Cybercriminalité : pourquoi les banques et les gouvernements doivent collaborer

Aujourd'hui, les deux camps cherchent des moyens de travailler plus étroitement ensemble afin de parvenir à un résultat plus positif pour tous.

Dans le cadre de cet effort concerté, le gouvernement et les institutions financières mettent à profit les avantages de la technologie moderne pour empêcher les fraudeurs de se livrer à leurs malversations. Cet article rappelle l'historique des approches disparates entre les gouvernements et les institutions financières pour lutter contre ce type de criminalité, et décrit les défis actuels et quels avantages pour l'ensemble de la société peut apporter un nouveau modèle faisant appel à une technologie de pointe, comme l'analyse de réseaux.

Quelle est la situation ?

Les cybercriminels sont des gens intelligents. Ils savent comment se frayer un passage à travers les faiblesses de la réglementation. La principale faiblesse exploitée à ce jour est l'isolement relatif des IF en matière de lutte contre la criminalité financière. C'est un défi universel, mais en France, la confidentialité des données a toujours été un sujet très sensible et les gouvernements ont toujours veillé à ce que les citoyens soient préservés de l'exploitation de leur vie privée et de leurs données. Bien que cette position ait été justifiée – en particulier à la lumière des récentes révélations concernant la confidentialité des données et les plates-formes de réseaux sociaux, elle a eu une conséquence involontaire, que les criminels ont été capables d'exploiter.

La législation visant à protéger les droits individuels à la vie privée a également empêché les banques de partager leurs informations sur les activités criminelles avec d'autres banques, et le partage au sein même des banques a été rendu également très difficile.

Prenons un exemple : un criminel trouve un stratagème pour commettre une fraude ou blanchir de l'argent, et il exécute son plan dans une agence bancaire située à Paris. Le délinquant peut alors se rendre à Lyon à 500 kilomètres de là et répéter exactement les mêmes étapes contre la même banque, en appliquant le même processus.

La réglementation sur la protection des données personnelles est structurée de telle sorte que les banques ne sont pas autorisées à partager des informations sensibles ou personnelles entre succursales. Même après avoir établi et prouvé avec succès le fait délictueux, la succursale de Paris ne serait pas en mesure de transférer l'information à une autre succursale. Le crime pourrait alors être répété plusieurs fois dans la même banque et la même approche réitérée dans différentes banques. On peut imaginer la frustration ressentie par les banques, constatant qu'elles sont braquées et qu'elles disposent des informations au sein de leur organisation pour prévenir la répétition de tels actes, mais qu'elles ne sont pas en mesure d'utiliser ces ressources dans leur lutte.

Un gros risque pour la réputation du gouvernement

Pendant des années, le gouvernement français a considéré qu'il s'agissait d'une affaire concernant les institutions financières, qu'il s'agisse des banques ou de leurs assureurs, et non d'un problème concernant le gouvernement, et il n'a pas voulu contourner la législation sur la protection des données. Les IF n'ont pas été en position d'agir.

Compte tenu des attentes croissantes de la communauté internationale en matière de lutte contre la délinquance financière, le gouvernement a compris qu'il y avait aussi un risque pour sa propre réputation et que le secteur financier pourrait être fragilisé s'il n'est pas en mesure de lutter de manière appropriée contre la criminalité financière. Les effets ressentis par les IF depuis des années pourraient avoir une incidence sur la réputation du gouvernement.

Il s'agit d'un changement d'approche important – plutôt que de voir les institutions financières suivre les orientations du gouvernement, les deux parties travaillent désormais ensemble pour leur bénéfice commun.

Des échanges de données à différents niveaux

Une fois convenue la nécessité d'étendre le partage des données, la première étape à franchir consiste à partager les informations pertinentes pour confirmer et prouver le crime financier (auteur, modèle, etc.). Si l'on se réfère à l'exemple donné ici, lorsque le délit financier est prouvé dans une succursale parisienne, l'information peut ensuite être transférée aux autres succursales.

Bien que le délit puisse encore se répéter dans ce cas, l'impact global s'en trouve considérablement réduit. En outre, l'autorisation serait donnée de partager les informations entre les banques, ce qui leur permettrait de s'organiser en sessions de travail au cours desquelles celles-ci pourraient partager les identités, les modèles, etc. des attaques dont elles ont été victimes.

Le premier effet serait de pousses les cybercriminels à modifier constamment leurs stratégies pour continuer à masquer leurs activités. Par exemple, un partage de données de ce type est effectué par l'Insurance Fraud Bureau au Royaume-Uni avec l'Insurance Fraud Register.

Toutefois, il ne s'agit que d'une première étape dans le processus de partage des données, car elle n'entre en vigueur qu'après l'accomplissement du premier crime financier. Bien qu'elle soit plus efficace, elle ne reste qu'une approche très réactive. Même en faisant preuve d'une forte réactivité, il s'écoule encore un certain temps entre la preuve du délit financier et sa prise en compte par tous les systèmes concernés.

L'étape suivante de la lutte consiste à faire obstacle au crime en augmentant l'échange de données avant que les faits délictueux ne se produisent. L'une des façons les plus innovantes pour y

parvenir est de créer un réseau rassemblant les données des différentes institutions financières.

Cette approche plus efficace est connue sous le nom de l'analyse de réseaux. En deux mots, la création d'un tel réseau consiste à créer des liens entre toutes les entités disponibles dans l'ensemble des données fournies par l'IF, afin de fournir une vue à 360 degrés du risque. Plus il y a de données, plus la vue d'ensemble de ce qui se passe est globale, et plus la détection du risque est efficace.

Dans notre exemple, le délinquant financier se rendrait dans plusieurs succursales en peu de temps et fournirait les mêmes détails à chacune d'elles (p. ex. téléphone mobile, adresse électronique, adresse physique). Dans l'architecture cloisonnée (en silo), personne ne disposerait des qualifications nécessaires pour pouvoir comparer les données et ce comportement suspect. Avec une approche s'appuyant sur l'analyse de réseaux, le lien serait évident et une enquête pourrait commencer immédiatement, avant le délit. À terme, il pourrait même être possible de refuser l'ouverture d'un compte au client.

Jusqu'à présent, l'approche de l'analyse de réseaux a été principalement déployée en utilisant les données d'une seule institution financière. L'étape suivante consiste à utiliser les données en provenance de plusieurs d'entre elles. Dans ce modèle, une organisation indépendante à but non lucratif se livre à un rapprochement entre les données de toutes les IF et fournit un retour d'information sur le risque de malversation à l'IF concernée.

Il existe de multiples initiatives sur ce modèle. L'une d'elles s'est déroulée en France dans le secteur de l'assurance, où le gouvernement a autorisé le partage de données après deux ans de négociations intenses pour partager collectivement les données provenant de différents établissements. Plus récemment, l'Association bancaire néerlandaise (Nederlandse Vereniging van Banken ou NVB) a lancé une initiative similaire dans le partage les données afin de rendre plus difficile le blanchiment d'argent dans le secteur financier néerlandais.

Un point autour du RGPD

L'une des questions les plus fréquemment posées au sujet du partage des données est celle du règlement général de l'UE sur la protection des données (RGPD). Si l'on veut maximiser la puissance de l'analyse de réseaux, il faudrait s'appuyer sur un plus grand partage des données, en admettant de moins en moins de limitations. À première vue, cela pourrait se trouver en contradiction avec le RGPD, qui impose des contraintes et des règles en matière de partage et de traitement des données.

La préoccupation des IF est justifiée, car elles pourraient se trouver en position de non conformité vis à vis des règlements. Toutefois, les législateurs ne veulent pas empêcher les IF de mener leurs activités de lutte contre la criminalité financière. Si l'on examine l'article 6 du RPGD, il est clair que les données peuvent être traitées pour le respect d'une obligation légale à laquelle l'IF est soumise (ce qui couvre la conformité et le financement de la lutte contre le terrorisme) ou pour des intérêts légitimes poursuivis par le responsable du traitement (qui couvrent largement la fraude).

Conclusion

Après des années de lutte contre la criminalité financière avec une réponse dispersée, le gouvernement et les institutions financières travaillent maintenant en collaboration. Le gouvernement met en place le cadre juridique nécessaire pour gérer les attentes en matière de confidentialité des données et accompagner les IF dans leur lutte contre la criminalité financière, et pour déployer à plus grande échelle des technologies innovantes, telles que l'analyse de réseaux. Les avantages pour les gouvernements, les IF et la société en général pourraient se révéler considérables.