CGI

La force de l'engagement[MD]

# BANKING. TRANSFORMED.

## Des experts de CGI discutent de la **protection des banques**

## Jerry

Jerry Norton, vice-président, Services bancaires mondiaux est responsable de la stratégie de CGI pour les marchés de gros et des entreprises. Responsable de la stratégie de CGI pour l'ensemble du segment, il est membre du conseil sur la croissance et du comité du secteur bancaire de CGI. Il se spécialise dans les changements s'opérant à l'échelle de l'industrie, qu'ils soient introduits par les domaines d'affaires ou technologiques, et ses perspectives sont sollicitées sur le marché mondial. En plus de son expertise sectorielle et de ses connaissances en technologie, Jerry possède une bonne compréhension de la conformité, de la réglementation ainsi que de la prévention et de la gestion des risques opérationnels. À l'heure actuelle, il se concentre principalement sur l'évolution des activités opérationnelles et des technologies dans le marché des paiements. Il donne régulièrement des présentations dans le cadre de conférences internationales axées sur les thèmes financiers de l'heure et participe à de nombreux groupes de réflexion. On le cite souvent dans les médias grand public et spécialisés.

## Jan

Jan Macek, vice-président, possède 18 ans d'expérience dans le secteur des TI et des services-conseils, et 11 ans d'expérience dans des postes de haute direction. Depuis 9 ans, il approfondit ses connaissances du secteur financier et se spécialise dans le domaine de la lutte contre la criminalité financière.

Chez CGI, ses responsabilités comprennent la direction d'une équipe assurant la prestation de services et l'offre de produits de CGI en République tchèque, en Slovaquie et en Europe de l'Est, la direction générale des services-conseils de pointe en matière de lutte contre le crime et de la solution HotScan360 de CGI, qui aide les clients de CGI à prévenir les menaces et les difficultés financières associées à la réglementation et aux politiques concernant la lutte contre le blanchiment d'argent.

En tant que membre du conseil bancaire mondial de CGI, Jan contribue à la stratégie de CGI pour le secteur bancaire.

# Des experts de CGI discutent de la protection des banques

Dans le cadre d'une série de conversations, des experts des services bancaires de CGI ont discuté de quatre volets essentiels de la transformation des banques : la modernisation, l'expansion, la protection et la numérisation. Cet aperçu présente les grandes lignes de la table ronde sur la protection des banques, à laquelle ont participé Jerry Norton, dirigeant des Services bancaires mondiaux de CGI, et Jan Macek, expert en crimes financiers de CGI.

## Premièrement, qu'entendons-nous par protection? Comment définiriez-vous ce terme?

**Jan :** La protection vise non seulement à assurer le maintien de l'argent en sécurité et la prévention des crimes financiers, mais également la sécurité des opérations et de l'ensemble du secteur bancaire. De nos jours, il faut assurer la protection de tout l'écosystème bancaire et de la quantité astronomique de données sur les clients traitées par les banques.

**Jerry :** D'après l'information tirée du Baromètre mondial CGI et de notre sondage auprès des clients du secteur bancaire, la confiance constitue l'aspect le plus important dans la relation entre une banque et son client. Elle constitue également un élément clé à l'ère numérique. Dans ce contexte, la protection est primordiale pour permettre aux banques de conserver la confiance de leurs clients, surtout en ce qui a trait aux services bancaires numériques. Lorsqu'une banque perd la confiance de sa clientèle, elle perd des clients. D'ailleurs, bien des exemples ont fait la manchette récemment.

Parmi les autres aspects importants de la protection, mentionnons la prévention des pertes et la conformité à la réglementation. La fraude peut entraîner d'énormes pertes financières et porter atteinte à la réputation d'une banque. Enfin, la réglementation exerce aussi beaucoup de pression sur les banques. Une protection efficace saura répondre à tous ces défis.

## Quels sont les principaux défis que doivent relever les banques pour demeurer protégées?

**Jan :** Plus les banques deviennent des entreprises numériques complexes, plus des pressions importantes sont exercées pour qu'elles protègent l'ensemble de leur organisation et de leur écosystème, ce qui a des répercussions sur leurs employés, leurs méthodes de travail et leurs technologies. De plus, la rapidité actuelle du traitement exerce une pression supplémentaire qui pousse les banques à leurs limites. Les clients veulent pouvoir effectuer des paiements et prendre des décisions dans l'immédiat, et les systèmes existants ne peuvent tout simplement pas répondre à la demande.

**Jerry :** Oui, et des paiements plus rapides entraînent des fraudes plus rapides.

**Jan :** L'automatisation est un autre défi de taille. Les banques automatisent le plus possible et intègrent l'apprentissage automatique et l'intelligence artificielle. Certains gestionnaires croient que l'automatisation n'a pas d'incidence sur le contrôle qu'ils exercent, mais ils confient la prise de décisions à des machines et perdent ainsi lentement le contrôle des processus. De plus, quelques lignes de code corrompu peuvent modifier complètement un processus et faire carrément des ravages.

À mon avis, le principal défi demeure néanmoins la nécessité pour les banques de consolider leurs mesures de protection des activités bancaires. Il n'est pas efficace d'avoir de multiples services responsables de ces activités. Sans une vue d'ensemble, les banques ne sont pas en mesure de tout voir ni de s'occuper des menaces continues provenant de toutes parts.

Tous ces défis engendrent des pressions sur les coûts. Le coût quotidien de la protection des banques augmente chaque année et devient un enjeu énorme pour les dirigeants. Pour une banque, dans son ensemble, ce coût représente près de 30 % des dépenses en TI. Les banques cherchent donc à contrôler ce coût. Comment peuvent-elles faire pour le réduire, ou du moins l'optimiser?

**Jerry :** Il est vrai que la protection des banques est souvent considérée comme une dépense désagréable, et non comme un générateur de revenus. Le contrôle des coûts est donc essentiel.

**Jan :** La sensibilisation constitue un autre défi pour les dirigeants. Chaque employé, client et partenaire joue un rôle important dans la sécurité globale d'une banque. Par exemple, une seule petite erreur commise par un client peut entraîner une violation de la sécurité ou de la réglementation et engendrer d'énormes coûts pour une banque. Il est donc essentiel que les banques sensibilisent leurs clients à la protection. À l'heure actuelle, les clients ne s'en font pas s'ils entrent leur carte par erreur dans un guichet automatique bancaire, car ils s'attendent à ce que leur banque les protège et paie pour leurs erreurs.

## Quelles sont les stratégies ou technologies pouvant aider les banques à surmonter ces défis?

**Jerry :** Les banques analysent habituellement les données en sous-ensembles, mais elles ont maintenant besoin d'une vue d'ensemble de ces dernières, qu'elles portent sur les clients ou les transactions. Une fois qu'une grande quantité de données est recueillie, des techniques astucieuses d'appariement de formes, l'apprentissage automatique et l'intelligence artificielle peuvent être utilisés pour vérifier efficacement la présence de faux positifs et améliorer les taux de réussite.

L'identité, l'intégration et la connaissance du client sont d'autres domaines clés dans lesquels les banques doivent s'améliorer. Des vérifications de sécurité efficaces au moment du premier contact avec une banque permettent de freiner les activités des personnes malfaisantes dès le début. Évidemment, les menaces ne proviennent pas uniquement de vos propres clients. Il existe également des problèmes dans l'acceptation de paiements provenant d'autres banques et réseaux, ainsi que de l'international. Il est essentiel que les banques comprennent le contexte entourant un paiement ou un risque.

**Jan :** Oui. Il est aussi important de mentionner que la lutte contre les crimes financiers n'est pas un domaine dans lequel les banques se font concurrence. En fait, elles ont tout avantage à partager leurs expériences, points de vue et tendances en la matière. Il s'agit d'une formule gagnante sur toute la ligne.

Il est donc urgent que les banques prennent conscience de la situation, qu'elles collaborent afin de protéger le secteur et qu'elles procèdent à une prise de position collective contre les activités suspectes. Les services de connaissance du client partagés joueront peut-être un rôle important.

**Jerry :** Oui, nos clients soulèvent régulièrement la nécessité des services partagés, et de nombreuses banques tiennent à créer un certain type de service de connaissance du client partagé. Cependant, ils font face à des obstacles. Premièrement, le RGPD empêche les banques d'échanger des renseignements personnels entre elles.

Deuxièmement, il y a une préoccupation plus vaste en matière de réglementation. De nombreux organismes de réglementation se méfient des services partagés et pensent qu'ils nuisent à la responsabilisation. Par exemple, il y a quelques années, CGI a travaillé avec un pays à mettre en place un service partagé fondé sur la protection. Techniquement, ce service partagé pourrait fonctionner et offrir des renseignements utiles dans le cadre de l'examen des ensembles de données de multiples banques. Par contre, dans ce cas, l'organisme de réglementation n'a pas accepté que le projet se poursuive pour des raisons de responsabilisation.

D'autres pays sont toutefois plus réceptifs. Aux États-Unis, par exemple, certaines organisations envisagent le concept des services partagés, sachant que les avantages d'une quantité de renseignements et d'une capacité de protection accrues surpassent les risques liés à la responsabilisation.

**Jan :** Oui, je crois que c'est très important puisque le secteur est de plus en plus interconnecté. Les banques ne sont plus des organisations indépendantes et isolées, et elles sont désormais connectées à des tiers par l'entremise d'API. Ainsi, la protection devient un enjeu sectoriel et il serait bon de voir apparaître une solution qui protège l'ensemble de l'écosystème bancaire puisque sa solidité se mesure à son maillon faible. De plus, le système bancaire ouvert entraînera une myriade de maillons faibles et de moyens détournés, de sorte que la collaboration à l'échelle du secteur sera encore plus importante.

## Quel rôle jouent les technologies émergentes dans la protection des banques?

**Jerry :** Les banques traitent d'énormes quantités de données en temps quasi réel. Pour protéger l'écosystème, elles doivent reconnaître les tendances liées à des parties connues, comme les clients, et à des parties inconnues, comme les personnes malfaisantes qui agissent incognito. Les technologies émergentes peuvent sans aucun doute aider les banques à accomplir cette tâche gigantesque. L'analyse de données, l'apprentissage automatique, l'intelligence artificielle et les technologies en temps réel et d'informatique en nuage sont d'une importance cruciale, tout comme certains concepts liés aux technologies de chaînes de blocs, comme le hachage et la segmentation en unités. Les solutions pour contrer la criminalité financière ne fonctionneront pas sans le recours à certaines de ces nouvelles technologies.

**Jan :** Je suis tout à fait d'accord pour dire que les technologies émergentes jouent un rôle essentiel dans la protection des banques. Par exemple, j'ai récemment parlé à un client dirigeant qui nous a demandé si nous pouvions gérer de nombreux types de fraude, y compris la fraude numérique, la fraude interne, la fraude commerciale, etc. Par contre, les approches en vase clos ne sont pas efficaces pour protéger les banques. Il est nécessaire de pouvoir obtenir rapidement une vue d'ensemble de la protection globale des banques, et non uniquement de la protection contre les crimes financiers. Il faut comprendre ce qui se passe dans chaque service. Par conséquent, le rêve de tous les chefs de la direction est de disposer d'un tableau de bord unique, ce qui exige le recours aux technologies émergentes.

Les banques sont constamment attaquées. Comme elles ne peuvent pas contrer toutes les attaques, la protection vise davantage à gérer les risques. Mais quel est le niveau de risque acceptable? Par exemple, un tableau de bord comportant des indicateurs de risques éventuels permettrait au moins, même s'il n'est pas exact à 100 %, d'alerter une banque et d'améliorer sa gestion des risques.

**Jerry :** Oui, exactement. Un tableau de bord présentant les risques ainsi que les coûts rendrait les chefs de la direction heureux.

## Les technologies émergentes peuvent donc aider les banques à transformer leur approche en matière de protection. À quoi ressemblerait donc une banque de l'avenir entièrement transformée?

**Jerry :** Une banque de l'avenir entièrement transformée regarderait vers l'avant et disposerait d'un tableau de bord aidant à prévoir les attaques plutôt qu'à réagir en cas d'attaque. Cette vision peut sembler trop poussée, mais il s'agit de l'utilisation de l'intelligence artificielle de l'avenir. L'idée consiste à avoir recours à l'intelligence artificielle pour détecter les activités inhabituelles et déterminer si elles sont frauduleuses.

Bien entendu, cette façon de faire soulève des problèmes sur le plan du maintien d'un équilibre entre la confiance des clients et les frustrations. La tolérance des clients à l'égard du blocage des paiements est faible. Dans une banque entièrement transformée, il devrait donc être possible de procéder à un tel blocage sans nuire aux clients.

Les tendances et profils permettent d'éviter toute répercussion sur le client. Par exemple, une modélisation des habitudes de chaque personne pourrait être comparée à son activité en temps réel. Le système avertirait alors la banque en cas d'activité inhabituelle. Cette tendance pourrait être assez facile à obtenir pour les habitudes d'achat normales. Ce sont les achats et transactions peu fréquents qui rendent les choses difficiles parce que, comme nous l'avons dit, les clients ont une faible tolérance à l'égard du blocage de paiements.

**Jan :** Absolument. De plus, si vous aviez des modèles comportementaux pour chaque client, vous pourriez les regrouper et établir quel est l'état normal pour la banque dans son ensemble. Cet état normal s'afficherait sur le tableau de bord en temps réel. Toutefois, il s'agit d'une vision de l'avenir et les banques n'en sont pas encore là.

## Qu'en est-il des clients? Comment interagiront-ils avec leur banque dans l'avenir?

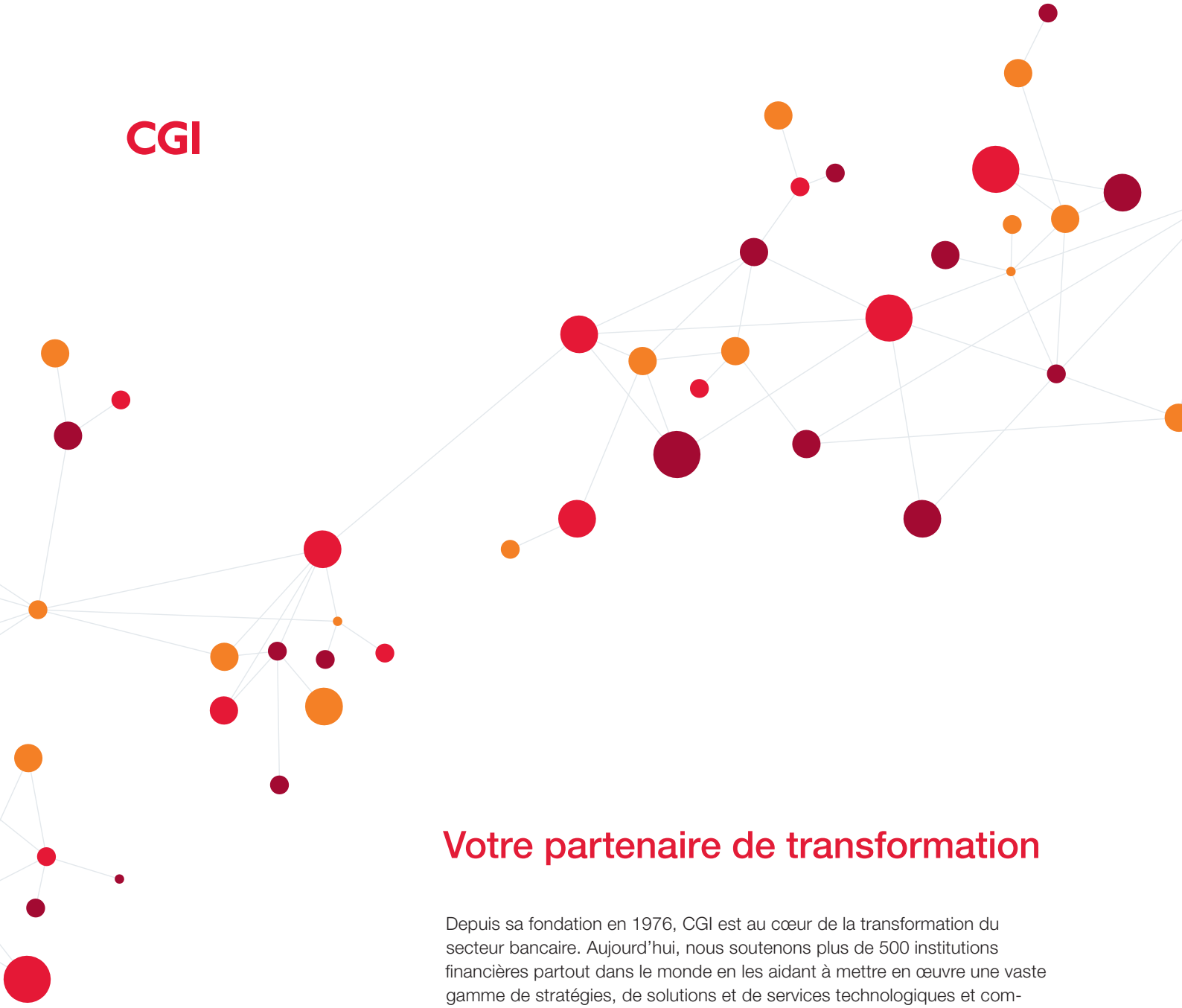
**Jerry :** Les interactions seront effectuées instantanément par voie électronique et exigeront des vérifications de sécurité plus rigoureuses en arrière-plan. Pour le client, il s'agira d'une façon de faire plus facile et fluide.

**Jan :** Nous savons tous que les vérifications de sécurité sont l'une des plus grandes frustrations des clients, des partenaires et des employés. Dans quelques années, j'imagine que les banques mettront en œuvre des solutions avancées de cyberauthentification et de cyberaccueil. Encore une fois, l'intelligence artificielle et la biométrie joueront un rôle essentiel, non seulement pour renforcer la sécurité, mais aussi pour faciliter les mouvements dans l'ensemble de l'écosystème.

## Enfin, quelles sont vos principales recommandations pour les banques?

**Jerry :** Ma première recommandation est d'acquérir une vue d'ensemble des données. L'idée est de mettre en place une architecture de protection qui scrute et gère les données des clients de manière globale pour tous les flux de transactions. Il s'agit d'un défi de taille, qui offrira des occasions d'affaires importantes une fois l'architecture mise en place correctement.

**Jan :** Absolument. Sur une note similaire, elles doivent également consolider les services qui gèrent actuellement la protection en vase clos. Elles pourront ainsi faire des gains à titre d'entreprises harmonieusement alignées. En travaillant avec nos experts, les banques peuvent évaluer leur architecture de protection actuelle, comprendre où les défis se situent et mettre en place les changements qui amélioreront la protection dans toute l'organisation.



# Votre partenaire de transformation

Depuis sa fondation en 1976, CGI est au cœur de la transformation du secteur bancaire. Aujourd'hui, nous soutenons plus de 500 institutions financières partout dans le monde en les aidant à mettre en œuvre une vaste gamme de stratégies, de solutions et de services technologiques et commerciaux axés sur le numérique. Notre compréhension approfondie des défis mondiaux complexes que doivent relever les banques, conjuguée à nos relations étroites à l'échelle locale, nous permet de bâtir des partenariats durables qui sont gages de succès.

La pratique de transformation numérique de CGI est ancrée autour de la création d'entreprises plus agiles et pouvant toujours s'adapter à l'évolution du marché et des besoins du client. CGI a axé sa pratique sur l'offre de capacités complètes dont les clients ont besoin pour permettre leur transformation et l'accroissement de leur agilité. Depuis plus de quatre décennies, nous aidons des organisations de premier plan du monde entier à concrétiser leurs plans d'innovation et de transformation tout en renforçant leurs infrastructures existantes.

Pour savoir comment nous pouvons vous aider à transformer vos activités, communiquez avec nous dès aujourd'hui. Nos conseillers seront heureux de discuter avec vous.

Banking.transformed@cgi.com