Élaboration d'une analyse de rentabilité pour les technologies de prévention des fraudes

Évaluer le véritable impact de la fraude sur les institutions financières, et toutes les implications des solutions de prévention des fraudes

Sommaire

Introduction

L'élaboration d'une analyse de rentabilité pour justifier les investissements dans des technologies de prévention des fraudes n'est malheureusement pas aussi simple qu'on pourrait le penser. L'impact de la fraude en ligne sur une institution financière est multiple et complexe. Les incidents de fraude et les efforts de prévention des fraudes affectent de nombreux aspects des services de la banque et de ses interactions avec les clients. Une analyse de rentabilité réaliste et robuste doit examiner un large éventail de composants, au-delà de la réduction des pertes liées aux fraudes et des coûts de gestion des fraudes.

Sur la base de longues discussions avec les institutions financières clientes, IBM a défini et classé en catégories les principaux composants de l'analyse de rentabilité à prendre en compte lors de l'examen des ramifications commerciales des nombreuses approches technologiques. Chaque banque accordera une importance différente aux facteurs, par conséquent ce qu'une banque peut considérer comme critique, une autre banque peut le considérer comme secondaire. Toutefois, avec les budgets limités et les difficultés généralement rencontrées par les centres de coûts, il incombe à toutes les institutions financières de reconnaître le véritable impact de la fraude sur leur société, ainsi que l'ensemble des implications des technologies de prévention des fraudes disponibles. Celles qui comprennent les fonctionnalités dévastatrices des logiciels malveillants avancés comprennent également que le secteur ne peut pas faire l'économie de technologies de prévention des logiciels malveillants.

IBM a collecté et classé en catégories les composants qui ont constitué les principaux éléments de l'analyse de rentabilité des technologies de lutte contre les fraudes de nos clients. Ce livre blanc explique comment chaque composant peut aider les institutions financières à créer un modèle réaliste de retour sur investissement. Des indicateurs sont fournis pour les composants, le cas échéant. Dans le cas contraire, nous fournissons une liste de considérations utilisées par les clients IBM dans leurs analyses de rentabilité.

Anticipation des pertes liées aux fraudes

L'un des objectifs principaux des technologies de prévention des fraudes consiste à éviter les pertes liées aux fraudes, c' est-à-dire les fonds volés non récupérés. Les institutions financières doivent examiner l'impact des technologies de prévention des fraudes sur la réduction de la fraude dans les catégories suivantes.

Pertes liées aux fraudes sur Internet

L'historique des pertes liées aux fraudes sur Internet doit être disponible immédiatement pour les institutions financières. De nombreuses institutions financières sont en fait plus préoccupées par les futures pertes potentielles, aux vues de la sophistication croissante des logiciels malveillants et de la fréquence des tentatives de cybercrime. Par exemple, pour contourner les moteurs de risque en ligne, certains logiciels malveillants sont conçus pour s'adapter aux comportements de navigation et de transaction des utilisateurs afin d'éviter l'exposition d'anomalies par rapport au profil de base de l'utilisateur.

Plusieurs institutions financières de moyenne et grande taille ont signalé une augmentation des tentatives de fraude, suite à la migration de la fraude en provenance des « méga-banques ». Du fait que les plus grandes institutions financières ont mis en œuvre de vastes programmes sophistiqués de prévention des fraudes, les cybercriminels se tournent désormais vers les institutions plus vulnérables qui ne disposent pas encore d'une protection adéquate. Un seul incident pourrait se traduire par des centaines de milliers (si ce n'est des millions) de dollars de pertes liées aux fraudes.

Pertes liées aux fraudes cross-channel

Les criminels dérobent de plus en plus d'identifiants en ligne pour commettre une fraude sur d'autres canaux et éviter la détection par les moteurs de risque en ligne. Malheureusement, la grande majorité des banques ne dispose pas de moyen simple pour détecter ce type de fraude, et ne peut donc pas déterminer l'ampleur de la fraude cross-channel visant leur institution. Nous nous attendons à une augmentation de la fraude cross-channel, car les cybercriminels s'engagent généralement sur la voie offrant le moins de résistance.

Un exemple de fraude cross-channel mis en évidence récemment par IBM, a pris la forme d'un programme élaboré d'escroquerie au chèque bancaire. Les criminels utilisaient des logiciels malveillants pour accéder aux comptes bancaires et afficher les images de chèque, collecter les historiques de transactions, et accéder à d'autres données commerciales. Ces informations étaient utilisées pour créer des chèques de contrefaçon sophistiqués, soutenus par une connaissance détaillée du compte et des historiques de transactions. Dans cet exemple, la banque classait finalement cette fraude comme escroquerie au chèque, sans réaliser que les informations requises pour commettre la fraude étaient initialement obtenues en ligne. Un client IBM a signalé une réduction de 30 % des escroqueries au chèque pour les clients protégés par IBM® Security Trusteer Rapport, comparé aux clients utilisant d'autres solutions ou aucune protection. Du fait que les criminels ne pouvaient pas accéder aux comptes protégés par Trusteer Rapport, ils ne pouvaient pas commettre ce type d'escroquerie au chèque cross-channel.

Un autre client IBM a observé une réduction de 93 % des cas de fraude dans les centres d'appel après la mise en œuvre de solutions IBM. Le client a attribué cette réduction au blocage de l'accès frauduleux aux comptes en ligne, empêchant les criminels de rassembler les informations nécessaires pour usurper l'identité de clients légitimes dans le centre d'appel. D'autres clients ont fait part de l'impact des produits de protection de terminaux d'IBM Security Trusteer sur la réduction des escroqueries au transfert et à la carte de débit, entre autres.

Composant	Exemples d'indicateur
Pertes liées aux fraudes sur Internet	Une banque est probablement à l'origine d'une perte de 345 000 dollars liée à la fraude dans le procès Patco
	Une autre banque est probablement responsable d'une perte de 560 000 dollars là encore liée à la fraude dans le procès Experi-Metal
	La plupart des banques considèrent qu'« un seul incident majeur suffit à provoquer d'importants dommages »
Pertes liées aux fraudes cross-channel	Un client a signalé une réduction de 30 % des escroqueries aux chèques pour les clients protégés par Trusteer Rapport
	Un client a signalé une réduction de 93 % des cas de fraudes dans les centres d'appel après la mise en œuvre d'IBM® Security Trusteer Pinpoint Criminal Detection
	IBM estime que la plupart des banques peuvent espérer réduire la fraude sur les autres canaux de 20 à 30 %, grâce aux solutions IBM Security Trusteer

Coûts de gestion des fraudes

Les institutions financières nécessitent d'importantes ressources pour gérer et surveiller les sessions et transactions en ligne, afin d'identifier les fraudes potentielles. Même les meilleurs systèmes de détection des fraudes basés sur le risque génèrent un nombre considérable d'alertes de faux-positifs, c'est-à-dire de transactions potentiellement frauduleuses qui sont en réalité des transactions légitimes. Les analystes des fraudes peuvent analyser des douzaines d'alertes afin d'en identifier une qui représente une transaction frauduleuse réelle.

Coûts de prévention des fraudes

Les institutions financières disposent d'une multitude d'options pour la création et le maintien de leur infrastructure de prévention des fraudes. Plusieurs technologies d'authentification et de détection des fraudes sont souvent déployées (avec plusieurs niveaux d'intégration), et nécessitent généralement d'importantes ressources humaines pour les opérations quotidiennes et la maintenance. Les moteurs de prévention des fraudes nécessitent souvent un investissement de départ important pour créer et intégrer les sources de données requises pour l'analyse. Ces systèmes exigent ensuite en permanence d'importantes ressources pour analyser les faux positifs, tels que l'embauche d'analystes des fraudes pour enquêter sur les alertes et sensibiliser les clients, des agents de centre d'appel pour répondre aux appels lorsque des transactions sont bloquées ou ré-authentifiées, et du personnel des opérations de paiement pour inverser ou récupérer les paiements frauduleux identifiés.

Plus une technologie unique est efficace pour la prévention des fraudes, moins il est nécessaire de disposer d'autres technologies pour en combler les lacunes. Les technologies qui préviennent les transactions frauduleuses avant même leur lancement sont préférables à celles qui tentent de détecter les transactions frauduleuses dans le flux de traitement des paiements.
Les deux sont nécessaires dans le cadre d'une solide plateforme de sécurité renforcée, mais la première est beaucoup plus efficace et fiable comme outil de prévention des fraudes.

Plusieurs clients IBM ont signalé une réduction de 50 à 90 % des alertes de faux-positifs générées par leurs moteurs de risque. Trusteer Rapport bloque quasiment toutes les tentatives de fraude basées sur des logiciels malveillants, afin qu'aucune transaction frauduleuse n'entre dans le système de traitement des paiements.

IBM® Security Trusteer Pinpoint Malware Detection détecte avec précision la présence et la sévérité des logiciels malveillants sur les dispositifs d'utilisateurs, améliorant ainsi grandement la précision des analyses du moteur de risque.

Coûts de résolution des problèmes liés aux fraudes

Lorsque les transactions frauduleuses réussissent, des ressources internes et externes sont souvent nécessaires pour communiquer avec le client puis analyser et éventuellement engager des poursuites contre l'événement. Les grands événements divulgués au public exigent également des relations publiques et une intervention juridique. Les clients commerciaux ont de plus en plus recours à des procès pour récupérer les fonds volés lors d'événements de cyberfraude. Bon nombre de ces cas sont résolus hors du tribunal, mais non sans entraîner des coûts juridiques importants et exiger des ressources internes.

L'élimination de quasiment toute la fraude permet d'éliminer quasiment tous les coûts de résolution des problèmes liés aux fraudes. Les clients IBM peuvent éviter certaines dépenses car les transactions frauduleuses ne sont pas autorisées à entrer dans le système de traitement, alors qu'elles peuvent être omises par les moteurs d'authentification et de risque de fraude.

Impact de la résolution des problèmes liés aux logiciels malveillants

Lorsqu'un périphérique client est soupçonné de contenir un logiciel malveillant, l'institution financière doit s'assurer que le logiciel malveillant est supprimé pour contribuer à éviter la fraude. De nombreuses institutions financières exigent de leurs clients qu'ils se chargent eux-mêmes de la résolution des problèmes, ce qui les conduit souvent à utiliser un service tiers. Cette dépense est souvent prise en charge par le client (avec des inconvénients importants) et parfois par la banque. Dans les deux cas, la banque fait appel à des représentants spécialisés du service client ou utilise des ressources de tiers pour résoudre le problème avec le client. Si le client assure lui-même la résolution des problèmes, la banque n'a aucune garantie que le logiciel malveillant a bien été supprimé, ni même que le client a essayé de supprimer le logiciel malveillant.

Trusteer Rapport permet de supprimer les logiciels malveillants, en les effaçant ou en les détruisant complètement, du périphérique d'un client. Aucune action du client n'est requise et la banque possède une visibilité complète de l'état du périphérique du client, pour contribuer à garantir que la suppression des logiciels malveillants a bien été accomplie. Plus important encore, ce service positionne la banque comme défenseur des clients, et ces derniers apprécient énormément que leur banque prenne en charge ce qui constituerait autrement une tâche très difficile.

Composant	Exemples d'indicateur
Coûts de prévention des fraudes	Les clients IBM signalent une réduction des alertes de faux-positifs de 50 à 90 %
	Plusieurs grandes entreprises ont remplacé des analystes de fraude en raison d'une forte réduction des alertes de faux-positifs, avec les solutions IBM Security Trusteer
	De nombreux clients ont déclaré que l'élimination de la fraude basée sur des logiciels malveillants avait contribué à éviter le recours à d'autres solutions technologiques
Coûts de résolution des problèmes liés aux fraudes	L'implication du personnel interne, des cadres ou du comité de direction s'avère fastidieuse et coûteuse
	Les services de conseil d'entités juridiques, de relations publiques et d'experts externes sont coûteux
Impact de la résolution des problèmes liés aux logiciels malveillants	Réduction des dépenses des banques consacrées à la résolution des problèmes par des spécialistes internes ou des tiers
	Suppression du problème de validation de l'élimination des logiciels malveillants sur les périphériques client

Impact sur les clients

Les institutions financières doivent mettre en œuvre des technologies de prévention des fraudes qui ont aussi un impact positif sur les relations avec les clients. La solution doit avant tout prévenir la fraude, mais il est également important qu'elle ne constitue pas un fardeau pour le client. Ce fardeau peut prendre la forme d'un contact excessif ou inutile pendant les enquêtes sur la fraude, de procédures d'authentification exigeantes, ou de limitations des transactions ou des services.

Impact sur la marque

Suite à un événement de fraude, les institutions financières doivent s'attendre à ce que le client affecté déplace une partie ou toutes ses activités vers une autre institution. Lorsque les événements de fraude deviennent publics, les banques connaissent également une fuite de liquidités supplémentaire des clients en raison de la perte de confiance. Certaines banques ne sont pas toujours en mesure de résister aux ramifications désastreuses associées à un événement de fraude majeur.

De nombreux clients IBM déclarent que leur objectif principal en matière de prévention des fraudes est simplement « que leur nom ne soit pas cité ». Le coût du recrutement de nouvelles entreprises est bien plus élevé que le suivi et le maintien des clients existants. Avec cette grande importance accordée à la fidélisation des clients et au maintien de leur confiance, de nombreuses banques valorisent plus que tout la protection de la marque.

Simplicité pour les clients

Les procédures de prévention des fraudes, lorsqu'elles sont excessives, peuvent affaiblir la qualité des relations avec la clientèle. Le fait d'exiger des procédures d'authentification fastidieuses telles que l'utilisation de jetons matériels ou des questions secrètes excessives peut sévèrement diminuer la simplicité des services offerts par Internet, qui est alors considéré avant tout comme une source d'ennuis. Même les solutions de détection des anomalies exécutées « en arrière-plan » peuvent provoquer plus d'alertes de faux positifs (des transactions identifiées comme potentiellement frauduleuses) que d'alertes concernant des transactions frauduleuses réelles. Ceci entraîne souvent un contact avec le client pour valider les transactions en cours d'investigation, ce qui peut conduire au mécontentement des clients lorsque ce contact n'est pas géré correctement.

En plus d'offrir une prévention des fraudes efficace, les produits IBM Security Trusteer n'exigent que peu voire aucune intervention des clients, contrairement à de nombreuses solutions d'authentification et de prévention des fraudes. Au-delà du fait que presque toutes les approches d'authentification peuvent être immédiatement contournées par des menaces de logiciels malveillants avancés et des programmes d'ingénierie sociale, les procédures d'authentification avancées peuvent être fastidieuses ou sources d'erreur pour les clients. Et les technologies basées sur du matériel ne sont pas toujours disponibles lorsque les clients veulent utiliser les services de banque en ligne.

Qui plus est, fournir aux clients une résolution automatisée des problèmes liés aux fraudes peut constituer un excellent outil de fidélisation de la clientèle. Les clients et petites entreprises traditionnels se doivent de reconnaître lorsque leurs périphériques sont infectés par des logiciels malveillants, sans compter qu'il leur faut réussir l'élimination de ces logiciels malveillants. Bien que de nombreux outils d'« élimination des logiciels malveillants », gratuits et payants, soient disponibles, il ne s'agit pour la plupart que de vulgaires applications antivirus, généralement peu efficaces pour supprimer les menaces de logiciels malveillants avancés, en particulier ceux de type « jour zéro ». Lorsque la banque intervient pour identifier et résoudre le problème de logiciels malveillants du client, cela peut créer une relation de confiance à long terme et fidéliser le client.

Avantages pour le client

La définition des ramifications négatives potentielles de « mauvaises » pratiques de prévention des fraudes est assez évidente. Ce qui est parfois moins évident est la manière dont les « bonnes » pratiques de prévention des fraudes peuvent améliorer les relations avec les clients. Une récente recherche académique démontre des associations positives testées de façon empirique entre les activités entreprises par les banques pour protéger les clients de la fraude, et la qualité et fidélité

des relations client. L'étude a démontré que les banques avaient connu une augmentation de la satisfaction, la fidélité, la confiance et les intentions d'achats croisés des clients en fournissant des outils de prévention des fraudes cohérents.[1] Cette influence est particulièrement vraie pour les clients qui ont déjà été victimes de fraude.

Comme exemple de l'influence positive que peut avoir une prévention des fraudes conviviale, un client a signalé une augmentation de 33 % de l'adoption de la banque en ligne après avoir commercialisé de façon proactive Trusteer Rapport auprès de sa base de clients et de revendeurs. La banque considère que le fait de fournir Trusteer Rapport démontre la solide position de la banque en matière de prévention des fraudes et de protection des clients. Cette protection optimisée a influencé les clients encore soucieux de la sécurité en ligne, qui se sont finalement inscrits à la banque en ligne.

Par ailleurs, de nombreuses banques limitent désormais l'envergure des offres de services en ligne, en raison du risque de fraude en ligne. Bon nombre de grandes banques n'offrent pas de fonctionnalités de virement en ligne, et presque toutes les banques limitent dans une certaine mesure les montants et fréquences des transactions. De meilleures fonctionnalités de prévention des fraudes contribuent à réduire les risques de fraude, ce qui va ensuite permettre aux banques d'offrir une plus grande variété de fonctionnalités en ligne avec moins de restrictions sur les transactions.

Composant	Exemples d'indicateur
Impact sur la marque	Des études de tiers indiquent que la moitié des clients affectés par une fraude déplacent leurs comptes bancaires
	Une fuite de liquidités supplémentaire des clients peut également être attendue après la divulgation au public d'un événement de fraude
	Les coûts d'acquisition de clients élevés font de la fidélisation des clients une priorité
Simplicité pour les clients	L'authentification fastidieuse ou des contacts excessifs ou inutiles par les enquêteurs de la fraude réduisent la satisfaction des clients
	Certaines procédures d'authentification avancées ne peuvent tout simplement pas être utilisées par les clients les moins expérimentés
	Les produits IBM Security Trusteer sont discrets, avec toutefois une présence bien visible : le mélange parfait pour le confort et la satisfaction des clients
	La suppression automatisée des logiciels malveillants et l'anticipation des dépenses potentielles peuvent conduire à un meilleur service client et une plus grande satisfaction de la clientèle
	La protection proactive contre les fraudes conduit à une meilleure satisfaction et fidélisation des clients
Avantages pour le client	Visibles, bien que discrètes, les technologies de prévention des fraudes démontrent l'importance accordée au service client et promeuvent une image de marque positive
	Des fonctionnalités de prévention des fraudes optimisées permettent aux institutions financières de fournir de plus vastes ensembles de services en ligne avec moins de restrictions
	L'offre proactive de Trusteer Rapport a permis à une banque d'augmenter l'adoption des services de banque en ligne de 33 %

Conclusion

Il incombe à toutes les institutions financières de trouver un ensemble de solutions de gestion des fraudes qui réduise efficacement les risques identifiés, tout en étant capable de s'adapter aux scénarios de risque futurs. Les techniques de fraude sont en constante évolution, car les fraudeurs testent les points faibles de l'armure des banques, et sont souvent assez inventifs pour en trouver les vulnérabilités. La simple concentration sur la protection de l'institution contre les fraudes connues conduira à un ensemble de solutions qui sera obsolète dès sa mise en œuvre, du fait de la nature évolutive de la fraude en ligne.

L'analyse de rentabilité pour les technologies de prévention des fraudes doit représenter comme il se doit tout l'éventail de coûts et avantages pour l'institution financière. L'élaboration de ce dossier permet aux organisations de prévention des fraudes de former les divisions commerciales appropriées, qui sont nécessaires pour remporter un plus grand soutien en faveur des investissements technologiques. Il peut également démontrer l'intérêt de mettre en œuvre des technologies qui préviennent efficacement les fraudes, tout en promouvant une expérience client positive.

Résumé des composants de l'analyse de rentabilité

Composant	Exemples d'indicateur
Pertes liées aux fraudes sur Internet	Une banque est probablement à l'origine d'une perte de 345 000 dollars liée à la fraude dans le procès Patco
	Une autre banque est probablement responsable d'une perte de 560 000 dollars là encore liée à la fraude dans le procès Experi-Metal
	La plupart des banques considèrent qu'« un seul incident majeur suffit à provoquer d'importants dommages ».
Pertes liées aux fraudes cross-channel	Un client a signalé une réduction de 30 % des escroqueries au chèque pour les clients protégés par Trusteer Rapport
	Un client a signalé une réduction de 93 % des cas de fraudes dans les centres d'appel après la mise en œuvre de la solution Trusteer Pinpoint Malware Detection
	IBM estime que la plupart des banques peuvent espérer réduire la fraude sur les autres canaux de 20 à 30 %, à l'aide des solutions IBM Security Trusteer
Coûts de prévention des fraudes	Les clients IBM signalent une réduction des alertes de faux-positifs de 50 à 90 %
	Plusieurs grandes entreprises ont remplacé des analystes de fraude en raison d'une forte réduction des alertes de faux-positifs, grâce aux solutions IBM Security Trusteer
	De nombreux clients ont déclaré que l'élimination de la fraude basée sur des logiciels malveillants avait contribué à éviter le recours à d'autres solutions technologiques

Composant	Exemples d'indicateur
Risque de conformité réglementaire	Amendes, sanctions, etc. résultant de la non-conformité
	Dépenses excessives consacrées à des technologies inutiles, car supposées nécessaires et efficaces
	De nombreux clients ont déclaré que l'élimination de la fraude basée sur des logiciels malveillants avait contribué à éviter le recours à d'autres solutions technologiques
Risque d'exposition aux litiges	Pertes directes liées aux fraudes absorbées par l'institution financière
	Coûts juridiques, internes et externes, notamment frais d'avocats et de témoins experts
	Mise à mal de la réputation auprès du public, des investisseurs, employés, organismes réglementaires et clients
	Investissements technologiques supplémentaires nécessaires pour résoudre les failles de sécurité qui ont rendu la fraude possible
Impact sur la marque	Des études de tiers indiquent que la moitié des clients affectés par une fraude déplacent leurs comptes bancaires
	Une fuite de liquidités supplémentaire des clients peut également être attendue après la divulgation au public d'un événement de fraude
	Les coûts d'acquisition de clients élevés font de la fidélisation des clients une priorité
Simplicité pour les clients	L'authentification fastidieuse ou des contacts excessifs ou inutiles par les enquêteurs de la fraude réduisent la satisfaction des clients
	Certaines procédures d'authentification avancées ne peuvent tout simplement pas être utilisées par les clients les moins expérimentés
	Les produits IBM Security Trusteer sont discrets, avec toutefois une présence bien visible : le mélange idéal pour le confort et la satisfaction des clients
	La suppression automatisée des logiciels malveillants et l'anticipation des dépenses potentielles peuvent conduire à un meilleur service client et une plus grande satisfaction de la clientèle
	La protection proactive contre les fraudes conduit à une meilleure satisfaction et fidélisation des clients

Composant	Exemples d'indicateur
Avantages pour le client	Visibles, bien que discrètes, les technologies de prévention des fraudes démontrent l'importance accordée au service client et promeuvent une image de marque positive
	Des fonctionnalités de prévention des fraudes optimisées permettent aux institutions financières de fournir de plus vastes ensembles de services en ligne avec moins de restrictions
	L'offre proactive de Trusteer Rapport a permis à une banque d'augmenter l'adoption des services de banque en ligne de 33 %

Pourquoi choisir IBM ?

Les entreprises du monde entier font confiance aux solutions de sécurité d'IBM pour la prévention des fraudes et la gestion de l'identité et des accès. Ces technologies éprouvées permettent aux entreprises de protéger leurs clients, leurs employés et leurs ressources stratégiques contre les menaces de sécurité les plus récentes. Dès que de nouvelles menaces apparaissent, IBM peut aider les entreprises à bâtir leur infrastructure de sécurité centrale avec un portefeuille complet de produits, de services et de solutions de partenaires commerciaux. IBM permet aux entreprises de réduire leurs failles de sécurité et de se concentrer sur la réussite de leurs initiatives stratégiques.

Pour en savoir plus

Pour en savoir plus sur les solutions de prévention des fraudes d'IBM Security Trusteer, contactez votre représentant ou votre partenaire commercial IBM ; vous pouvez également consulter le site Web suivant : **ibm.com**/security

À propos des solutions de sécurité IBM

IBM Security propose l'un des portefeuilles les plus sophistiqués et intégrés en matière de produits et de services de sécurité pour les entreprises. Supporté par la recherche et le développement IBM® X-Force® de réputation internationale, ce portefeuille offre une intelligence dédiée à la sécurité pour aider les entreprises à protéger de manière globale leurs employés, leurs infrastructures, leurs données et leurs applications. Il offre des solutions pour la gestion des identités et de l'accès, la sécurité des bases de données, le développement d'applications, la gestion des risques, la gestion des terminaux, la sécurité des réseaux, etc. Ces solutions permettent aux entreprises de gérer efficacement les risques et d'implémenter une sécurité intégrée pour la sécurité des réseaux, etc. Ces solutions permettent aux entreprises de gérer efficacement les risques et d'implémenter une sécurité intégrée pour les appareils mobiles, le cloud, les réseaux sociaux et les autres architectures stratégiques. IBM dispose de l'un des services de recherche, développement et mise en œuvre les plus importants du monde, surveille 13 milliards d'événements de sécurité par jour dans plus de 130 pays et détient plus de 3 000 brevets relatifs à la sécurité. De plus, IBM Global Financing vous aide à acquérir les capacités logicielles dont votre entreprise a besoin de la manière la plus rentable et stratégique possible. Nous accompagnons les clients pouvant obtenir un crédit afin de personnaliser une solution de financement capable de répondre à vos objectifs stratégiques et de développement, de permettre une gestion efficace des liquidités et d'améliorer votre coût de revient total. Financez un investissement informatique de premier ordre et allez de l'avant avec IBM Global Financing. Pour plus d'informations, consultez le site : **ibm.com**/financing

Compagnie IBM France
17, avenue de l'Europe
92275 BOIS COLOMBES CEDEX

Août 2014

[1] Arvid O.I. Hoffmann et Cornelia Birnbrich, « The impact of fraud prevention on bank-customer relationships: An empirical investigation in retail banking », International Journal of Bank Marketing, Vol. 30 N° 5, 2012. http://www.arvidhoffmann.nl/Hoffmann_Birnbrich_2012.pdf

Trusteer a été acquis par IBM en août 2013.

WGW03044-FRFR-01