EQUIFAX®

Rapport annuel 2023 sur la sécurité

Nous avons intégré **la sécurité dans tout ce que nous faisons**, depuis notre stratégie d'engagement des employés et de fusions et acquisitions jusqu'à notre infrastructure technologique, en passant par notre plateforme Data Fabric personnalisée, le développement de nouveaux produits et notre approche en matière d'intelligence artificielle.

Mark W. Begor

Président-directeur général
Equifax

Une gestion fiable des données est plus importante que jamais.

Alors que nous nous approchons de la mise en œuvre du nuage EquifaxMC, nous tirons parti de nos nouvelles capacités infonuagiques, de notre fabrique de données unique, de nos données différenciées et de nos capacités d'intelligence artificielle (IA) d'IA EFX pour offrir de nouvelles solutions aux clients et aux consommateurs dans chacun des 24 marchés que nous servons. Notre objectif d'aider les gens à profiter de la meilleure situation financière possible et notre engagement à être respectueux des consommateurs à chaque point de contact guident nos actions.

Plus d'une décennie d'innovation grâce à l'IA EFX nous donne de l'élan. Equifax possède plus de 90 brevets qui soutiennent son approche en matière d'IA et d'apprentissage automatique, et nous intégrons nos techniques brevetées d'IA au développement et à la livraison de produits pour permettre aux clients d'accéder plus rapidement aux renseignements. L'utilisation réussie de l'IA exige des données détaillées, exactes et de grande qualité, ce qui rend plus importante que jamais une gestion fiable des données, rendue possible par la solidité des programmes de cybersécurité.

Au cours des six dernières années, nous avons mis sur pied l'un des programmes de cybersécurité les plus avancés et les plus efficaces au monde. Notre programme de cybersécurité a encore gagné en maturité en 2023, surclassant tous les autres principaux produits du secteur pour une quatrième année consécutive. De plus, notre cote de posture de sécurité continue de dépasser les moyennes du secteur des technologies et des services financiers.

Nous nous sommes imposés comme chef de file en intégrant la sécurité dans tout ce que nous faisons, depuis notre stratégie d'engagement des employés et de fusions et acquisitions jusqu'à notre infrastructure technologique, en passant par notre plateforme Data Fabric personnalisée, le développement de nouveaux produits et notre approche en matière d'intelligence artificielle. Peu importe le rôle, la question de la sécurité touche chacun de nos emplois, et nous lui accordons tous la priorité.

Au fil de notre parcours comme chef de file dans ce domaine, nous discutons de nos apprentissages et nous collaborons étroitement avec les clients, les décideurs et d'autres organisations. Nous contribuons ainsi à façonner l'avenir de la cybersécurité afin de mieux protéger nos propres données tout en faisant progresser l'ensemble du secteur. Comme le souligne notre rapport annuel 2023 sur la sécurité, le changement est constant. En ce qui concerne la préparation à l'avenir de la cybersécurité, il est impératif que nous-mêmes, ainsi que nos partenaires partout dans le monde, continuions de relever la barre. Nous nous engageons à être un chef de file de l'industrie en matière de cybersécurité.

Rapide, adaptable et implacable.

L'ingéniosité, la rapidité et le spectre des cyberattaques menées au cours de la dernière année – allant de rudimentaires à sophistiquées – soulignent la portée et l'ampleur de la lutte dans laquelle nous sommes engagés en tant que cyberdéfenseurs.

Qu'il s'agisse d'hypertrucages à la fine pointe de la technologie de l'intelligence artificielle lors de vidéoréunions ou de piratages psychologiques simples sous forme de centres d'assistance, le cyberpaysage a mis en lumière le guide bien trop fructueux des pirates informatiques : Utilisez des technologies de pointe quand vous le pouvez, et faites preuve de simplicité quand cela vous convient. Mais par-dessus tout, soyez impitoyables et adaptez-vous rapidement.

Nous avons adopté une mentalité similaire en 2023.

Lorsque nous avons découvert que des pirates informatiques ciblaient les centres de soutien technique d'autres entreprises, nous avons rapidement mis au point un nouveau cas d'usage révolutionnaire pour notre plateforme sans mot de passe : l'authentification biométrique des appelants. Nous avons ainsi éliminé 94 % des authentifications fondées sur les connaissances en seulement deux mois.

Afin d'anticiper la menace imminente d'hypertrucage par l'IA menant à la fraude, nous avons formé nos employés de façon proactive pour les préparer aux risques potentiels et avons commencé à travailler sur une solution technique, et ce, des mois avant que des membres de l'entreprise ne soient touchés.

Quand les fournisseurs n'avaient pas de correctifs pour les vulnérabilités nouvellement annoncées, nos équipes mondiales ont rapidement mis en œuvre des contrôles créatifs d'atténuation des risques, souvent en moins de 24 heures.

Nous avons su nous adapter rapidement, tirer parti de technologies de pointe dans la mesure du possible et faire preuve de débrouillardise au besoin.

Notre posture de sécurité en 2023 est sans aucun doute liée aux investissements d'Equifax en matière de technologies et de talents, mais c'est notre engagement à l'égard de l'amélioration constante et de l'adaptation rapide qui nous distingue vraiment, tant pour les grandes initiatives que pour les solutions à court terme.

J'éprouve une grande fierté quand je pense aux progrès réalisés par l'équipe d'Equifax en 2023. **Nous sommes mieux placés que jamais pour protéger nos employés, nos clients et nos consommateurs.**

Jamil Farshchi

Chef principal de la sécurité de l'Information
Equifax

Notre incidence :
La sécurité chez Equifax en 2023

En moyenne, **plus de 12 M de cybermenaces** sont contrées chaque jour.

Lancement de **plus de 222 000** simulations pour tester le niveau connaissances en sécurité de notre main-d'œuvre à l'échelle mondiale.

Plus de 23 000
employés et entrepreneurs ont reçu une formation personnalisée sur la sécurité.

Plus de 7 500
utilisateurs externes ont eu accès à notre cadre de contrôles de la sécurité et de la confid entialité.

Plus de 2 800
questionnaires et vérifications au nom des clients ont été remplis.

Plus de 1 900
analyses approfondies des risques des fournisseurs tiers avec une cote de risque critique.

Plus de 600
organisations soutenues par les services liés aux brèches de données d'Equifax, avec un programme de protection de l'identité offert à plus de 13,5 millions de victimes de brèches de données dans 135 pays au nom de nos clients.

Plus de 400
professionnels de la cybersécurité protègent les données des consommateurs.

Plus de 320
vérifications automatisées de sécurité infonuagique surveillées en temps réel.

Plus de 100
innovations de nouveaux produits (INP) ont été mises sur le marché en toute sécurité pour la quatrième année consécutive.

Participation à **plus de 50** forums pour relever les cybermenaces mondiales.

51
attestations et autorisations ont été octroyées par des vérificateurs externes.

45
évaluations de la sécurité physique effectuées, confirmant que les contrôles appropriés sont en place.

Réalisation de **16** simulations d'exercices sur maquette pour se préparer aux scénarios de crise.

8
acquisitions entièrement intégrées du point de vue de la sécurité.

Obtention d'un pointage en matière de maturité du système de sécurité supérieur aux normes de l'industrie pour une **4e** année consécutive.

Portrait de la situation : La cybersécurité en 2023

Les thèmes ci-dessous sont représentatifs des thèmes prévalents de la dernière année.

Le passé est le prologue

Une grande partie des menaces que nous avons relevées dans nos rapports annuels précédents – rançongiciels, attaques par contournement de l'authentification multifacteur, vulnérabilités de la chaîne d'approvisionnement et attaques d'envergure contre des nations – demeurent à la fois omniprésentes et de plus en plus sophistiquées, ce qui fait que le nombre de brèches de données en 2023 a dépassé le record précédent de plus de 70 %[1]. Cette augmentation nous rappelle qu'à mesure que de nouveaux risques émergent, les risques existants doivent être priorisés avec autant de vigilance.

Crise des identifiants

En 2023, une attaque ciblée contre un fournisseur de services de gestion des identités et des accès a démontré l'ampleur des défis liés à la défense contre la menace croissante des attaques liées à l'identité. Qu'il s'agisse d'hameçonnage, de piratage psychologique ou de bourrage d'identifiants, presque tous les secteurs ont été touchés. Des attaques ont été lancées contre les secteurs du divertissement, des biens de consommation et de la biotechnologie, pour ne nommer que ceux-là.

Exploration de l'IA

Les équipes de sécurité ont vu des cas de clonage vocal et même de clonage vidéo activé par l'IA, où des pirates informatiques se sont fait passer pour des dirigeants commerciaux et ont demandé aux employés de prendre des mesures non autorisées, ce qui a fait perdre des millions aux entreprises. Des équipes prudentes ont aussi rapidement établi que toute l'IA n'est pas créée de façon égale – les formules internes d'IA avec des données exclusives et judicieusement sélectionnées sont beaucoup moins risquées et beaucoup plus efficaces que les solutions externes d'IA, qui reposent sur des ensembles de données publiques et des algorithmes génériques.

Impératif de gouvernance

Partout dans le monde, les organismes gouvernementaux ont travaillé à accroître la responsabilité en matière de sécurité. Parmi eux, mentionnons les règles de la Securities and Exchange Commission (SEC) des États-Unis sur la divulgation annuelle d'informations importantes concernant la gestion des risques de cybersécurité, la stratégie et la gouvernance. À la suite de l'annonce de ces règles, un groupe de pirates informatiques spécialisés dans les rançongiciels a déposé une plainte auprès de la SEC contre une de ses victimes qui n'aurait pas respecté le délai de notification d'une cyberattaque.

À mesure que de nouveaux risques émergent, les risques existants **doivent être priorisés** avec autant de vigilance.

[1]Centre de ressources sur le vol d'identité, rapport sur les violations de données 2023

Nos actions :
Initiatives de sécurité et résultats d'Equifax en 2023

Renforcement de notre culture de sécurité interne

La sécurité fait partie de notre ADN. Chez Equifax, nous pensons que la sécurité est l'affaire de tous; nous avons continué de renforcer la formation en matière de sécurité en **lançant plus de 222 000 simulations** pour évaluer en toute sécurité la façon dont notre personnel réagit face à différents scénarios de sécurité, comme des attaques d'hameçonnage.

Nous avons mobilisé notre personnel dans le cadre d'une campagne interne aux résultats records pour le **Mois de la sensibilisation à la cybersécurité** : des milliers d'employés ont mis à l'épreuve leurs connaissances en matière de cybersécurité et se sont familiarisés avec les documents clés liés à la sécurité.

Nous avons **amélioré notre carte de pointage sur la sécurité des employés** pour permettre une mesure plus personnalisée des comportements clés (comme le traitement des données et la navigation sécurisée) et intégré une pondération fondée sur les répercussions pour améliorer la priorisation fondée sur les risques.

Renforcement de la gouvernance du contrôle continu

Nous avons **normalisé** la façon dont nous mesurons notre posture et notre rendement en matière de contrôle, ce qui nous assure une évaluation structurée et fiable de nos mesures de sécurité.

Le pointage du risque quantifiable et continu a contribué à une meilleure harmonisation des priorités et à une exécution plus efficace des améliorations en matière de sécurité.

Nous sommes aussi passés à une plateforme de sécurité infonuagique de nouvelle génération qui **intègre les contrôles aux processus** dans le nuage Equifax[MC], ce qui permet aux utilisateurs d'agir de la bonne façon.

Efficacité accrue

En automatisant les composantes répétitives des flux de travaux (tout en maintenant la supervision humaine) et en favorisant l'**amélioration des processus**, les temps de réponse (et les temps d'exécution des tâches courantes) ont baissé.

Nous avons réduit le temps d'**analyse de chasse aux cybermenaces** (de 87,5 %), le temps de réponse du **centre de gestion de la sécurité** (de 99,6 %) et le temps de traitement des **tickets de soutien pour la prévention des pertes de données** (de 75 %). Nous avons automatisé la **détection des appareils** et davantage.

Vers une sécurité sans friction

Pour donner le coup d'envoi à **notre transition vers un système de connexion sans mot de passe – ainsi que vers le remplacement des identifiants des employés par des données biométriques dans une variété d'applications et de systèmes**, nous avons mis en œuvre un système de réponse vocale interactive pour les appels des employés au centre de soutien technique, éliminant ainsi les identifiants les plus faibles et les plus facilement manipulables au sein des entreprises d'aujourd'hui.

Pour améliorer l'efficacité opérationnelle, nous avons introduit une **option d'approbation par courriel en un clic** dans notre plateforme interne de droits d'accès, ce qui réduit le temps administratif tout en maintenant des protocoles d'authentification robustes.

Et grâce à un programme d'automatisation de la conformité qui est né de nos efforts intégrés et interfonctionnels, nous avons **profondément intégré nos exigences en matière de sécurité des applications** au nuage Equifax.MC

Croissance de l'entreprise alimentée par nos efforts

Nous avons obtenu **34 % plus de certifications qu'en 2022**, tout en réduisant le coût par certification de 19 %, en harmonisant les contrôles et en réutilisant les données probantes. Nous avons ainsi été en mesure de mieux répondre aux exigences des clients actuels et potentiels.

Dans le cadre de ces efforts, nous avons élaboré un **processus d'évaluation des cadres de conformité des États** qui permet à Equifax de mieux servir les gouvernements des États américains dans le nuage.

Nous avons rendu le processus de validation de la sécurité des **produits et des services basés sur le nuage Equifax**MC plus facile pour nos clients, ce qui leur a permis de mettre en correspondance les politiques qu'ils voient dans leur tableau de bord Contrôle infonuagique avec les contrôles correspondants des politiques du cadre de contrôle de la sécurité d'Equifax.

Collaboration externe élargie

Nous avons **eu des dialogues productifs sur la sécurité avec un grand nombre d'intervenants** – des étudiants de l'Université de Californie, des membres de conseils d'administration à la conférence du New Zealand Institute of Directors, des représentants du ministère de la Technologie du Costa Rica, des directeurs financiers au conseil des finances de CNBC – et des douzaines de parties prenantes d'autres emplacements sur différents aspects de la question.

Des mesures ont été prises à la suite de ces échanges. Par exemple, nous avons participé au lancement d'un **cours national de sensibilisation à la cybersécurité** au Costa Rica. Nous sommes également devenues l'une des rares – sinon la seule – entreprises publiques à **faire en sorte que notre cadre de contrôles de la sécurité et de la confidentialité soit libre**, permettant depuis l'accès à plus de 7 000 utilisateurs dans plus de 95 pays.

Accélérer la sécurité à grande échelle

Nous avons accéléré la croissance de notre programme de sécurité, ce qui a permis à de nombreux autres intervenants d'intégrer nos pratiques, grâce à la conception conjointe, à des partenariats public-privé et à la transparence.

Déploiement de notre approche :

Grâce à la conception conjointe avec les fournisseurs

Nous avons contribué à améliorer la sécurité de la chaîne d'approvisionnement.

Lancé en 2022, le Contrôle infonuagique d'Equifax offre à nos clients une visibilité en temps réel sur la sécurité des produits infonuagiques qu'ils nous ont achetés. Bien qu'il s'agisse d'une première dans l'industrie, nous ne voulons pas être un cas unique.

Pour stimuler un plus large changement dans l'industrie, nous avons donc travaillé côte à côte avec notre fournisseur pour créer une nouvelle version, la faisant évoluer vers un stade où d'autres entreprises peuvent utiliser la même solution pour offrir à *leurs clients* cette visibilité en temps réel, permettant ainsi à l'industrie de réduire sa dépendance aux questionnaires.

Nous avons élaboré une approche unique en son genre pour l'authentification au centre de soutien technique.

Lorsque les employés appellent le soutien technique d'Equifax, ils peuvent maintenant utiliser une application mobile pour s'authentifier automatiquement et entrer en contact avec un agent. Cette capacité n'existait pas en mode « prêt à l'emploi » : des formes plus faibles d'authentification multifacteur sont aujourd'hui la norme pour les centres de soutien technique.

Nous avons travaillé à trouver un fournisseur qui partageait notre conception d'une meilleure façon de faire. Nous nous sommes associés pour intégrer cette capacité à l'offre de ce fournisseur, ouvrant la voie à une utilisation par ses autres organisations clientes pour tirer profit de l'outil.

Grâce à des partenariats public-privé

Nous nous sommes associés au gouvernement du Costa Rica pour former ses citoyens.

L'équipe interne de formation et de sensibilisation à la cybersécurité d'Equifax a pour mission d'aider nos employés et nos contractuels à appliquer des pratiques exemplaires en matière de sécurité. Cette équipe a collaboré avec l'institut national de formation du Costa Rica et le ministère de la Technologie pour lancer une formation virtuelle gratuite à l'échelle nationale sur les pratiques exemplaires en matière de sécurité numérique au quotidien.

Nous croyons que les entreprises individuelles devraient contribuer à promouvoir l'éducation, car lorsque le grand public prend des mesures pour réduire les risques en ligne, tout le monde en profite.

Nous avons continué à travailler en étroite collaboration avec le FBI et l'Agence de cybersécurité et de sécurité des infrastructures.

En 2023, l'Agence de cybersécurité et de sécurité des infrastructures (CISA) et le Federal Bureau of Investigation (FBI) nous ont fourni des renseignements sur la façon dont un groupe bien connu de pirates informatiques spécialisés dans les rançongiciels envisageait d'attaquer Equifax. Nous avons adapté nos contre-mesures. La menace est arrivée alors que nous étions avertis et que l'équipe était prête.

La CISA et le FBI fournissent ces renseignements à un éventail d'entreprises. Il est essentiel d'ouvrir les voies de communication, d'écouter les commentaires reçus et de savoir quoi faire lorsque vous entendez quelque chose.

en misant sur la transparence

Nous avons publié notre cadre de contrôles de la sécurité et de la confidentialité.

En nous appuyant sur le cadre de cybersécurité (NIST CSF) et le cadre de protection de la vie privée (NIST PF) du National Institute of Standards and Technology, nous avons élaboré un cadre intégré, interactif et de pointe qui augmente la capacité d'action et la responsabilité au moyen d'exigences techniques. Nous avons donc publié ce cadre pour aider d'autres personnes à élaborer ou à améliorer leurs propres programmes de cybersécurité.

Le cadre a été consulté par 7 500 utilisateurs dans plus de 95 pays, y compris des utilisateurs travaillant au sein d'entreprises du classement Fortune 500, de jeunes entreprises de technologie et de petits organismes sans but lucratif. De nombreux utilisateurs ont comparé notre cadre au leur pour cibler les domaines où ils peuvent améliorer leurs programmes en se basant sur les contrôles que nous utilisons. Avant la publication du nôtre, certaines petites organisations n'avaient même pas de cadre en raison du temps et des efforts que cela exige.

Nous avons aidé la communauté de la conformité en matière de sécurité à réduire au minimum les efforts et les coûts.

Le Conseil des normes de sécurité des données de l'industrie des cartes de paiement (PCI SSC) a des exigences rigoureuses pour assurer la sécurité des données des cartes des clients. Nous nous engageons à nous conformer entièrement à ces normes de la manière la plus efficace et la plus économique possible.

Cet engagement a mené à l'élaboration de directives exhaustives et détaillées sur 15 modèles avancés qui simplifient la conformité des systèmes réglementés par les normes PCI. Nous avons donc été invités à nous joindre au groupe d'intérêt spécial du Conseil PCI pour la segmentation, où les directives d'Equifax ont été intégrées à la prochaine révision des normes PCI. Le fait de partager notre approche interne entraîne un changement dans l'industrie.

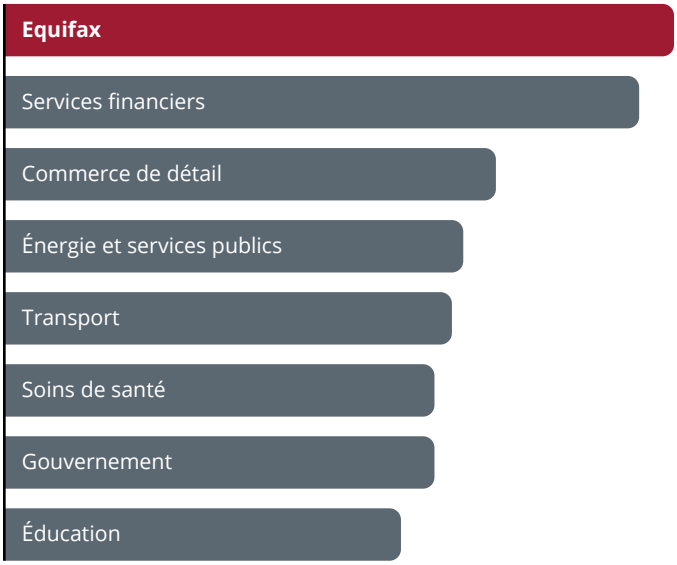
Déploiement de notre approche grâce à la conception conjointe avec les fournisseurs et des partenariats public-privé, en misant sur la **transparence**.

Étalonnage indépendant

Maturité du système de sécurité

Nous collaborons avec un cabinet de recherche et de consultationde premier plan à l'échelle mondiale pour effectuer une analyse approfondie de la maturité de l'ensemble de notre programme de sécurité.

Pointage de maturité du système de sécurité



Qu'est-ce que la maturité du système de sécurité?

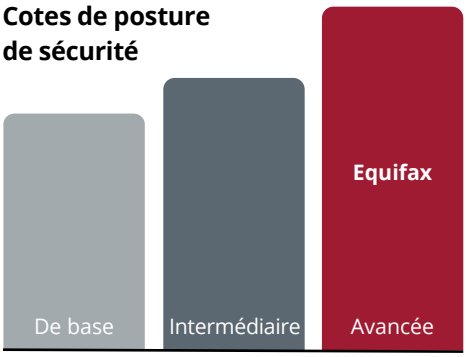
La maturité d'une organisation en matière de sécurité représente sa capacité à s'adapter aux menaces cybernétiques et à gérer les risques au fil du temps.

Notre programme de cybersécurité a gagné en maturité en 2023, surclassant tous les autres principaux produits du secteur pour une quatrième année consécutive.

Posture de sécurité

Un service de production de rapports sur la cybersécurité de premier plan surveille continuellement la posture de notre programme de sécurité et évalue les risques de l'écosystème de notre chaîne d'approvisionnement.

Cotes de posture de sécurité



Il s'agit des catégories de notation attribuées par le service des rapports qui effectue le suivi de notre posture. Equifax maintient une notation qui nous positionne dans la catégorie la plus élevée.

Qu'est-ce que la posture de sécurité?

La posture de sécurité d'une organisation renvoie à son état de préparation et à sa capacité à détecter les menaces et les risques de la sécurité, à y réagir et à s'en remettre.

Notre cote en matière de posture de sécurité a dépassé les moyennes du secteur des technologies et des services financiers pour une troisième année consécutive.

Sommaire des résultats
La sécurité chez Equifax en 2023

Maturité du système de sécurité et posture de sécurité

Nous avons obtenu un pointage record en matière de maturité du système de sécurité, mesuré par une firme mondiale de recherche et de services-conseils de premier plan, surpassant toutes les principales références de l'industrie pour une quatrième année consécutive.

Notre cote en matière de posture de sécurité dépasse les moyennes du secteur des technologies et des services financiers pour une troisième année consécutive.

Cybersécurité

Nous avons surveillé en temps réel 321 vérifications automatisées de sécurité infonuagique, assurant une meilleure visibilité de la posture de notre environnement infonuagique.

Nous avons consolidé les fonctions du centre de gestion de la sécurité et de l'équipe d'intervention en cas d'incident de cybersécurité, créant un modèle à plusieurs niveaux pour la détection et l'intervention 24 heures sur 24, 7 jours sur 7, tout au long du cycle de vie; et nous avons réduit le temps de traitement de 99,6 %.

Nous avons appliqué l'authentification multifacteur pour tous les accès à distance à notre réseau, réduisant ainsi le risque d'accès non autorisé.

Conformité

Nous avons obtenu 51 certifications de vérificateurs externes (une augmentation de 34 % par rapport à 2022), lesquelles confirment notre conformité aux exigences commerciales, juridiques, contractuelles et réglementaires.

Nous avons réalisé des économies de 3 150 heures grâce à l'automatisation de la conformité et à l'harmonisation des contrôles tout en maintenant une supervision humaine robuste.

Nous avons harmonisé l'exécution des vérifications pour réaliser des gains d'efficacité, ce qui se traduit par un taux de réutilisation des données probantes de 29 %.

Fusions et acquisitions

Nous avons intégré huit acquisitions au sein des unités commerciales ou des régions internationales d'Equifax avec des échéanciers accélérés et des contrôles des coûts plus rigoureux, sans négliger les exigences de sécurité de base.

Nous avons fait preuve d'une diligence raisonnable rigoureuse à l'égard de trois acquisitions, dont Boa Vista Serviços, notamment en réalisant une analyse exhaustive des vulnérabilités, un examen du code et une évaluation des compromissions et des contrôles clés avant la signature.

Gestion des risques

Réalisation d'analyses approfondies des risques associés à tous les tiers fournisseurs à risque critique et élevé (1 970).

Réalisation d'évaluations des risques pour toutes les demandes des entreprises (6 453).

Nous avons établi une base quantitative pour le pointage du risque en temps réel qui est examinée par la direction à intervalles réguliers, ce qui aide à harmoniser les priorités en matière de sécurité et de technologie.

Gestion de crise

Réalisation de 16 simulations d'exercices sur maquette et simulations de crise en temps réel avec des intervenants de l'entreprise. Ces intervenants comprennent :
- le président-directeur général et l'équipe de direction;
- 12 équipes de gestion de crises régionales et d'unités commerciales.

Nous avons mis en place de nouvelles ressources pour les employés afin de soutenir notre engagement continu envers la sécurité de nos employés. Voici les principales améliorations :
- plans d'intervention d'urgence révisés;
- guides de référence rapide pour les interventions d'urgence;
- matériel de formation amélioré.

Formation sur la sécurité

Nous avons réalisé 210 406 simulations générales et 12 169 simulations ciblées pour tester la réponse de notre personnel aux problèmes potentiels en matière de sécurité.

Nous avons maintenu une cote globale de sensibilisation à la sécurité de 91,9 %, surclassant les normes de l'industrie.

Nous avons amélioré notre réaction aux tentatives d'hameçonnage, avec un taux de signalement de 59,5 % à l'échelle de l'entreprise (hausse de 16,2 % par rapport à 2022).

Nous avons amélioré notre carte de pointage sur la sécurité des employés pour permettre une mesure plus personnalisée des comportements clés (comme le traitement des données et la navigation sécurisée) et intégré une pondération fondée sur les répercussions pour améliorer la priorisation fondée sur les risques.

Nous avons déployé Security Central, un centre intranet simplifié et convivial où les utilisateurs peuvent joindre la ligne d'assistance 24 heures sur 24, 7 jours sur 7, trouver les responsables de la sécurité des systèmes d'information dédiés à leurs fonctions, accéder aux politiques, aux contrôles, aux FAQ et plus encore.

Nous avons établi une base quantitative pour le pointage du risque en temps réel, ce qui aide à harmoniser les priorités en matière de sécurité et de technologie.

Sommaire des résultats

Services liés aux brèches

Nous avons soutenu 608 organisations ainsi que leurs clients et leurs employés pour les aider à réagir aux cyberincidents et à s'en remettre.

Au nom de nos clients, nous avons offert une protection de l'identité à plus de 13,5 millions de victimes de brèches de données dans 135 pays.

Mobilisation des clients

Nous avons rempli plus de 2 800 questionnaires et vérifications au nom des clients pour assurer la conformité, améliorant la capacité de traitement de 51 %.

Nous avons lancé la deuxième version de Contrôle infonuagique, une solution unique en son genre qui permet aux clients de voir en temps réel la posture de cybersécurité de leurs produits et services basés sur le nuage Equifax.MC

– Une nouvelle fonction permet aux utilisateurs de mettre en correspondance les politiques qu'ils voient dans le Contrôle infonuagique avec les contrôles corre spondants du cadre de contrôles de la sécurité d'Equifax.

Produits et services

Nous avons mis en marché de façon sécuritaire plus de 100 innovations de nouveaux produits pour la quatrième année consécutive.

Nous avons élaboré un processus d'évaluation simplifié pour le Texas Risk and Authorization Management Program (TX-Ramp), reproductible dans tous les cadres de conformité des États, ce qui permet à Equifax de mieux servir les gouvernements des États américains dans le nuage.

Protection des renseignements personnels

Réduction du temps d'intégration infonuagique grâce à l'automatisation de la classification des données tout en assurant une application uniforme des contrôles de protection des données.

Consolidation des outils de contrôle des appareils en une seule plateforme, assurant l'uniformité de la gestion de l'accès aux appareils externes à l'échelle de l'entreprise.

Publication d'une politique de confi dentialité décrivant la façon dont nous recueillons, traitons et stockons les renseignements personnels des employés.

Fraude

Nous avons simplifié les processus et consolidé les outils pour accroître la détection et l'atténuation des fraudes, et ainsi protégé plus de 150 000 consommateurs (une augmentation de 405 % par rapport à 2022).

Sécurité physique et enquêtes

Nous avons réalisé 45 évaluations de la sécurité physique et 16 tests de pénétration physique afin de confirmer que des contrôles appropriés sont en place pour protéger les employés, les données et les actifs.

Grâce à l'amélioration des processus et de l'automatisation, notre Centre de gestion de la sécurité physique a amélioré notre temps de réponse aux alarmes prioritaires locales (3 min, soit 13 % plus rapidement qu'en 2022).

Talent et diversité

Nous avons continué de promouvoir l'inclusivité au sein de notre main-d'œuvre; 59 % des membres de notre équipe de sécurité aux États-Unis étant d'origines diverses, et 31 % de notre main-d'œuvre s'identifiant comme des femmes (contre 24 % en moyenne dans l'industrie).

Douze employés ont obtenu leur diplôme de la cohorte de mentorat individualisé Women Amplifying Voices in Equifax Security (WAVES) en 2023.

La Human Rights Campaign (HRC) a reconnu Equifax comme le meilleur employeur LGBTQ+ dans son rapport sur l'indice d'égalité en entreprise publiée en 2023. Deux membres de l'équipe de sécurité nous ont aidés à obtenir cette reconnaissance en siégeant au conseil d'administration du groupe-ressource d'employés FIERTÉ d'Equifax.

Défense des intérêts et partenariats

Participation à plus de 50 forums visant à promouvoir une cybersécurité renforcée pour les entreprises, les gouvernements et la société.

Élaboration de directives exhaustives détaillant 15 modèles avancés qui aident à éliminer ou à réduire les coûts et les efforts de conformité pour les systèmes réglementés par les normes de sécurité des données de l'industrie des cartes de paiement (PCI); partenariat avec le Conseil PCI pour faire connaître ces efforts dans l'ensemble de la communauté de conformité.

Nous avons fait en sorte que notre cadre de contrôles de la sécurité et de la confidentialité soit libre; il a depuis été consulté par plus de 7 000 utilisateurs dans plus de 95 pays.

Partenariat avec l'institut national de formation du Costa Rica et le ministère de la Technologie pour lancer une formation virtuelle gratuite à l'échelle nationale sur la cybersécurité.

Publication du premier *Security Pulse* pour l'Australie et la Nouvelle-Zélande, un rapport qui détaille l'état de la sécurité dans la région.

Échanges avec la commission de l'énergie et du commerce de la Chambre des représentants pour formuler des commentaires et appuyer des renseignements et démontrer leur soutien à l'égard de la Loi sur la vie privée et la protection des données américaines (ADPPA).

Au nom de nos clients, nous avons offert une protection de l'identité à plus de 13,5 millions de victimes de brèches de données dans 135 pays.

Avons-nous atteint la ligne d'arrivée? Non, pas dans le domaine de la sécurité.

Nos priorités en 2024

Éliminer les secrets

Nous modifions le paradigme traditionnel de l'authentification en remplaçant l'utilisation de mots de passe secrets statiques par des méthodes plus dynamiques et intrinsèquement sécurisées. Nous remplacerons les identifiants des employés par des données biométriques dans une variété d'applications et de systèmes pour un niveau de sécurité, une convivialité et une économie de temps inégalés.

Réduire les risques liés à la chaîne d'approvisionnement

Les attaques par des tiers continuent d'augmenter, ce qui accentue la nécessité de valider le niveau de sécurité et de conformité de nos fournisseurs. De nouveaux outils et processus nous permettent de continuer d'obtenir une vue plus complète des fournisseurs et de leurs positions de risque. Nous optimiserons également nos méthodes pour obliger les fournisseurs à respecter nos normes de pointe.

Miser à fond sur l'IA

En 2024, nous continuerons de tirer parti des avantages positifs de l'IA. Nous y voyons plus qu'un moyen d'optimiser et d'automatiser les processus. Nous la considérons comme un outil pour améliorer notre compréhension et notre préparation. Nous utiliserons l'IA pour synthétiser nos ensembles de données, tester notre posture de sécurité et obtenir une vue vraiment complète qui tient compte des défis et des scénarios que les systèmes traditionnels à base de règles pourraient ignorer.

equifax.com