La cyber sécurité : une opportunité de développement et de business pour le secteur financier

Nicolas FERREIRA,

Directeur Général Adjoint chez Finance Innovation.

Organisateur de l'événement Cyber Day – Cybersécurité et Métiers de la Finance : une opportunité de transformation pour la banque et l'assurance

La sécurité est un des piliers fondateurs de toute relation avec ses clients, et c'est un des atouts majeurs de l'écosystème financier qui, étant responsable de masses financières conséquentes, est sensibilisé depuis longtemps au sujet. S'il est toujours possible de faire mieux, et toujours nécessaire de rester à la pointe de la lutte contre des risques cyber évoluant très rapidement, les acteurs de la finance ont un niveau de maturité certain. Ils sont un tiers de confiance reconnu, et c'est d'ailleurs un de leurs avantages concurrentiels majeurs face aux fintechs et autres acteurs technologiques.

Dans ce contexte changeant, la question est de savoir comment, dans le cadre d'une digitalisation toujours plus poussée, la protection contre les risques cyber et la lutte contre la fraude peuvent être une opportunité pour développer de nouveaux business models et de nouvelles relations avec ses clients. Comment la sécurité, socle de confiance, peut faciliter et fluidifier les relations avec le client, tout en établissant le bon niveau de sécurité, qui doit être rassurant sans entraver les parcours.

La cybersécurité, au-delà de l'informatique

Afin d'intégrer la cybersécurité au sein d'une démarche réellement tournée vers le business, elle doit être approchée sous un angle élargi, au-delà de la vision IT traditionnelle : les failles informatiques qui pourraient être exploitées, permettant à des intrus d'infiltrer les systèmes, afin soit de voler des données, soit de bloquer des systèmes et demander des rançons (rançongiciels). Les RSSI et CISO sont les gardiens du temple, mais ils peuvent parfois être cornérisés, coupés des métiers, en ayant une approche purement informatique. Ils peuvent être perçus comme des freins à l'innovation, au lieu d'être un atout dans la relation avec le client.

Pour autant, qu'il s'agisse de l'entrée en relation avec le client, l'analyse crédit, la gestion de patrimoine ou la gestion backoffice et la conformité, la fraude documentaire, l'usurpation d'identité ou la fraude informatique se mélangent de plus en plus : y a-t-il finalement une réelle sécurité lorsqu'un client envoie un scan d'une pièce justificative par mail ? Comment vérifier son authenticité, et même l'identité de celui qui a envoyé le mail ? Les outils technologiques pour sécuriser l'identification d'un client ou une transaction relèvent-ils de la cybersécurité ou du KYC ? Le règlement DORA sur la résilience opérationnelle numérique invite justement à avoir une approche élargie des risques.

L'innovation fintech au service de la sécurité

Un grand nombre de solutions proposées par des fintechs et startups permettent d'intégrer de la sécurité de manière agile et le moins douloureuse possible pour le client : Netheos mets

en place par exemple des solutions de souscription à distance et de signature électronique, alors que Share ID, grâce à des technologies de reconnaissance faciale, permet l'authentification d'une personne grâce à son sourire, et ce sans stockage de données personnelles biométriques. Enfin, il existe également des approches combinant sécurité et conformité comme celles proposées par exemple par Vialink, afin d'adresser largement la sécurisation du parcours client et le KYC.

Le paiement est un terrain de jeu particulièrement fertile pour la fraude, mais aussi pour l'innovation : MoneyTrack utilisera ainsi la technologie blockchain pour sécuriser les versements par les mutuelles, collectivités et institutions financières à des particuliers. Stream Mind utilise l'intelligence artificielle afin de croiser les coordonnées bancaires et personnelles pour sécuriser les virements, alors que la carte Handsome s'attaque à la fraude lors du paiement en caisse par les malvoyants, qui sont très souvent victimes de fraude lors du passage en caisse. Sans parler bien sûr du Buy Now Pay Later, dont une grande partie du métier des fintechs est la gestion du risque lié à la fraude comme ce que propose Algoan.

Au-delà des solutions de sécurisation internes et techniques du secteur financier, les institutions financières doivent-elles être des acteurs plus proactifs dans la protection de l'économie ?

Le banquier, l'assureur, sont des tiers de confiance des entreprises. Ils sécurisent leur quotidien de plusieurs manières, que ce soit financièrement ou dans leur business (par exemple en fournissant ou prescrivant des solutions de paiement sécurisées pour les commerçants et e-commerçants). Dans ce cadre, ces institutions ont à la fois la légitimité et un réel intérêt à contribuer également à la sécurisation face aux risques cyber et à la fraude de leurs clients.

Un client bien protégé face aux menaces cyber est tout d'abord un client moins risqué financièrement, mais c'est aussi un client plus serein et mieux fidélisé. Il existe désormais des initiatives de la part du secteur bancaire afin de sécuriser leurs clients : LCL s'est associé par exemple à Almond et Board of Cyber, afin d'encourager ses clients à faire un diagnostic de vulnérabilité et engager une démarche de protection.

Le Crédit Agricole Alpes Provence, partant du constat que la sécurité devien,t de plus en plus un enjeu fort pour ses clients, a créé sa filiale Cyber Way, alliant diagnostic et accompagnement à la mise en place de bonnes pratiques face au risque cyber.

Et l'assurance dans tout ça ?

Le secteur de l'assurance n'est pas en reste et poursuit son travail de couverture des risques, en clarifiant son offre et en l'adaptant aux divers types d'acteurs :

- Les TPE/PME sont peu attaquées, mais leurs systèmes informatiques sont plus vulnérables et leur pronostic vital est souvent engagé quand cela arrive : selon une étude de la CCI, 60% des entreprises subissant une attaque mettent la clé sous la porte dans les six mois après une cyberattaque
- Les ETI sont de plus en plus des cibles de choix : elles présentent des retours financiers intéressants pour les attaquants tout en étant moins bien protégées que les grands groupes
- Les grands groupes sont globalement bien couverts, mais face à la difficulté de prévoir les risques et couvrir des masses financières importantes, ils pourraient de plus en plus avoir recours aux captives en internalisant la gestion de ces risques

Afin de répondre à ces problématiques de nouvelles offres d'assurance cyber émergent, notamment avec des insurtechs comme Stoïk ou DattaK, dont l'objectif est double : 1/ faciliter la montée en compétence des TPE/PME en matière de risques cyber et 2/ leur permettre de bénéficier d'une couverture assurancielle simple et adaptée à leur taille.

Notre économie est depuis plusieurs années face à un stress permanent en termes de sécurité numérique, avec la digitalisation forcée suite à la crise Covid et la généralisation du télétravail, la guerre en Ukraine, mais aussi un mouvement de fond de digitalisation depuis les années 2000. La mise en lumière des risques cyber doit être une opportunité pour les institutions financières de renouer avec leurs clients, en affirmant leur rôle de tiers de confiance grâce à l'innovation. ■