement si une tentative de fraude ou un vol risque d'être commis. De plus, avec une segmentation et une limitation d'accès correctement réalisée, il est beaucoup plus facile de trouver d'où viennent les vols où la perte et comment agir rapidement.

Outils informatiques (mentionnés par 12 sondés):

Les outils informatiques sont des softwares et hardwares informatiques de sécurité qui sont utilisés contre une attaque venant de l'extérieur. Les outils informatiques peuvent être des antivirus, des pare-feu, des back-ups, des serveurs sécurisés...

Les sondés numéro 5, 7, 9 et 12 ont expliqué que la sécurité informatique dans les banques contre les menaces extérieures est très élevée. Mais la taille de la banque et le nombre de succursales qu'elle possède complexifiaient la protection de données. En effet, une petite banque aura plus de facilité à se protéger de serveurs informatiques, en raison du nombre limité de succursales qu'elle possède. Les responsables de la sécurité peuvent instaurer une protection efficace et similaire pour chacun de ses locaux. Au fur et à mesure que la taille de la banque grandit, le nombre de locaux augmente et la sécurité informatique doit être modifiée avec une augmentation de serveur pour stocker les données. Et parmi un de ces nombreux serveurs, il est possible que l'un d'eux soit moins bien protégé et plus exposé à un risque de pertes de données.

Citation recueillie

Sondé numéro 5 : *« Lorsqu'un grand établissement bancaire a plusieurs succursale à l'étranger, cela a pour conséquence d'avoir plusieurs serveurs dans le monde qui sont interconnectés. Il est possible, parmi l'une de ces succursales, une soit mal ou moins bien sécurisé et s'expose à un risque important. »*

Un outil de sécurité qui a été donné par les sondés 5 et 12 est l'utilisation d'un "Water Mark". Il s'agit d'un tatouage numérique qui est inséré sur des dossiers PDF confidentiels. Ces fichiers présentent l'avantage d'apporter une meilleure protection des fichiers sans présenter une différence qui soit perceptible par rapport un document semblable sans protection. Si un de ces fichiers venait à être exploité par un employé, par exemple envoyée par email, la banque serait immédiatement avertie que des données confidentielles risquent de sortir et la transmission en serait bloquée.

Citation recueillie

Sondé numéro 5 : *«Ces outils utilisés pour une meilleure protection ne sont plus considérés comme des outils logiciels, mais plus comme faisant partie de l'organisation et de la gouvernance. »*

Un autre outil pour protéger les données est la numérisation des comptes clients et collaborateurs (mentionnée par 10 sondés). Il s'agit de distinguer un compte d'un client par un numéro. Seul un nombre restreint de personnes connaissent l'identité derrière ce numéro, les autres peuvent continuer à travailler sans avoir besoin de connaître l'identité du client. Cette mesure présente l'avantage d'éviter qu'un collaborateur soit tenté de consulter le compte de certains clients ou qu'une personne extérieure à la banque ne puisse exploiter l'information.

Recrutement et personnel :

Les interviewés ont aussi expliqué qu'un travail supplémentaire était réalisé pour trouver le candidat idéal pour un poste recherché. La recherche d'informations sur les candidats était plus minutieuse et plus longue. Certains sondés ont parlé de la méthode de screening, qui consiste à sélectionner un candidat selon des critères bien précis et vérifier s'il est adéquat pour la fonction recherchée. La demande de certains documents comme casier judiciaire, certificats de travail des précédents emplois sont toujours demandés. Des établissements prenaient contact avec les anciens employeurs d'un candidat pour vérifier la fiabilité des informations recueillies.

Si beaucoup de moyens sont entrepris pour trouver le bon candidat, les banques ont aussi réalisé beaucoup d'efforts sur son personnel existant. En effet, depuis plusieurs années, les banques tiennent à jour les données concernant le personnel. Le but est d'éviter d'avoir un collaborateur ne répondant plus à des critères de la banque (un casier judiciaire, problème financier)

Formation du personnel et tests (mentionnés par 8 sondés):

Les collaborateurs suivent des formations continues en interne pour qu'ils soient à jour sur leur métier, la sécurité, sur le blanchiment d'argent et l'éthique des affaires. De plus, il arrive que des tests soient réalisés pour vérifier que les collaborateurs soient à jour. Un sondé a donné des exemples de test utilisés :

Citation recueillies

Sondé numéro 9 : *« Lorsque nous faisons des tests, cela se passe en 2 parties. Il y a un premier test de mise en situation, où nous observons le comportement des employés. Il y a un second test, où les collaborateurs répondent à un questionnaire. Selon les résultats obtenus, les personnes devront suivre une formation de remise à niveau pour combler leurs lacunes et des sanctions peuvent être données quand les résultats sont très décevants. »*

Sondé numéro 12 : *« La tendance actuelle peut être définie en trois points:*

- *Il y a, d'abord, la formation des collaborateurs à l'éthique des affaires.*
- *Il y a, ensuite, une formation du collaborateur pour son métier et de l'attitude à avoir à l'intérieur et à l'extérieur de la banque.*
- *Et pour finir la mise en place d'un système de sanctions contre certains comportements qui peuvent aller à des actions pénales pour des cas graves. »*

Les banques réalisent aussi des tests de leur sécurité informatique. La sondée numéro 10 explique que sa banque va mandater des hackers pour tenter de s'introduire et de prendre le contrôle du système informatique. À la fin des tests, un rapport est remis avec les résultats obtenus.

Interdiction de périphérique externe (mentionné par 7 sondés) :

Avec les différentes affaires qui ont secouées la Suisse, les banques ont pris des mesures sur l'utilisation de périphériques externes. En effet, les collaborateurs n'ont pas l'autorisation d'utiliser des clés USB, des disques ou autres formes d'outils de stockage externe sur le poste de travail.

Citation recueillie

Sondé numéro 2 : *« L'usage de clé USB n'est autorisé que sur validation du supérieur et une personne est présente lors de l'extraction. »*

Autres mesures :

La sondée numéro 10 a donné plusieurs exemples de mesures qui sont mises en place dans l'établissement où elle travaille :

« Les banques mandatent des hackers pour essayer de prendre le contrôle du système informatique, effectuer des tests d'intrusion dans le système de la banque pour détecter les faiblesses de la banque.
Le fichier central fait l'objet d'une sécurité très renforcée, car il regroupe toutes les données importantes de la banque. Le nombre de personnes ayant accès au fichier central est très restreint et toute personne voulant y accéder devra enlever tout type d'appareils ou outils pour éviter un vol ou copie des données.
Les nettoyages des locaux sont effectués quand les collaborateurs sont présents dans les locaux.

Concernant les clients, la banque va mettre en place prochainement une application IPAD qui permettra d'afficher sur tablette des informations bancaires du client. Cela évitera de devoir imprimer les documents. Un client qui ressort de son entretien avec son gestionnaire n'aura pas à sortir avec les documents papier. De plus, le gestionnaire n'aura plus besoin de détruire les documents imprimés, si le client n'a pas souhaité les prendre avec lui »

Les méthodes présentées par les sondés peuvent être classées en deux types :

- Des moyens techniques, avec utilisation de l'informatique pour surveiller et contrôler les actions sur le poste de travail.
- Des moyens organisationnels, qui exigent des collaborateurs à suivre des procédures et à respecter des règles de travail.

Les sondés ont tous constaté qu'il y a eu une augmentation de la surveillance et du nombre de contrôles, avec de nouvelles procédures qui sont instaurées.

Citations recueillies

Sondée numéro 1 : *« Crédit Suisse avait instauré des nouvelles mesures pour ses employés. La première mesure était que les collaborateurs aient aux moins deux semaines de vacances consécutives avec interdiction formelle d'avoir un contact avec son travail. La deuxième mesure c'était de bloquer les accès de la boîte e-mail des collaborateurs entre 18 heures et 8 heures du matin. Ces mesures éviteraient que les collaborateurs apportent du travail à domicile. Mais la véritable raison est qu'il devient plus facile de surveiller et de détecter une tentative de fraude. »*

Sondé numéro 2 : *« Les nombreuses procédures permettent de mettre des bâtons dans les roues aux collaborateurs. »*

Un autre sondé a dit qu'en théorie certaines mesures organisationnelles devraient être respectées, mais dans la pratique elles sont contraignantes pour la banque.

Citation recueillie

Sondé numéro 7 : *« on essaye d'adapter la théorie à la pratique sans la calquer exactement, sinon le travail et l'organisation seront moins efficaces. Les procédures règlent les opérations standards et courantes actuellement avec la complexité fiscale et autre nouvelle réglementation nous devons gérer tous les jours des exceptions qui ne sont pas couvertes par les procédures. »*

Le sondé numéro 5 avait expliqué, durant notre entretien, que la sécurité des données sensibles avait été sous-estimée par les banques. Après l'affaire HSBC, les banques ont lancé des programmes pour une meilleure sécurité des données jusqu'en 2010. Malheureusement, elles ont réduit leur budget pour la sécurité d'environ 5 % avec la crise financière et le risque de vols de donnée n'était pas aussi nombreux. Toutefois, elles ont changé d'opinion avec les nouvelles affaires qui ont éclatées comme celle de Julius Baer et la banque Sarrasin.

Mais ces protections de données varient selon les types des banques. Dans les banques privées, les dirigeants de la banque ont apporté leur fortune personnelle, et la banque va éviter de prendre des risques importants. C'est pourquoi les exigences et la surveillance sont très élevées. Ces banques vont s'assurer que les collaborateurs soient concernés par la discrétion et la confidentialité. Les comptes sont numérisés et un nombre restreint de personnes connait l'identité du client.

La sécurité informatique est moins importante dans les banques non étrangères. Les clients ont un compte numéroté ou un pseudonyme. Cela évite d'avoir le nom lorsqu'un client réalise une transaction. La protection est compensée par une organisation différente pour accéder aux données clients.

Dans les banques étrangères qui sont établies en Suisse, la protection des données est bien différente. La confidentialité des données clients n'est pas la priorité de ces banques, qui considèrent cela comme un coût important. Elles préfèrent dépenser dans d'autres domaines, comme les publicités pour les investissements.

4.6 Les contributions de l'ASB et la FINMA

Si pour les sondés, les banques ont une part de responsabilités importantes dans les pertes de données bancaires, elles ne sont pas les seules qui ont sous-estimé ce risque et pris des mesures.

Depuis 2008, le nombre d'affaires de vols de données bancaires qui sont sorties dans la presse a augmenté. La FINMA a réalisé une enquête sur l'affaire HSBC terminée en mars 2011 et a mis un blâme à la banque. Entre 2008 et 2013, la FINMA a apporté quelques modifications à sa circulaire "2008/21 Risques opérationnels - banque". Toutefois, ces changements concernent les autres risques opérationnels. Fin 2013, cette circulaire sera mise à jour en ajoutant 9 nouveaux principes et 53 chiffres marginaux qui concernent la perte et les vols de données bancaires.

Principe 1 : Gouvernance :

Ce principe concerne la gestion du risque de données confidentielles. Il s'agit de mettre en place une gouvernance pour la protection des données.

Principe 2 : Données d'identification de clients :

Ce principe détermine les données nécessaires à l'identification clients. Les données d'identification ne sont pas les mêmes selon les services.

Principe 3 : lieu de stockage et accès aux données :

Ce principe détermine où se trouve les données et contrôle le flux d'accès à ces informations, en mettant à jour les personnes qui ont accès à ces informations et l'identification de l'emplacement où sont stockées les données.

Principe 4 : normes de sécurité liées à l'infrastructure et à la technologie :

Ce principe concerne les moyens techniques utilisés pour la protection de données. Cela inclut également les moyens de contrôle pour surveiller une soustraction de données.

Principe 5 : sélection, surveillance et formation des collaborateurs qui ont accès aux CID (Client Identifying Data, données d'identification du client) :

Ce principe concerne les collaborateurs clés de la banque qui travailleront avec des informations confidentielles. La banque est tenue de sélectionner, former et surveiller ces employés clés.

Principe 6 : identification et contrôle des risques en relation avec la confidentialité des CID :

Ce principe concerne la mise en place de moyens d'identification, d'analyse de scénario et la mise en place de contrôle pour ces scénarios.

Principe 7 : limitation du risque en relation avec la confidentialité des CID :

Ce principe concerne les moyens utilisés pour limiter la perte de données client comme segmentation de l'information, des tests et la mise en place de scénarios, quand une grande quantité de données est modifiée ou migrée.

Principe 8 : incidents en rapport avec la confidentialité des CID, communication interne et externe :

Ce principe attend des banques qu'elles préparent une stratégie de communication claire en lien avec l'incident subit, en plus du rapport d'enquête.

Principe 9 : externalisation d'activités et prestations de services à grande échelle traitant des CID :

Ce principe explique que les banques, ayant des activités externalisées, doivent prendre en compte que ces prestataires de services n'ont pas tous la même politique de confidentialité et la banque doit choisir en fonction de ses règles de sécurité.

L'Association Suisse des Banques a aussi pris des mesures pour lutter contre les vols et pertes de données bancaires. En octobre 2012, elle a sorti un rapport nommé *« Data Leakage Protection »* qui présente 13 types de pertes de données, leur définition, les scénarios possibles et 15 contrôles à réaliser.

Tableaux 4

Catégorie des risques

Famille	**Nombre de scénario**
Storage Media	9
Mobile devices	4
E-Mail	3
Internet	3
Paper	11
Video-/Telefone Conferences	8
Repair/Disposal of electronic devices	5
Backup/Archival	5
Employee	12
Outsourcing	2

Source : SWISSBANKING, *Data leakage Protection,* Octobre 2012

Présentation du dossier

Le dossier est présenté tout d'abord par les différents types de pertes de données avec les contrôles et lesquels effectuer. Ensuite, il est expliqué comment lire et comprendre les contrôles. Ils possèdent plusieurs caractéristiques :

Type de contrôle à effectuer :

- Technique : Contrôle est à réaliser sur le matériel informatique et sur les logiciels.
- Organisationnel : Contrôle est à réaliser sur l'organisation et/ou les processus.

Nature du contrôle:

- Prévention : Le contrôle est effectué avant qu'un incident se produise.
- Détection : Le contrôle détecte un incident le plus tôt possible après sa réalisation.
- Correction : Le contrôle détecte un incident et réagit rapidement pour atténuer son risque.

Catégorie de contrôle:

- Base : Les moyens des banques sont suffisamment efficaces pour traiter un scénario.
- Recommandé : Des moyens de contrôle doivent être utilisés pour traiter un scénario.
- Futur: des moyens de contrôles supplémentaires sont nécessaires, mais ne sont pas encore disponibles pour le moment.

Chaque contrôle reçoit une évaluation selon les coûts pour ces contrôles et la capacité de réduction du risque.

Figure 4

Exemple de contrôle

SwissBanking

4.8 Data Leakage Source: Paper

4.8.1 Introduction / Definition

Subject: Any kind of physical paper (printer output, scanner output, facsimile documents, multi-functional device output, postal mail, all kinds of documents) which may expose sensitive information due to:

- Misdirection of print output;
- Accessibility of paper for unauthorized persons during absence of staff;
- Misrouting of scanned documents;
- Non-professional disposal of maculation;
- Misaddressed or misdirected letter/facsimile (internal and external);
- Letter/facsimile/print output gets read/copied/stolen by third during receipt;
- Post office misdelivery;
- Print/copy/scan job gets repeated by unauthorized persons;
- Reading along by unauthorized persons (e.g. in the train, remote office, etc.);
- Mistakenly unnoticed printing order;
- Lost or stolen documents.

4.8.2 Scenario: Print output becomes misdirected

Description: IP conflict, faulty print queue
Likelihood: High

Nr.	Controls				Rating		
#	Measures	technical (T) organizational (O)	preventive (P) detective (D) corrective (C)	Baseline (B) Recommended (R) Future (F)	costs (efficiency)	effectiveness (risk reduction)	Potential
5.01	training and awareness instructions for new employees, updates for long-time employees	O	P	B	☺	☺	☺
5.02	certificate based printer connection	T	P	R, F	☺	☺	☺
5.03	make sure that print starts not until user is authenticated at the output device (pull printing)	T	P	R	☺	☺	☺

Source : SWISSBANKING, *Data leakage Protection,* Octobre 2012, P27

Dans cet exemple, nous pouvons voir au point 4.8, le type de risque qui est traité, concerne la perte de document papier.
Le point 4.8.1 donne une définition et une explication de de la perte de donnée liée au papier.
Le point 4.8.2 donne une description du scénario de la perte de données, ainsi que des contrôles à effectuer pour une bonne protection.

Ce que nous pouvons constater, c'est que les moyens de contrôle utilisés sont des outils techniques. Ce sont uniquement des moyens de prévention qui sont utilisés. Le point 5.01 est la seule mesure qui doit être déjà appliquée dans les établissements bancaires et les deux autres mesures sont recommandées ou à mettre en place dans le futur (point 5.02). Nous pourrions penser que certaines banques, notamment les petites banques, n'ont pas les moyens de pouvoir installer ces mesures dans leur établissement. En termes de coûts, l'instauration de ces contrôles peut couter cher. En termes de réductions de risques, la formation du personnel est moyennement efficace. Tandis que les deux mesures techniques obtiennent une bonne appréciation de la réduction du risque pour l'ASB. Au final, ces trois contrôles obtiennent des résultats mitigés.

On peut observer que ce dossier est très intéressant, car il répertorie différents scénarios et regroupe les contrôles qui sont à effectuer. Les banques peuvent alors améliorer leur contrôle. On peut regretter que ce dossier n'inclue pas des directives à suivre contre une attaque de l'extérieur, par exemple une tentative de hacking, d'intrusion ou bien d'espionnage. Il ne contient pas non plus des moyens d'agir quand les informations sont perdues, ce qui est fort regrettable, car il aurait été intéressant d'avoir une directive commune pour chaque banque.

Ces efforts mis en place par les deux groupes ne reçoivent pas le même commentaire.
Pour le sondé numéro 5, ces efforts réalisés par l'Association Suisse des Banques et la FINMA sont importants, mais il a fallu attendre 4 ans et plusieurs cas des vols de données bancaires, pour que les deux groupes réagissent. Cependant, ces mesures prises sont beaucoup moins contraignantes que les mesures faites par les organes de surveillance de Singapour et de Hong-Kong. Il donne pour exemple un rapport à remplir de 183 questions concernant la sécurité informatique.

Pour 4 sondés, ces mesures sont bien accueillis et estiment que la FINMA est tout aussi impliquée que les deux autres autorités. Le sondé numéro 7 ajoute que les différentes mesures instaurées par les autorités de Singapour et Hong-Kong servent à montrer leur sérieux aux restes du monde, mais en pratique, elles font autant d'effort que la FINMA.

4.7 Les raisons des vols de données bancaires

Les sondés ont donné leur impressions sur les affaires qui ont été rendues publiques ces dernières années. Si toutes les personnes interrogées ont mis en évidence que les voleurs étaient très souvent des personnes qui avaient un problème dans leur vie personnelle ou au travail, le problème pouvait se situer ailleurs.

Plusieurs personnes interrogés estiment que la crise financière de 2008 a permis de voir que certains pays avaient des problèmes de liquidités avec des rentrées fiscales faibles. Ils ont commencé à collaborer pour lutter contre l'évasion fiscale. Quelques pays étaient prêts à rémunérés des banquiers pour livrer les noms de clients qui auraient caché de l'argent en Suisse. Les personnes peuvent se retrouver à céder à la tentation.

Citation recueillie

Sondé numéro 11 : *« Si vous êtes à la place de Monsieur Brikenfeld et qu'on vous propose 100 millions de dollars et 2 ans prison, pour donner des informations confidentielles, il est compréhensible que réfléchissiez à l'offre. Avec cet argent, n'importe qui peut arrêter de travailler. »*

Pour un autre sondé, il pense que toutes ces attaques contre la Suisse ont pour but de discréditer les banques suisses.

Citations recueillies

Sondé numéro 3 : *« Depuis le début de la crise financière, il y a une guerre économique entre la Suisse et les autres pays du monde, car un tiers des fortunes mondiales sont gérées en Suisse. Cela ne gêne pas ces pays que la Suisse s'occupe ces avoirs, mais ils veulent récupérer ces actifs pour que ces revenus soient réalisés sur leur territoire. C'est pourquoi ils veulent supprimer le secret bancaire suisse pour affaiblir et discréditer la place financière suisse. »*

Sondé numéro 4 : *« Il n'est pas nécessaire d'avoir beaucoup de noms de clients pour ternir la réputation de la banque. Si la personne ayant volée des données sensibles veut les revendre à des États, elle aura besoin de beaucoup de noms de client. Tandis qu'un petit nombre est suffisant pour remettre aux journalistes et porter atteinte à la réputation d'une banque. »*

Pour 2 sondés, l'échange automatique pourrait réduire la pression que subissent la Suisse et ses banques.

Citations recueillies

Sondé numéro 8 : *« Le vol de données bancaires est un cas rare dans les banques, il y a eu quelques affaires qui ont éclaté dans les journaux depuis la crise 2008. Cela s'explique par la pression des États qui ont un problème avec leur fiscalité et avec le manque de liquidité dans leur compte. On voit que les Allemands sont prêts à payer des disques ou clés USB contenant des données de clients, car ils savent qu'ils pourront récupérer des recettes avec les fraudeurs. Je pense qu'avec l'échange automatique des données, ce genre de cas va se raréfier. »*

Sondé numéro 12 : *« L'échange automatique des données sera mis en place en Suisse, car la survie de la place financière est enjeu. Si par*

exemple, un accord avec les États-Unis ne venait pas à se réaliser, les banques suisses auraient le marché américain qui leur sera fermé avec des conséquences importantes pour le secteur bancaire suisse. »

L'autre problème se trouve dans la banque, avec une mauvaise gouvernance, qui peut avoir un impact négatif pour la banque. Il peut s'agir de favoriser des collaborateurs au détriment de d'autres, les règles ne s'appliquent pas ou ne sont pas suivi par certaines personnes. Une gouvernance présentant des lacunes risque de créer un sentiment de « normalisation » des actes d'employé. Par exemple, si un employé observe que des collègues peuvent utiliser des clés USB sans que personne leurs fasse de remarque, il peut trouver normal que lui aussi utilise une clé USB car les autres le font aussi. Le sondé numéro 11 avait donné plusieurs cas qu'il a pu observer dans divers établissements :

« J'avais vu dans un établissement bancaire que certains collaborateurs n'avaient pas la même surveillance que les autres collaborateurs pour la même fonction. Nous ne pouvions pas effectuer un audit efficace. Ces non-droit ou zones d'ombre sont un véritable problème pour la banque et peuvent amener des tensions ou des frustrations au sein de la banque. Si nous mettons des processus et procédures, ils doivent s'appliquer à tous les collaborateurs et il ne devrait pas y avoir de passe-droit, que l'on soit le directeur ou le simple employé du back-office. Un autre exemple que j'ai vu était un poste de travail qui était partagé par différents collaborateurs et il y avait un post-it collé à proximité du bureau avec le code d'accès.

Un autre point le barrage hiérarchique. Souvent, les employés du bas de la pyramide connaissent mieux les fonctionnements opérationnels que les tops managers.
Ils sont conscients des lacunes, mais n'osent pas, ne veulent pas, car ne se sentent pas concernés ou ne peuvent pas communiquer (et souvent ne savent pas à qui communiquer) alors qu'ils ont des solutions. Ce constat est valable dans tous les domaines dans les grandes structures très hiérarchisées. »

Dans les remarques du sondé numéro 11, nous pouvons aussi un autre élément qui pouvait inciter des personnes à commettre un vol de données, il s'agit des défauts dans l'organisation. En effet, une personne qui commet un vol de donné a toujours une opportunité pour exploiter une faille dans la banque cela peut être une absence de contrôle dans une tâche à réaliser ou bien le collaborateur a un niveau d'accès suffisamment important pour masquer son action.

Ce que nous pouvons observer c'est qu'une personne a besoin de trois éléments pour qu'ils puissent commettre un vol :

- Une opportunité de commettre un vol ou une fraude
- Un facteur motivationnel
- Une capacité de minimiser le vol

4.8 Nouvelles méthodes de vols

Nous avons pu observer avec les différents exemples donnés par les sondés et le rapport de l'ASB que la perte de données peut venir de n'importe où. Pour plusieurs sondés, les manières de voler des informations peuvent aller très loin dans l'imagination et les banques peuvent difficilement faire face aux vols. L'une des nouvelles méthodes de vols qui a été observée chez UBS, est de prendre en photo avec son Smartphone des données confidentielles, le collaborateur se retrouve avec des données sensibles sur lui et si un autre employé ne l'a ne pas dénoncé, la banque n'a aucun moyen de lutter contre ce genre de méthode.

Une autre méthode de vols, qui pourrait être utilisée contre les banques, concerne le programme d'espionnage américain qui a été rendu publique par Edward Snowden. Nous avons appris que le service de renseignement américain pouvait espionner n'importe quelle personne utilisant un ordinateur qui exploite Google, Facebook, Yahoo, Windows et d'autres groupes. Des micros étaient cachés dans des locaux comme dans le siège de l'ONU ou de Bruxelles. Par exemple, les Américains étaient au courant des stratégies que les membres de l'Union européenne allaient utiliser pour les négociations de libre-échanges sur certains produits. Si les médias n'ont pas parlé des banques, les sondés ont fait part de leur préoccupation de cette affaire, car toutes les informations qu'ils possèdent sont potentiellement accessibles par les services secrets de renseignement américain. Ce qui demande davantage de prudence aux banquiers, car ils doivent faire attention à ce qu'ils écrivent et ce qu'ils envoient par email. Si leur agenda électronique est synchronisé avec Google, ces informations peuvent également être accessibles par le service des renseignements américains.

4.9 Les recommandations des sondés

À la question numéro 6, les sondés ont pu donner leur avis la répartition des rôles dans les banques.

Pour 8 sondés, il est très clair qu'il faut mieux redéfinir les rôles. Mais parmi ces sondés, trois d'entre eux expliquent qu'il est assez compliqué de pouvoir redéfinir les rôles, car il y a le problème de coûts, d'effectifs, et de moyens. Toujours dans ce groupe, des sondés ont expliqué que la redéfinition des métiers n'était qu'une possibilité pour une amélioration des protections de données et ont proposé d'autres idées. Pour deux sondés, le changement commençait à se mettre en place et un sondé constate qu'il y a une spécialisation des collaborateurs dans un métier précis. Pour 4 sondés, la redéfinition a déjà été faite ou bien n'est pas nécessaire, car les rôles sont déjà bien définis. Ci-dessous, les recommandations des sondés sont présentées et classées en deux groupes :

Groupe 1 :

Ce premier groupe comprend des méthodes de protection qui sont déjà présentes dans la banque et mentionnées dans le sous-chapitre : « méthodes de protection » :

- Sécurité informatique à jour contre menace de l'extérieur.
- Segmentation et limitation des accès.
- Traçabilité des mouvements.
- Travail plus approfondi dans le recrutement.
- Mise à jour des informations clients.
- Formation.
- Test.

Si ces mesures sont déjà présentes dans les banques, les sondés expliquent qu'il s'agit de continuer à les améliorer et être régulièrement à jour.

Groupe 2 :

Certains sondés ont donné d'autres points qui pourraient améliorer la protection de données :

<u>Contrôle des comportements étranges, la négligence, la paresse et l'inattention :</u>

Il s'agit de rendre attentif les collaborateurs et d'avoir un comportement irréprochable dans son travail, de respecter les règles internes et externes. Les pertes de données bancaires sont très souvent originaires d'une erreur humaine et il s'agit pour le sondé de supprimer les comportements à risques comme laisser des codes d'accès visibles

par d’autres personnes ou bien laisser des dossiers confidentiels sans surveillance. Cela passe par une formation sur le comportement à avoir et l'organisation des tests surprises pour observer la réaction des collaborateurs.

Améliorer la gouvernance :

Pour plusieurs sondés, la perte de données bancaires est la conséquence d’un problème organisationnel ou une gouvernance qui n’est pas adaptée. Une gouvernance efficace pour les sondés se résume par déterminer qu’elles sont les données sensibles à protéger, qui y a accès, comment les protéger, quelle sont les règles que tous les collaborateurs doivent respecter. Les sanctions doivent être applicables aussi bien à l’employé en bas de l’échelle qu’au manager.

Echange d’informations entre services :

Le sondé numéro 9 propose de créer une base de données communes, qui regroupe différents rapports et indicateurs de différents services pour que chaque intervenant possède les mêmes informations. Cela permettrait d’améliorer la communication entre les services et de centraliser les informations.

5. Recommandations

Il est difficile de pouvoir émettre des recommandations aux banques, car il y a beaucoup de moyens qui existent déjà pour se protéger contre les pertes de données. J'ai essayé de proposer des recommandations, en tenant compte des informations qui m'ont été données par les sondés, ainsi que les leçons que j'ai tiré d'une affaire, à laquelle j'ai été confronté.

En effet, dans un de mes emplois précédents, nous avons eu une collaboratrice qui avait détourné de l'argent, en supprimant des transactions. Ensuite, elle récupérait la recette des écritures effacées. Plusieurs raisons lui ont permis de commettre son vol. Tout d'abord, le magasin possédait une seule caisse et il n'y avait pas besoin d'avoir un collaborateur supplémentaire. Elle pouvait commettre son vol sans difficulté. Ensuite, elle avait compris comment les transactions étaient enregistrées dans le système, sans éveiller des soupçons dans la comptabilité. Pour finir, elle faisait partie d'un petit groupe d'employés, en qui la gérante avait une grande confiance. Un jour, lorsque nous avons fait l'inventaire des marchandises, nous avons constaté une différence importante entre les marchandises que nous avions comptées et ce que nous devions trouver dans la comptabilité. Après une enquête, nous avons pu remonter jusqu'à elle. Il est difficile d'expliquer ce que nous ressentons, dans ce genre de situation. Nous avions le sentiment d'avoir été trahis par la personne, car nous lui faisions confiance. Nous étions également frustrés, parce qu'elle nous a jamais donné d'explications sur son attitude. Cette affaire a eu des répercussions dans l'entreprise, mais également dans ma façon de travailler et les relations avec mes collègues.

5.1 Améliorer la gouvernance

Une des premières recommandations concerne à améliorer la gouvernance. La banque doit mettre en place des procédures et des règles de conduites qui doivent être applicables à tous les employés. Il faut que les objectifs soient clairement définis et compris par tous les employés de la banque.

La mise en place de règles de conduite et de travail qui doivent être respectée aussi bien par les dirigeants, que les collaborateurs du reste de la hiérarchie. Des sanctions doivent être appliquées pour le non-respect des règles. Le but est d'éviter d'avoir des collaborateurs qui soient favorisés et de créer de la jalousie ou bien du mécontentement. J'ai pu observer, dans ma propre expérience, que lorsqu'un collaborateur ne respectait pas un point du règlement et que la gérante ne l'avertissait

pas du non-respect des règles, des employés commençaient à négliger certaines règles.

Les collaborateurs doivent pouvoir s'exprimer librement avec les autres collègues et leurs supérieurs hiérarchiques. Le but n'est pas que les supérieurs soient des psychologues ou des confidents, mais il doit se crée une relation de confiance au sein du groupe de travail. Les managers connaitront ainsi mieux le travail de leurs collaborateurs, mais ils pourront aussi mieux intervenir dans la résolution d'un problème.

5.2 Création d'une base de données des méthodes

Durant les entretiens, plusieurs sondés ont mentionné que les événements du passé étaient utilisés pour assurer une meilleure gestion des risques, en informant les autres établissements. Toutefois, aucun des sondés, ni aucun document ne faisait mention d'une base de données, qui répertoriait les vols de données qui se sont produits, dans le passé et qui était à disposition pour les banques.

Un employé de la Banque Privée Edmond de Rothschild a expliqué que l'Association Suisse des banques a mis en place une base de données qui s'appelle E-Alarm. Elle permet d'informer ou d'alerter les banques entre elle sur des cas qui leur sont arrivés. Par exemple, fraude par e-banking, vol de sac-à-main à la sortie de la banque ou encore expliquer une procédure à suivre en cas d'attaque. Malheureusement, cette base de données ne répertorie pas les cas qui se sont produit en interne.

L'idée serait de créer une base de données similaire regroupant les différentes affaires qui ont touché le milieu bancaire, aussi bien les fraudes, les erreurs, que les vols et pertes de données.

Les affaires seraient présentées de la manière suivante :

- Date de la menace : Il s'agit d'observer les différents cas rencontrés par le passé et relever une éventuelle évolution des méthodes.
- Origine de la menace : Les menaces seraient répertoriées, selon le nature (interne/externe, vol papier, vol cd,…)

- Présentation de la menace : Les personnes feraient une description du cas, en n'omettant pas des informations clés pour bien comprendre l'histoire.
- Etablissement concerné : Quel type de banque et leur taille est touché; banque commerciale, privée, universelle. Le nom de la banque n'est pas mentionné.
- Service concerné : Le service qui a été attaqué et qui est intervenu dans la gestion du cas.
- Cause de la menace : Les raisons qui ont permis à cette attaque et les documents ciblés.
- Intervention : Les actions entreprises pour traiter le cas.
- Conséquence : Les conséquences que la banque a subies.
- Type de contrôle : À quel moment peut-on intervenir dans la gestion du risque (prévention, détection, correction)
- Analyse de spécialiste : En prenant pour exemple le recueil de cas du site http://www.bankingombudsman.ch, une analyse sera réalisée par des experts du domaine, qui donneront leur avis la réaction de la banque et les points à améliorer.

Cette base de données ne pourra être consultée que par un nombre restreint de collaborateurs.

Le but de cette base est d'avoir une communication simplifiée entre les banques. Cela évite d'envoyer un message aux autres banques à plusieurs reprises. De plus, tout comme la messagerie SWIFT, le langage sera le même pour toutes les banques.

L'avantage de cette base est qu'elle permet de garder une trace des méthodes rencontrées et utilisées pour mieux traiter un cas. Les banques pourront faire une analyse de leurs moyens de protection et vérifier si elles sont en mesure de se prémunir contre le vol.

De plus, les banques pourront avoir un accès à des méthodes de vols qu'elles n'auraient jamais imaginé pouvoir se réaliser

L'inconvénient de la mise en place de cette base de données serait son coût en argent et en travail.

6. Conclusion

Ce travail a permis de mieux comprendre les problèmes des vols de données bancaires, auxquelles les banques sont confrontées.

Nous avons remarqué, avec les histoires racontées, que la fuite ou la perte de données pouvait se produire dans n'importe quel service et la menace pouvait venir d'un employé de la banque. Un collaborateur qui a un problème ou bien qui est attiré par une rémunération contre des données de volées en était très souvent la cause.

Les banques éprouvent des difficultés à détecter les tentatives de vols de données, car leurs auteurs font preuve d'imagination, pour éviter de se faire remarquer. C'est donc très souvent un collègue de ce dernier qui va avertir sa hiérarchie.

Nous avons observé qu'il existait des méthodes pour protéger les données. Par exemple, segmenter et limiter les accès aux données évitent qu'un employé ait une concentration importante d'informations. La traçabilité des activités des collaborateurs sur le poste de travail permet de surveiller les comportements étranges, comme la consultation d'un compte non-autorisé, l'impression de documents ou l'utilisation d'une clé USB. Mais ces moyens présentent aussi leurs limites, car il est possible de voler des données sensibles sans laisser une trace dans le système, par exemple en prenant des photos avec son Smartphone. C'est pourquoi, il est aussi important que les banques responsabilisent leurs collaborateurs sur le risque de pertes de données.

6.1 Conclusion personnelle

J’ai pris beaucoup de plaisir à faire ce travail de recherche. J'ai pensé que j’aurais de la difficulté à obtenir des informations auprès des sondés, dû au fait qu'il s'agit d'un sujet sensible. Pourtant, tous les sondés se sont prêtés au jeu et j’ai pu faire la rencontre de personnes formidables.

J’ai beaucoup appris sur les moyens mis en place par les banques pour se protéger contre la fuite et le vol de données. J’ignorais par exemple, qu’il n’était plus possible d’utiliser des disques ou des clés USB et qu’il est possible de surveiller les moindres faits et gestes des collaborateurs.

J’ai aussi regretté de ne pas avoir eu plus de temps pour approfondir mes recherches sur le sujet. Par exemple, en faisant une comparaison avec d’autres secteurs d’activités ou avec des banques dans d’autres pays pour connaitre leurs méthodes de protection de données confidentielles. Malheureusement, ces idées me sont venues après avoir fini mes interviews. J'espère que j’étudierais ces pistes dans un prochain travail.

7. Bibliographie

Livre :

CORDEL, Frédéric, *Gestion des risques et contrôle interne, de la conformité à l'analyse décisionnelle*, Paris, 2013, 392 pages.

FRAGNIERE, Emmanuel, SULLIVAN, George, *Risk Management: Safeguarding Company Assets,* Boston, 2006, 133 pages.

FRANGIERE, Emmanuel, TUBEROSA, Jean, MORESINO, Francesco, TURIN, *Nathalie, Comment pratiquer l'étude de marché ? Méthodes et applications,* 2013, 150 pages.

GUERTCHAKOFF, Serge, Comprendre le secret bancaire, Genève, 2009, 150 pages.

SCHICK, Pierre, VERA, Jacques, BOURROUILH-PAREGE, Olivier, Audit interne et référentiels de risques, Paris, 2010, 341 pages.

Thèse et mémoire :

CHAPPOT, Thomas, l'*espionnage bancaire* (1930-1935). Travail de mémoire, Faculté des lettres, Section d'histoire, Université de Lausanne, 2010.

Norme :

FINMA, *Circ.-FINMA 08/21 « Risques opérationnels* – banques », Berne, 2008.

FINMA, *Révision partielle de la circulaire 2008/21 : Risques opérationnels – banques,* Berne, 2013

Rapport:

Département fédéral des finances DFF, *Place financière Suisse, Chiffre Clé,* Berne, mars 2013.

ERNST & YOUNG, Comment identifier et évaluer les risques et quels sont les axes d'amélioration, 2010, Suisse.

SWISSBANKING, *Data Leakage Protection*, Bâle, 2012, 52 pages.

SWISSBANKING*, Manuel e-Alarm*, Bâle, 2017, 28 pages.

Internet:

B3B, *FINMA : Plus de contrôles pour mieux protéger les données des clients des banques suisses,* 2013, http://www.b3b.ch/blog/2013/06/09/finma-plus-de-controles-pour-mieux-proteger-les-donnees-des-clients-des-banques-suisses/

B3B, *S'offrir des données bancaires volées dès 150 dollars sur le web*, 2013, http://www.b3b.ch/blog/2013/05/26/soffrir-des-donnees-bancaires-volees-des-150-dollars-sur-le-web/

KPMG, *Fraude: les managers causent les plus grands dommages,* 2013, http://www.kpmg.com/ch/fr/mediareleases/2013/pages/forensic-fraud-barometer-2013.aspx (consulté le 05.05.2013)

LE COURRIER, *Rudolf Elmer, l'ennemi intérieur*, 2011, http://www.lecourrier.ch/rudolf_elmer_l_ennemi_interieur

LE PARISIEN, *Evasion fiscale : HSBC confirme un vol de données bancaires entre 2006 et 2007,* 2009, http://www.leparisien.fr/economie/evasion-fiscale-hsbc-confirme-un-vol-de-donnees-bancaires-entre-2006-et-2007-09-12-2009-738624.php

LE TEMPS, GREMAUD, Rinny, *Mieux comprendre le Secret Bancaire Suisse*, 2010, http://www.letemps.ch/Page/Uuid/31c02508-1653-11df-a430-6a61ad960d6c/Le_secret_bancaire_suisse#.Ug30qZLp3uc

LOMBARD STREET, *Affaire UBS : série noire*, 2010, http://lombard-street.ch/2010/01/08/affaire-ubs-serie-noire/

LOMBARD STREET, *Espionnage bancaire : rumeurs affaires et secrets*, 2010, http://lombard-street.ch/2010/09/17/espionnage-bancaire-rumeurs-affaires-et-secrets/

PWC, *Cybercrime in the spotlight, Swiss Economic Crime Survey*, 2011, Suisse, http://www.unirisc.ch/public/pwc_global_economic_crime_survey_11_CH_e.pdf

RTS, *L'employé d'UBS a photographié son écran pour voler les données bancaires*, 2012, http://www.rts.ch/info/suisse/4481106-l-employe-d-ubs-a-photographie-son-ecran-pour-voler-les-donnees-bancaires.html

SWISSBANKING, *L'importance de la place financière suisse,* Juillet 2012, http://www.swissbanking.org/fr/20120702-2400-factsheet_finanzplatz_schweiz-rva.pdf

SWISSINFO, *Le «whistleblower» Rudolf Elmer face à la justice*, 2011, http://www.swissinfo.ch/fre/societe/Le_whistleblower_Rudolf_Elmer_face_a_la_justice.html?cid=31566728
SWISSINFO, HSBC: *Le fisc suisse a aussi utilisé des données volées*, 2010, http://www.swissinfo.ch/fre/Dossiers/Le_secret_bancaire_dans_la_tourmente/Actualites/HSBC:_Le_fisc_suisse_a_aussi_utilise_des_donnees_volees.html?cid=8148618
TRIBUNE DE GENEVE, *Vol de données bancaires: prison réclamée contre un employé du Credit Suisse*, 2011, http://archives.tdg.ch/actu/economie/vol-donnees-bancaires-prison-reclamee-contre-employe-credit-suisse-2011-12-12
TRIBUNE DE GENEVE, *Julius Baer: nouveau vol de données bancaires*, 2012, http://www.tdg.ch/economie/Julius-Baer-nouveau-vol-de-donnees-bancaires/story/15356257

8. Annexe

8.1 Annexe 1 : Retranscriptions des entretiens

Entretien 1

Profession : Data et Management Specialist

Q.1 Pourriez-vous me présenter brièvement les étapes principales de votre carrière ?

La sondée a fait une formation au Collège à Genève. Elle a ensuite suivi une formation continue à l'Université de Genève nommée « Contrôle de Gestion », afin d'étudier la comptabilité et trouver un travail dans ce domaine. Elle est débutée sa carrière professionnelle dans une société de décoration, où elle a occupé un poste de comptable pendant 1an½. Elle a travaillé pour une société trading spécialisée dans les matières premières alimentaires, où elle a également occupé le poste de comptable durant 2an½. Depuis 2011, elle travaille auprès d'une importante banque suisse, où elle occupe le poste de « Data et Management Specialist ». Elle a suivi une spécialisation bancaire, à Zurich. Cette formation est proposée aux très bons jeunes éléments de la banque et se déroule en 2 parties. La première partie consiste à apprendre à travailler avec les collaborateurs (gérer une équipe, les conflits, comment réussir,…). La deuxième consiste à approfondir les métiers dans la banque. Elle a choisi de faire une spécialisation de généraliste, car : « la banque c'est comme un arbre avec plusieurs branches. Si je me spécialisais dans un métier en particulier, je pourrais difficilement faire un autre emploi dans la banque. C'est pourquoi j'ai choisi une formation de généraliste où je touche à tous ». De plus, elle suit une formation complémentaire pour pouvoir former des apprentis.

Q.2 Pourriez-vous décrire vos fonctions principales ?

Elle occupe le poste de « Data et Management Specialist ». Sa fonction est de gérer les successions. Lorsqu'un client décède, ses successeurs doivent établir des démarches auprès de la banque. Son rôle est de vérifier si les documents requis par la banque sont disponibles et donc laisser libres les avoirs aux héritiers.

Q.3 Avez-vous été confronté à des tentatives de vols de données au cours de votre carrière ?

Durant sa carrière professionnelle et chez UBS, elle n'a pas été confrontée à une tentative de vols de données. Un collègue lui a raconté le cas d'une personne qui a voulu accéder aux comptes e-banking d'un client.

Q.4 Comment intervenez-vous lorsqu'une tentative de vol est sur le point de s'y produire ?

Dans la continuité de la question précédente, elle ne connait pas suffisamment la manière dont la banque intervient. Elle pense que, c'est le service informatique qui intervient lorsqu'une tentative de vol est sur le point de s'y produire. Elle a toutefois donné son avis sur les différentes affaires de ces dernières années. Elle explique « en observant les cas, les personnes qui ont volé des données sensibles n'étaient que des pions et qu'ils avaient préparé leur action depuis un moment. »

Q.5 Quelles sont les tendances dans le milieu bancaire pour se prémunir contre les vols et fuites de données?

La sondée n'a pas pu établir une comparaison avec ce qui se faisait avant dans la banque. Ce qu'elle a pu affirmer c'est que le niveau de sécurité informatique est élevé. L'accès aux données d'un client est limité à un certain nombre d'employés de la banque. Par exemple, son collègue, qui occupe le même poste, ne pourra pas avoir accès son portefeuille client. De plus, les employés obtiennent des « attributions d'accès » pour chaque client. « Par exemple, un trader n'aura pas accès aux données du coffre ou fortune du client, mais uniquement son portefeuille. Si tous les collaborateurs avaient accès aux données de tous les clients de la banque, la surveillance serait ingérable. »

Elle a aussi donné des exemples qu'elle a lu dans un article :

« Crédit Suisse avait instauré des nouvelles mesures pour ses employés. La première mesure était que les collaborateurs aient aux moins deux semaines de vacances consécutives avec interdiction formelle d'avoir un contact avec son travail. La deuxième mesure c'était de bloquer les accès de la boîte e-mail des collaborateurs entre 18 heures et 8 heures du matin. Ces mesures éviteraient que les collaborateurs apportent du travail à domicile. Mais la véritable raison est qu'il devient plus facile de surveiller et de détecter une tentative de fraude. »

Q.6 Pensez-vous qu'il faudrait redéfinir les rôles des différents intervenants pour une meilleure sécurité des données ?

Pour la sondée, il est très difficile de redéfinir les rôles des intervenants. Par exemple : « Si les collaborateurs possèdent plusieurs accès concernant un ou plusieurs clients la qualité du service sera moins bonne et la surveillance ingérable ». Pour la sondée, l'amélioration de la sécurité de données se fait au niveau du recrutement. Aujourd'hui, la banque exige un casier judiciaire vierge, une attestation de non-poursuite et les attestations de travail des anciens employeurs. Concernant ce dernier document, la banque prend contact avec l'ancien employeur pour mieux connaitre le profil.

Entretien 2

Profession : Responsable d'opération bancaire

Q.1 Pourriez-vous me présenter brièvement les étapes principales de votre carrière ?

Le sondé a étudié au Collège de Genève. Il a ensuite débuté sa carrière dans la banque Union des Banques Suisse, où il a suivi la formation de base de la banque ainsi que divers cours (internes, externes et diverses formations continues) en rapport avec les opérations bancaires. Il a ensuite rejoint une importante banque privée suisse. Dans la banque, il s'occupe de diverses opérations bancaires. Un travail qu'il l'intéresse, car : « Depuis 30 ans, les opérations bancaires, comme le trafic des paiements, sont devenues techniques ». Il a aussi suivi une formation pour devenir formateur pour apprentis, étudiants maturités professionnelles et pour adultes.

Q.2 Pourriez-vous décrire vos fonctions principales ?

Le sondé gère une équipe de 7 personnes, avec laquelle il est responsable de diverses opérations bancaires. Il s'occupe de toutes les étapes d'un ordre; de la demande d'exécution du client, jusqu'à la confirmation auprès de la contrepartie. Cela inclut, la réclamation d'un client pour un cas particulier par exemple un ordre qui n'est pas parti. De plus, il est formateur des apprentis dans la banque.

Q.3 Avez-vous été confronté à des tentatives de vols de données au cours de votre carrière ?

Avant de raconter, le sondé explique que la banque forme ces employés lorsqu'il y a une tentative de vol, de fraude ou de blanchiment d'argent. Au cours de sa carrière, il lui est arrivé d'être confronté à des « petites » tentatives.

Pour le premier cas: « il arrive que des personnes externes à la banque posent des questions embarrassantes pour pouvoir soutirer des informations sensibles. Par exemple, un client ou une personne veut faire un virement auprès d'un client de la banque et demande les coordonnées bancaires. Dans ce genre de situation, les collaborateurs sont formés pour ne pas révéler une information sensible, avec des cours de communications. »

Le second cas c'est les vols des coordonnées des cartes des clients. Des hackers tentent de s'introduire dans les serveurs de la banque en déjouant les systèmes de sécurités de la banque (pare-feu).

Q.4 Comment intervenez-vous lorsqu'une tentative de vol est sur le point de s'y produire ?

Le sondé nous explique : « La banque prend très au sérieux la menace des données bancaires, c'est l'image de la banque qui peut être touchée. », et qu'aujourd'hui les banques profitent des expériences passées. Quand un collaborateur a un doute ou bien soupçonne une tentative de vols, il doit avertir sa hiérarchie et alerter le gestionnaire du risque. Ce dernier s'occupe des affaires complexes et de la gestion du risque de la banque. Il va établir une enquête et analyser le cas avant d'intervenir (l'enquête peut durer quelques minutes pour les cas très simples comme durer plusieurs jours pour les cas complexes). De plus, la banque va aussi avertir les autres banques via la messagerie interbancaire, qu'il y a une nouvelle tentative de vol ou de fraude.

Q.5 Quelles sont les tendances dans le milieu bancaire pour se prémunir contre les vols et fuites de données?

La banque exige que tous ses collaborateurs soient régulièrement à jour sur les nouvelles règles, en particulier concernant le blanchiment d'argent et contre le financement du terrorisme.

Le sondé explique que chaque collaborateur à un accès limité au strict minimum nécessaire. Un collaborateur ne peut pas avoir accès à la base de données de tous les clients de la banque, ni pouvoir effectuer des opérations sur un compte, si cela n'est pas sa fonction.

Un autre point mentionné durant l'entretien, c'est la traçabilité du travail des collaborateurs et leur consultation.

Lorsque notre sondé exécute des opérations qui peuvent être sensibles, elles doivent être justifiées et validées par une autre personne.

Les contrôleurs internes de la banque voient les mouvements qu'effectuent les collaborateurs dans la banque. Si un employé va consulter 10x le compte d'un client ou bien extraire des données, l'employé devra justifier ses consultations et extractions.

Pour améliorer la protection des données et la sphère privée, la banque a numérisé les comptes des clients et des collaborateurs. Les comptes sont devenus anonymes. Seulement un nombre limité de personnes peuvent avoir accès aux comptes.

Q.6 Pensez-vous qu'il faudrait redéfinir les rôles des différents intervenants pour une meilleure sécurité des données ?

Pour le sondé il est très important de bien définir le rôle de chaque intervenant. C'est pourquoi il pense que le logiciel de la banque doit être limité pour que l'employé puisse accomplir ses fonctions. Cela évite qu'un employé dépasse ses fonctions et expose la banque à des risques importants. Le sondé fait une comparaison avec des ouvriers : « un plombier a sa propre boîte à outils, il n'est pas censé s'occuper du tableau électrique même s'il sait comment le réparer. Dans la banque c'est pareil un collaborateur travaillant dans le trafic des paiements ne doit pas avoir accès aux fonctions des sécurités informatiques ». Le sondé ajoute que les nombreuses procédures permettent « de mettre des bâtons dans les roues aux collaborateurs» car pour tout type d'action, même anodine, il faut faire des demandes d'autorisations et justifier. Cela permet d'avoir une meilleure traçabilité des clients et des collaborateurs.

Entretien 3

Profession : Compliance Officer

Q.1 Pourriez-vous me présenter brièvement les étapes principales de votre carrière ?

Le sondé a suivi une formation de Broker, dans la banque Union des Banques Suisse ; « La banque offre d'excellentes formations qui sont à la pointe sur les métiers de la banque. ». Il rejoindra la Police judiciaire, dans la Brigade Financière, où il intervenait dans des enquêtes dans le domaine financier. Il a ensuite travaillé pour la banque JP Morgan, au poste de Global Securtiy & Investigation, qui s'occupe de la sécurité et risque de la banque. Aujourd'hui, il travaille pour la banque Lombard Odier, où il occupe la fonction comme Senior Compliance Officer.

Q.2 Pourriez-vous décrire vos fonctions principales ?

Le sondé travaille dans la compliance. Une de ses principales fonctions consiste à vérifier que l'établissement est en conformité et respecte les différentes prescriptions légales. C'est pourquoi il doit identifier et évaluer le risque de compliance pour une meilleure gestion du risque qui peut en découler. « Aujourd'hui le plus gros risque de la banque, c'est le légale, pour ne pas commettre une action qui ne soit pas autorisé avec une autre juridiction. Se tenir informer des lois US est important pour éviter d'avoir des problèmes avec eux, car on peut être impacté sans même avoir eu un lien avec les autorités américaines. »

Q.3 Avez-vous été confronté à des tentatives de vols de données au cours de votre carrière ?

Au cours de sa carrière professionnelle, le sondé n'a pas été confronté à une tentative de vols de données bancaires. Pour le sondé, il n'existe pas de distinction entre une fraude et un vol : « Une fraude ou un vol c'est pareil, la banque sera impactée. »

Q.4 Comment intervenez-vous lorsqu'une tentative de vol est sur le point de s'y produire ?

Le sondé explique que ce n'est pas le compliance qui va intervenir, mais le Unit Risk Manager. Lorsqu'il y a un risque potentiel de s'y produire, le service doit en aviser le Unit Risk Manager. Ce dernier va établir une enquête et vérifier que les actions de l'employé sont conformes avec les Lois Bancaires. Il est important de rappeler la violation du secret bancaire en Suisse est puni par la loi. C'est pourquoi la banque a beaucoup de contraintes légales, qui l'oblige à avoir un comportement irréprochable.

Q.5 Quelles sont les tendances dans le milieu bancaire pour se prémunir contre les vols et fuites de données?

Le sondé explique, il y a un plus grand contrôle lors de l'engagement. La banque va vouloir davantage connaître les collaborateurs et les candidats, pour vérifier s'ils ne sont pas potentiellement des personnes à risque, en ayant une activité extravagante (jouer beaucoup aux jeux de hasard), des problèmes financiers… car ils peuvent nuire à l'image de la banque. Pour le sondé, le risque de vols de données sensibles n'est pas assez appréhendé dans le milieu bancaire. « C'est un risque qui est très rare de voir se réaliser et sous-estimer par la banque. Toutefois ces dernières années, il s'est matérialisé à plusieurs reprises comme l'affaire HSBC ou bien l'affaire Hildebrand. » Si un collaborateur a un comportement différent ou bien suspect, le Unit Risk Manager va avoir un entretien avec l'employé pour connaître ses problèmes ou son attitude suspects. Pour le sondé, si un employé venait à avoir un comportement suspect et qu'il y a un fort potentiel de risque qu'il commette une action néfaste pour la banque, il ne faudrait pas le garder.

Q.6 Pensez-vous qu'il faudrait redéfinir les rôles des différents intervenants pour une meilleure sécurité des données ?

En ce moment, la banque commence à remodeler les rôles des collaborateurs. Les collaborateurs deviennent des spécialistes dans leur fonction dans leurs tâches et ne font que cela. Ils ne peuvent pas avoir accès à des données qui ne sont pas attribuées pour leur fonction. Les comptes clients des clients sont numérisés et des collaborateurs (ex. :back-office) travailleront avec des données de client dont ils ne pourront pas connaître. Mais cela dépend du poste occupé et sa fonction. Il ajoute aussi : « Depuis le début de la crise financière, il y a une guerre économique entre la Suisse et les autres pays du

monde, car un tiers des fortunes mondiales sont gérées en Suisse. Cela ne gêne pas ces pays que la Suisse gère ses avoirs, mais ils veulent pouvoir gérer ces actifs pour que ces revenus soient réalisés sur leur territoire. C'est pourquoi ils veulent supprimer le secret bancaire suisse pour affaiblir et discréditer la place financière suisse. Dans le compliance, il y a un problème avec les normes suisse et internationale. Il est préférable que les fonctions de compliance soient occupées par des Suisses, car ils sont plus aptes à comprendre les enjeux de la place financière suisse. Mais ce raisonnement peut s'appliquer à d'autre fonction, on l'a vue avec l'affaire Falciani. »

Entretien 4

Profession : Indépendant

Q.1 Pourriez-vous me présenter brièvement les étapes principales de votre carrière ?

Le sondé avait suivi une formation de niveau universitaire dans le domaine de l'informatique et dans la psychologie. Il a réalisé l'ensemble de sa carrière à la banque. Il a eu le privilège d'avoir travaillé avec de grandes banques universelles et banques privées de la place financière suisse, où il a occupé différentes fonctions par exemple dans le trading ou une fonction dirigeante importante d'une banque.

Q.2 Pourriez-vous décrire vos fonctions principales ?

Actuellement, il travaille comme indépendant. Il est responsable de monter une société financière dans la gestion de fortune. Cette fonction consiste à :

- Établir un business model
- Trouver des partenaires pour le projet
- Vérifier différentes réglementations
- Établir les procédures
- Traiter les différentes contraintes Juridiques.

Q.3 Avez-vous été confronté à des tentatives de vols de données au cours de votre carrière ?

Le sondé n'a jamais été confronté à une tentative de vols de données au cours de sa carrière.

Q.4 Comment intervenez-vous lorsqu'une tentative de vol est sur le point de s'y produire ?

Le sondé explique qu'il est difficile de déceler un employé qui risque de voler des données. Pour éviter un vol de données, il y a d'abord un travail préventif qui est réalisé dans la banque. Cela passe par des mesures organisationnelles très complexes en déterminant « qui a accès à quoi et avec quel règlement ». Par exemple, un informaticien doit ne pas avoir accès aux données des clients, mais doit pouvoir travailler sur les supports sans aucune coordonnée du client visible. Il y a ensuite le support informatique qui accroit la protection des données dans différents serveurs et le besoin d'un mot de passe pour accéder.

Q.5 Quelles sont les tendances dans le milieu bancaire pour se prémunir contre les vols et fuites de données?

Le sondé nous explique qu'au niveau des supports techniques internes à la banque, il n'y a pas eu de changement significatif depuis les évènements ayant touché HSBC, mais il y a une augmentation de vigilance dans les banques, de la Finma et des auditeurs externes. La Finma ne veut pas avoir de nouvelle affaire HSBC et Julius Baer. Elle demande cabinet d'audit de faire un « état des lieux » dans les banques, pour connaître leurs faiblesses et pouvoir les corriger. « Depuis, certaines banques ont dû combler leur lacune. Cependant, le risque reste un des plus grands dangers des banques pour les vols de données bancaires. Il n'est pas nécessaire d'avoir beaucoup de noms de clients pour ternir la réputation de la banque. Si la personne ayant volée des données sensibles veut les revendre à des États, elle aura besoin de beaucoup de noms de client. Tandis qu'un petit nombre est suffisant pour remettre aux journalistes et porter atteinte à la réputation d'une banque. »

Q.6 Pensez-vous qu'il faudrait redéfinir les rôles des différents intervenants pour une meilleure sécurité des données ?

Pour le sondé, il est important de bien définir le rôle de chacun. Il faut pour cela donner un accès au strict minimum, aux collaborateurs. Ils doivent pouvoir réaliser leur travaille avec les moyens qu'ils leurs sont fournis. Ils n'ont pas besoin d'avoir accès à des outils ou programmes qui ne sont pas attribués à leur fonction. Dans l'affaire HSBC, Monsieur Falciani avait accès aux données des clients, alors qu'il était un informaticien. On constate que la répartition des rôles chez HSBC n'avait pas été faite. Le sondée explique aussi qu'il ne faudrait pas limiter la taille du portefeuille client d'un collaborateur : « Cela ne sera pas raisonnable de réduire la taille ou de restreindre le portefeuille d'un gestionnaire. Il serait difficile de pouvoir constituer un portefeuille : On se base sur le nombre de clients ? La fortune du client ? De plus, cela ne serait pas souhaitable par les banques, car il faut accorder une certaine liberté au gestionnaire dans son travail. »

Entretien 5

Profession : Senior Manager Risk Assurance Financial Servies

Q.1 Pourriez-vous me présenter brièvement les étapes principales de votre carrière ?

Le sondé a obtenu une licence en Informatique de Gestion à la HEC de Lausanne, ainsi qu'un master en Business Informatique système. Il a également obtenu 2 certifications dans l'audit informatique. Il a débuté sa carrière auprès d'Ernst & Young en tant qu'auditeur bancaire en informatique. Il a ensuite travaillé 7 ans à Zurich toujours dans l'audit bancaire informatique, où il a eu plusieurs clients comme des banques privées et UBS. Depuis deux ans, il est Senior Manager en Risk Assurance Financial Services.

Q.2 Pourriez-vous décrire vos fonctions principales ?

Le sondé occupe le poste de Senior Manager Risk Assurance Financial Services. Il est responsable d'une équipe de 12 personnes, dans la région romande et du Tessin, de l'audit informatique. Il doit effectuer :

- Le contrôle et la gestion des systèmes informatiques dans les banques.
- Réalisation de mandats spéciaux (ex. : audit SAP, migration, sécurité…)
- Responsable du budget et de l'organisation de l'équipe
- Gestion de carrières des collaborateurs
- Participation à des présentations à l'Université de Lausanne ou conférence Compliance Officier à Lugano, par exemple.

Q.3 Avez-vous été confronté à des tentatives de vols de données au cours de votre carrière ?

Il n'a jamais été confronté une tentative de vols de données, mais il a pu observer des exemples d'erreurs qui peuvent se réaliser dans des établissements bancaires.

Le premier cas présenté : deux collaborateurs travaillant pour la même banque, mais dans des bureaux différents (Genève et New-York), qui doivent collaborer pour un travail ou projet. Les deux parties doivent échanger des données sensibles et font des échanges via e-mail. Le problème c'est que la donnée qui était sécurisée dans les serveurs de la succursale à Genève se retrouve aussi dans les serveurs de New-York. La banque se retrouve avec des données qui ne sont plus sécurisées dans leurs locaux et ignore que risquent ces informations. Le sondé explique : « Lorsqu'un grand établissement bancaire a

plusieurs succursales à l'étranger, cela a pour conséquence d'avoir plusieurs serveurs dans le monde qui sont interconnectés. Il est possible, parmi l'une de ces succursales, une est mal ou moins bien sécurisée et s'expose à un risque important. »

« Des données perdues par négligence peuvent être monnayées par une personne externe. »

Q.4 Comment intervenez-vous lorsqu'une tentative de vol est sur le point de s'y produire ?

D'un point de vue de l'audit externe et en faisant lien avec l'exemple. La banque est dans l'obligation d'en aviser et expliquer le cas à la Finma et aussi son auditeur. La Finma va ensuite mandater l'audit pour effectuer un audit et va exiger un rapport sur :

- Savoir ce qui s'est passé, comment. Il s'agit de savoir si c'est un cas déjà connu ou un nouveau qui ne s'est pas encore produit dans un établissement.
- Savoir pourquoi cela s'est produit. La Finma veut savoir si il 'y a un moyen d'éviter ce genre de situation à l'avenir.
- Est-ce qu'il y a un moyen de corriger l'erreur produise. Dans l'exemple, la Finma voudra savoir s'il est possible de supprimer totalement ces données dans les serveurs envoyés.
- Selon le rapport établi par la boite d'audit. La Finma peut :
- Demander un plan de remédiation à la banque
- Une amende
- Obliger la banque à avertir ces clients que leur donnée ne se trouve plus en sécurité dans les serveurs de la banque et qu'il se trouve à l'étranger.

Le cabinet d'audit va réaliser l'état de la situation et va transmettre le rapport à la Finma.

Q.5 Quelles sont les tendances dans le milieu bancaire pour se prémunir contre les vols et fuites de données?

Après l'affaire HSBC, les banques ont lancé des programmes pour une meilleure sécurité des données. Malheureusement, elles ont réduit leur budget pour la sécurité avec la crise financière et que le risque de vols de donnée n'était pas aussi nombreux. Toutefois, elles ont changé d'opinion avec les nouvelles affaires qui ont éclaté comme Julius Baer et la banque Sarrasin. Durant ces 4 dernières années, il n'y a pas beaucoup d'efforts qui ont été faits

par la Finma et par l'ASB pour lutter contre les vols de données bancaires. C'est seulement en octobre 2012, que l'Association Suisse des banquiers a sorti un dossier pour les banques, présentant une quinzaine de scénarios pour éviter des pertes de données sensibles. En 2013, La Finma va mettre à jour sa circulaire sur les risques opérationnels, en incluant neuf nouveaux principes concernant la protection de données. Ce qu'on peut constater, c'est que les deux groupes veulent mieux protéger les banques, mais ils sont moins contraignants que les organes de surveillance de Hong-Kong et Singapour, où les banques doivent répondre à environ 180 questions concernant la sécurité informatique.

Q.6 Pensez-vous qu'il faudrait redéfinir les rôles des différents intervenants pour une meilleure sécurité des données ?

Pour le sondé ce qui doit changer ce sont les mentalités dans les banques. Il explique : « Les banques investissent beaucoup dans la sécurité pour se protéger contre une attaque venue de l'extérieur avec par exemple des firewalls et autres outils de sécurité, mais moins d'effort son réaliser pour les attaques venant en interne. »

Ce qui est important c'est de mettre en place une autre gouvernance. La banque doit se poser la question : « Où se trouve ses données sensibles et qui s'occupe de ces données ? », car ces données sensibles se trouvent dans plusieurs serveurs (serveur comptable, serveur ebanking,…). « Lorsqu'on sait où se trouvent nos données, il est plus facile de se protéger. En cas d'extraction de données, il y possible de protéger le fichier des clients en cachant les coordonnées du client, ou bien d'avoir « Water Mark »(sorte de tampon invisible) qui signale que des données confidentielles sont transmises et la transmission sont bloqués. Ces outils utilisés pour une meilleure protection, ne sont plus considéré comme des outils logiciels, mais plus comme faisant partie de l'organisation et de gouvernance. »

Entretien 6

Profession : Responsable de la surveillance des gestionnaires de fortunes

Q.1 Pourriez-vous me présenter brièvement les étapes principales de votre carrière ?

Le sondé a débuté sa carrière par un apprentissage dans une importante banque. Le sondé explique: « Elles offrent d'excellentes formations pour les jeunes et la possibilité de voir différents métiers ». Après sa formation, il a travaillé dans différentes banques suisses, en tant qu'auditeur interne. Aujourd'hui, il travaille pour la FINMA, où il est responsable de la surveillance des établissements de gestions fortunes.

Q.2 Pourriez-vous décrire vos fonctions principales ?

Le sondé est actuellement responsable de la surveillance des gestionnaires de fortunes en Suisse. Il se déplace régulièrement dans différentes sociétés de gestions de fortunes, où il effectue divers contrôles. À la fin de son mandat, il effectue un rapport et émet des recommandations.

Q.3 Avez-vous été confronté à des tentatives de vols de données au cours de votre carrière ?

Le sondé n'a jamais été confronté à des vols de données bancaires au cours de sa carrière. Le sondé précise : « Les banques préfèrent éviter qu'on ébruite un vol commis, la réputation de la banque en sera affectée. Cependant, les banques sont tenues de signaler à la FINMA, lorsqu'une fuite de données venait à se produire ». Le sondé recommande de lire l'enquête de la FINMA de mars 2011, sur le cas de la Banque HSBC.

Q.4 Comment intervenez-vous lorsqu'une tentative de vol est sur le point de s'y produire ?

Lorsqu'une fuite de données se produit, la FINMA doit être tenue informée par la banque. Le sondé explique les différentes étapes: « Dès que nous sommes averties, nous mandatons la société d'audit, qui enquêtera pour savoir ce qui s'est passé, comment cela s'est produit, quels étaient les défaillances de la banque et trouver une solution. Une fois le rapport remis, selon la gravité du cas, la banque de réaliser corrigé ces défaillances ou nous donnons une amende ». Le sondé ajoute que dans des cas exceptionnels, la FINMA peut enquêter directement.

Q.5 Quelles sont les tendances dans le milieu bancaire pour se prémunir contre les vols et fuites de données?

Aujourd'hui, les banques réalisent un travail important dans la formation de leurs collaborateurs. De plus elles améliorent leurs procédures et l'organisation de la banque. Le sondé explique que les banques ne sont pas les seuls acteurs financiers à travailler sur le sujet: « Il y a l'Association Suisse des Banquiers qui a émis un dossier aux banques avec des directives à respecter pour différents cas de pertes de données bancaires. La FINMA va remettre une nouvelle circulaire sur les risques opérationnels avec davantage d'informations concernant les vols de données bancaires. »

Q.6 Pensez-vous qu'il faudrait redéfinir les rôles des différents intervenants pour une meilleure sécurité des données ?

Pour le sondé, il faut très clairement définir le poste et les différentes tâches qui sont attribuées: « Si les collaborateurs possèdent plusieurs accès concernant un ou plusieurs clients la qualité du service sera moins bonne et la surveillance ingérable. »

« Il peut exister 30 à 40 fonctions dans une banque, si cette dernière définit le rôle de chaque fonction avec les tâches, la banque pourra réaliser une meilleure surveillance et détecter d'où provient l'erreur ». Pour le sondé, d'autres éléments peuvent permettre une meilleure protection: « l'usage d'outils externe par exemple les clés USB, doit être interdit. Il faut aussi réaliser régulièrement des tests et contrôles, si par exemple un employé a des accès qu'il n'est pas censé avoir ou bien une utilisation des outils de manières étranges par exemple consulter régulièrement le compte d'un même client ».

Entretien 7

Profession : Chiefs Operation Officer

Q.1 Pourriez-vous me présenter brièvement les étapes principales de votre carrière ?

Le sondé commence par nous parler des diverses formations qu'il a suivies. Il a d'abord obtenu une maturité avant de suivre une formation en sécurité informatique auprès d'une importante banque suisse. Il a également suivi des modules de formation en sécurité informatique « De Blasi ». Actuellement, il effectue un MBA.

Le sondé a ensuite fait une liste de différents postes qu'il a occupés. Il a débuté sa carrière professionnelle auprès d'une importante banque suisse, où il a travaillé durant 10 ans. Il a, par la suite, été auditeur informatique pour RNB, qu'il quittera après le rachat par HSBC. Il a également occupé les fonctions de CIO et COO dans deux banques privées.

Q.2 Pourriez-vous décrire vos fonctions principales ?

L e sondé nous rappelle son poste actuel, il est COO (Chiefs Operation Officer) dans une banque privée de la place financière suisse. Il est responsable de la gestion informatique de la banque. C'est-à-dire qu'il s'occupe de l'infrastructure informatique, de la sécurité informatique, de la logistique et de passer les écritures opérationnelles bancaires.

Q.3 Avez-vous été confronté à des tentatives de vols de données au cours de votre carrière ?

Le sondé n'a jamais été confronté à une tentative de vols de données bancaires au cours de sa carrière. Il explique : « il est très rare de voir des fuites de données dans les banques. De plus, il est difficile de repérer une personne qui va commettre un vol de données. J'ai eu la chance de travailler avec des gens très professionnels et d'une grande confiance ».

Cependant, il a donné un exemple de vols de données : « Lorsqu'un collaborateur veut essayer d'extraire des données sensibles, il peut imprimer des documents bancaires en deux exemplaires. Il peut justifier cette double impression dans le cadre de son travail et l'autre qu'il a remis à un autre service. Tandis, que voler des informations avec un CD ou dans une clé USB est plus compliqué, car les ordinateurs sont surveillés ».

Q.4 Comment intervenez-vous lorsqu'une tentative de vol est sur le point de s'y produire ?

Le sondé raconte : « Il est difficile d'intervenir dans ce genre de cas. Ces personnes vont commettre leur action dans leur coin. Ce que nous pouvons faire c'est de déceler un changement d'humeur d'une personne, car cela peut être un premier signal pour nous. Souvent ce sont des personnes frustrées ou qui ont un problème avec la hiérarchie qui commettent ce genre de méfait. Nous essayons d'avoir un entretien avec la personne pour comprendre les raisons de leur mécontentement et trouver des solutions".

Q.5 Quelles sont les tendances dans le milieu bancaire pour se prémunir contre les vols et fuites de données?

Pour se prémunir contre les vols des données, les banques segmentent leurs programmes informatiques. Le sondé apporte quelques précisions: « Un collaborateur aura un accès aux outils nécessaires à son travail, il aura accès uniquement aux informations concernant son métier. Par exemple, il pourra consulter les portefeuilles titre de la clientèle suisse, mais n'aura pas la possibilité de voir la clientèle américaine. » Le sondé explique qu'il peut y avoir des cas exceptionnels où un collaborateur peut avoir un accès plus important, comme par exemple : « Dans les petites structures, il peut arriver qu'un collaborateur, dans le cadre de son travail, ait besoin de faire une extraction importante d'informations (exemple dans la base de données de la clientèle : suisse, francophone,…). Il est possible de lui ouvrir les accès temporairement à ces données. Ce genre de situation, la personne doit avoir l'autorisation de la hiérarchie et pour que le travail soit effectué correctement, le Security Officer de la banque doit être présent pour surveiller le travail du collaborateur. »

Q.6 Pensez-vous qu'il faudrait redéfinir les rôles des différents intervenants pour une meilleure sécurité des données ?

Le sondé explique qu'en théorie il faudrait mieux redéfinir les rôles des collaborateurs. Mais dans la pratique, il est plus difficile de mettre cela en place. Il nous explique que les petites et moyennes banques peuvent difficilement changer les rôles dans leur établissement, car elles ont un effectif moins important que les grandes banques. Pour le sondé, il faut que les banques aient bien défini les rôles de chaque personne. Il explique : « En déterminant le rôle de chaque fonction, nous savons qui a accès à quoi. Il devient plus facile de

mettre en place une organisation efficace. L'affaire HSBC a montré les carences de la banque, car il s'est retrouvé avec beaucoup trop d'accès pour le travail qui lui était demandé ».

Pour le sondé, il est très important de mettre en place des procédures efficaces et qui doivent être respectées par tous les collaborateurs. Cependant, ce dernier point n'est applicable qu'en théorie. En pratique, il est très difficile de travailler en respectant à la lettre les procédures, car elles seraient trop contraignantes pour la banque. Il précise : « on essaye d'adapter la théorie à la pratique sans la calquer exactement, sinon le travail et l'organisation seront moins efficaces. Les procédures règlent les opérations standards et courantes actuellement avec la complexité fiscale et autre nouvelle réglementation nous devons gérer tous les jours des exceptions qui ne sont pas couvertes par les procédures. »

Entretien 8

Profession : Risk Manager

Q.1 Pourriez-vous me présenter brièvement les étapes principales de votre carrière ?

Le sondé a suivi et a obtenu un diplôme d'ingénieur électronique. Il a suivi un Master of science en électronique, puis un master à Paris en télécommunication dans le domaine de la fréquence et le transfert d'informations. Dans le cadre de son cursus de formation, il a travaillé dans une importante société d'électronique. Il a débuté sa carrière professionnelle dans une importante banque française, où il a travaillé dans les salles de marché. Après la sixième année, il rejoint une autre banque française, où il occupera le poste de risk manager. Il mettra en place la partie risk management des produits structurés pour la Suisse. Il rejoindra au début des années 2000 une banque cantonale suisse, où il deviendra responsable de la gestion des risques de marché, ainsi que les opérations de back-office. Dans le courant de l'année 2008, il rejoint une importante banque privée suisse, à Genève, où il occupe le poste de Risk Manager.

Q.2 Pourriez-vous décrire vos fonctions principales ?

Le sondé occupe le poste de Risk Manager. Il est responsable de la gestion des risques opérationnels de la banque. Ses fonctions principales sont d'établir la surveillance, de définir des outils de travail pour avoir une vue d'ensemble et d'avoir un langage commun pour chaque collaborateur. Il organise des workshops pour les collaborateurs de la banque.

Q.3 Avez-vous été confronté à des tentatives de vols de données au cours de votre carrière ?

Il n'a jamais été confronté à une tentative de vols de données bancaires. Pour le sondé, le vol ou la fuite de données est très rare et il est difficile de voir qu' une personne s'apprête a effectué un vol. Il ajoute : « on s'attend pas qu'un collaborateur puisse le faire ».

Le sondé a raconté un cas qui s'était produit dans sa banque « Il m'est arrivé d'avoir des tentatives d'extorsion ou des usurpations pour voler des données, mais c'était des petites tentatives sans succès. ». Il arrive qu'une personne mal intentionnée envoie, par fax, une demande à la banque de créditer un compte

(le compte de l'escroc), avec un faux document bancaire dont il était très difficile de voir que c'est un faux.

Q.4 Comment intervenez-vous lorsqu'une tentative de vol est sur le point de s'y produire ?

Le sondé revient sur son exemple et explique que dans ce genre de situation, la personne qui avait traité le cas, a eu la bonne réaction. Elle a trouvé étrange que la banque ait reçu un ordre de paiement via fax, alors que la banque travaille avec la messagerie Swift. Il a pris contact avec la banque qui aurait transmis le fax, pour vérifier que c'était bien elle qui avait envoyé par fax et pour connaitre le motif.

Concernant le vol interne, il est très difficile de déceler des personnes qui commettent ce genre d'action, car elles ont une très bonne connaissance des diverses procédures internes. Cela leur permet de faire preuve d'imagination quand elles passent à l'acte. Pour le sondé, la seule façon d'intervenir dans un vol de données est de surveiller un changement de comportement d'un collaborateur. *« On ne* s'attend pas à ce qu'un collaborateur puisse commettre un vol. Mais il existe des pistes, par exemple, les personnes qui commettent des fraudes ou vols internes sont très souvent frustrées ou bien qui ont un problème avec leur supérieur hiérarchique. ». *Le* sondé explique qu'une enquête sera réalisée pour comprendre ce changement. S'il y a un risque élevé, la banque limitera les accès au collaborateur et aura un entretien avec la personne.

Q.5 Quelles sont les tendances dans le milieu bancaire pour se prémunir contre les vols et fuites de données?

Pour le sondé, il n'y a pas eu de changement important depuis la crise de 2008, car la banque est consciente du risque.

Une mesure qui existe dans les banques pour se prémunir contre des vols est de limiter les accès aux outils des collaborateurs. Cette mesure permet d'éviter que des collaborateurs aient une trop forte concentration d'accès d'informations. Le sondé rappelle que les vols de données bancaires, comme l'affaire HSBC, sont des cas rares. Il explique aussi qu'un accord avec les différents États pour un échange automatique pourrait raréfier ces vols. Le sondé ajoute: « le vol de données bancaires est un cas rare dans les banques, il y a eu quelques affaires qui ont éclatées dans les journaux depuis la crise 2008. Cela s'explique par la pression des États qui ont un problème avec leur

fiscalité et avec le manque de liquidité dans leur compte. On voit que les Allemands sont prêts à payer des disques ou clé USB contenant des données de clients, car ils savent qu'ils pourront récupérer des recettes avec les fraudeurs. Je pense qu'avec l'échange automatique des données, ce genre de cas va se raréfier »

Q.6 Pensez-vous qu'il faudrait redéfinir les rôles des différents intervenants pour une meilleure sécurité des données ?

Le sondé explique que les rôles sont bien définis dans sa banque et doivent l'être aussi dans les autres banques. Il explique que définir le rôle de chaque fonction permet de mieux ségréger les accès des collaborateurs. Ainsi, la banque pourra effectuer une meilleure traçabilité et surveillance en cas de défaillance dans l'organisation. Le sondé donne l'exemple suivant :« Si vous avez un collaborateur qui a accès uniquement au portefeuille titre d'un client, cette information n'est d'aucune utilité pour pouvoir la revendre à un état par exemple. Il devra reconstituer toutes les données du client pour qu'il y ait un réel intérêt. »

Entretien 9

Profession : sans emploi

Q.1 Pourriez-vous me présenter brièvement les étapes principales de votre carrière ?

Le sondé a suivi une formation universitaire. Il a également suivi des formations continues avec un DAS en gestion du risque et un CAS en audit interne. Il a débuté sa carrière professionnelle dans une banque commerciale, où il avait pour fonction la gestion du risque de la banque. Il a, par la suite, travaillé dans une banque privée, où il était responsable de la gestion des risques généraux de la banque, pour ensuite se s'est concentré sur la gestion des risques opérationnels.

Q.2 Pourriez-vous décrire vos fonctions principales ?

Le sondé est actuellement sans emploi. Dans son dernier travail, il a occupé le poste de gestionnaire de risques. Il a eu pour fonction :

- La gestion des risques de crédits : déterminer où sont les risques pour la banque dans les crédits commerciaux et hypothécaires, en établissant un rapport mensuel.
- L'établissement de différents rapports trimestriels pour différents types de risques (humain, crédit, opérationnel)
- Mise en place d'un système de contrôle interne
- Mis en place de nouveaux processus et nouveaux contrôles

Q.3 Avez-vous été confronté à des tentatives de vols de données au cours de votre carrière ?

Le sondé n'a jamais été confronté à une tentative de vols de données bancaires. Il connait uniquement les affaires qui ont été médiatisées ces dernières années.

Le sondé affirme : « un collaborateur qui veut voler des données, il réussira, car il aura trouvé une défaillance dans l'organisation de la banque. »

Le sondé se souvient d'une histoire qu'une connaissance lui a racontée: « C'était une banque qui avait externalisé son parc informatique. Son sous-traitant avait changé son parc informatique. Toutefois, il avait oublié d'effacer les informations stockées sur les anciens disques durs ».

Q.4 Comment intervenez-vous lorsqu'une tentative de vol est sur le point de s'y produire ?

Le sondé explique qu'il est difficile de détecter une tentative de vols. Pour le sondé, l'intervention débute dès qu'un changement de comportement est observé auprès d'un employé. Cependant, il ne s'agit pas de contrôler les faits et gestes de chaque collaborateur, car cela pourrait rompre la confiance et le respect entre les collaborateurs et leur supérieur. Par exemple: « un employé qui ne parle pas, qui a l'air inquiet ou mécontent, va retenir l'attention des personnes autour de lui. Dès lors, nous commençons à nous renseigner de ce changement d'humeur. On a un entretien avec la personne pour comprendre son attitude étrange. Si nous constatons qu'il y a un risque important de la personne, nous augmentons sa surveillance et limitons ses accès. »

Le sondé revient sur l'histoire racontée dans la question précédente en expliquant comment il aurait agi: « La banque aurait dû s'informer auprès du sous-traitant, à savoir qu'elles sont les changements qu'il a effectués, comment il a protégé les données de la banque. Il aurait dû détruire les disques durs par une entreprise spécialisée, pour éviter une possible reconstruction. »

Q.5 Quelles sont les tendances dans le milieu bancaire pour se prémunir contre les vols et fuites de données?

Pour le sondé, il existe plusieurs mesures pour les banques pour se prémunir contre les vols de données.

Il y a le fait de vérifier les différents profils dans la banque et de connaitre leur accès. « Il s'agit de contrôler que des collaborateurs n'ont pas des accès qu'ils ne sont pas censés avoir. Ce genre de cas peut arriver lorsqu'un employé change de poste dans la banque. »

Une autre mesure mise en place : « Le travail à domicile et les ordinateurs portables ont des accès limités aux données. Des données sensibles ne pourront pas être consultées. »

Pour le sondé, la mise en place de moyens techniques n'est pas suffisante. C'est pourquoi il faut aussi sensibiliser les collaborateurs des risques.

Cela passe par des formations en interne.

Des tests de simulation: « par exemple : mettre une clé USB sur un poste, envoyer de faux emails aux collaborateurs et voir le comportement des collaborateurs. »

Le sondé donne des précisions sur les tests qui sont effectués : « lorsque nous faisons des tests, cela se passe en 2 parties. Il y a un premier test de mise en situation, où nous observons le comportement des employés. Il y a un second test, où les collaborateurs répondent à un questionnaire. Selon les résultats obtenus, les personnes devront suivre une formation de remise à niveau pour combler leurs lacunes et des sanctions peuvent être données quand les résultats sont très décevants. »

Après toutes ces explications, le sondé présente son Smartphone et explique que ce dernier est une nouvelle menace pour les banques et qu'elles ne peuvent pas faire grand-chose contre les collaborateurs qui prennent des photos avec leur téléphone.

Q.6 Pensez-vous qu'il faudrait redéfinir les rôles des différents intervenants pour une meilleure sécurité des données ?

Actuellement, les rôles sont redéfinis dans les banques. La FINMA va sortir à la fin de l'année la Circulaire sur les risques opérationnels avec de nouveaux principes concernant la fuite de données. Pour le sondé, il est très important de responsabiliser les employés sur les risques opérationnels, car le facteur humain en est très souvent la cause. Le sondé estime que la communication entre les différentes fonctions de la banque devrait être: « Il faut prendre le temps de communiquer avec les autres et ne pas hésiter à aller leur parler. Le rôle du Risk Manager est d'être en contact avec les autres, aller sur le terrain pour les aider. »

Le sondé propose de créer une base de données commune, qui regroupe différents rapports et indicateurs de différents services pour que chaque intervenant possède les mêmes informations.

Entretien 10

Profession : Membre de direction, Responsable du Contrôle Interne

Q.1 Pourriez-vous me présenter brièvement les étapes principales de votre carrière ?

La sondée travaille dans une banque privée sur Genève, où elle occupe la fonction de contrôle interne de la banque. Auparavant, elle avait travaillé dans le domaine de l'audit bancaire, dont 8 ans en audit interne et 4 ans en audit externe.

Concernant la formation, elle a étudié à la Haute École de Commerce de Lausanne. Elle a complété sa formation avec un CIA en audit interne, Certified Financial Services Auditor, ainsi qu'une formation Swiss Fund.

Q.2 Pourriez-vous décrire vos fonctions principales ?

Au sein de la banque, elle occupe la fonction de contrôleur interne de la banque. Cette fonction est rattachée à la direction.

Elle doit s'assurer et effectuer les contrôles de 2e niveau.

Elle vérifie que ces contrôles ont été mis en place correctement. Pour mettre en place ces contrôles, elle doit réaliser un mapping des différents risques, leur gravité et les conséquences qu'il peut y avoir. Les gros risques font l'objet de contrôle plus fréquent et plus important.

Q.3 Avez-vous été confronté à des tentatives de vols de données au cours de votre carrière ?

La sondée a connu un cas dans le passé. « Il s'agissait d'un employé qui travaillait à l'hotline de l'entreprise. Il arrivait qu'il se connecte au poste de travail d'un collaborateur. Il a utilisé l'accès aux fichiers des ressources humaines de l'établissement, pour l'utiliser pour son usage personnel ».

Q.4 Comment intervenez-vous lorsqu'une tentative de vol est sur le point de s'y produire ?

La sondée revient sur son histoire, en expliquant que l'établissement a pu intervenir grâce à une procédure de dénonciation, qui a été mise en place.

D'autres moyens existent pour intervenir contre les vols de données bancaires. Des enquêtes peuvent être mandatées par la direction, quand un collaborateur présente un changement dans son comportement et qui pourrait être inquiétant

pour la banque. Si l'enquête démontre un réel risque pour la banque, ces accès seront limités et il sera confronté à son supérieur.

Q.5 Quelles sont les tendances dans le milieu bancaire pour se prémunir contre les vols et fuites de données?

La sondée explique qu'il a plusieurs mesures que les banques ont prises pour se prémunir contre les vols et fuites de données bancaires, en donnant plusieurs exemples:

Les banques font plus attention lors du recrutement du personnel. Elles vérifieront que les candidats n'ont pas des antécédents ou des vices qui pourraient porter atteinte à la banque.

Les banques mandatent des hackers pour essayer de prendre le contrôle du système informatique, effectuer des tests d'intrusion dans le système de la banque pour détecter les faiblesses de la banque.

Le fichier central fait l'objet d'une sécurité très renforcée, car il regroupe toutes les données importantes de la banque. Le nombre de personnes ayant accès au fichier central est très restreint et toute personne voulant y accéder devra enlever tout type d'appareils ou outils pour éviter un vol ou copie des données.

Les nettoyages des locaux sont effectués quand les collaborateurs sont présents dans les locaux.

Concernant les clients, la banque va mettre en place prochainement une application IPAD qui permettra d'afficher sur tablette des informations bancaires du client. Cela évitera de devoir imprimer les documents. La sondée apporte des précisions sur ce dernier point avec un exemple: « un client qui ressort de son entretien avec son gestionnaire n'aura pas à sortir avec les documents papier. De plus, le gestionnaire n'aura plus besoin de détruire les documents imprimés, si le client n'a pas souhaité les prendre avec lui ».

Q.6 Pensez-vous qu'il faudrait redéfinir les rôles des différents intervenants pour une meilleure sécurité des données ?

Pour la sondée, il est important que la banque responsabilise les collaborateurs sur les pertes de données, car c'est un risque humain avant tout et qui peut avoir de grave répercussion sur la réputation de la banque. La sondée estime que la banque doit effectuer un travail important lors du recrutement du personnel en faisant une meilleure vérification des candidats (screening) et mettre à jours régulièrement les données collaborateurs (au moins une fois par année).

La sondé ajoute que les collaborateurs doivent connaitre leur fonction et les tâches qui lui sont attribués. Un comportement étrange, par exemple une personne qui essaye de se connecter sur une boîte email qui n'est pas la sienne ou bien qui souhaite se connecter en dehors des heures de travail, peut être rapidement détectée.

Entretien 11

Profession : Travail dans service public et consultant

Q.1 Pourriez-vous me présenter brièvement les étapes principales de votre carrière ?

Le sondé a suivi une formation universitaire en science économique et sociale. Il a débuté sa carrière professionnelle dans un fiduciaire en tant qu'auditeur. Il a, par la suite, travaillé durant de courtes durées (1-2 ans) dans une autre fiduciaire, puis dans une banque privée. Il rejoint ensuite une banque cantonale, où il a occupé différents postes comme auditeur, asset manager ou bien adjoint. Actuellement, il travaille dans un service public et consultant.

Q.2 Pourriez-vous décrire vos fonctions principales ?

Durant sa période à la banque, il a occupé différentes fonctions:

- Administrateur de la banque cantonale à Luxembourg
- Responsable du management et de la direction.
- Conseiller en Private Banking

Q.3 Avez-vous été confronté à des tentatives de vols de données au cours de votre carrière ?

Le sondé n'a jamais été confronté à une tentative de vols de données bancaires au cours de sa carrière. Il a ensuite fait une distinction entre deux types de données bancaires.

« Il existe pour moi deux types de données bancaires. Il y a les données qui ont été médiatisées par Monsieur Falciani, établir un CD contenant des données sensibles de clients, qu'on essaye de transmettre en échange d'argent. Et il y a le deuxième type qui est plutôt « emprunter » des données. C'est-à-dire, qu'il y a un gestionnaire qui quitte son établissement bancaire pour aller chez le concurrent ou bien se mettre à son propre compte et qui veut récupérer le portefeuille client qu'il a géré. »

Q.4 Comment intervenez-vous lorsqu'une tentative de vol est sur le point de s'y produire ?

Pour se prémunir contre « l'emprunt » du gestionnaire, le sondé explique : « En général, un employé avec des envies d'ailleurs va préparer son départ. S'il souhaite rejoindre un concurrent, il va parler des clients qu'il pourra amener à la banque. Il avertira ensuite ses clients pour les tenir informer et pour les « fidéliser ». Pour éviter le départ des clients, la banque doit être à l'écoute de ses collaborateurs et surveiller un comportement étrange. De plus, la banque met toujours deux personnes qui sont régulièrement en relation avec le client, avec un conseiller attitré et un remplaçant ou assistant. Le but étant que le client crée une relation avec les deux. De plus, le chef du conseiller doit aussi établir une relation avec le client. C'est un élément important pour garder les clients, car le supérieur crée un lien entre le client et la banque. »

Le sondé insiste sur un élément important: « un client n'appartient jamais à personne. Ce n'est pas la propriété d'une banque ».

Q.5 Quelles sont les tendances dans le milieu bancaire pour se prémunir contre les vols et fuites de données?

Le sondé ne connait pas trop la tendance en ce moment dans les banques, car il n'y travaille plus depuis 3-4 ans. Il pense notamment qu'il y a eu des changements importants depuis les différentes affaires qui ont été rendues publiques.

Toutefois, le sondé a expliqué comment il effectuait le contrôle du support informatique : « Lorsque j'étais auditeur, j'étais amené à effectuer un contrôle des accès des différents employés. Pour chaque employé, un pointage était effectué. Si nous constations qu'un collaborateur avait des accès trop importants pour sa fonction, nous demandions des explications. Certains accès étaient justifiés, mais il est arrivé que certains employés ne soient même pas au courant qu'ils avaient accès à certains outils. »

Q.6 Pensez-vous qu'il faudrait redéfinir les rôles des différents intervenants pour une meilleure sécurité des données ?

Pour le sondé cela paraît être une évidence de redéfinir les rôles. Il donne un exemple : « Imaginez que vous travaillez depuis trois semaines chez Métal OR et que votre patron vous remet la clé du coffre, où est stocké l'or. Ce

genre de comportement ne devrait pas se réaliser et malheureusement l'affaire HSBC a montré qu'elle n'a pas défini clairement son rôle. »

Pour le sondé, c'est une histoire de pouvoir et de contrôle qui est la cause des différentes affaires. Il est important que chaque poste soit clairement défini dans son travail, ses accès, ses moyens de surveillance de contrôle. Le sondé se rappelle d'un cas qui l'avait surpris, dans un établissement bancaire « J'avais vu dans un établissement bancaire que certains collaborateurs n'avaient pas la même surveillance que les autres collaborateurs pour la même fonction. Nous ne pouvions pas effectuer un audit efficace. Ces non-droit ou zones d'ombre sont un véritable problème pour la banque et peuvent amener des tensions ou des frustrations au sein de la banque. Si nous mettons des processus et procédures, ils doivent s'appliquer à tous les collaborateurs et il ne devrait pas y avoir de passe-droit, que l'on soit le directeur ou le simple employé du back-office. Un autre exemple que j'ai vu était un poste de travail qui était partagé par différents collaborateurs et il y avait un post-it collé à proximité du bureau avec le code d'accès.

Un autre point le barrage hiérarchique. Souvent, les employés du bas de la pyramide connaissent mieux les fonctionnements opérationnels que les tops managers.

Ils sont conscients des lacunes, mais n'osent pas, ne veulent pas, car ne se sentent pas concernés ou ne peuvent pas communiquer (et souvent ne savent pas à qui communiquer) alors qu'ils ont des solutions. Ce constat est valable dans tous les domaines dans les grandes structures très hiérarchisées. » Pour le sondé : « Environ 70% des risques opérationnels sont dus à l'humain. La paresse, la négligence ou bien l'oubli sont les pires menaces de la banque »

Entretien 12

Profession : Auditeur Interne

Q.1 Pourriez-vous me présenter brièvement les étapes principales de votre carrière ?

et Q.2 Pourriez-vous décrire vos fonctions principales ?

Le sondé a débuté sa carrière dans une banque, en tant que conseiller à la clientèle. Il a également suivi une formation interne sur la gestion de crédit.

Ensuite, il a occupé le poste de crédit officer, où il supervisait les crédits importants de la banque.

Avec la crise des ateliers à Vevey, il a été responsable de la gestion des affaires contentieuses. Son travail consistait à assainir les entreprises. Cette tâche était inédite : « A l'époque, peu de personnes savaient faire ce genre de travail. Il y avait quelques juristes, mais pour les autres, c'était quelque chose de nouveau ».

Il a, par la suite, occupé le poste d'auditeur interne dans une banque cantonale, où il a établi des audits de crédits, la gestion des 80 points de vente et le traitement des fraudes. Le sondé explique : « le travail d'un auditeur peut être comparé à un cancérologue, il faut un travail sérieux, professionnel et le respect de la personne. Je n'ai pas fait le parcours classique d'un auditeur où l'on finit l'université pour devenir auditeur externe puis auditeur interne. Cependant, ma compétence technique acquise par le passé m'a permis de faire ce travail ».

Pour compléter ses compétences, il a suivi une formation de CAS en Audite interne. Cela lui a ouvert l'accès au Master de lutte en criminalité économique.

Actuellement, il travaille pour les CHUV en tant qu'auditeur interne, pour renforcer les systèmes de contrôles des CHUV. En parallèle, il a participé au pôle de recherche en criminalité économie (ILCE).

Q.3 Avez-vous été confronté à des tentatives de vols de données au cours de votre carrière ?

Le sondé a connu une exploitation de données. Il s'agissait d'un gestionnaire qui a voulu récupérer le portefeuille client qu'il a géré, après son départ de la banque.

Le sondé a donné un deuxième exemple avec une histoire qui a été publiée dans les journaux, où une employée aurait transmis des informations internes de la banque à un enquêteur externe.

Q.4 Comment intervenez-vous lorsqu'une tentative de vol est sur le point de s'y produire ?

Pour se prémunir contre l'exploitation des clients par le gestionnaire, la banque met en place deux axes. Dans un premier temps, elle va chercher à connaître ces bons clients, en les rencontrant au moins 1 fois par année avec deux collaborateurs. Cette mesure permet à la banque de créer une relation avec le client. Ensuite, pour se prémunir contre un départ d'un des deux collaborateurs, il y aura toujours le deuxième qui aura aussi créé des liens avec le client. Dans un deuxième temps, la banque va bloquer sur une durée de 6 mois le collaborateur qui a annoncé son départ. Durant cette période, il n'aura aucune relation avec le client. Le but est de mettre à l'écart le gestionnaire pour que son remplaçant puisse créer un lien avec le client. Le sondé précise que l'employé est toujours salarié de la banque, mais il reste à la maison. Pour le sondé : « Il faudrait que la personne continue à faire quelque chose au sein de l'établissement, par exemple la mise en place de cours ».

Dans le deuxième exemple donné par le sondé, il est généralement impossible de faire quelque chose dans ce genre de situation, mais il existe des actions pénales qui peuvent être considérées comme un avertissement pour les autres collaborateurs.

Q.5 Quelles sont les tendances dans le milieu bancaire pour se prémunir contre les vols et fuites de données?

La tendance actuelle peut être définie en trois points:

- Il y a, d'abord, la formation des collaborateurs à l'éthique des affaires.
- Il y a, ensuite, une formation du collaborateur pour son métier et de l'attitude à avoir à l'intérieur et à l'extérieur de la banque.
- Et pour finir la mise en place d'un système de sanctions contre certains comportements qui peuvent aller à des actions pénales pour des cas graves.

Le sondé ajoute qu'il y a aussi des mesures organisationnelles et techniques que les banques ont établies par exemple:

- L'interdiction du téléphone portable pour un usage personnel.
- La limitation d'accès sur le support informatique (blocage des sites de réseaux sociaux, USB,…)

- La mise en pratique des mesures de sanctions pour les comportements indélicats.
- Un meilleur contrôle des candidats pendant la phase de recrutement.
- Une modification des critères pour le recrutement. Le sondé donne l'exemple pour le recrutement des gestionnaires, où la banque va exiger qu'ils soient des résidents suisses.

Q.6 Pensez-vous qu'il faudrait redéfinir les rôles des différents intervenants pour une meilleure sécurité des données ?

Pour le sondé, les banques doivent se remettre en question. « Si nous voulons lutter contre les vols de données et différentes fraudes, il faut comprendre que les banques ont deux types de capital. Il y a le capital physique qui est connu et visible sur le bilan et il y a le capital informatif qui comprend le savoir-faire des collaborateurs, par exemple»

Pour le sondé, cela passe par une limitation des accès aux collaborateurs à réduire au strict minimum pour leur travail. Cela se résume en trois points : « 1) Si on ne peut pas avoir une information, on ne la cherche pas

2) Limiter l'accès par différents moyens

3) Identifier les flux internes (la taille des listes et combien de fois un employé consulte une liste ».

Le sondé donne l'exemple d'un auditeur interne qui a beaucoup d'accès dans la banque:

« Ce qu'il faut savoir, c'est que l'auditeur peut avoir accès à toutes les informations de la banque et presque rien ne lui est interdit. Ce qu'il faudrait faire, c'est que les auditeurs devraient s'annoncer à leur supérieur + justifier les raisons pour lesquelles ils veulent faire le contrôle »

8.2 Annexe 2 : Aperçu des avis d'alerte sur E-Alarm

Avis d'alertes actuels Toutes les catégories

Page 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32

Titre	**ESCROQUERIE PAR "SOCIAL ENGINEERING"**	Détails
Catégorie	Ordres de paiement (y compris e-Banking)	
Publié le	24 septembre 2013	
Versions	19 septembre 2013	
Lieu	Rte de la Blécherette 101 - 1014 LAUSANNE	
Texte	Changement du date de l'événement (ancien: 11 mars 2013) Mercredi 11 septembre 2013 à 12h27, une banque de la place lausannoise a ...	

Titre	**CARD-TRAPPING (Collet Marseillais)**	Détails
Catégorie	Cartes et automates	
Publié le	23 septembre 2013	
Lieu	Lucerne	
Texte	Le 16.09.2013, près d'un Bancomat situé à Lucerne, les objets figurant en annexe ont été mis en sécurité par la police. Le ...	

Titre	**Tentative de vol à l'arraché sur un client en dehors de la banque**	Détails
Catégorie	Vol (y compris vol par astuces)	
Publié le	18 septembre 2013	
Lieu	St. Gallerkappel / SG	
Texte	Le vendredi 13.09.2013 vers 15h30, un client a été menacé par un inconnu en dehors de la succursale St. Gallenkappel de la Banque ...	

Titre	**Fraude en matière d'e-banking**	Détails
Catégorie	Ordres de paiement (y compris e-Banking)	
Publié le	10 septembre 2013	
Lieu	Weinfelden TG	
Texte	Une cliente a constaté en date du 3.9.2013 que la somme de CHF 1504.-- avait été débitée de son compte-épargne et la somme de CHF ...	

Titre	**Prétendus appels de clients de l'étranger**	Détails
Catégorie	Généralités	
Publié le	9 septembre 2013	
Lieu	acrevis Bank AG, 9001 St.Gall	
Texte	Le vendredi 6 septembre 2013, un homme dont l'identité ne nous est pas connue a essayé, à plusieurs reprises auprès de plusieurs ...	

Titre	**Vol par astuce du 3 septembre 2013**	Détails
Catégorie	Vol (y compris vol par astuces)	
Publié le	4 septembre 2013	
Lieu	Ibach SZ	
Texte	Les mêmes voleurs par astuce qui ont agit à Bienne et Berne le 28 août, à Martigny, Brig et Susten le 29 août, et à Appenzell le 2 ...	

Titre	**Fraude par opération de change/Vol par astuce du 3 septembre 2013**	Détails
Catégorie	Vol (y compris vol par astuces)	
Publié le	4 septembre 2013	
Lieu	Ville de Zurich	
Texte	Alors que divers vols par astuce ont eu lieu ces derniers jours à Berne, Bienne, Martigny, Brigue, Susten, Appenzell et Altdorf, ...	

Titre	**Fraude par opération de change/Vol par astuce du 2 septembre 2013**	Détails
Catégorie	Vol (y compris vol par astuces)	
Publié le	3 septembre 2013	
Versions	2 septembre 2013	
Lieu	Appenzell	
Texte	Les voleurs par astuce qui ont agit à Bienne et Berne le 28 août, ainsi quà Martigny, Brig et Susten le 29 août (cf. avis ...	

Source : SWISSBANKING, *Swiss E-Alarm,* http://www.e-alarm.ch/ealarm/html/report_view_list.jsp

8.3 Annexe 3 : Exemple d'avis d'alerte sur E-Alarm

Rückzug von Banknoten

Type	Information
Categorie	Billets de banque et papiers d'identité
Publié le	L'information n'a pas encore été publiée.
Valable jusqu'à	2.7.2009
Versions	12. Juin 2007
Lieu	F Basel
Contact	F Schweizerische Bankiervereinigung, Peter Muster, Aeschenplatz 7, 4051 Basel, EMail: peter.muster@sba.ch, Tel. +41 61 295 9393

Wie die "Bank of England" mitteilt, werden die **Banknoten zu £ 10.- des alten Typs (Motiv: Charles Dickens, Serie E)** ihre gesetzliche Zahlungskraft mit Ablauf des **31. Juli 2007** verlieren.

F Die meisten Geschäftsbanken und die "Bank of England" lösen die ausserkursgesetzten Banknoten jedoch auch nach diesem Zeitpunkit zum Nennwert ein. Ein Verfalldatum, nach dem diese Banknoten jeglichen Wert verlieren, wurde nicht festgelegt.

Zusätzliche Informationen sind auf der Website der "Bank of England" zu finden, unter:
www.bankofengland.co.uk/banknotes/.

£ 10.- Front

£ 10.- Back


£ 10.- Detail

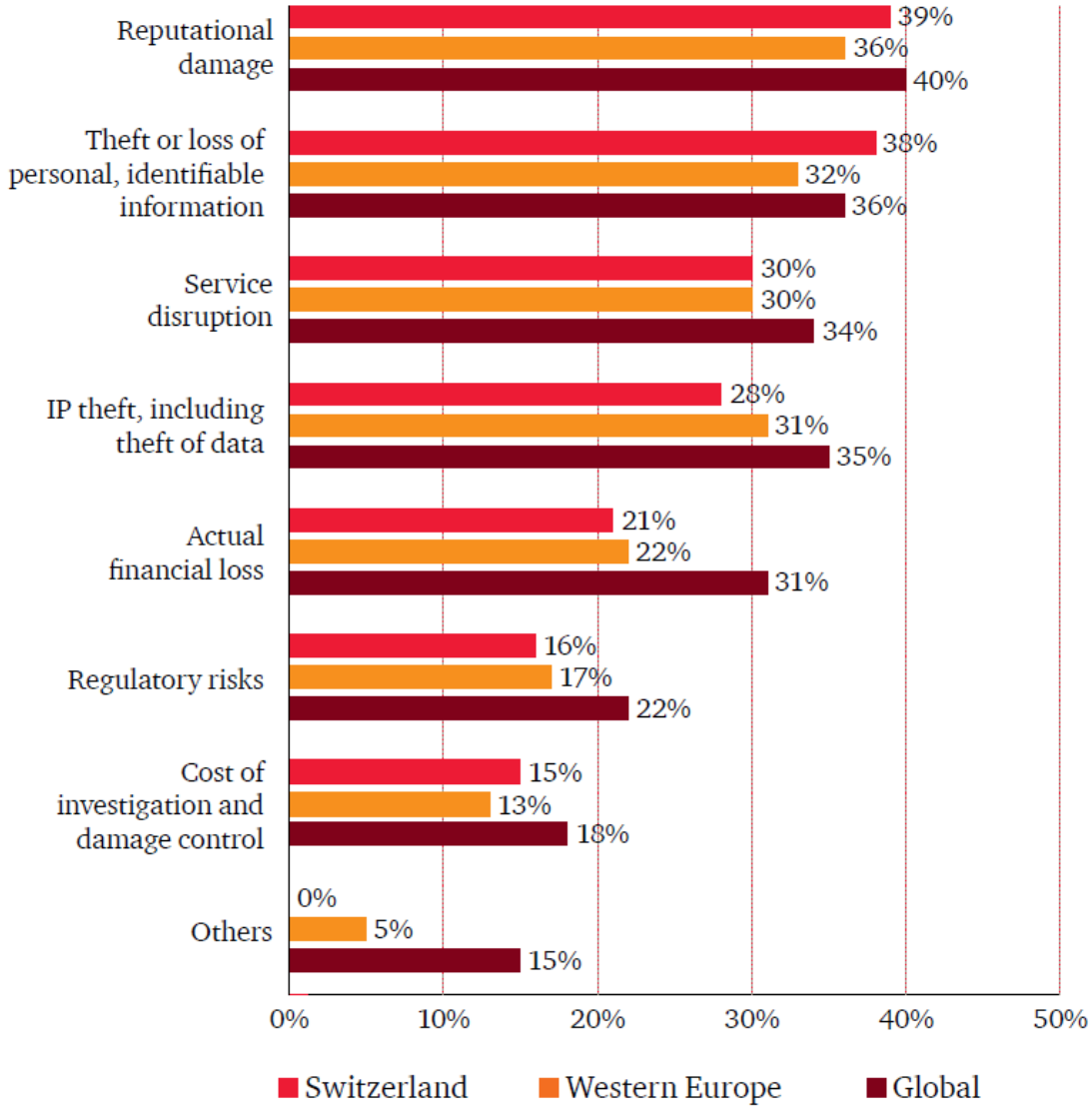
Annexe
Value of notes in circulation

Versions linguistiques
Deutsch | Französisch

Source : SWISSBANKING, *Manuel E-Alarm,* Juillet 2007, Page 19

8.4 Annexe 4 : Les impacts de la cybercriminalité

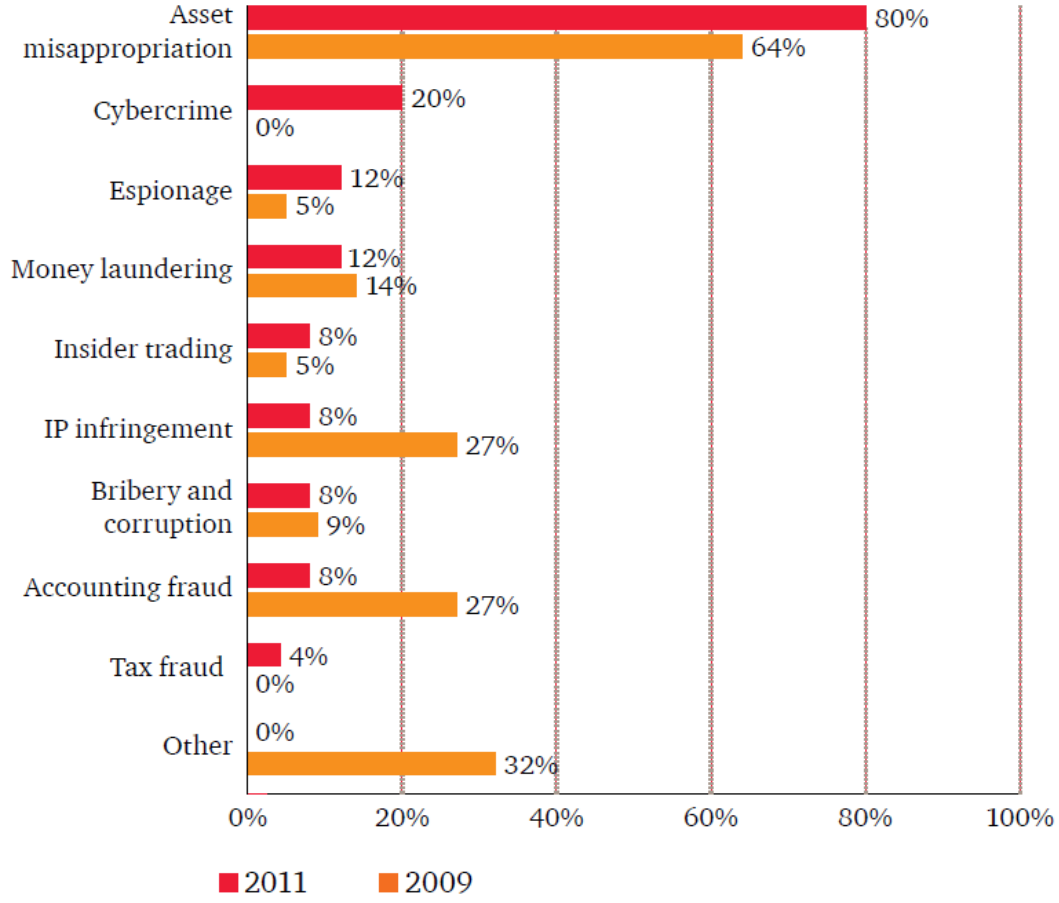
Figure 4: Concerns about the effects of cybercrime on the organisation (% of respondents who stated very concerned)



Source : PWC, *Cybercrime in the spotlight, Swiss Economic Crime Survey 2011*, Novembre 2011, Page 9

8.5 Annexe 5 : Les types des fraudes

Figure 10: Types of economic crime in the last 12 months compared to 2009 (% of reported frauds)



Source : PWC, *Cybercrime in the spotlight, Swiss Economic Crime Survey 2011*, Novembre 2011, Page 18

8.6 Annexe 6 : les profils des fraudeurs

Figure 11: Internal fraudsters (% of reported frauds)

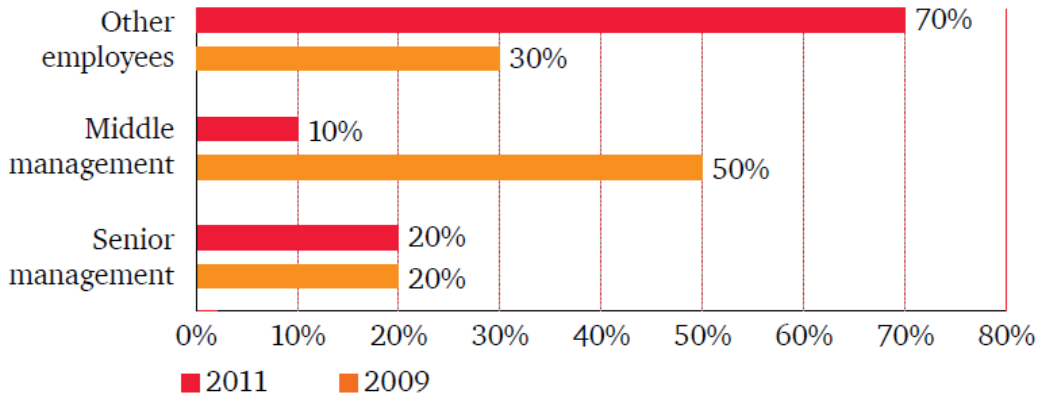
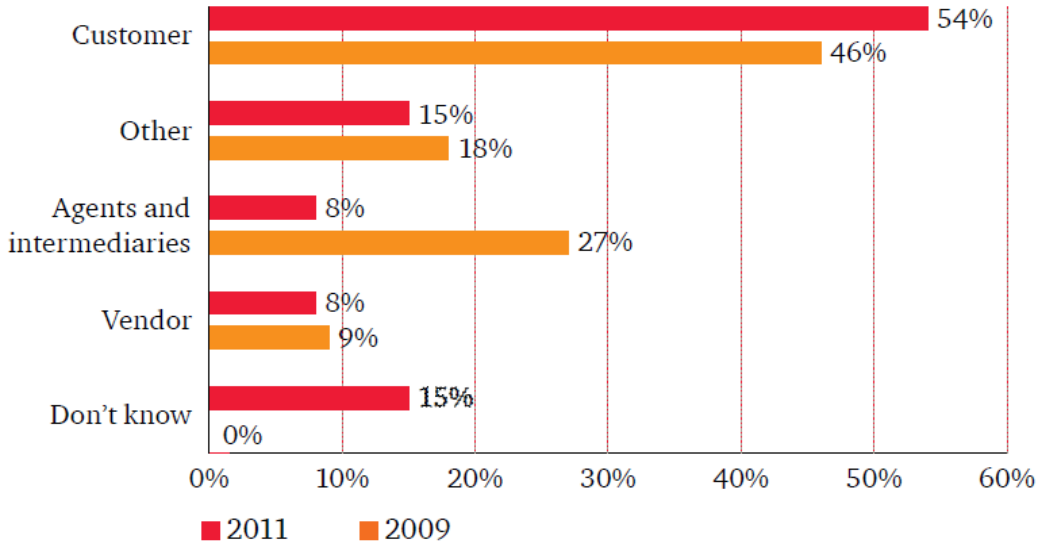


Figure 12: External fraudsters (% of reported frauds)



Source : PWC, *Cybercrime in the spotlight, Swiss Economic Crime Survey 2011*, Novembre 2011, Page 20