EQUIFAX®

Rapport annuel 2022 sur la sécurité

Tables des matières

Lettre du PDG
Mark W. Begor

La prochaine étape en matière de cybersécurité

L'année 2022 a été fructueuse pour la nouvelle Equifax, qui est passée de la création du nuage EquifaxMD à l'exploitation sécuritaire de ce nuage à des fins d'innovation de nouveaux produits et de croissance. Equifax n'est plus seulement une agence d'évaluation du crédit. Elle est devenue une entreprise diversifiée des secteurs des données, des analyses et des technologies œuvrant au sein de 24 marchés dans le monde. De plus, nous nous sommes engagés à collaborer de nouvelles manières avec les clients et consommateurs, et ce, tout en évoluant et en innovant pour répondre à leurs besoins changeants.

La cybersécurité est essentielle à ce partenariat.

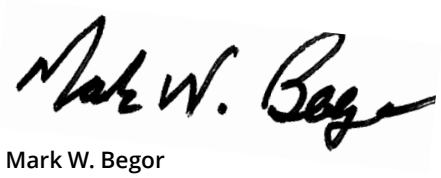
Lorsque je me suis joint à l'entreprise en 2018, je me suis personnellement engagé à ce qu'Equifax devienne une entreprise chef de file de l'industrie en matière de sécurité des données et à bâtir une culture où la sécurité s'inscrit dans l'ADN de notre équipe mondiale — où toute l'équipe Equifax est responsable de la sécurité. Nous avons transformé notre organisation à tous les niveaux pour tenir cette promesse. La sécurité est intégrée à tout ce que nous faisons, que ce soit en matière d'engagement de nos employés, d'infrastructure technologique, d'environnement de données, de développement de produits ou de stratégies de fusion et d'acquisition.

Au cours des cinq dernières années, nous avons mis sur pied l'un des programmes de cybersécurité les plus avancés et les plus efficaces au monde. Notre degré de maturité a surpassé toutes les normes de l'industrie et parmi les entreprises analysées, notre posture s'est établie parmi les meilleures (1 % des meilleures entreprises technologiques et 3 % des meilleures entreprises de services financiers) pendant trois années consécutives.

La transparence a été essentielle à la croissance et à la solidité de notre programme de sécurité. Nous croyons qu'améliorer la communication, la collaboration et la transparence est la clé d'une sécurité renforcée. Afin de communiquer activement les pratiques exemplaires acquises durant la mise en œuvre du changement, nous avons élaboré ce rapport et avons continué d'échanger quotidiennement avec nos clients, les décideurs et d'autres organisations au sujet des défis et des possibilités en matière de cybersécurité au cours de la dernière année.

L'année 2022 a été marquée par de nouvelles menaces pour l'infrastructure mondiale de cybersécurité. Equifax a agi en se défendant contre 39 millions de menaces à la cybersécurité chaque jour et en effectuant plus de 374 000 simulations pour tester sa main-d'œuvre à l'échelle mondiale et se préparer pour l'avenir.

Bien que je sois enthousiasmé par nos progrès, le travail n'est pas terminé. La prochaine étape en matière de sécurité à Equifax s'accompagne d'une évolution continue et d'un engagement inébranlable à aider nos clients, nos partenaires et les consommateurs à renforcer leur propre posture de cybersécurité au profit de toute l'industrie, puisqu'Equifax veille à ce que les organisations de l'industrie deviennent également des chefs de de file en matière de sécurité.



Mark W. Begor
Président-directeur général
Equifax

Lettre du CISO
Jamil Farshchi

Façonner l'avenir.

Les cinq dernières années ont filé à toute vitesse, mais ont parfois semblé durer une éternité. Je me suis joint à Equifax il y a cinq ans et j'ai élaboré pour notre programme de sécurité une stratégie de réduction des risques au minimum et de maximisation de la croissance de l'entreprise. Cette stratégie comportait trois axes : Construire > Maturer > Guider.

Elle a fonctionné. Nous sommes devenus des chefs de file en matière de sécurité, et ce rapport en est la preuve. Nous faisons encore face à des cyber-risques (ce sera toujours le cas), mais ils sont maintenant gérés par les plus grands talents, armés de technologies de prochaine génération et supervisés par le meilleur système de gouvernance. Nous contribuons également à la plus importante période de croissance d'Equifax en 124 ans d'histoire, ce qui est tout aussi important. Des mesures de sécurité de pointe contribuen aux résultats financiers!

Maintenant, quelles sont les prochaines étapes? Qu'est-ce qui vient après l'axe « Guider »? Un mot : **Façonner.**

Nous travaillons activement à façonner les comportements, les technologies et les pratiques en matière de sécurité au-delà de l'entreprise. Pourquoi? Parce que nous sommes très interconnectés et dépendants les uns des autres. L'ancien axiome voulant que « vous êtes aussi solide que votre maillon le plus faible » est plus vrai aujourd'hui que jamais. Ce n'est pas suffisant qu'Equifax soit une entreprise chef de file en matière de sécurité – nous devons ***tous*** l'être.

Les menaces de 2022 ont mis cet impératif en évidence. Des infrastructures vulnérables. Une course au cyberarmement qui s'accélère. Des États-nations qui s'enhardissent. Plus de 50 % des incidents de sécurité sont attribuables à des brèches dans la chaîne d'approvisionnement. Ce sont des défis que personne ne peut résoudre seul.

Notre réponse réside dans l'établissement de partenariats. Nous avons défini une vision audacieuse et collaboré pour relever certains des défis les plus complexes en matière de sécurité.

Nous avons fait appel à des fournisseurs de services de sécurité pour concevoir des technologies de formations, de chaîne d'approvisionnement et d'identité infonuagiques de prochaine génération. Nous nous sommes associés au Federal Bureau of Investigation (FBI) pour améliorer nos partenariats public et privé. Nous avons présenté notre plan de partenariat pour promouvoir les pratiques exemplaires en matière de gouvernance d'entreprise. Nous nous sommes associés à des dirigeants d'entreprises, de gouvernements et d'organismes sans but lucratif pour sensibiliser les intervenants mondiaux aux principaux cyber-risques. Et ce n'est que le début.

C'est ce qu'il faut faire. La coopération est le multiplicateur de force qui nous permettra de gagner la course au cyberarmement. Nous le devons, à nos pays, à nos collectivités et à chacun d'entre nous.

L'année 2022 a été difficile sur le plan de la cybersécurité, et 2023 nous réserve sûrement des surprises. Mais ensemble, nous pouvons gagner ce combat. Allons de l'avant en s'engageant à changer les choses.

Jamil Farshchi
Chef principal de la sécurité de l'information
Equifax

Notre impact

+ de 39 M de cybermenaces défendues en moyenne chaque jour

+ de 374 000 simulations lancées pour tester notre effectif mondial en sécurité

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

+ de 2 700 questionnaires et vérifications remplis au nom des clients d'Equifax pour assurer la conformité

+ de 750 analyses approfondies des fournisseurs tiers présentant un niveau de risque critique.

+ de 600 professionnels en cybersécurité qui protègent les données des consommateurs

+ de 280 clients intégrés au tableau de bord de visibilité en temps réel de la sécurité infonuagique

+ de 160 contrôles de sécurité en nuage automatisés surveillés en temps réel

+ de 110 nouveaux produits Equifax mis sur le marché en toute sécurité

+ de 40 forums ont participé pour relever les cyber-défis mondiaux

38 attestations et autorisations obtenues de vérificateurs externes

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

14 exercices de simulation pour se préparer aux scénarios de crise

4 nouvelles acquisitions qui ont fait l'objet d'une évaluation rigoureuse des risques

3 années consécutives d'obtention d'un pointage de maturité de la sécurité supérieur aux normes de l'industrie

Portrait de la situation

Les thèmes mentionnés ci-dessous résument les principales menaces liées à la connaissance de la situation macroéconomique dont nous avons été témoins en 2022.

Attaques d'envergure contre des nations

Albanie. Australie. Costa Rica. Estonie. Finlande. Monténégro. L'un après l'autre, ces pays ont subi des attaques majeures contre leurs infrastructures. Cette réalité montre à quel point les acteurs malveillants sont audacieux : ils s'en prennent à des gouvernements et nuisent aux services publics, au commerce et aux soins de santé. Mais rien n'a supplanté la cyberattaque contre l'Ukraine, qui a impliqué toutes sortes de moyens, des virus effaceurs jusqu'au piratage d'appareils périphériques connectés.

Vulnérabilités de la chaîne d'approvisionnement

La plupart des entreprises comptent des centaines de partenaires dans la chaîne d'approvisionnement numérique. L'année dernière, le nombre d'attaques par des tiers a connu une forte hausse. Ces attaques ont touché plus de dix millions de personnes. Cela a démontré sans équivoque que si un maillon faible est compromis, les conséquences peuvent résonner sur de nombreuses organisations intégrées.

Attaques par contournement de l'authentification multifacteur

L'authentification multifacteur est depuis longtemps un contrôle incontournable de l'arsenal de défense. Par contre, ses limites sont actuellement mises à l'épreuve. Que ce soit par des astuces d'ingénierie sociale ou par la force brute des demandes répétées, les cybercriminels ont trouvé des moyens de contourner l'authentification multifacteur.

Rareté des talents

Puisqu'il manque plus de trois millions de travailleurs en cybersécurité dans le monde, la main-d'œuvre dans ce domaine a été submergée en 2022. Cette pénurie de talents a été exacerbée par la légère hausse des éléments à protéger en raison d'une numérisation accrue. Sur une note positive, ce défi a poussé les centres d'opérations de cybersécurité vers des percées en matière d'efficacité. En effet, ces derniers ont tiré parti de l'intelligence artificielle et de l'automatisation pour se défendre contre les attaques au lieu de recruter du personnel supplémentaire.

Le domaine de la sécurité continue d'évoluer à un rythme effarant

Nous gardons une longueur d'avance en utilisant le cadre d'évaluation de l'état des menaces d'Equifax. Notre équipe suit l'évolution rapide du domaine de la cybersécurité et évalue le niveau de menace auquel fait face l'entreprise en conséquence.

Cadre des conditions de menace d'Equifax

Le service de la sécurité d'Equifax gère le niveau de menace auquel fait face l'entreprise, lequel varie en fonction de divers facteurs, comme le taux de compromission d'autres entreprises technologiques. Pour chaque niveau de menace — soit surveillé, supérieur, élevé, sévère — nous avons mis en place une série de processus prédéfinis qui dictent diverses actions à notre équipe. Le niveau de menace auquel nous faisons face est régulièrement communiqué à l'équipe de la haute direction et au conseil d'administration de l'entreprise, et il est demeuré surveillé tout au long de 2022.

- Sévère
- Élevé
- Supérieur
- Surveillé

Nos mesures

Renforcement de la sécurité infonuagique

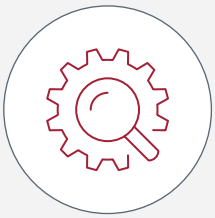
Nous avons continué de renforcer la posture de sécurité du nuage Equifax en atteignant un niveau de sécurité égal pour l'environnement multinuagique et en améliorant la sécurité des conteneurs.

Nous avons également conçu un ensemble de mesures de sécurité pour notre réseau mondial qui définissent un modèle et accélèrent l'intégration des applications et le temps de réponse aux clients pour les applications infonuagiques essentielles.

Sensibilisation accrue des employés à la sécurité

Nous avons élargi nos cartes de pointage de sécurité pour inclure les fournisseurs d'Equifax, instaurant ainsi les mêmes normes élevées pour tout notre personnel. De plus, nous avons collaboré avec notre fournisseur de services n matière de formations en vue d élaborer conjointement de nouvelles mesures ciblées pour certains comportements clés.

À titre d'exemple de sensibilisation accrue à la cybersécurité, les employés ne cliquent plus sur les courriels de simulation d'hameçonnage que nous envoyons, et ils sont plus nombreux à les signaler (et par conséquent, ils signalent aussi les vrais courriels d'hameçonnage).

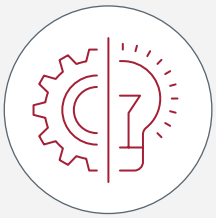


Optimisation de notre portefeuille de fusions et acquisitions

Equifax continue de réinvestir son solide rendement dans des acquisitions stratégiques visant la consolidation afin de renforcer l'entreprise et de stimuler la croissance future du secteur non hypothécaire.

L'équipe de la sécurité a amélioré nos processus d'acquisition en établissant des priorités de contrôle à plusieurs niveaux, un sous-ensemble de contrôles clés et des rapports fondés sur les risques. Pour nous assurer que les entreprises nouvellement acquises respectent nos normes rigoureuses, nous avons procédé à l'harmonisation des contrôles pour quinze acquisitions.

Nos mesures - la suite



Modernisation et connexion de nos outils de sécurité

Afin d'accroître les leviers d'exploitation de notre équipe, nous avons amélioré notre ensemble d'outils de sécurité dans les domaines de la protection des points d'extrémité, de la gestion des accès, de la journalisation et de la reconnaissance des images. Il en résulte une meilleure gouvernance ainsi qu'une réduction des risques et des frictions pour l'entreprise.

Ces améliorations sont en grande partie le fruit des partenariats avec des fournisseurs de technologies pour concevoir conjointement des solutions maintenant offertes dans l'ensemble du marché, permettant ainsi de renforcer la sécurité dans tout l'écosystème commercial.

Stimulation de la croissance d'entreprise

Plus de 280 clients ont adopté Contrôle infonuagique, un tableau de bord qui fournit des renseignements en temps réel sur la posture de sécurité des produits et services infonuagiques d'Equifax qu'ils utilisent.

De plus, nous avons obtenu de nouvelles certifications qui créent des possibilités pour l'entreprise. Nous nous conformons à la Health Insurance Portability and Accountability Act (HIPAA) des États-Unis pour deux environnements clés et avons une attestation de sécurité d'installation secrète du gouvernement du Canada.

Transparence et collaboration avancées

Nous avons misé sur notre engagement continu auprès de nos parties prenantes partout dans le monde en priorisant les sujets et les occasions de partenariat qui ont le plus d'incidence sur es progrès en matière de cybersécurité.

Nous avons notamment partagé notre expertise sur la création de partenariats efficaces entre les conseils d'administration et les chefs principaux de la sécurité de l'information et sur l'instauration d'un dialogue efficace entre les organisations publiques et privées, en collaboration avec des organisations telles que le Bipartisan Policy Center, le Swiss Cyber Institute et la National Association of Corporate Directors.

Insister sur la collaboration et la transparence

Façonner l'avenir

La sécurité à grande échelle exige un travail d'équipe. En 2022, nous avons collaboré avec des intervenants externes de multiples façons.

Au départ, nous avions une vision stratégique pour notre programme et la sécurité en général, mais aucun produit n'existait pour concrétiser cette vision. Cela ne nous a pas arrêtés. **Nos relations avec les fournisseurs, qui étaient auparavant transactionnelles, sont devenues transformatrices.** Nous avons coopéré pour mettre sur le marché des solutions de prochaine génération. En plus de modeler nos propres capacités de pointe partenariats font progresser l'ensemble de l'industrie.

- Nous avons cherché un mécanisme positif et motivant pour cibler, enseigner, mesurer un ensemble de **comportements sécuritaires** à adopter par les employés. Par conséquent, nous avons collaboré avec notre fournisseur de formations pour améliorer la profondeur et la portée de son offre, notamment avec des mesures complètes et une rétroaction en temps réel.
- Aucun produit prêt à l'emploi ne répondait à notre vision de la mise en œuvre des mesures de **sécurité de la chaîne d'approvisionnement**. Nous nous sommes donc tournés vers la conception. Nous nous sommes associés à un fournisseur de logiciels de sécurité de premier plan pour transformer un produit émergent en un outil novateur de transparence infonuagique entièrement opérationnel pour les clients.
- Nous voulions une solution basée sur l'infonuagique et unifiée en matière de gouvernance et d'administration de l'identités et de gestion des accès privilégiés. Il n'en existait aucune. Nous avons donc choisi un partenaire pour répondre à nos exigences en matière de conception et travailler main dans la main avec nous à la création d'une solution dotée de **capacités intégrées** de prochaine génération axées sur l'infonuagique, non seulement pour nous, mais aussi pour tous les autres intervenants sur le marché.
- Nous avons collaboré avec l'équipe d'ingénierie de Ping Identity pour automatiser nos **capacités d'authentification** et avons reçu le prix Cloud Identity Champion pour notre travail qui permet de faire progresser l'industrie.

Présentation du plan directeur du conseil d'administration en matière de partenariats avec ces groupes afin d'aider les gestionnaires à améliorer le dialogue avec les responsables de la sécurité de l'information, et ainsi mieux comprendre les cyber-risques :

National Association of Corporate Directors	The New York Stock Exchange (NYSE) Board Advisory Council	Glass Lewis Investors Perspective	Service de sécurité et gestion des risques de Gartner	Réseau des comités d'audit d'EY

Collaboration avec des législateurs, des organismes gouvernementaux, des ONG et des organismes de réglementation :

- Le chef principal de la sécurité de l'information d'Equifax a été nommé **conseiller en mobilisation stratégique auprès du FBI**.
- Nous avons établi un partenariat avec le **Bipartisan Policy Center** pour relever les défis associés aux principaux risques en matière de cybersécurité des entreprises, des gouvernements et de la société en 2023.
- Nous avons collaboré avec le **Costa Rica Cyber Security Cluster** pour favoriser l'établissement de partenariats public-privé entre le ministère des Sciences et de la Technologie, la chambre des industries du Costa Rica, les universités et d'autres entreprises.
- Nous avons collaboré avec la **Chilean Cybersecurity Alliance** pour contribuer aux politiques de cybersécurité au Chili.
- Nous avons également appuyé la cyber-résilience de l'Australie et de la Nouvelle-Zélande par le biais de **CISOLens**.

Cyber-gouvernance

L'importance accrue de la réglementation en matière de cybergouvernance fait de la sécurité une responsabilité fondamentale du conseil d'administration et de l'équipe de direction.

Et comme nous disposons déjà d'un solide partenariat avec nos hauts dirigeants et notre conseil d'administration, nous partageons nos apprentissages durement acquis à la fois pour orienter la réglementation et aider les organisations à s'y conformer.

En vertu du dernier règlement du New York State Department of Financial Services (NYDFS), **le chef de la direction et le chef de la sécurité de l'information doivent cosigner une attestation annuelle de conformité aux mesures de sécurité**, et un conseil d'administration doit :

- Posséder une expertise et des connaissances importantes en matière de cyber-risques pour assurer une surveillance efficace.
- Approuver les politiques, les procédures et l'évaluation des risques en matière de sécurité de l'entreprise.
- Recevoir des rapports du chef principal de la sécurité de l'information au moins une fois par année.
- Examiner tout problème important découlant des évaluations de la vulnérabilité et des tests d'intrusion.

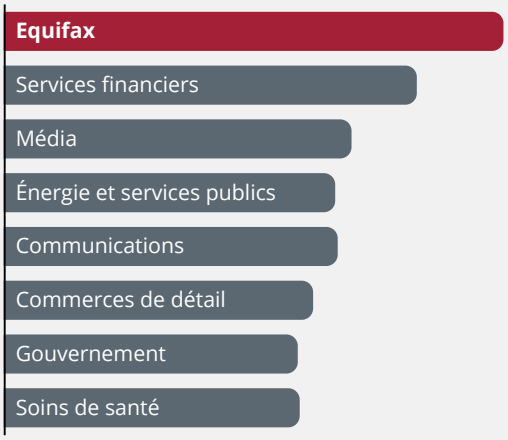
Selon Glass Lewis, leader en matière de services-conseils aux investisseurs, notre transparence est **« tout à fait unique et remarquable ».**

Analyse comparative indépendante

Maturité des mesures de sécurité

Un cabinet de recherche et de conseil international de premier plan effectue chaque année une analyse approfondie de la maturité de l'ensemble de notre programme de sécurité.

Pointage de maturité en matière de sécurité 2022



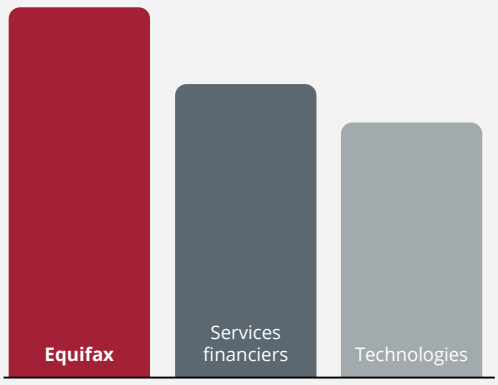
Qu'est-ce que la maturité des mesures de sécurité?
La maturité d'une organisation en matière de sécurité représente sa capacité à s'adapter aux cybermenaces et à gérer les risques au fil du temps.

À la fin de 2022, la maturité de notre programme de cybersécurité a surpassé tous les principaux indices de référence du secteur pour une deuxième année consécutive.

Posture de sécurité

Un service de signalement de cybersécurité de premier plan surveille continuellement la posture de notre programme de sécurité et évalue le risque de notre écosystème de la chaîne d'approvisionnement.

Pointage de posture de sécurité 2022



Qu'est-ce que la posture de sécurité?
La posture de sécurité d'une organisation est sa préparation et sa capacité à identifier les menaces et les risques liés à la sécurité, à y répondre et à s'en remettre.

À la fin de 2022, nos capacités en matière de sécurité nous ont permis de nous classer parmi 1 % des meilleures entreprises de technologie et 3 % des meilleures entreprises de services financiers analysées.

Résumé des résultats

Maturité et posture de sécurité	• Optimisation des dépenses liées à la cybersécurité à 9,2 % du budget des TI, sous la moyenne du secteur (9,9 %). • Obtention d'un pointage de maturité en matière de sécurité supérieur à toutes les normes de l'industrie pour une troisième année consécutive. • Obtention d'un pointage de posture de sécurité nous classant parmi 1 % des meilleures entreprises de technologie et 3 % des entreprises de services financiers analysées.
Cybersécurité	• Mise en œuvre de 349 vérifications automatisées de sécurité infonuagique surveillées en temps réel. • Forte amélioration de la sécurité des applications; 96 % des applications vérifiées faisant partie de l'analyse automatisée à la fin de 2022 (comparativement à 69 % en août). • Authentification multifacteur (MFA) pour tous les accès à distance à notre réseau. • Passage à des outils de prochaine génération pour la protection des points d'extrémité, la gestion des accès, la journalisation et la reconnaissance des images.
Conformité	• Obtention de 38 certifications de vérificateurs externes (une augmentation de 45 % par rapport à 2021), lesquelles confirment notre conformité aux exigences commerciales, juridiques, contractuelles et réglementaires. • Equifax Canada a obtenu l'attestation de sécurité d'installation secrète du gouvernement du Canada. • Conformité à la HIPAA pour deux environnements clés : Kount (notre plateforme de protection contre la fraude) et nos services de protection contre les brèches.
Fusions et acquisitions	• Nous avons fait preuve d'une diligence raisonnable rigoureuse à l'égard des quatre acquisitions réalisées en 2022, notamment en réalisant une analyse exhaustive des vulnérabilités, un examen du code et une évaluation des compromissions et des contrôles clés avant de signer toute entente. • Nous avons développé une nouvelle stratégie d'intégration de la sécurité à trois niveaux pour s'assurer que les nouvelles entités adoptent rapidement les contrôles d'Equifax. • Nous avons procédé à l'harmonisation des contrôles de sécurité pour 15 acquisitions d'Equifax.
Gestion des risques	• Réalisation d'analyses approfondies des risques associés à tous les fournisseurs tiers présentant un risque critique (plus de 750). • Adoption de la solution Contrôle infonuagique par plus de 280 clients. Il s'agit d'une plateforme unique sur le marché qui offre aux clients une visibilité en temps réel de la sécurité des produits et services infonuagiques d'Equifax qu'ils utilisent.
Gestion des crises	• Réalisation de 14 simulations d'exercices sur maquette et simulations de crise en temps réel avec des intervenants de l'entreprise. Ces intervenants comprennent : – Le conseil d'administration – Le président-directeur général et l'équipe de direction – 12 équipes de gestion de crises régionales et d'unités commerciales
Confidentialité	• Mise en œuvre du chiffrement côté client de Google Workspace pour chiffrer les données sensibles qui y sont stockées.

Résumé des résultats - la suite

Formation en matière de sécurité	• Réalisation de 15 simulations globales et de 18 simulations ciblées pour tester les comportements sécuritaires de notre main-d'œuvre en matière de sécurité. • Élargissement de la portée de notre Aperçu de la sécurité à 23 500 employés d'Equifax, contractuels et à temps plein. • Maintien d'un pointage de sécurité aggrégé de 91, surpassant les normes de l'industrie. • Réduction du taux de clics moyen des employés lors des simulations d'hameçonnage à 4,2 % (amélioration de 10 % par rapport à 2021). • Ajout de nouveaux comportements à la carte de pointage de la sécurité des employés en fonction des postes, notamment sur le plan de la navigation sécurisée et du traitement des données sensibles.
Services d'atteinte à la vie privée	• Soutien de 716 organisations et de leurs clients pour les aider à réagir aux cyber incidents et à s'en remettre.
Engagement des clients	• Plus de 2 700 questionnaires et vérifications au nom de clients d'Equifax pour assurer la conformité.
Produits et services	• Mise en marché sécurisée de 113 nouveaux produits pour nos clients. • Sécurité des produits intégrée dès l'étape de la conception. Équipes des produits conseillées et développeurs disposant d'un outil libre-service pour corriger les vulnérabilités.
Fraude	• Mise en place de capacités de pointe en matière de lutte contre la fraude qui intègrent l'apprentissage automatique, l'intelligence artificielle et l'amélioration des intrants des fournisseurs, tout en réduisant les frictions avec les consommateurs.
Sécurité matérielle et enquêtes	• Réalisation de 12 tests d'intrusion physique pour cerner les points à améliorer sur une base continue afin de prévenir les accès non autorisés aux installations. • Réalisation de 38 évaluations de la sécurité physique confirmant 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 pour ce qui suit : – Alarmes locales hautement prioritaires : 3 min 21 s (16 % plus rapide qu'en 2021). – Rapports de renseignements entrants : 2 min 7 s (58 % plus rapide qu'en 2021).
Talents et diversité	Augmentation continue de la diversité de notre main-d'œuvre : • 13 % des membres de l'équipe de sécurité aux États-Unis sont noirs (comparativement à la moyenne de l'industrie de 9 %). • 27 % des membres de l'équipe de sécurité aux États-Unis s'identifient comme des femmes (comparativement à la moyenne de l'industrie de 24 %).
Plaidoyer et partenariat	• Participation à plus de 40 forums visant à promouvoir une cybersécurité renforcée pour les entreprises, les gouvernements et la société. • Partenariat avec le Bipartisan Policy Center pour relever les principaux risques en matière de cybersécurité pour les entreprises, les gouvernements et la société en 2023. • Chef principal de la sécurité de l'information nommé à titre de conseiller en mobilisation stratégique auprès du FBI pour faire progresser la relation du FBI avec le secteur privé.

Rien ne nous arrête

Optimisation de nos outils et processus

Nous avons établi et documenté des politiques et des mesures clés. Les pratiques de sécurité sont normalisées et intégrées à la stratégie d'affaires globale d'Equifax. Nous avons atteint une étape de notre parcours de maturité où il est temps de nous concentrer sur l'optimisation.

Nous améliorerons nos outils, nos données, et nous perfectionnerons notre main-d'œuvre afin d'élargir notre appareillage en fonction de l'objectif visé. Cela nous permettra de contrer efficacement les menaces, qui sont en constante évolution, et de garder une longueur d'avance dans la course au cyberarmement.

Vers une sécurité sans friction

Les employés vont faire leur travail, quoi qu'il arrive. Si les contrôles sont fastidieux, les employés les contourneront et ils feront des erreurs, augmentant les risques. Ils seront également ralentis dans leurs tâches et trouveront donc les mesures de sécurité irritantes. Une sécurité sans friction aide à réduire les risques et à améliorer la productivité de la main-d'œuvre.

Bien que nous ayons réalisé des progrès significatifs dans l'intégration du libre-service et de l'automatisation à l'échelle de l'entreprise, nous n'avons pas terminé. Nous peaufinerons et mettrons à l'échelle les capacités que nous avons introduites en 2022, en modulant chaque expérience utilisateur afin qu'il soit facile pour tous les intervenants d'agir de la bonne façon.

Renforcement de la protection de l'identité

Le terme « vérification systématique » est surutilisé. Toutefois, les principes qui sous-tendent cette notion, à savoir éviter les suppositions, assurer une surveillance continue et s'appuyer sur la vérification, sont d'une importance capitale.

Bien que nous appliquions déjà les principes d'accès « juste à temps » et « temporel » pour les ressources privilégiées, nous ne ménagerons aucun effort dans notre quête visant à protéger la vie privée des consommateurs et à réduire au minimum les risques d'attaques grâce à une sécurité à niveaux multiples.

equifax.com