MASTER 2 CHARGEE DE CLIENTELE PROFESSIONNELLE
Année universitaire 2020/2021

MÉMOIRE

Présenté par

Mlle Chloé CHRISTOPH

« La Cybercriminalité Bancaire »

Directeur du mémoire : *M. Abdelkader MATMOUR*

Remis le 16/06/2021

Soutenance le 24 juin 2021
Devant le jury de soutenance :
***Abdelkader MATMOUR* Tuteur universitaire**
***Doris LEDERMANN* Représentant de l'ESB**
***Camille MEYER* Maître de stage**

L'École supérieure de la banque
L'Expertise CFPB

BANQUE POPULAIRE ALSACE LORRAINE CHAMPAGNE

Faculté des sciences économiques et de gestion
Université de Strasbourg

« La force et la fraude sont les deux armes principales des hommes en guerre. »

Thomas HOBBES

REMERCIEMENTS

Ainsi s'achève ma dernière année d'étude supérieure…

Je tiens à remercier en tout premier lieu la Banque Populaire Alsace Lorraine Champagne pour m'avoir donné ma chance il y maintenant 2 ans à moi et mon parcours « atypique ».

Merci à Nicolas Ometz et Cécile Da Costa, mes tuteurs lors de mon arrivée au sein de la BPALC à l'agence d'Erstein pour ma première année de Master en alternance.
Merci pour vos conseils, votre accompagnement et vos sourires.

Merci à Camille Meyer, ma tutrice à l'agence d'Obernai et désormais amie, pour sa disponibilité, ses connaissances, son humour et son goût des choses bien faites.
Elle a particulièrement contribué à cet aboutissement et je lui en suis grandement reconnaissante.

Merci à Marc-Antoine Cadot, directeur de l'agence d'Obernai, pour sa confiance à mon égard.

Mes remerciements se tournent également vers M. Matmour et Mme Ledermann, mes deux responsables de formation qui chapeautent tous deux ce Master d'une main de maître. Merci pour ces deux belles années d'études, à la fois au PEGE et à l'ESB.

Enfin merci à ma famille pour son soutien indéfectible et à mes amis pour leur encouragement, leur présence et leur bienveillance. Certains camarades de classe deviendront des amis de longue date, je n'en ai aucun doute.

Aujourd'hui, je suis arrivée au but que je me suis fixée il y a maintenant 2 ans : intégrer une agence bancaire et devenir une chargée de clientèle professionnelle.
Je commence donc ma vie professionnelle avec des bases saines et solides et il me tarde de m'épanouir dans ce beau métier.

SOMMAIRE

INTRODUCTION

Qui n'a jamais été tenté par un email, un courrier ou parfois même un appel qui vantait les mérites d'un produit ou d'un service en l'échange de quelques informations personnelles puis bancaires ? La fraude informatique, aussi appelée cybercriminalité, est aujourd'hui extrêmement développée et se renouvelle constamment pour contrer les diverses protections qui peuvent être mises en place par les institutions publiques ou privées.

C'est une notion complexe et dense, qui touche de nombreux domaines, dont la banque. Les attaques perpétrées contre les organismes bancaires sont quotidiennes et elles peuvent avoir de lourdes conséquences sur ceux qui la clientèle touchée, du client particulier au PDG d'une multinationale. Ces attaques ont mis du temps à être correctement identifiées puis efficacement contrées.

« J'ai reçu un courriel de ma banque me demandant mon identifiant de connexion et le mot de passe de consultation de mon compte en ligne. Ils m'avaient alors expliqué qu'ils avaient besoin de mettre à jour mes données de connexion. Le problème c'est que ce n'était pas ma banque. Mon compte a été vidé. »[1]

Des témoignages comme ceux-ci fleurissent par centaine sur internet, chaque jour, laissant la majorité des victimes dans des situations de grand désarroi.
Les banques, par leur caractère indispensable et pécuniaire, sont une cible de choix pour les cybercriminels qui sévissent aujourd'hui sur la toile.

Il est aujourd'hui certain que le développement des réseaux de communication, l'accès facilité et continu aux informations au sein des organisations et la digitalisation des opérations courantes ont conduit à l'accroissement de la cybercriminalité au cours des dernières années. Cette évolution des mœurs et des outils a de facto diversifié les canaux par lesquels les attaques ou les dysfonctionnements peuvent survenir, rendant les organisations sans cesse plus exposées.

[1] www.interieur.gouv.fr, 06.01.2009

Les artisans, commerçants, professions libérales, TPE, PME… dont nous nous occupons en tant que conseiller de clientèle professionnelle doivent faire face à ces attaques d'un nouveau genre afin de préserver leur activité et plus largement leur société.

Ce développement amène à nous interroger sur le concept de la cybercriminalité bancaire et quels en sont les impacts qu'elle peut avoir sur une entreprise ? Quelle est la place du banquier dans cette lutte contre l'invisible ?

Pour traiter ces problématiques, la première partie de ce mémoire sera consacrée à la notion de cybercriminalité a proprement dite. Afin de comprendre ce terme dans son ensemble, cette partie reviendra sur des définitions essentielles à la bonne compréhension du sujet de ce mémoire, sur une contextualisation actuelle ainsi que sur le poids du digital dans l'essor de ce concept.

La deuxième partie sera elle consacrée à l'analyse des conséquences de la cybercriminalité sur la banque comme sur le client professionnel.

Enfin, la troisième partie nous permettra de mettre en exergue les moyens de lutte qui ont émergé ces dernières années, de part une règlementation française et européenne renforcée mais également grâce aux outils propres des banques actuelles.

PARTIE 1 : LA NOTION DE CYBERCRIMINALITÉ

I) Définition

a) Définition générale de la cybercriminalité

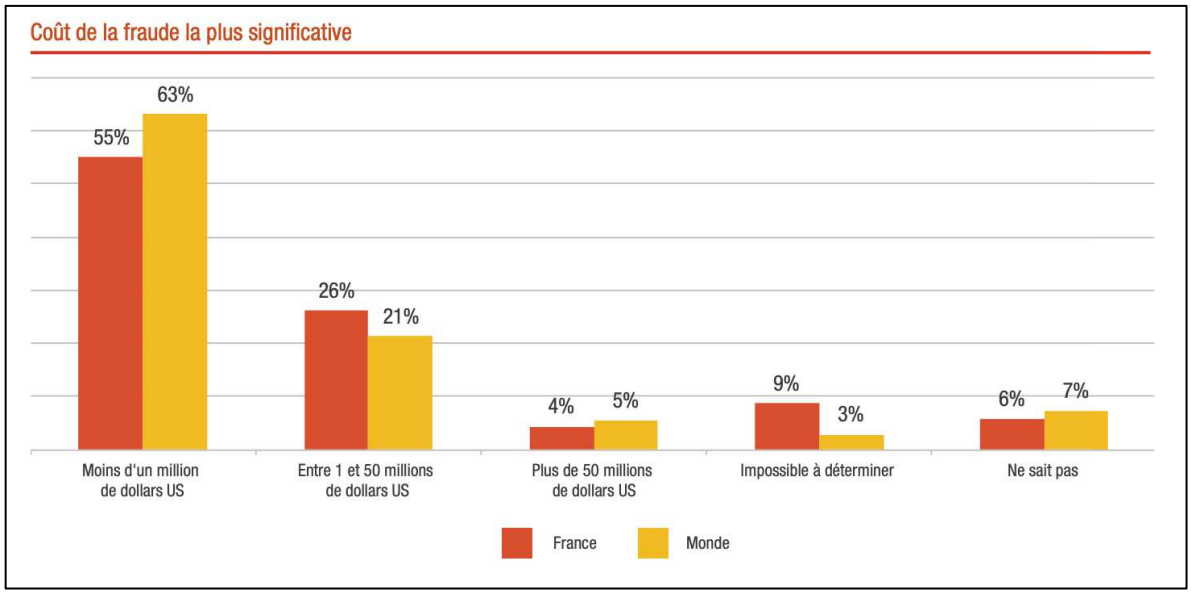
Comprendre la notion de cybercriminalité passe dans un premier temps par un petit exercice d'étymologie : en décomposant le terme, la définition apparaît d'elle-même.
« Cyber » : Élément servant à former des composés en rapport avec le multimédia, Internet, le web.
« Criminalité » : Ensemble des actes criminels dans une période et un milieu donné.
La cybercrimalité se définit donc tout simplement par des actes criminels perpétrés grâce et au travers des outils multimédias et d'Internet.

D'une manière plus générale, elle découle de la famille des fraudes informatiques, elle peut être interne ou externe à l'organisation touchée et plusieurs processus sont aujourd'hui utilisés. Elle représente aujourd'hui une réelle menace : d'après l'étude annuelle de PWC (entreprise d'audit et de conseil aux entreprises), la cybercriminalité demeure, en 2020 et pour la deuxième année consécutive, la première fraude dont ont été victimes les entreprises françaises avec 33%[2] des entreprises touchées, devant le détournement d'actifs pour 29% et la fraude comptable pour 29% également.

D'après l'ouvrage de Perreira Brigitte sur la lutte contre la cybercriminalité, on relève neuf types d'infractions : « *l'accès illégal aux systèmes et données informatiques, tel que le piratage ; l'interception illégale ; l'atteinte à l'intégrité des données ; l'atteinte à l'intégrité des systèmes (virus, spam et déni de service) ; le marché noir de la production ou la vente de moyens de commettre les infractions (infractions d'abus de dispositif) ; la fraude informatique ; la falsification informatique ; les infractions se rapportant à la pornographie enfantine ; les infractions liées aux atteintes à la propriété intellectuelle et aux droits connexes »*[3]

[2] Étude annuelle PwC's Global Economic Crime and Fraud Survey, 2020
[3] Pereira, Brigitte. « La lutte contre la cybercriminalité : de l'abondance de la norme à sa perfectibilité », Revue internationale de droit économique, vol. t. xxx, no. 3, 2016, pp. 387-409.

Pour les sociétés touchées, l'impact est pluriel et significatif à travers des coûts directs et indirects. D'un point de vue économique, le coût de la fraude est estimée à plusieurs millions de dollars, en fonction de la taille de l'entreprise touchée. Plus indirectement, l'impact peut également être social et psychologique : pour l'image de l'entreprise, la méfiance engendrée par cette fraude, les pertes d'opportunités commerciales…



PwC's Global Economic Crime & Fraud Survey 2020

b) La cybercriminalité bancaire

Et dans le milieu bancaire, qu'en est -il ? Afin de le comprendre, j'ai décidé de m'adresser directement à un spécialiste de la fraude au sein de mon organisation bancaire. Il m'expliquait, et je reprendrai ses mots, qu'il est aujourd'hui beaucoup plus intéressant pour un criminel de passer par la fraude informatique que par le hold-up d'une banque à main armée.

En effet, attaquer une banque « physiquement », tenter de dérober l'intégralité du contenu des coffres mais finalement se faire arrêter par les forces de l'ordre, c'est être puni de trente ans de réclusion criminelle et de 150 000 euros d'amende au minimum. Attaquer une banque par la voie informatique, c'est peut-être 2 ans de peine encourue et à peine 30 000€ d'amende… les cybercriminels se sentent donc relativement impunis, risquent beaucoup moins que leurs pairs et disparaissent le plus souvent

avant même d'avoir pu être identifier. Cette idée d'impunité explique en grande partie pourquoi les organisations bancaires sont les plus touchées par ce type de fraude.

Au travers de l'essor de la digitalisation, que j'aborderai dans une autre sous partie plus en détails, on remarque assez aisément une stratégie opératoire rondement ficelée et quasiment intraçable : le cybercriminel vole ou achète de la *data* (ndlr : une base de données numériques), passe par un processus de manipulation ciblée, par téléphone ou par mail, pénètre les outils informatiques de sa cible et procède à des opérations de type virements instantanées, retraits digitaux, ajout de bénéficiaires…
Les conséquences peuvent être catastrophiques, pour les clients particuliers comme professionnels, mais aussi pour l'établissement bancaire : atteinte à l'intégrité, atteinte aux actifs, atteinte à la réputation et à la confiance (des clients, du marché, des collaborateurs).

c) Émergence

Manipuler, frauder, escroquer, extorquer des fonds… ces termes existent depuis toujours et ont toujours accompagné les personnes physiques ou morales.

Alors certes, aujourd'hui les processus utilisés sont principalement informatiques, vous recevez un mail douteux, qui finit dans vos spams mais qui attire tout de même votre attention au point de cliquer sur un lien lourd de conséquence… Une arnaque bien connue, directement inspirée d'une une escroquerie du XVIIIe siècle nommée "lettres de Jérusalem". En 1836, le célèbre Eugène-François de Vidocq, ancien délinquant et bagnard devenu chef de la Sûreté nationale pendant la Restauration, explique dans son ouvrage intitulée « Les Voleurs », comment, au travers d'une correspondance bien argumentée et pleine de promesses, il réussissait à dérober des sommes notables à la principauté de l'époque.

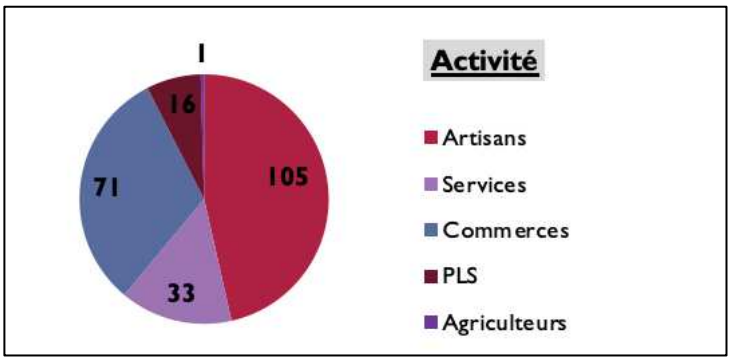
Aujourd'hui, loin de ces procédés épistolaires et révolus, les cybercriminels passent par des mails, piratent les applications, se font passer par des techniciens employés par la banque pour les accompagner dans la digitalisation de leurs opérations et accèdent plus ou moins librement à toutes les ressources des clients.

Les typologies d'attaques se renouvellent sans cesse, poussant la cyber sécurité bancaire à identifier tous types de fraudes afin de les contrer au mieux et de pouvoir lutter efficacement contre celle-ci.

II) Contextualisation

a) Les professionnels aujourd'hui

En tant que conseillère bancaire, il m'est aujourd'hui essentiel de pouvoir proposer un accès digital à mes clients professionnels. Tous les cœurs de métiers sont aujourd'hui représentés au sein des portefeuilles des chargés d'affaires. Par exemple dans celui dont j'assure la gestion quotidienne, j'ai à la fois des artisans et commerçants mais également des professions libérales et de service, comme le montre le graphique ci-dessous.



Composition du portefeuille en %

Bien que tous différents, les professionnels d'aujourd'hui ont tous besoin d'une gestion optimisée et facilitée à leur comptes bancaires, dans un souci d'ordre comptable, fiscal et opérationnel. Il est à noter également qu'un espace digital efficient permet d'opérer plus simplement des paiements fournisseurs comme des paiements clients, deux parties essentielles et nécessitant le plus souvent des actions rapides, devant être anticipées par souci d'image, de confiance et de relationnel.

On constate de plus en plus que nos clients professionnels payent leurs fournisseurs par virement, ce moyen de règlement ayant augmenté de 24%[4] au cours des dernières années, et c'est tout à fait légitime : c'est rapide (en moyenne 24 à 48h de délais interbancaires), simple (il suffit d'ajouter le bénéficiaire pour pouvoir effectuer un paiement) et sécurisé (que ça soit en direct ou via l'application, les établissements bancaires redoublent de vigilance sur ce type d'opérations.)

Et malgré la vigilance de mise, c'est ici que se situe le cyber risque : par des procédés parfois complexes, parfois enfantins. Les bénéficiaires ajoutés sur les espaces bancaires en ligne de nos clients ne sont plus ceux utilisés dans le cadre de paiement et de relation fournisseurs : ce sont des comptes, situés en France ou à l'étranger, sur lesquels sont virés des fonds plus ou moins conséquents en quelques secondes à peine. Un impact financier et psychologique pour nos professionnels, qui amènent parfois à des indemnisations de la part de la banque, parfois non.

b) La crise du COVID 19.

Elle n'est plus à présenter : la récente crise sanitaire a modifié et impacté de manière durable le milieu bancaire et ses clients. De la façon de travailler à la manière de communiquer, il est certain que de nouvelles méthodes sont désormais ancrées dans la gestion quotidienne des opérations bancaires. En parallèle, il est également à souligner la hausse des cyberattaques sur le milieu des professionnels et entreprises : les cybercriminels sont dans une mouvance constante et ont un potentiel d'adaptabilité hors-normes. A noter qu'ils se sont également greffés sur les incertitudes et sur le caractère soudain de cette crise sanitaire sans précèdent.

A travers le télétravail, la baisse des effectifs et les difficultés de communication au sein des organisations, l'exposition aux cyberattaques a été beaucoup plus forte, la majorité des entreprises et des professionnels tentant tant bien que mal de faire face au désarroi financier engendré par cette crise avant tout autre chose.

[4] Source : étude Harris Interactive 2016

Les professionnels ont évidemment dû adapter leur gouvernance en matière de cyber sécurité afin de pallier les attaques malveillantes. D'après le site internet *Viepublique.fr,* un site gouvernemental permettant aux citoyens d'échanger et de s'exprimer, la plateforme d'aide et d'accompagnement *cybermalveillance.gouv.fr* a été fréquenté de manière exponentielle tout au long de la crise du COVID19 : +155% par rapport à 2019. Les visites ont même atteint un pic record de 600% au printemps 2020, soit au premier confinement. Le site relate également que les demandes émanant de professionnels ont augmenté de 20%.

Au sein du milieu bancaire, l'adaptation a pris le temps également : nous étions face aux mêmes problématiques que nos clients, à devoir gérer des fermetures d'agences au public, le développement du télétravail de nos collaborateurs et une gestion totalement à distance des opérations courantes. Thierry Rodmacq, responsable de la coordination de la fraude externe au sein de la BPALC, m'indiquait pendant son interview qu'il a effectivement constaté une hausse de la fraude entre 2019 et 2020 :

« *On a eu des scénarios typiques COVID, c'est à dire des fraudes sur les masques, sur le matériel médical, sur les primes COVIDS : le fraudeur se sert de l'actualité. Il profite également du télétravail pour essayer de tester nos systèmes de sécurité de télétravail…Notons également un peu plus de fraude au président, comme les entreprises sont désorganisées, on se fait passer pour un président pour faire un virement. La conclusion à en tirer c'est vraiment cette capacité d'adaptation du fraudeur. Il sait s'adapter en permanence ! »*

« Avez-vous observé des fraudes sur des PGE[5] *par exemple ? »*

« Je n'ai pas eu de cas qui est remonté. J'ai vu en revanche de la fraude à la prime COVID. Le fraudeur avait fait une demande de prime, se l'ai faite virer sur le compte du client et après il a tenté de récupérer la prime on se faisant passer pour les impôts, en indiquant une erreur. C'est un scénario très bien élaboré, on revient sur tout ce qui lié à la manipulation. »[6]

[5] PGE : prêt garanti par l'État
[6] Citation tirée de l'interview disponible en annexe

Fort heureusement donc, et malgré une hausse des cyberattaques, la cyber sécurité active et évolutive a su contrer les différentes attaques dont ont pu être potentiellement victimes nos clients. Il reste tout de même à souligner cette capacité d'adaptation particulièrement impressionnante et qui amène à un renforcement de la vigilance autour de cette problématique.

III) L'essor de la digitalisation et son impact sur la cybercriminalité

a) La digitalisation bancaire

Avant d'aborder ce chapitre il me parait essentiel de revenir sur la notion de digitalisation bancaire et il est important également de différencier « banque en ligne » et « banque digitale ».

Une banque en ligne, ou néo banque, c'est une banque qui ne dispose pas d'agence physique, qui propose une gamme de produits similaires à une banque de réseau et qui passe uniquement par des applications et des conseillers à distance. On estime que 6% de la clientèle est passée à 100% sur ce type de banque désormais pour un total d'environ 4 millions de comptes ouverts.

Une banque digitale, c'est le versant numérique des banques de réseaux : en effet, toujours dans cette nécessité de s'adapter au marché, les banques classiques ont optimisé leur application, afin de proposer des interfaces qualitatives et intuitives à leurs clients et également dans une démarche d'autonomisation de la clientèle.

La Fédération bancaire française (FBF) a récemment publié son étude concernant les pratiques des Français en termes d'utilisation et de relation avec leur banque. Il en ressort que 66% des Français, soit un peu plus de 33 millions de citoyens, ont téléchargé l'application de leur banque et l'utilisent pour toutes sortes d'opérations courantes.

Il est aujourd'hui impensable qu'un établissement bancaire fonctionne sans une application dédiée à ses clients : cette mouvance est à la fois synonyme de progrès,

d'indépendance et de suivi 24/7. C'est un réel gain de temps pour la clientèle bancaire, mais également pour les conseillers : l'autonomie des clients permets la quasi-disparition des actes chronophages qui peuvent rythmer la journée du conseiller. C'est ainsi que la digitalisation des opérations est devenue un réel levier de rentabilité et donc de PNB pour les banques d'aujourd'hui.

b) La porte ouverte à la cybercriminalité

Quelle est la place de la digitalisation dans la cybercriminalité ? Dans une volonté qui est d'orienter au maximum le client dans une démarche *selfcare* au travers de la mise en place d'outils digitaux, on remarque que les cybers criminels se sont clairement adaptés à ces outils et les utilisent aujourd'hui pleinement dans le cadre de la fraude externe.

Voici un exemple de fraude au sein de mon établissement par l'utilisation de l'espace en ligne d'une cliente, tiré de l'interview avec le coordinateur de la fraude externe à la BPALC :

« Le fraudeur a appelé notre cliente, a joué sur la peur en se faisant passer pour le service technique Banque Populaire, en lui disant qu'il y'avait une attaque informatique sur son profil, un piratage de son compte et qu'elle allait recevoir un numéro par SMS qu'il faudra lui ensuite donner pour sécuriser son système … ce qu'il se passait réellement, c'est que le fraudeur était en train de changer le mot de passe sécurisé de notre cliente, donc il avait son smartphone, il changeait le mot de passe sécurisé et l'échange de SMS c'était pour valider le changement de mot de passe. Avec ce code sms, le fraudeur a pu prendre la main sur l'espace cyber du client et a commencé à faire des virements depuis le compte épargne sur le compte chèque et a tenté de faire un virement vers un bénéficiaire externe de 15 000€. La cliente, du fait qu'il y a des codes SMS qui signalent des changements de mot de passe, a vu les virements et a eu la présence d'esprit de contacter notre service client et nous avons pu tout bloquer in extremis.
On est typiquement dans un exemple de manipulation, pour rentrer dans le cyber du client, faire un virement mais aussi une connaissance parfaite des outils ! Toutes les applications mobiles qu'on peut avoir, les fraudeurs les connaissent parfaitement et ça

toutes banques confondues. Le fraudeur va utiliser un mixte entre le fait de rentrer dans le système, car il avait accès au numéro de carte de la cliente, il avait également le numéro d'abonné… Il avait quand même déjà un certain nombre de données, certainement achetées sur le darkweb. Il est donc parti d'un fichier, qui lui a fait l'objet d'une fraude cyber pure, c'est à dire qu'il y a des gens qui vont se spécialiser dans l'attaque qui consiste à pirater des sites ou des choses comme ça, qui volent des données, et qui revendent les fichiers sur le darkweb.
Certains fraudeurs sont spécialisés dans la récupération de data, qu'ils revendent ensuite et qui sont achetés par les cybercriminels.
L'exemple de cette cliente regroupe la de récupération de data, par l'attaque cyber et ensuite de la manipulation, tout en utillsant un support smartphone avec une appli mobile »

Cet exemple est intéressant car il détaille tout le processus qui peut être mis en place autour d'une attaque cyber. On retrouve donc ce schéma en 3 actes qui passe par le vol de données, la manipulation et pour terminer le piratage informatique dédié au vol d'argent à proprement parlé.

Le concept de manipulation est ici à souligner car il est parti prépondérante de la cybercriminalité bancaire : dans le cadre d'un vol de fonds, sur un client particulier ou professionnel, M. Rodmacq m'expliquait que dans 80% des cas, les fraudeurs passent par une manipulation de leur cible, en usurpant leur identité, en promettant de fortes compensations financières par suite de certains services rendus (encaissement d'un chèque revenant ensuite impayé par exemple) et que c'était majoritairement cette manipulation qui amenait à l'aboutissement de l'opération.

c) La fraude au président

Dans le milieu des professionnels, on constate une fraude plus récurrente que les autres : la fraude au président.

On retrouve la définition de cette fraude sur le site du ministère de l'économie, avec l'appui de la DGCCRF : *« L'arnaque au président consiste pour le fraudeur à contacter une entreprise cible, en se faisant passer pour le président de la société mère ou du*

groupe. Le contact se fait par courriel ou par téléphone. Après quelques échanges destinés à instaurer la confiance, le fraudeur demande que soit réalisé un virement international non planifié, au caractère urgent et confidentiel. La société sollicitée s'exécute, après avoir reçu les références du compte étranger à créditer. »

Est également constaté depuis quelques mois et d'autant plus depuis la crise sanitaire, l'usurpation d'identité d'une administration publique, comme expliqué sur le site du ministère de l'économie également :
« Cette dernière variante de cette fraude se déroule en deux étapes : le fraudeur usurpe l'identité d'une administration, la direction générale des finances publiques, en utilisant nom, sceaux et timbres de l'État (Marianne) et citant des articles législatifs pour prétexter un contrôle auprès d'une entreprise cible. Sous couvert de cette fausse identité, le fraudeur réclame des informations sur l'entreprise et sur ses clients.
Par la suite, le fraudeur se fait passer pour l'entreprise cible auprès de ses clients et annonce un changement de compte bancaire, le paiement des futures factures seront donc payées sur le nouveau compte appartenant au fraudeur. »

C'est typiquement l'une des fraudes les plus communes, qui touche les entreprises de taille importante (plus de 1Mk€ de CA par an) comme les petites PME ou les artisans commerçants (entre 100 et 450k€ de CA par an). Il est important de souligner également que la crise sanitaire a amplifié ce type de fraude, du fait de l'absence de certains responsables sur une longue période et l'augmentation du traitement des opérations par voie digitale.

La mutation du procédé de tromperie et d'escroquerie associée à l'apport du digital, a rendu la fraude au président excessivement efficace et pouvant être lourde d'impacts.

PARTIE 2 : QUELLES CONSÉQUENCES ?

Après cette remise en situation sur la notion de cybercriminalité et une contextualisation dans l'environnement d'aujourd'hui, cette deuxième partie sera dédiée à l'exposition des conséquences de cette fraude.

I) Conséquences pour la banque

a) Financières

Le coût de la cybercriminalité dans le milieu bancaire français est aujourd'hui difficilement estimable. Les chiffres trouvés dans le cadre de ce travail de recherche sont soit obsolètes, soit prennent une dimension internationale qui ne me permets pas d'exposer clairement le coût de cette fraude sur nos établissements bancaires français.

Néanmoins, il me parait essentiel de citer les chiffres tirés d'un sondage réalisé par Kapersky Lab et B2B International en 2017 pour démontrer que les conséquences financières sont bien réelles : sept banques sur dix ont déjà été touchées par des cyberfraudes, et un incident cyber mené à son terme coute en moyenne 1 million d'euros aux banques touchées.

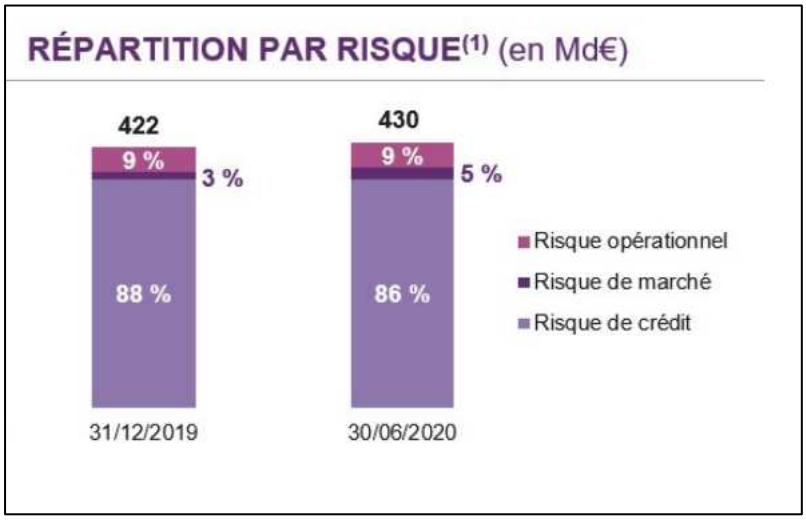
Pour mieux comprendre ce coût il est important de le décomposer : une attaque cyber aboutie, c'est en premier lieu une fuite d'informations protégées, une pénétration au sein du système de sécurité de la banque et enfin un vol de fonds plus ou moins important en fonction de la cible concernée. C'est ce schéma complet et abouti qui amène à une atteinte réelle des actifs et résultats d'un système bancaire.
Une fraude aboutie amène à une révision complète des systèmes de sécurité et en l'investissement plus ou moins conséquents de nouveaux dispositifs de cyber sécurité.

Dans cette optique de toujours pouvoir suivre l'évolution des cybers attaques sur le système bancaire, la Banque centrale européenne (BCE) a décidé en 2018 de développer des tests d'intrusion dans les systèmes informatiques bancaires, afin

d'identifier les lacunes de ceux-ci mais également dans l'optique de préparer au mieux les employés aux attaques pouvant être perpétrées.

De la protection centrée sur les données, à l'authentification adaptative, en passant par l'analytique des identifications et la gestion et protection des appareils, ces tests permettent une préparation plus globale pour les systèmes de sécurité bancaire.

Afin d'illustrer ces conséquences financières, je me suis également tournée vers M. Rodmacq afin d'avoir un retour sur sa part sur le réel impact financier que peut avoir les cyberattaques aujourd'hui : encore une fois, ce sont des chiffres qui sont tenus secrets par la plupart des établissements bancaires, notamment à cause du risque d'image qui peut réellement impacter la confiance accordée en nos banques.



Rapport sur les risques - BPCE 2020

Notons, comme nous pouvons le voir sur l'illustration ci-dessous, que le risque opérationnel (dans lequel la cybercriminalité est inclue) représente 9% du poids du risque en 2020. Le risque majeur pour un établissement de crédit restant le risque de crédit.

b) En termes d'image

La banque est un domaine régit principalement par la confiance de la clientèle. La gestion des avoirs et du patrimoine de nos clients est une matrice prépondérante de notre métier et la cybercriminalité vient compromettre cette confiance établie depuis des années et qui est particulièrement fragile. Il est évident que les données chiffrées sont compliquées à obtenir à cause du risque d'image liées à l'aboutissement de ces cybers attaques.

Pour rappel, le risque d'image c'est la perte de confiance, de crédibilité ou de notoriété d'une banque auprès du marché et de sa clientèle à la suite d'un incident opérationnel qui pourraient ternir sa réputation et dès lors ses perspectives et ses futurs profits.

Dans le milieu bancaire, on se souvient tous de l'exemple de Jérôme Kerviel, un banquier qui en janvier 2008, à la suite d'une fraude interne particulièrement bien ficelée et qui a causé des pertes de marché records (environ 4,9 milliards d'euros). A l'époque, le PDG Daniel Bouton n'avait pas averti le président de la FED et avait fait une déclaration publique indiquant que J. Kerviel était un génie solitaire. Cette dissimulation et ce déni assumé publiquement ont entaché de manière significative la réputation et l'image de la Société Générale.

Dans le cadre d'une cyberattaque dans le milieu bancaire, il faut savoir que la réglementation porte un regard lourd sur la gestion du risque d'image, comme l'explique M. Rodmacq dans l'interview :

« A l'heure actuelle, parce que le préjudice d'image est énorme, et par suite de la réglementation RGPD, en cas de fuite de données, on est obligé de prévenir les concernés, si c'est une fuite de données massive on est obligé de prévenir par voie de presse et si c'est une petite faille de données, on prévient individuellement chaque client victime. Les lois en France font que, par exemple un organisme comme une banque ne peux pas cacher une fuite de données. Le système bancaire sont extrêmement précautionneux par rapport à leur sécurité informatique et on considère que la sécurité informatique est un risque majeur en termes de risque à long terme car le jour où nous avons une attaque qui fonctionne, ça peut nous coûter très cher. »

A noter également que si la fraude aboutie, les clients sont demandeurs d'une indemnisation à hauteur de leur préjudice, et qu'en cas de refus de la part de l'établissement bancaire, le client touché pour ternir l'image de la banque en relatant son histoire auprès de tiers, privés ou publics.

II) Conséquences pour le client professionnel

Les conséquences de ces cyberattaques sont plurielles :

- Une paralysie des systèmes : par suite d'une attaque, les entreprises se retrouvent paralyser dans le cadre du suivi de leur activité.

- Le vol ou la perte de données sensibles : les données constituent aujourd'hui une source d'agent notable dans le cadre du vol de la DATA et c'est parfois des années de sourcing qui disparaissent.

- La création de brèches dans un système de sécurité : une attaque aboutie met en évidence les failles d'un système de sécurité déjà en place et amène à une refonte complète de cette composante de l'entreprise pour améliorer sa sérénité et sa pérennité.

- L'exposition à un chantage (ransomware…) : une illustration de ransomware est proposée en détail dans la sous-partie ci-dessous. Un ransomware est un logiciel visant à demander une rançon à la suite de la prise en otage de données.

- L'atteinte à la réputation : c'est des relations de longues dates, avec des fournisseurs ou des clients, qui peuvent être mise à mal dans le cadre d'une cyber attaque.

- Un préjudice commercial : le vol de données sensibles peut avoir un impact sur le secteur concurrentiel dans lequel officie l'entreprise touchée, avec une dévalorisation de celle-ci ou une tétanie d'activité le temps de remettre sur pieds les différents logiciels de prévention aux risques.

a) Coûts directs : impact sur le CA

Outre des conséquences significatives pour les établissements bancaires, c'est également notre clientèle qui est directement affectée. Selon des procédés qui sont connus désormais, mais qui tendent à évoluer et à se renouveler constamment, on constate que l'impact sur le résultat d'une société touchée par une cyber attaque reste conséquent.

D'après l'étude menée par Euler Hermes, le leader européen de l'assurance fraude, et l'Association nationale des Directeurs Financiers et de Contrôle de Gestion (DFCG), sur plus de 200 entreprises implantées en France, 1 entreprise sur 3 a subi un préjudice supérieur à 10 000€ en 2019 et 10% des entreprises ont subi un préjudice supérieur à 100 000€ en 2019. De quoi fragiliser fortement la trésorerie des entreprises et dans certains cas compromettre une activité déjà impactée par la crise sanitaire subit depuis plus d'un an maintenant.

En parallèle, 1 entreprise sur 2 a vu ses partenaires commerciaux être victimes de fraudes en 2019 : le problème des cyberattaques est donc étendu à toutes les parties prenantes d'une société.

Afin d'illustrer davantage cette sous partie sur les conséquences financières, je parlerai du cas de la société Lise Charmel, fabriquant de lingerie française, qui a été mise en redressement judiciaire en février 2020.
Cette situation est liée en grande partie à une attaque d'un « rancongiciel »[7] en octobre 2019, soit 4 mois avant le redressement judicaire.
Tous les postes de travail et tous les fichiers se sont retrouvés pris en otage et cryptés. S'en est suivi une demande de rançon afin de pouvoir disposer de la clé de déchiffrement. Le directeur du groupe, Olivier Piqet, a indiqué que cette cyberattaque avait touché les 1 150 salariés du groupe, en France mais également à l'étranger.

La production ayant été complétement bloquée pendant un certain temps et le redémarrage ayant été très lent, les retards de livraison se sont accumulés au point

[7] Logiciel de rançon ou logiciel d'extorsion, logiciel malveillant qui prend en otage des données personnelles.

que la société eut été obligée de demander sa mise en redressement judiciaire afin de retrouver une certaine sérénité. L'impact sur le chiffre d'affaires de la société a été estimé à plusieurs millions d'euros de pertes.
A ce jour, peu d'informations sont disponibles concernant le redressement judiciaire de cette société, qui semble toujours de mise.

Toujours d'après l'étude menée par Eurler Hermes, il apparaît que plus de 7 entreprises sur 10 ont été victimes d'au moins une tentative de fraude sur l'année 2019. Ce qui est intéressant également, c'est que les entreprises ciblées le sont parfois plusieurs fois d'affilées (jusqu'à 5 fois !) et ce par les mêmes cybercriminels, jusqu'à ce que les systèmes de défense mis en place par l'entreprise cèdent.

En parallèle de cette perte sèche dans le cadre d'une extorsion de fonds ou de demande de rançon, il est également important de parler des autres types de couts directs auxquels on ne pense pas tout de suite :

- Le coût lié aux enquêtes techniques afin d'identifier et de tracer l'origine de la fraude
- Le coût lié aux mises en conformité réglementaires après la cyberattaque, à l'amélioration des dispositifs de cybersécurité et à la sécurisation des données clients post-incident.
- Les honoraires d'avocats et frais de justice
- Dans le cadre d'une politique transparente et d'une logique de remise en confiance, il convient également de notifier la fraude à chaque client de manière individualisée et personnalisée.

b) Les couts indirects et dégâts immatériels

A côté de la faille économique et financière dont est victime notre client à l'instant où la cyberattaque est opérée, il y toute une dimension liée aux coûts indirects et aux dégâts immatériels qui doit être prise en considération également.

- Augmentation des primes d'assurance et du coût de la dette

En plus de l'assurance responsabilité civile professionnelle dont doit être équipée la majorité de notre clientèle, des options d'assurances additionnelles peuvent être envisagées pour se prémunir du cyber risque. En cas d'attaque aboutie, on peut donc constater sur le court/moyen long terme, une augmentation des primes d'assurances.

Dans le cadre d'un financement mis en place pour pallier la perte de bénéfice engendrée par la cybercriminalité, l'entreprise touchée doit également faire face à une augmentation du coût de sa dette et de sa charge de remboursement.

- Érosion du chiffre d'affaires par suite de la perte de contrats clients

Après un vol ou un piratage de données informatiques, il est certain que les fichiers clients sont durablement impactés et parfois, certaines données ne sont jamais récupérées. C'est donc tout un travail qui part en fumée pour notre client professionnel, qui se doit de recréer une base de données client saine et durable.
Sur des devis en cours, c'est parfois plusieurs mois de contacts et de prospection clientèle qui se retrouve alternés.

- Dépréciation de l'image de la société

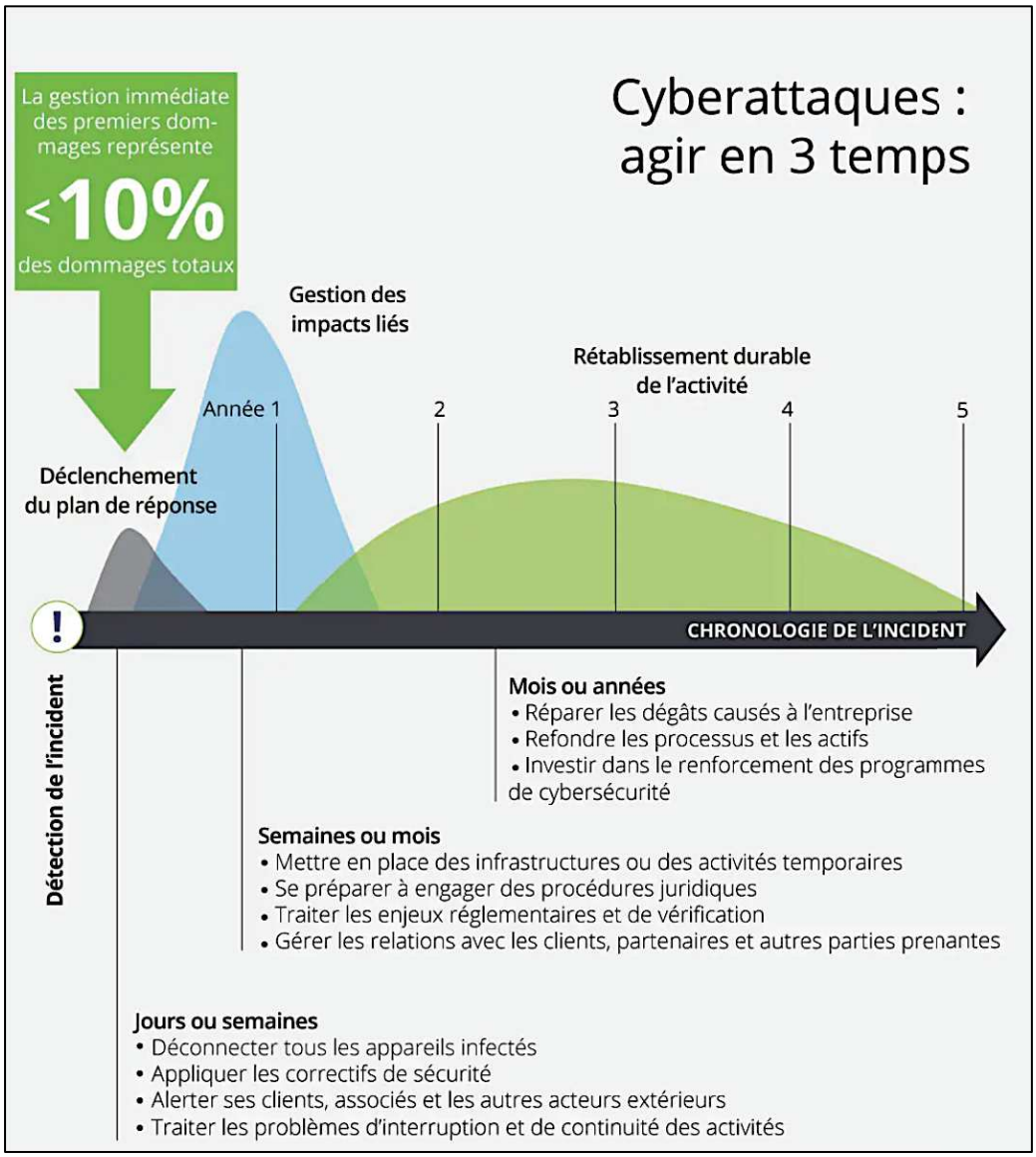
Le risque d'image : attenant aux établissements bancaires comme aux sociétés. La cybercriminalité a cette particularité d'affecter de manière plurielle et similaire les organisations touchées. Ici notamment, il est important de souligner le réel impact sur la réputation des sociétés touchées, du côté des fournisseurs comme des clients.

c) La durée de rétablissement

Il me parait également important d'ajouter un volet sur le temps nécessaire pour se remettre des conséquences d'une attaque.

Pour cela, j'utiliserai essentiellement l'analyse proposée par le cabinet Deloitte sur les cyberattaques qui, sous la forme du schéma ci-dessous, démontre clairement que la cybercriminalité à un impact sur le long terme pour nos entreprises.

Notons qu'en qualité de partie prenante dans la gestion des entreprises, la banque est généralement informée des attaques subies dans les 24 à 48H suivant l'opération frauduleuse en question.



Capture d'écran site Deloitte.fr

PARTIE 3 : QUELS MOYENS DE LUTTE ?

Même si elle est redoutable et en constante mouvance, la cybercriminalité fait aujourd'hui face à de nombreux moyens de lutte qui permettent tous de la limiter et d'y faire face.
En parallèle du cadre réglementaire et législatif, les banques se sont également dotées de moyens de lutte, à travers de nombreux outils d'équipements clients.

I) La réglementation française et européenne

a) Le cadre juridique et pénal

Les lois autour de la sécurité informatique et des données la composant se sont étoffés depuis le milieu du XXème siècle, pour arriver aujourd'hui à un cadre pénal stricte et adapté.

La première fois que la lutte contre la cybercriminalité est abordée au sein d'un texte de loi remonte à 1978, avec la loi informatique et libertés du 06 janvier.[8] On la retrouvera ensuite dans la loi Godfrain de 1988[9] sur la fraude informatique qui a permis de sanctionner la suppression et la modification des données, de même que les atteintes aux systèmes d'information.

Pour s'adapter à l'évolution constante des formes de cybercriminalité, beaucoup de lois ont ensuite été revues, complétées ou illustrées par des cas de jurisprudences qui faisaient état des principaux cas de cyber délinquances, comme la loi de 2001 relative à la sécurité quotidienne[10] et celle de 2003 sur la sécurité intérieure.[11]

[8] Loi n° 78-17 du 6 janvier 1978, *JORF*, 7 janvier 1978 (Légifrance).
[9] Loi n° 88-19 du 5 janvier 1988, JORF, 6 janvier 1988, p. 231
[10] Loi n° 2001-1062 du 15 novembre 2001, JORF, 16 novembre 2001
[11] Loi n° 2003-239 du 18 mars 2003, JORF, 19 mars 2003, p. 4761

Plus récemment, il convient également de mentionner celle du 13 novembre 2014, sur les dispositions relatives à la lutte contre le terrorisme et le vol des données informatiques[12] et la loi du 24 juillet 2015 relative au renseignement[13]

Comme le montre cette présentation non exhaustive, le cadre pénal autour de la cybercriminalité a été obligé d'évoluer avec les types d'infractions commises et le public touché. On note également un besoin de s'adapter aux supports affectés par les cybers attaques, ce qui amène de facto à un renouvellement constant du cadre juridique et pénal autour de ce thème.

Dans mon travail de recherche, j'ai également pu constater la création d'une agence nationale en 2009 par l'État français, appelée l'ANSSI : l'agence nationale de la sécurité des systèmes d'informations.
Celle-ci s'est spécialisée dans la formation, l'accompagnement et les campagnes de communication autour de la cybercriminalité française. En 2020 et à la suite de la crise financière, le report annuel d'activité de l'agence était sans appels : le COVID 19 a fragilisé les structures françaises et une hausse considérable des rançon logiciels a été observée. Au 31/12/2020, l'ANSSI a donc dénombré par moins de 192 signalements avec ce type de méthode.

Tous ces paramètres sont évidements appliqués au sein de nos établissements bancaires respectifs, dans un souci d'harmonisation du cadre légal, juridique et pénal autour de la cybercriminalité et ses conséquences.

Au travers de mes recherches, j'ai pu constater que les lois sont rarement énoncées dans la documentation interne car elles sont prépondérantes et en constante évolution.

[12] Loi n° 2014-1353 du 13 novembre 2014, JORF, 14 novembre 2014, p. 19162 ; E. Chauvin et F. Vadillo, « Quand la lutte anti-terroriste fait évoluer la notion de vol : les modifications de l'article 323-3 du Code pénal introduites par l'article 16 de la loi du 13 novembre 2014 », Gaz. Pal., 15-16 avril 2015, pp. 6-8.

[13] Loi n° 2015-912 du 24 juillet 2015, JORF, n° 171, 26 juillet 2015, p. 12 735.

b) Le RGPD

Pour donner suite à l'évolution constante des outils numériques et informatique, l'année 2018 a vu naître le Règlement Général sur la protection des données personnelles (RGPD).

La CNIL (la Commission nationale de l'informatique et des libertés) définit le RGPD comme suit :

« Le RGPD encadre le traitement des données personnelles sur le territoire de l'Union européenne. Le contexte juridique s'adapte pour suivre les évolutions des technologies et de nos sociétés (usages accrus du numérique, développement du commerce en ligne…). Ce nouveau règlement européen s'inscrit dans la continuité de la Loi française Informatique et Libertés de 1978 et renforce le contrôle par les citoyens de l'utilisation qui peut être faite des données les concernant.
Il harmonise les règles en Europe en offrant un cadre juridique unique aux professionnels. Il permet de développer leurs activités numériques au sein de l'UE en se fondant sur la confiance des utilisateurs. »[14]

Le RGPD a considérablement impacté le traitement de l'information et des données informatique, et le secteur bancaire n'a été aucunement laissé pour compte.
Les données bancaires de nos clients sont considérées comme des données sensibles, c'est-à-dire « des données qui révèlent la prétendue origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale d'un individu »[15].

Ainsi, le traitement de celles-ci s'est entièrement renforcé et a permis une amélioration des droits gravitant autour de la protection des données personnelles des clients bancaires, le RGPD ayant imposé le renforcement des mesures de sécurité mises en place par les banques pour la collecte et le stockage de ces données.

[14] https://www.cnil.fr/fr/rgpd-de-quoi-parle-t-on
[15] https://www.cnil.fr/fr/definition/donnee-sensible

Dans le cadre de la lutte contre la cybercriminalité bancaire, l'impact du RGPD est à ce jour difficilement mesurable et aucune étude à ce jour témoigne des conséquences, positives ou non, de cette nouvelle réglementation.

Néanmoins, étant donné le renforcement de la sécurité dans le stockage des données personnelles des clients, il y a fort à parier que les conséquences de ce règlement soient globalement positives.

c) DSP

En parallèle et dans un souci de renforcement de la sécurité de l'information et des systèmes de paiements, la seconde directive européenne sur les services de paiement (DSP2) est entrée en vigueur le 13 janvier 2018.
Dans un souci de contextualisation, il convient d'expliquer DSP1 pour comprendre la nécessité de l'évolution vers DSP2.

- **DSP1**

La DSP 1 (Directive sur les Services de Paiement 1) a été conçue par l'Union européenne pour réglementer les services de paiement.
Cette réglementation concerne tous les États membres de l'UE ainsi que l'Espace économique européen (EEE). Elle est entrée en vigueur en décembre 2009 avec un objectif : encourager la concurrence entre banques/prestataires en Europe, afin de proposer de meilleurs services, et ainsi protéger les consommateurs.

Plusieurs améliorations notables sont nées de cette directive : la sécurité des paiements en ligne a été renforcée, le statut de prestataire de service de paiements a été encadré et la zone unique de paiement SEPA a vu le jour, pour harmoniser et réduire le coût des virements et des prélèvements automatiques en UE et dans l'EE.

Arrivée en 2009 et compte tenu de l'évolution constante des systèmes informatiques et des plateformes de paiements, la DSP 2 a été proposée en 2018, pour combler les failles de la DSP1, notamment sur l'identification des clients au moment d'une

transaction, jugée trop faible car trop simple (un simple mot de passe sur une application)

- **DSP2**

Pour donner suite à ces lacunes identifiées, la DSP2 est entrée en vigueur en 2018 et se base notamment sur un point prépondérant : une authentification forte, également appelée authentification multi-facteurs, avec un moins deux des trois preuves suivantes :

- Une information connue de l'interlocuteur seul (l'habituel mot de passe, la réponse à une question secrète, etc.) ;
- La reconnaissance d'un équipement électronique appartenant à l'utilisateur (smartphone, ordinateur, clé USB, carte à puce, carte magnétique, certificat électronique, etc.) ;
- La biométrie physique ou comportementale de l'utilisateur, via un trait unique à chaque individu (empreinte digitale, scan rétinien, reconnaissance vocale ou faciale, etc.).

Au sein d'une agence bancaire à compter de 2019, j'ai pu apprécier la mise en place de cette nouvelle directive auprès de notre clientèle particulière et professionnelle.
Des campagnes de communication et de sensibilisation ont été menées sur les espaces internet et les applications de nos clients.

Pour les clients professionnels, le changement a opéré à compter de juillet 2020 avec un temps fort en octobre 2020 avec la mise en place de l'authentification forte via l'envoi d'un code de sécurité à usage unique et en novembre 2020 avec l'ajout d'un outil informatique « de confiance » pour identifier les clients au moment du paiement sur internet.

Quel est réellement l'impact de cette directive à ce jour ? Comme pour le RGPD, il est difficile d'avoir des chiffres cohérents aujourd'hui, après seulement 6 mois de mise en place. Néanmoins, je constate qu'en agence les fraudes sur internet sont moins fréquentes : les identifications à deux facteurs ont permis de renforcer la sécurité sur les achats internet et les professionnels ont pu sécuriser leur opération également.

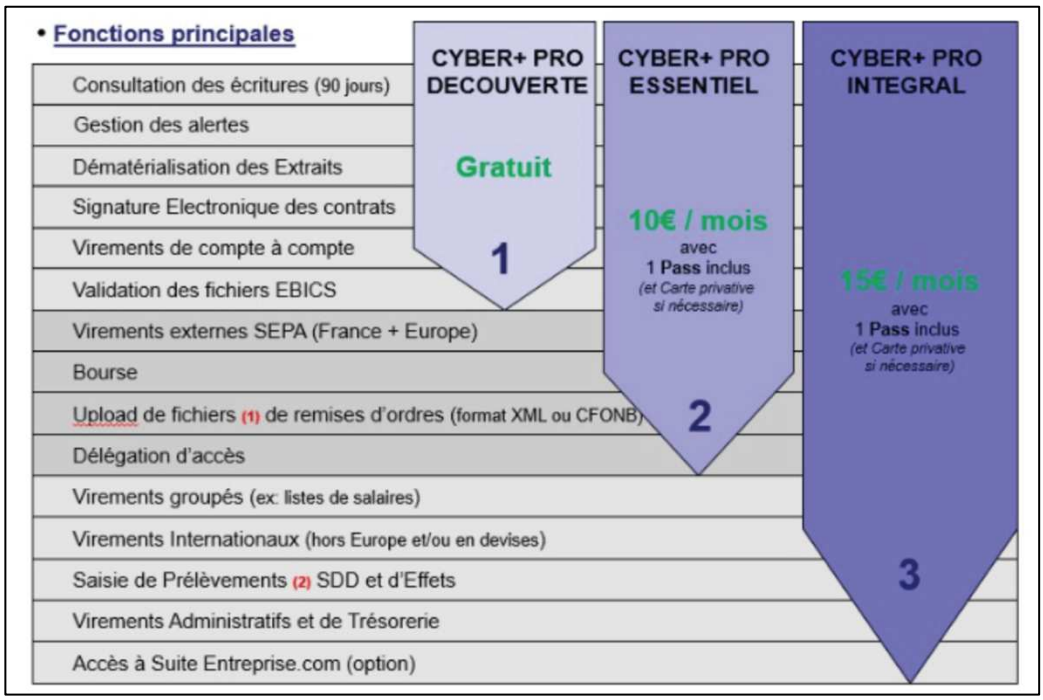
II) Les outils bancaires

a) Les outils digitaux

Les applications bancaires qui sont aujourd'hui mises à la disposition des clients professionnels sont de plus en plus complètes et le critère de sécurité et l'un des plus importants, si ce n'est le plus important !

Véritable levier à l'autonomie dans la gestion de ses comptes et de ses paiements, le professionnel d'aujourd'hui requiert, en plus d'un conseiller proactif et disponible, un outil digital qualitatif, intuitif et sécurisé.

A la BPALC, nous disposons de l'application Cyberplus Pro, décomposée en plusieurs formules comme suit :



Documentation interne BPALC

Dans un souci de sécurité et de lutte contre la fraude externe, les opérations de virements ont été plafonnées à 50k€ par virement, 100k€ par jour et 250k€ sur 30 jours calendaires.

De plus, depuis la DSP, l'application a renforcé la connexion sécurisée et a mis en place des actions d'identifications supplémentaires :

- Le PassCyberplus : un boitier sécurisé qui génère un code unique afin de valider les opérations sensibles
- Le Securpass Pro : associé à une CB, il permet de valider l'enrôlement d'un appareil mobile
- Le sms : utilisé en mode secours s'il y a un oubli du Pass.

Ces 4 outils d'authentification sont attribués à une personne physique : le professionnel en tant qu'EI ou alors une personne agissant pour le compte d'une entreprise (souvent le dirigeant de la société).

Réunis autour du pro dans sa gestion de la banque à distance, ces outils permettent de lutter efficacement contre la fraude en permettant de cumuler plusieurs moyens d'authentifications forts pour le professionnel et d'éviter les piratages de codes répétitifs par des techniques comme le phishing par exemple.

b) Les assurances

Couplée à une assurance multirisques professionnels comme option ou en contrat d'assurance à part entière, ces dernières années ont vu naitre une nouvelle forme de contrat d'assurance : l'assurance contre les risques de fraude.

N'ayant pas ce type d'offre à la BPALC, je me suis tournée vers la firme SMA Assurance qui, via sous contrat VIGIPRO, assure les entreprises et les professionnels contre les conséquences de la fraude et des actes de malveillance (escroquerie, abus de confiance, faux et usage de faux, atteinte aux systèmes d'information).

On retrouve une prise en charge des différents frais pouvant impacter l'entreprise lors d'une fraude, interne ou externe :

- les pertes financières directes ou indirectes, y compris les frais supplémentaires d'exploitation,
- les frais de recours,
- les frais et les honoraires d'experts,
- les frais de reconstitution originale des systèmes d'information,
- les frais de récupération et de remise en état des biens assurés[16]

La primes d'assurances sont calculées en fonction du chiffre d'affaires et de la taille de l'entreprise. Néanmoins, celle-ci ne peuvent être déduites du résultat fiscal (à l'inverse d'une assurance Homme Clé par exemple)

c) La formation des chargés de clientèle professionnelle

C'est un élément qui est revenu maintes et maintes fois dans notre échange avec M. RODMACQ, coordinateur de la fraude externe au sein de la BPALC, comme il le souligne ci-dessous :

« Je dispose de formations particulières en qualité de coordinateur de la fraude, mais pour moi il reste encore un énorme travail de sensibilisation à faire autour de la cybercriminalité et de la fraude en général. Les jeunes collaborateurs qui entrent sont formés d'une façon générale sur le risque opérationnel et en particulier sur la fraude. Moi ce que j'aimerai en tant que coordinateur de la fraude externe, c'est qu'il y a des modules réguliers. Le réseau est demandeur qui plus est ! »

La formation des CCPRO aux risques opérationnels est un élément essentiel pour contrer la hausse de la cybercriminalité, avec une notion importante de sensibilisation : identifier les risques, présenter les conséquences, développer et apprendre les techniques pour contrer les attaques cyber.
Il est important également de bénéficier de formations complètes et régulières, car, comme souligné plusieurs fois dans ce mémoire, la fraude s'adapte très rapidement aux nouveaux outils et aux réglementations mis en place au fil des ans.

[16] https://www.groupe-sma.fr/SGM/jcms/jizhprod_70458/fr/assurance-contre-les-risques-de-fraude

Aussi, des conseillers bien formés sont vecteurs de communication et de formation auprès de leur clientèle : apprendre à nos dirigeants d'entreprises à se méfier, se protéger, expliquer nos outils afin qu'ils puissent les intégrer et les utiliser à bon escient.

Conclusion

En France et plus largement dans le monde au cours des dernières années, la cybercrimalité a fragilisé tous types de structures : des collectivités, des services d'États, des entreprises, des professionnels, des particuliers et des banques.

Cette nouvelle forme d'attaque, qui démontre une capacité remarquable d'adaptation aux nouvelles technologies et aux nouveaux outils digitaux, est lourde de conséquences et peut avoir des impacts financiers importants pour les acteurs économiques touchés.

Il est aujourd'hui crucial de considérer ce risque comme majeur étant donné l'essor de la digitalisation : à la fois indispensable pour développer une activité et accroître sa rentabilité, c'est également devenu une véritable porte d'entrée pour les cybercriminels qui n'hésitent pas à passer toutes les barrières de sécurité pour arriver à leur fin.

Le domaine bancaire n'est pas épargné : véritable mine de données sensibles et de fonds diversifiés, il est une cible de choix pour les cybercriminels et se doit d'intensifier et de renforcer sa sécurité de manière perpétuelle.

Pour contrer ces attaques, plusieurs armes : un cadre légal et juridique harmonisé et évolutif et des outils bancaires et d'assurances.

Ce qui pose la question suivante : n'y a t-il pas un impact positif à la cybercriminalité ? Peut-elle permettre le développement commercial d'un établissement bancaire et si oui dans quelle mesure ? Comment un professionnel attaqué aujourd'hui peut-il devenir infaillible demain ?

En somme, ce mémoire a permis de démontrer l'impact réel des attaques digitalisées aujourd'hui et de réfléchir à la meilleure manière de les contrer, d'un point de vue professionnel et bancaire, le tout dans une logique d'accompagnement et de protection quotidienne.

Bibliographie

Ouvrages :

- A. Chapelle **, Gestion des risques opérationnels, guide des meilleures pratiques en banque et assurance,** 2020
- JL Siruguet, E. Fernandez, L. KOESSLER **, Le contrôle interne bancaire et la fraude**, 2006
- B. Perreira, **La lutte contre la cybercriminalité : de l'abondance de la norme à sa perfectibilité**, 2016
- M. Kohlmann, **La Cybercriminalité**, 2016

Articles et rapports :

Arnaud Lefèvre, **Parole d'expert - Étude Fraude 2021** , Article Option Finance, 2021

Zhanna Malekos Smith and Eugenia Lostri James A. Lewis **The Hidden Costs of Cybercrime,** rapport Macfee.

Jean-Louis DI Giovanni, **PwC's Global Economic Crime and Fraud Survey,** 2020

Webographie :*

Serge Braudo , Dictionnaire de droit privé, définition de la fraude
https://www.dictionnaire-juridique.com/definition/fraude.php

Paul Manuel Hilario, Les fraudes bancaires en France - Faits et chiffres
https://fr.statista.com/themes/3222/les-fraudes-bancaires-en-france/#dossierSummary

Ariane Beky, Cybercriminalité : un coût élevé pour l'économie mondiale, 2020
https://www.silicon.fr/cybercriminalite-cout-economie-mondiale-352969.html#

Philippe Trouchaud, Cybersécurité : comment limiter les risques face au COVID-19 ?
https://www.pwc.fr/fr/expertises/gestion-des-risques/gestion-de-crise/covid-19/comment-gerer-l-impact-du-covid-19-sur-la-cybersecurite.html

Définitions cyber du dictionnaire le Robert
https://dictionnaire.lerobert.com/definition/cyber

Définition criminalité dictionnaire le Robert
https://dictionnaire.lerobert.com/definition/criminalite

Laurent Dufour, Trésorerie D'entreprise : Les Différents Moyens De Paiement, 2020
https://www.leblogdudirigeant.com/fiche-pratique-tresorerie-dentreprise-differents-moyens-de-reglement/

Cybersécurité : des signalements plus nombreux en 2020 , 2021
https://www.vie-publique.fr/en-bref/279580-cybersecurite-hausse-des-actes-de-piratage-informatique-en-2020

Pierre Ropert, Histoires d'arnaques : du mail du prince nigérian aux "lettres de Jérusalem", 2018
https://www.franceculture.fr/histoire/avant-les-mails-de-princes-nigerians-au-xviiieme-siecle-larnaque-aux-lettres-de-jerusalem

Benoit Danton, Etude : Les Français soulignent leur confiance dans leurs banques, 2021
http://www.fbf.fr/fr/espace-presse/communiques/etude---les-francais-soulignent-leur-confiance-dans-leurs-banques

Eric Vernié, Fraude au président : la crise sanitaire a déclenché une nouvelle vague d'attaques, 2021
https://theconversation.com/fraude-au-president-la-crise-sanitaire-a-declenche-une-nouvelle-vague-dattaques-153013

David, Faillites de PME après une cyberattaque : ce n'est pas une légende, 2020
https://www.oppens.fr/faillite-pme-cyberattaque-lise-charmel/

Plus de 7 entreprises sur 10 ont subi au moins une tentative de fraude cette année, 2020
https://www.eulerhermes.fr/actualites/etude-fraude-2020.html

Cyberattaques : comment chiffrer les impacts ?
https://www2.deloitte.com/fr/fr/pages/risque-compliance-et-controle-interne/articles/cyberattaques-chiffrer-les-impacts.html

Définition donnée sensible par la CNIL
https://www.cnil.fr/fr/definition/donnee-sensible

Quel est l'imapact du RGPD pour les banques ?
https://donnees-rgpd.fr/donnees-sensibles/impact-rgpd-banques/

Héléne Touchkov, De la DSP 1 à la DSP2 : comment évolue la sécurité de vos transactions ?
https://www.certeurope.fr/blog/de-la-dsp-1-a-la-dsp2-comment-evolue-la-securite-de-vos-transactions/

DSP2 : une sécurité renforcée pour vos opérations bancaires en ligne, 2020
https://www.bforbank.com/mag/tendances/dsp2-securite-renforcee-pour-operations-bancaires-en-ligne.html

Assurance contre les risques de fraude, VIGIPRO
https://www.groupe-sma.fr/SGM/jcms/jizhprod_70458/fr/assurance-contre-les-risques-de-fraude

**Liens triés par ordre d'utilisation et de citation dans le mémoire*

ANNEXE

RETRANSCRIPTION INTERVIEW THIERRY RODMACQ

Coordination fraude externe – Risques opérationnels

Vendredi 28 mai 2021

Bonjour Thierry et merci pour ce temps d'échange dans le cadre de mon mémoire de fin d'étude. Avant tout, pouvez-vous vous présenter en quelques mots ? Quel poste occupez-vous et depuis combien de temps ? Avez-vous une spécialité ?

J'occupe le poste de responsable de la coordination sur le pôle de la fraude externe. J'occupe ce poste depuis sa création, c'est le groupe qui a créé une filière coordination de la fraude, donc je suis le premier coordinateur de cette nouvelle filière depuis 2 ans maintenant. Cette filière dépends elle d'un service plus important, avec de multiples activités, notamment le SSI, la sécurité système d'information géré par M Thierry Gicquel, qui s'occupe également de la cyber sécurité : on se partage un peu les tâches ! Il y a le service des risques opérationnels, tenu par M Vincent Martin, à savoir que moi je fais 20% de risque opérationnel dans mon emploi du temps. Il y a aussi le service CNIL, SSI et RGPD (protection des données), tenu par Philippe Évrard.
Dans le service dans lequel je suis, il y a aussi une rubrique « plan de continuité d'activité »

Et en quoi consiste cette rubrique exactement ?

Le plan de continuité d'activité fini consiste à comment définir, en cas de crise, les problématiques de continuité du métier : il y a ce qu'on appelle des plans de continuité métiers, par exemple s'il y a une crise demain, comme un incendie au siège, quelles sont les activités prioritaires, quels les moyens de communication, etc… Il y a tout un plan de gestion de crise, géré par le PCA qui ont également un rôle de coordination quelque part, parce que les responsables des plans de continuité c'est avant tout les métiers. Le tout coordonnée par cette cellule de crise et gestion de cellule de crise également au sein de notre service.

Quelle différence faites-vous entre de la fraude interne et la fraude externe ?

Avant la création de la filière de la coordination fraude externe, celle-ci était gérée par les mêmes personnes qui gèrent la fraude interne.
La fraude interne est principalement liée au défaut de procédure, provoqué par les employés et qui touche au risque opérationnel. Le risque opérationnel, c'est l'ensemble des pertes ou provisions engendré par un dysfonctionnement d'un certain nombre de processus qui sont classés par le régulateur, ce qu'on appelle les 7 catégories bâloises. Dans ces 7 catégories bâloise « risques opérationnels », on trouve la fraude externe, on trouve la fraude interne, on trouve ce qu'on appelle les dysfonctionnements des processus, le défaut de conseil, les problèmes de dysfonctionnement informatique, le dommage aux biens et aux personnes, etc…
En bref : tout ce qui n'est pas du risque de crédit pur au niveau des banques.
La frontière est mince entre les deux, c'est-à-dire qu'en fraude externe par exemple, lors d'un piratage de la boîte mail d'un client avec l'envoi d'une demande de virement par mail, on est sur de la fraude externe. Mais la procédure veut que l'employé de banque fasse un contre-appel au titre de

de l'opération, si cet employé ne le fait pas, on a aussi quelque part de la fraude interne du fait qu'il y n'y a pas eu le suivi des procédures.
Les frontières sont faibles et c'est au cœur de votre mémoire : quand on parle de cybercriminalité, on en vient très vite à la frontière entre de la fraude traditionnelle et de la faute qui intègre la cyber technologie.
Nous avons décidé de bien distinguer la fraude externe de la fraude interne par suite d'une recrudescence des fraudes et justement cette problématique de bien différencier fraude interne et fraude externe. S'en est suivi une réglementation, une législation, des moyens humains, de l'organisation du service.

Comment est composée l'équipe qui gère la fraude externe au sein de la BPALC ?

Nous sommes divisés en métiers : un métier autour des chèques, autour du multimédia … et le coordinateur lui est là pour faire parler ces gens-là. La coordination n'est pas là pour faire de la production. Disons que je suis moteur dans la mise en œuvre de plans d'action, pour pouvoir mettre en place des protocoles de lutte contre la fraude. Je suis aussi moteur dans la sensibilisation.

Avez-vous observé une recrudescence de cette cybercriminalité au cours des dernières années ?

Aujourd'hui l'attaque cyber va passer par de la manipulation, voire de l'intimidation. Tout l'intérêt d'une coordination. On peut également avoir des menaces à distance, pour qu'une personne sorte des fonds, des choses comme ça. Il faut dire que c'est beaucoup plus intéressant pour des fraudeurs d'utiliser des moyens cyber aujourd'hui, que d'utiliser des fraudes de types classiques.
Avec de la cybercriminalité, vous risquez peut-être 2 ans de prison et 30 000€ d'amende. Les peines encourues sont assez faibles ! Les criminels agissent à distance, ils se sentent relativement impunis. Il y a un appel d'air important sur la cybercriminalité.

Diriez-vous que la cybercriminalité a accompagné la digitalisation des opérations ?

La volonté des banques aujourd'hui c'est que le client travaille de plus en « *selfcare* », donc on va être sur des scénarios plus techniques en rapport aux outils. Les fraudeurs se sont adaptés aux nouvelles technologies parce que c'est une adaptation permanente.
Le dernier exemple en date, cette semaine par exemple, le fraudeur a appelé notre cliente, il a joué sur la peur en se faisant passer pour le service BP, lui disant qu'il y'a une attaque informatique sur son profil, un piratage de son compte et qu'elle va recevoir un numéro par SMS qu'il faudra lui ensuite lui donner pour sécuriser son système … ce qu'il se passait réellement c'est que le fraudeur était en train de changer le mot de passe sécurisé de notre cliente, donc il avait son smartphone, il changeait le mot de passe sécurisé et l'échange de SMS c'était pour valider le changement de mot de passe. Avec ce code sms, le fraudeur a pu prendre la main sur l'espace cyber du client et a commencé à faire des virements depuis le compte épargne sur le compte chèque et a tenté de faire un virement de 15 000€. La cliente, du fait qu'il y a des codes SMS qui signalent des changements de mot de passe, a vu les virements et a eu la présence d'esprit de contacter notre service client et nous avons pu tout bloquer in extremis.
On est typiquement dans un exemple de manipulation, pour rentrer dans le cyber du client, faire un virement mais aussi une connaissance parfaite des outils ! Toutes les applications mobiles qu'on peut avoir, les fraudeurs les connaissent parfaitement et ça toutes banques confondues. Le fraudeur va utiliser un mixte entre le fait de rentrer dans le système, car il avait accès au numéro de carte de la cliente, il avait également le numéro d'abonné… Il avait quand même déjà un certain nombre de données, certainement achetées sur le darkweb. Il est donc parti d'un fichier, qui lui a fait l'objet d'une fraude cyber pure, c'est à dire qu'il y a des gens qui vont se spécialiser dans l'attaque qui consiste à pirater des sites ou des choses comme ça, et qui revendent les fichiers sur le darkweb.

Certains fraudeurs sont spécialisés dans la récupération de data, qu'ils revendent ensuite et qui sont achetés par les cybercriminels.
L'exemple des 15 000€ c'est un bon exemple de récupération de data, par l'attaque cyber et ensuite de la manipulation, tout en manipulant un support smartphone avec une appli mobile sur smartphone.
Tout est fait à distance, les numéros de téléphone en général sont issus de cartes prépayées, les adresses IP passent sous VPN, c'est-à-dire par les serveurs intermédiaires donc c'est très difficile de tracer le la personne. Les montants ne sont pas si considérables et la police ne va pas forcément passer énormément de temps et n'a pas forcément la compétence de traquer ce genre de personne. Il y a donc un sentiment d'impunité de la part des fraudeurs aujourd'hui, qui officient principalement dans des petits cas pour être moins recherchés.

Vous pensez que la banque en particulier est principalement touchée par ce type de d'attaque de vol de données et de manipulation ?

A l'heure actuelle, parce que le préjudice d'image est énorme, et par suite de la réglementation RGPD, en cas de fuite de données, on est obligé de prévenir les concernés, si c'est une fuite de données massive on est obligé de prévenir par voie de presse et si c'est une petite faille de données, on prévient individuellement chaque client victime. Les lois en France font que, par exemple un organisme comme une banque ne peux pas cacher une fuite de données. Le système bancaire sont extrêmement précautionneux par rapport à leur sécurité informatique et on considère que la sécurité informatique est un risque majeur en termes de risque à long terme car le jour où nous avons une attaque qui fonctionne, ça peut nous coûter très cher.
Le risque cybercriminel est un risque majeur au sein de la banque, il faut partir sur le fait que nous sommes vulnérables. C'est vraiment le sens de la lutte contre les fuites informatique !
Celle-ci peut arriver aussi par le biais des prestataires, c'est à dire que la banque travaille avec de multiples prestataires (traitement de chèques, distributeurs, …) et le la sécurité informatique de ces prestataires est soumise à des cahiers des charges. Un pirate peut aussi passer par un prestataire pour remonter jusqu'à nous.

Qu'est-ce qu'il peut y avoir justement par exemple dans ce cahier des charges ?

Concrètement quand il y a un nouveau prestataire qui arrive, il va y avoir une analyse de risque sur l'intégrité des systèmes, ce qu'on appelle le DICP (disponibilité, intégrité, confidentialité, preuves) Ces analyses de sécurité informatique qui sont faites et qui sont demandées à chaque prestataires.

Avez-vous observé une corrélation entre hausse de la fraude et crise du COVID 19 ? Si oui, que pensez-vous de cette corrélation ?

Oui, une légère augmentation de fraude par rapport à l'année dernière. On peut dire que la fraude s'est adaptée ! On a eu des scénarios typiques COVID, c'est à dire des fraudes sur les masques, sur le matériel médical, sur les primes COVIDS, le fraudeur se sert de l'actualité. Il profite également du télétravail pour essayer de tester nos systèmes de sécurité de télétravail, …
Notons également un peu plus de fraude au président, comme les entreprises sont désorganisées, on se fait passer pour un président pour faire un virement. La conclusion à en tirer c'est vraiment cette capacité d'adaptation du fraudeur. Il sait s'adapter en permanence !

Avez-vous observé des fraudes sur des PGE par exemple ?

Je n'ai pas eu de cas qui est remontés. J'ai vu en revanche de la fraude à la prime COVID

Le fraudeur avait fait une demande de prime, se l'ai faite virer sur le client et après il a tenté de récupérer la prime on se faisant passer pour les impôts, en indiquant une erreur. C'est un scénario très bien élaboré, on revient sur tout ce qui était manipulation et toutes ces choses-là.
La cyberattaque pure reste rare, elle est toujours associée de près ou de loin à de la manipulation. Le mail de phishing par exemple, on a bien amené la personne à cliquer sur un lien avant la fraude réelle. Les techniques de manipulation et de tromperie sont toujours présentes à un moment ou un autre dans une fraude.
Quelles sont aujourd'hui les méthodes les plus utilisées selon vous ?

Il y a une phase de récupération de données, une phase de manipulation et une phase de rapatriement. On peut on peut définir les méthodes en 3 temps. On récupère de la data par tous les moyens possibles, ce qui est de la cybercriminalité brute, on manipule et ensuite il faut qu'on arrive à amener l'argent dans des paradis. Les techniques ce sont de faire rebondir les fonds de compte on compte, pour les amener dans un dans un pays sanctuariser. Parfois les fonds arrivent en Chine on ne peut plus rien faire d'accord. Il suffit d'amener les fonds dans des pays où il n'y a pas de coopération (…). On est vraiment dans une organisation avec plusieurs intervenants avec de la spécialisation efficace.
On observe aussi une hausse de la fraude aux faux placements : les fraudeurs proposent des placements qui soit ne génèrent pas d'intérêts, soit qui en génèrent mais qui sont récupérés par la suite par les fraudeurs, selon un système de pyramide de Ponzi.

Ce qui rends la recherche des fraudeurs encore plus complexe je pense ?

Oui c'est certain, il faut être capable de remonter toutes les filières !
Il y a quelques filières aussi qui sont spécialisés au niveau de la police, ils vont se spécialiser dans les grosses arnaques. On a quand même des filières policières en France qui savent faire et qui savent remonter les filières. L'un des principaux moyens pour lutter contre la fraude reste la sensibilisation. Il faut sensibiliser les gens, il faudrait presque faire des cours dans les écoles pour apprendre aux jeunes générations à faire attention à leurs données personnelles ! Les récentes statistiques montrent qu'une entreprise sur deux en France a été victime de fraude. La fraude est aujourd'hui totalement sous-estimée en France par les entreprises. La notion de fraude n'est pas évidente à définir qui plus est,

Quelles conséquences financières et en termes d'image pour la BPALC ?

Je ne vais pas pouvoir vous communiquer les chiffres exacts de la fraude à la BPCE.
Les chiffres de la fraude, sur la partie fraude globale, en termes de risque opérationnels, sont publiés mais le détail n'est pas publié. La fraude est devenue le premier risque opérationnel de la banque : c'est à dire que quand on compare les risques opérationnels via les 7 catégories bâloises dont nous avons parlé, la fraude représente le premier des risques opérationnels, devant le défaut de conseil ou devant des problématiques de perte de documents.

Cela explique en partie la mobilisation d'une équipe complète de la gestion de cette typologie de risque ?

Au niveau bancaire, le risque numéro un reste le risque de crédit. Les risques opérationnels globaux ne représentent que 10% des risques
C'est donc une chose qu'on prend très au sérieux. Sur l'année 2020, on est sur 2 millions d'euros de fraude globale, et en fraude brute, c'est-à-dire en fraude brute, on était 11 millions. À la BPLAC, on est sur 1000 fraudes réussies, hors fraude à la CB (qui est la fraude la plus commune) sur l'exercice 2020.

Il y a également un risque d'image autour de ce type de fraude, par exemple avec une fraude au président, quelqu'un qui se fait passer pour un faux président de l'entreprise et qui va faire un virement à l'étranger de 100 000€ par exemple, même si le la banque elle ne va pas être cherché en responsabilité, le client va quand même toujours avoir une forme de suspicion vis-à-vis de la banque qui aurait dû voir ou repérer que l'opération était atypique.

Il peut aussi reprocher à la banque ne pas l'avoir suffisamment sensibilisé sur le risque de fraude ! Il y a aussi un risque que l'entreprise se trouve en difficulté financière à cause de cette fraude.
Il y a toujours un peu une tentation de se retourner contre la banque et de considérer que la banque aurait dû faire preuve de plus de diligence.
Les clients ont aujourd'hui besoin d'être rassurés dans le sens est ce que les outils de la banque sont suffisamment sécurisés. On doit renforcer la communication et la sensibilisation, expliquer aux clients les risques, lui donner des conseils, ...
Leur indiquer par exemple que jamais un technicien de la banque va vous appeler pour vous demander vos codes, y compris dans le cadre des entretiens
Dans une autre mesure, je travaille aujourd'hui avec la direction commerciale, pour leur expliquer les scénarios de fraudes afin qu'ils optimisent leur communication et leurs propositions commerciales.

A quelles conséquences pensez-vous pour un client professionnel ? Peut-il y avoir des conséquences significatives sur son chiffre d'affaires ? Quels impacts à court / moyen terme ?

Une fraude bien opérée peut clairement amener à une faillite du professionnel.
Moi personnellement je n'en ai jamais rencontré, mais il y a des cas.
Il y a eu il y a peu de temps une fraude sur un cabinet comptable de 15M€ à travers une fraude au président. (Article dans les annexes). On voit que ce cabinet justement s'est retourné contre la banque à la suite de cette fraude au président ! L'association l'implique dans un manque de vigilance et de défaillance d'une des employés. Le législateur peut considérer que c'est à la banque de surveiller les flux. Si l'opération est passée par l'agence ça nous est déjà arrivé de devoir payer des fraudes au président. Devant un juge, ce sera à la banque de prouver que le client a été négligent. La charge de la preuve revient toujours à la banque. Ça serait à nous de prouver que le client a donné ses codes par suite d'une manipulation. Sur ce cas de fraude par exemple, on voit que ce sont des individus qui ont réussi à prendre possession de l'ordinateur donc là on est bien dans la cyberattaque, auprès d'une comptable en télétravail. On est en même temps sur la cybercriminalité et de la manipulation

La réglementation actuelle, française et européenne, a permis de renforcer la protection des clients bancaires, pro comme particulier. Pensez-vous que cette réglementation est suffisante ? Comment pourrait-elle être encore améliorée ?

Il y a toute la réglementation bâloise et la fameuse DSP2, qui nous obligent, notamment au niveau des cartes mais aussi avec les commerçants, à procéder à de l'identification forte à 2 facteurs.
Et aujourd'hui, pour contrer cette double authentification, les fraudeurs rentrent dans des procédés de manipulations toujours plus complexes et aboutis.

A titre informatif, nous sommes obligés de déclarer tous les ans les cas de fraudes sur chèques, virement, etc que nous avons eues à la Banque de France.
On se doit de respecter des ratios de fraude également et on peut être imputés de sanctions.
Si si par exemple on commence à voir une augmentation de fraude anormale, la Banque de France peut par exemple contrainte à augmenter nos barrières de sécurité.
Si on remarque une augmentation des fraudes sur CB, on peut également être pénalisés par le réseau Visa ou Mastercard pour défaut de vigilance sur les comptes ouverts.

Au niveau BPALC, plusieurs moyens sont mis en place pour protéger nos clients (securpass, securipro, DSP2, …). Que pensez-vous de ceux-ci ? Que pensez-vous de la formation des CCPRO sur la fraude ?

Alors déjà en termes d'effectif sur notre département pour lutter contre la fraude nous ne sommes pas assez. Je dispose effectivement de formations particulières, mais pour moi il reste encore un énorme travail de sensibilisation à faire autour de la cybercriminalité et de la fraude en général. Les jeunes collaborateurs qui entrent sont formés d'une façon générale sur le risque opérationnel et en particulier sur la fraude. Moi ce que j'aimerai en tant que coordinateur de la fraude externe, c'est qu'il y a des modules réguliers. Le réseau est demandeur qui plus est ! On est plus sur un souci d'effectif et de productivité.