PROTECTION DES DONNÉES RAPPORT 2021

N'est plus facultatif : Investir dans les données et la sécurité de l'information maintenant ou payer plus tard

Nous protégeons ce qui compte.

Shred-it®
Une Solution Stericycle®

Table des matières

Avant-propos

Si jamais il y a eu une année qui a souligné l'importance croissante d'investir dans la gestion sécurisée des documents, la protection des données numériques et la sécurité de l'information, c'est bien 2021.

La COVID-19 a remodelé notre façon de travailler et notre environnement de travail, mettant du stress sur les systèmes, les partenariats et les réseaux. Bien que les cyberviolations à profil élevé aient le plus d'attention des médias, les violations physiques divulguées, y compris le vol de documents, ont tout de même représenté 43 % des actifs violés en 2021.[1]

Il est essentiel que les chefs d'entreprise de tous les secteurs reconnaissent que le fait de garder un profil bas n'est pas suffisant. Ils doivent comprendre les enjeux importants en jeu et les implications d'une protection inadéquate des données, non seulement pour protéger leur rendement commercial, leurs ventes et le cours de leur action, mais aussi pour protéger leur réputation et fidéliser les clients. Ils doivent également prioriser les efforts pour planifier les menaces nouvelles et émergentes, à l'intérieur et à l'extérieur de leurs murs. De plus, puisque la majorité des États travaillent actuellement sur des factures complètes de confidentialité des consommateurs, les entreprises doivent rester informées des changements apportés à la législation sur la protection des données pour assurer la conformité. Les dirigeants avertis tireront parti de ces moments sans précédent pour promouvoir la confiance et établir un nouveau type de relation avec les clients en priorisant la sécurité de l'information.

Pour soutenir sa mission d'aider les organisations à protéger les renseignements confidentiels du monde et à prévenir les atteintes à la sécurité des données, Shred-it, une solution de Stericycle, a tiré parti des résultats détaillés d'un sondage approfondi mené auprès de cadres supérieurs, de propriétaires de petites et moyennes entreprises et de consommateurs partout en Amérique du Nord pour produire son 11e rapport annuel sur la protection des données (RPP). En tant que chef de file de l'industrie en matière de destruction sécurisée des renseignements, nous nous engageons à protéger la santé et le bien-être des relations de confiance de nos clients, de la réputation de la marque et des résultats. Le DPR 2021 a été développé pour offrir des perspectives pratiques et les prochaines étapes recommandées, au-delà de la simple comptabilité des résultats du sondage.

Merci à nos contributeurs au sondage 2021. Vous comprenez que personne n'est à l'abri de la menace d'une violation de données, et vos idées servent de renforcement puissant de l'importance de la sécurité de l'information, afin de protéger vos données, votre réputation et vos activités. À nos lecteurs, sachez que Stericycle, par l'entremise de notre solution de destruction sécurisée des renseignements Shred-it, est dans la lutte avec vous. Notre équipe se tient debout, prête à aider à naviguer dans les complexités du paysage en constante évolution de la protection des données pour façonner un monde plus sain et plus sûr pour tous, partout, tous les jours.

S. Cory White
Vice-président directeur et directeur commercial | Stericycle

Principaux points à retenir de la révélation des rapports 2021 :

- Avec l'augmentation des règlements et des risques financiers, le fait de maintenir un profil bas n'est pas suffisant
- La réputation de la sécurité des données joue un rôle crucial dans les perspectives et les comportements des consommateurs
- Les menaces internes continuent de planer et les entreprises doivent être vigilantes

Sommaire de gestion

Les lois et les règlements sur la protection des données ont évolué au cours des 10 dernières années, afin de mieux protéger les données des consommateurs et d'encourager les entreprises à agir, et d'autres changements sont à l'horizon. Plusieurs États, comme la Californie, le Colorado et la Virginie, ont récemment mis en œuvre des lois sur la protection des renseignements personnels des consommateurs, et d'autres sont censés suivre, car la majorité des États travaillent sur une législation complète sur la protection de la vie privée des consommateurs. De plus, le Canada a déjà adopté la Loi sur la protection des renseignements personnels et les documents électroniques.

Bien que l'impact financier d'une violation de données dans l'ensemble soit potentiellement élevé, le coût de la non-conformité est un contributeur de premier plan.

> **Selon le rapport 2021 d'IBM sur le coût d'une violation de données,[2] « sur une sélection de 25 facteurs de coûts qui amplifient ou atténuent les coûts de violation de données, les défaillances de conformité ont été le facteur d'amplification des coûts. »**

En plus des mesures réglementaires et des amendes ainsi que des frais juridiques, les violations de données peuvent également avoir un impact dévastateur sur les résultats d'une entreprise, y compris la baisse de la réputation de la marque et la perte de clients. Compte tenu des ramifications associées aux violations de données, il est important de comprendre comment une violation de données peut se produire et comment les entreprises peuvent se préparer au mieux. Les violations de données se classent dans deux catégories principales, physiques et numériques. **Les violations physiques** comprennent le vol d'articles ou d'équipement comme les dossiers des employés, les déclarations fiscales, les renseignements sur les clients et les dossiers médicaux. **Les violations numériques** comprennent un accès non autorisé,une erreur du système ou humaine, ou une attaque délibérée contre un système ou un réseau.

Violation physique

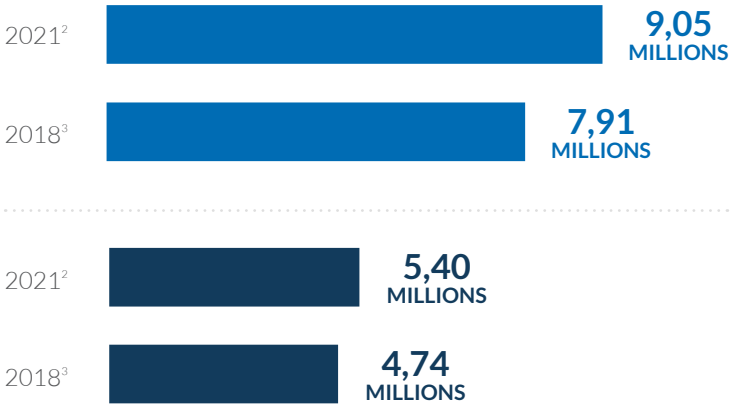
LES DOCUMENTS PAPIERS | LES ORDINATEURS PORTABLES | LES DISQUES DURS EXTERNES

Violation numérique

LES LOGICIELS MALVEILLANTS | LE RANÇONGICIEL | L'HAMEÇONNAGE

Le coût moyen d'une atteinte à la protection des données a connu une croissance notable depuis 2018

(Mesuré en millions de dollars étatsuniens) — É.-U. — CANADA



Plus de

50 % DE

ÉTATS

devraient mettre en œuvre la législation sur la protection de la vie privée des consommateurs[4]

Renseignements clés

Basé sur des données de sondage approfondies en 2021 et une analyse des dirigeants et des consommateurs nord-américains, le DPR 2021 de Shred-it révèle des perspectives essentielles sur le paysage en constante évolution de la sécurité de l'information. Le rapport de cette année présente des recommandations simples et pratiques aux dirigeants d'entreprise en première ligne pour assurer la sécurité de leurs données, soulignant les thèmes clés suivants :

L'incidence d'une violation de données est susceptible de se produire et les entreprises ne peuvent pas être préparées

Environ quatre chefs d'entreprise sur dix évaluent le risque d'une tentative de violation de données au cours des 12 prochains mois comme étant un « 4 » ou un « 5 » sur une échelle de risque à 5 points, « 5 » étant le risque le plus élevé. Cela peut laisser les entreprises non préparées, car plus de la moitié des entreprises interrogées n'ont pas de plan d'intervention en cas d'incident.

La réputation de la sécurité des données joue un rôle important dans les perspectives et les comportements des consommateurs

Les consommateurs continuent de prendre très au sérieux la sécurité de leurs renseignements personnels. Plus de 80 % des consommateurs décident avec qui faire affaire en fonction de la réputation de sécurité des données d'une entreprise.

Les menaces internes continuent à augmenter

Bien que les tiers malveillants soient des sources de violations de données dans de nombreux cas, les initiés « fiables » (partenaires externes (40 %) et les erreurs des employés (22 %) sont probablement la cause. Cela souligne la nécessité pour les entreprises d'avoir des mesures préventives en place pour toutes les sources de données.

Les répondants à l'enquête comprennent :

- Cadres supérieurs
- Consommateurs
- Propriétaires de petites et moyennes entreprises

DANS CINQ INDUSTRIES :

- Soins de santé
- Finances
- Services professionnels
- Assurance
- Immobilier

Investir dans la sécurité des données et de l'information ne peut plus être considéré comme facultatif

4 SUR 10 CHEFS D'ENTREPRISE évaluent le risque d'une tentative de violation de données au cours des 12 prochains mois comme un « 4 » ou un « 5 » sur une échelle de risque de 5 points

Plus de **50 %** DE **CHEFS D'ENTREPRISE** n'ont pas un plan d'intervention

Plus de **80 %** DE **CONSOMMATEURS** décident avec qui faire affaire en fonction de la réputation de sécurité des données d'une entreprise

40 % DES **VIOLATIONS DE DONNÉES** sont causés par des partenaires externes ET PRESQUE **25 %** par erreur d'employé

AVEC DES RÈGLEMENTS CROISSANTS ET DES RISQUES FINANCIERS

Garder un profil bas n'est pas suffisant

Étant donné la forte probabilité que les entreprises subissent une violation de données, il est essentiel qu'elles se préparent avant que la violation ne se produise. La complaisance ne fonctionnera pas, car aucune organisation n'est immunisée. Peu importe que vous traitiez des données électroniques ou papier, les risques sont les mêmes. Par le passé, le maintien d'un profil bas a permis à certaines organisations d'y arriver. Ce n'est plus le cas, car tout le monde crée des données, et avec des données, elles deviennent une cible.

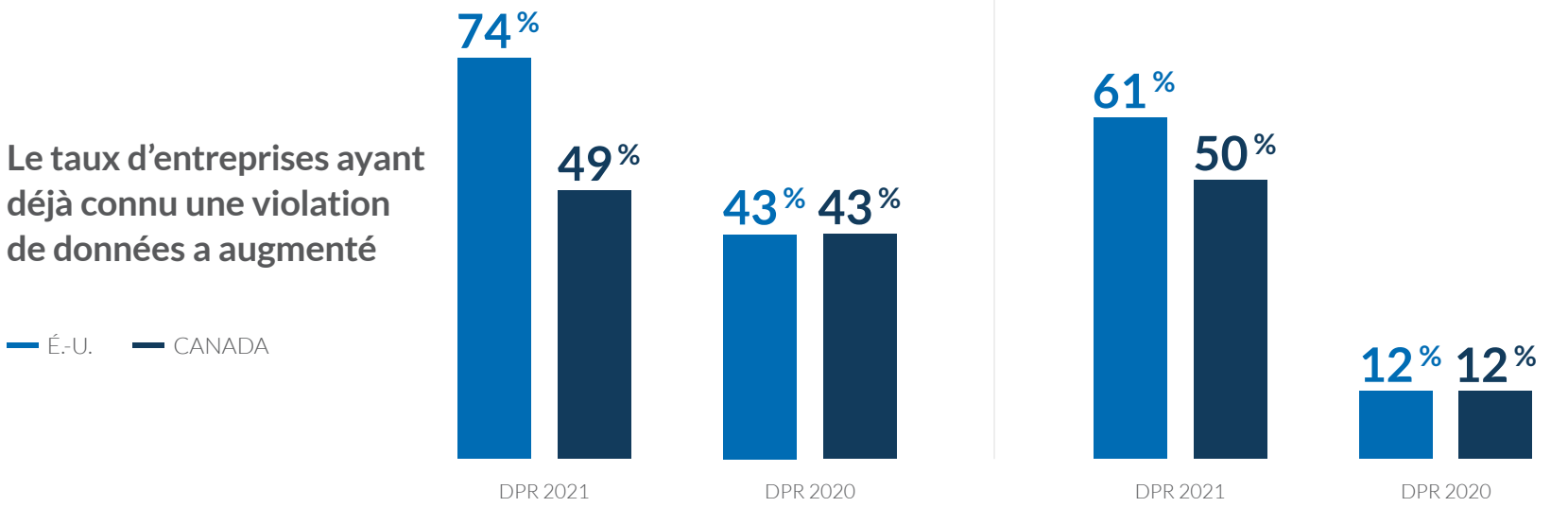
L'incidence des violations de données continue de grandir

Les résultats du DPR de cette année indiquent que les trois quarts des grandes entreprises aux États-Unis qui ont déjà été interrogées ont déjà connu une violation de données, ainsi que plus de la moitié des petites et moyennes entreprises interrogées aux États-Unis. Il s'agit d'une augmentation importante par rapport au DPR de 2020. Bien qu'elles ne soient pas aussi répandues qu'aux États-Unis, les grandes entreprises au Canada ont également constaté une augmentation de la violation des données.

Selon le rapport de fin d'année 2020 de Risk Based Security, en 2020, plus de 37 milliards de dossiers ont été exposés à des milliers de personnes à l'échelle mondiale, soit une augmentation de 141 % par rapport à 2019.[5] Cela ne présage rien de bon pour les entreprises nord-américaines, car 1 personne sur 4 craint qu'une tentative de violation des données soit très probable pour leur entreprise au cours des 12 prochains mois.

Bien que les cyberattaques font les manchettes, les violations de données physiques sont également une préoccupation. Un rapport récent de Verizon montre que les violations physiques avec la divulgation de données connues comptaient 43 % des actifs violéss.[1]

Le taux d'entreprises ayant déjà connu une violation de données a augmenté



En 2020,

37

MILLIARDS DE DOSSIERS

ont été exposés à des milliers de personnes dans le monde, soit une augmentation de 141 % par rapport à 2019[5]

Impact des violations de données trop importantes pour être ignoré

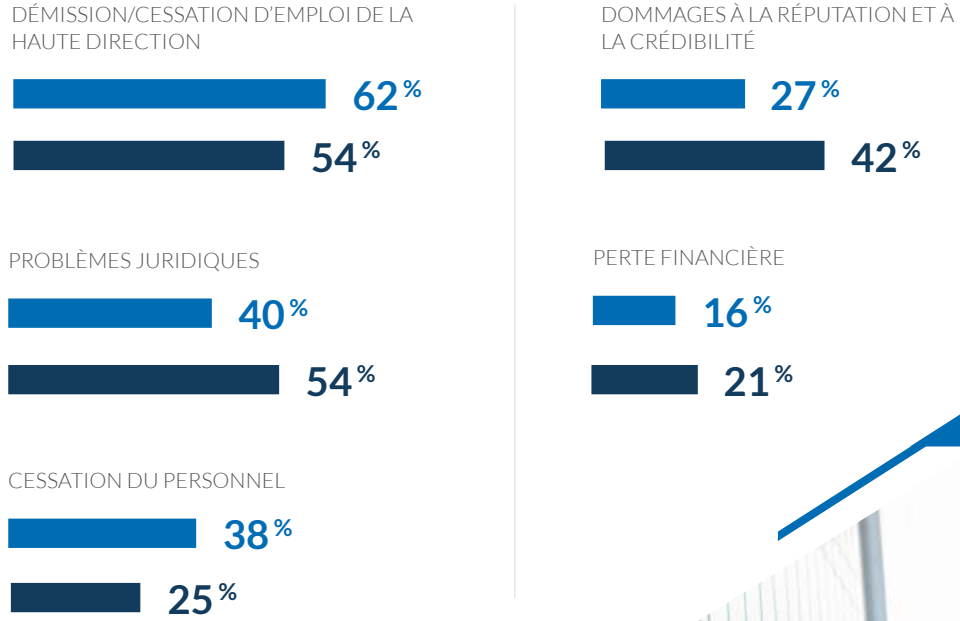
Bien que les infractions à la vie privée des consommateurs soient certainement une source de notification des entreprises, elles sont d'autres conséquences importantes lorsqu'une violation de données se produit. Parmi les dirigeants nord-américains de grandes entreprises, la démission de la haute direction ou la cessation d'emploi et les questions juridiques ont été les conséquences les plus citées.

De plus, les dirigeants de grandes entreprises au Canada étaient plus susceptibles (42 %) de citer des atteintes à leur réputation et à leur crédibilité par rapport à leurs homologues étatsuniens (27 %).

27 % DE **GRANDES ENTREPRISES ÉTATSUNIENNES** ET **42 %** DE **GRANDES ENTREPRISES CANADIENNES**

interrogés citent une atteinte à leur réputation et à leur crédibilité à la suite d'une violation de données

Conséquences des violations de données indiquées par les cadres supérieurs



Les entreprises manquent de planification adéquate, ce qui les expose à des risques

Bon nombre des entreprises interrogées ont indiqué qu'elles n'ont pas de plan d'intervention en cas d'incident (cadre supérieur : 63 % aux États-Unis, 58 % au Canada; PME : 67 % aux États-Unis, 57 % au Canada). Cela s'avère problématique pour réagir rapidement lorsqu'une violation de données se produit.

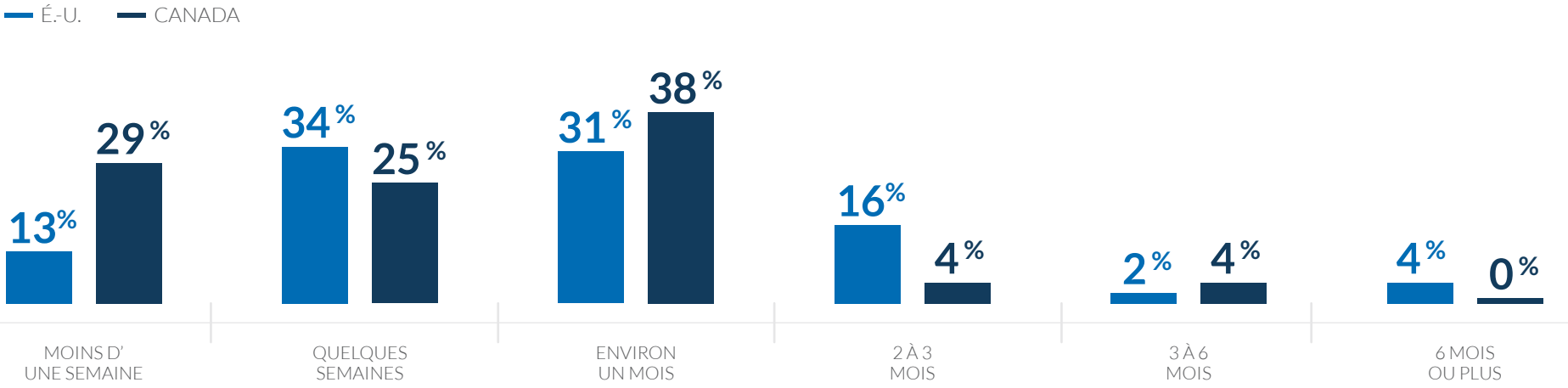
> **Bien que de nombreux chefs d'entreprise nord-américains résolvent les problèmes créés par une violation de données en un mois, quelques-uns prennent plus de temps, même jusqu'à six mois ou plus.**

Lorsque le coût estimé d'une violation de données est de 13 786 $ par jour,[ii] il est impératif que les entreprises aient un plan d'intervention en cas d'incident et qu'elles rectifient rapidement.

63 % DE CADRES SUPÉRIEURS D'ENTREPRISES ÉTATSUNIENNES ET **58 % DE CADRES SUPÉRIEURS D'ENTREPRISES CANADIENNES**

interrogés indiquent qu'ils n'ont pas de plan d'intervention en cas d'incident

Délai de résolution des problèmes créés par une violation de données, comme indiqué par les cadres supérieurs



RÉPUTATION DE LA SÉCURITÉ DES DONNÉES

Joue un rôle crucial dans les perspectives et les comportements des consommateurs

Bien que l'implication financière d'une atteinte à la sécurité des données soit importante, la perte de consommateurs et de leur loyauté représente également une menace majeure pour les résultats d'une entreprise. Les consommateurs ont défini des attentes quant à la manière dont leurs données doivent être traitées et iront ailleurs si leurs attentes ne sont pas satisfaites. Il est essentiel de maintenir la confiance et la fidélité des consommateurs.

Les consommateurs continuent d'être préoccupés par le fait que leurs données confidentielles restent privées

Conformément aux résultats des DPR antérieurs, les consommateurs continuent de prendre très au sérieux la sécurité de leurs renseignements personnels. Plus de 80 % indiquent un niveau d'importance extrêmement élevé (88 % aux États-Unis et 90 % au Canada). De plus, un consommateur nord-américain sur trois indique que les entreprises ne répondent pas à leurs attentes en matière de communications transparentes et opportunes concernant les fuites de données.

Les consommateurs ont de bonnes raisons de s'inquiéter. Le sondage de cette année a révélé que, bien que les consommateurs canadiens (38 %) se portent mieux, près de sept consommateurs étatsuniens sur dix (69 %) ont indiqué qu'ils ont été personnellement touchés par une violation de données. Cela semble être une tendance croissante, car le DPR 2020 a montré que 53 % des consommateurs étatsuniens croient que leurs données personnelles et leurs renseignements sont moins sûrs qu'il y a dix ans.

Lorsqu'on leur a demandé de donner leur point de vue sur les raisons pour lesquelles les entreprises ne répondent pas à leurs attentes en matière de protection de leurs données personnelles, les consommateurs ont déclaré :

> **« Trop de violations et d'attaques ne sont révélées que lorsque l'entreprise se fait prendre ou est forcée de révéler la violation. »**

> **« Les entreprises ne se soucient vraiment pas des données personnelles jusqu'à ce qu'elles fuient. »**

Presque

70 % DES **CONSOMMATEURS ÉTATSUNIENS**

ont été personnellement touchées par une violation de données en 2021, comparativement à **53 %** en 2020

Plus de

80 % DES **CONSOMMATEURS**

interrogés indiquent un niveau d'importance extrêmement élevé dans la sécurité des renseignements personnels

Les consommateurs agiront si leurs données sont compromises

Également conformes aux conclusions du DPR 2020, les consommateurs prendront des mesures si leurs données sont compromises. La majorité des consommateurs interrogés (82 % aux États-Unis et 83 % au Canada) décide avec qui faire affaire en fonction de la réputation d'une entreprise en matière de sécurité des données.

De plus, un rapport sur les tendances de l'expérience client 2020 de Zendesk[6] montre qu'environ la moitié des consommateurs changeront de marque après une mauvaise expérience, et après plus d'une mauvaise expérience, ce nombre atteint un chiffre alarmant de 80 % qui changerait de marque. Et cela ne s'arrête pas là.

Environ trois consommateurs sur dix (32 % aux États-Unis et 25 % au Canada) partageront leur expérience avec d'autres et près d'un consommateur sur quatre (23 % aux États-Unis et 20 % au Canada) cessera de faire affaire avec l'entreprise responsable de la violation.

Cela correspond aux données de 2020, où 29 % ont partagé leur expérience avec les autres et 24 % ont cessé de faire affaire avec l'entreprise touchée.

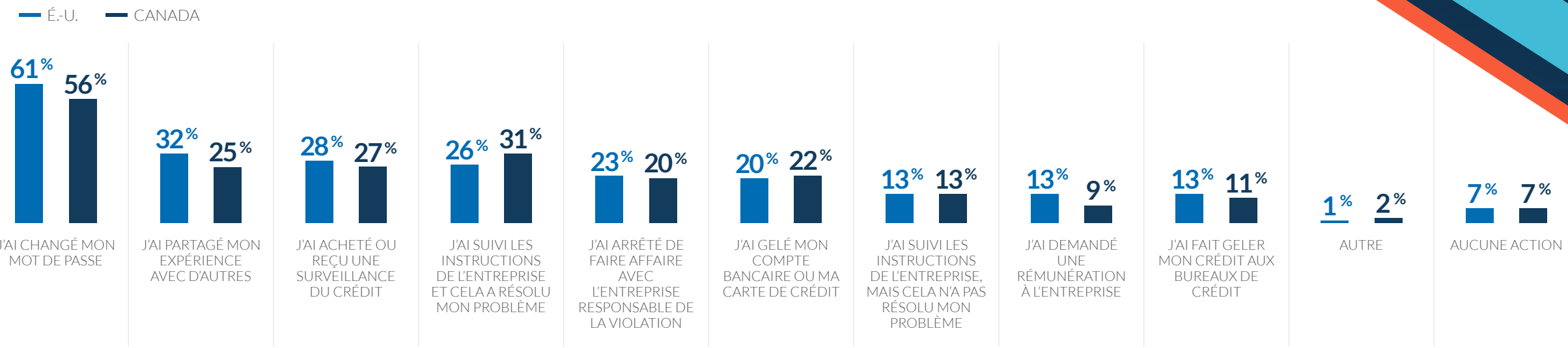
Presque

1 EN 4

CONSOMMATEURS

interrogés ont cessé de faire affaire avec l'entreprise responsable de la violation de données

Mesures prises par les consommateurs après une violation de données



LES MENACES INTERNES CONTINUENT À AUGMENTER

et les entreprises doivent être vigilantes

Lorsqu'il s'agit de sécurité de l'information, les employés peuvent être à la fois la plus grande force de l'entreprise et sa plus grande faiblesse. Les acteurs malveillants deviennent de plus en plus sophistiqués et plus difficiles à repérer, et sans les connaissances appropriées, les employés et les fournisseurs sont sensibles, ce qui rend les entreprises vulnérables. Par conséquent, les entreprises doivent s'assurer qu'elles sont vigilantes à tous les niveaux ou qu'elles doivent faire face aux conséquences.

Des initiés « de confiance » sont susceptibles d'être à l'origine d'une violation de données

Avec l'option de sélectionner toutes les réponses qui s'appliquent, les entreprises indiquent que les violations de données proviennent de diverses sources. La présence d'étrangers malveillants (55 %) continue de présenter une menace pour la sécurité de l'information des grandes et des petites entreprises en Amérique du Nord. De plus, il y a un nombre alarmant d'initiés « de confiance » qui sont la source des violations de données.

Aux États-Unis, cela comprendrait les violations causées par des initiés malveillants (53 %), des partenaires externes (40 %) et des erreurs des employés (22 %). Cela est en hausse par rapport au DPR 2020 de l'année dernière qui montrait un cadre supérieur sur quatre citant des escroqueries d'ingénierie sociale et un sur cinq citant des menaces externes de fournisseurs ou d'entrepreneurs ainsi qu'un sur cinq citant la perte physique ou le vol d'informations sensibles.

En 2021,

53 % DE

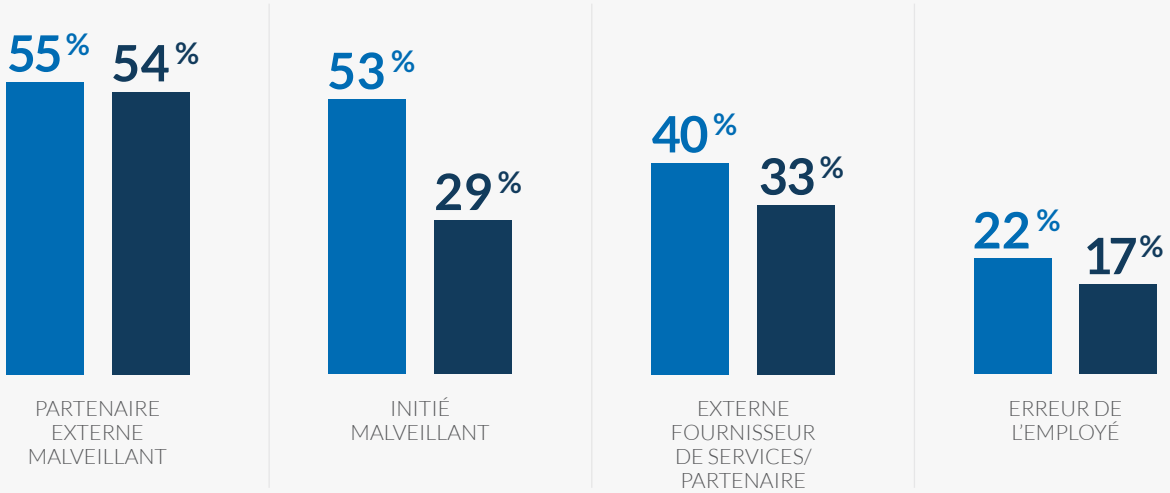
VIOLATION DE DONNÉES

ont été causés par des initiés malveillants

La pandémie de COVID-19 a également rendu la gestion de la sécurité de l'information plus difficile pour certaines entreprises.

Près de 30 % des petites et des moyennes entreprises situées aux États-Unis et 41 % au Canada ont indiqué que la pandémie rendait la protection des données plus difficiles. De plus, environ sept personnes sur dix indiquent qu'ils se préoccupent du respect des politiques de confidentialité de l'entreprise pendant la pandémie.

Source des violations de données indiquée par les cadres supérieurs



Les entreprises indiquent l'importance de détruire les matériaux sensibles, mais n'ont probablement pas de service de déchiquetage de papier

Bien qu'elles aient indiqué l'importance de détruire les documents sensibles lorsqu'ils ne sont plus nécessaires pour se protéger, les entreprises sont les moins susceptibles de mentionner qu'elles disposent de services de déchiquetage de papier, sans doute l'une des méthodes les plus simples pour remédier aux vulnérabilités de sécurité.

Le travail à distance continue également d'avoir une incidence sur les menaces à la sécurité, avec plus de la moitié des employés interrogés travaillant hors site, 63 % des employés étatsuniens et 45 % des employés canadiens impriment régulièrement des documents de travail.

> **Parmi ceux qui impriment des documents hors site, un sur quatre les éliminent simplement à la poubelle ou les recyclent, ce qui pourrait exposer leur entreprise à un risque de violation de la sécurité de l'information.**

Cependant, un sondage Shred-it distinct a révélé que 56 % des entreprises sont intéressées par un service qui fournit la destruction de documents combinée à la formation et à la consultation des politiques. Ils peuvent être essentiels pour toute entreprise de toute taille qui cherche à construire des mesures de protection électroniques et sur papier. De plus, une majorité d'entreprises (environ 90 %) sont d'accord pour dire que la durabilité environnementale est un facteur important dans la décision de l'entreprise avec laquelle s'associer.

56 % DE

ENTREPRISES

s'intéressent à un service qui combine des solutions de confidentialité et d'information avec la destruction de documents

Environ

90 % DE

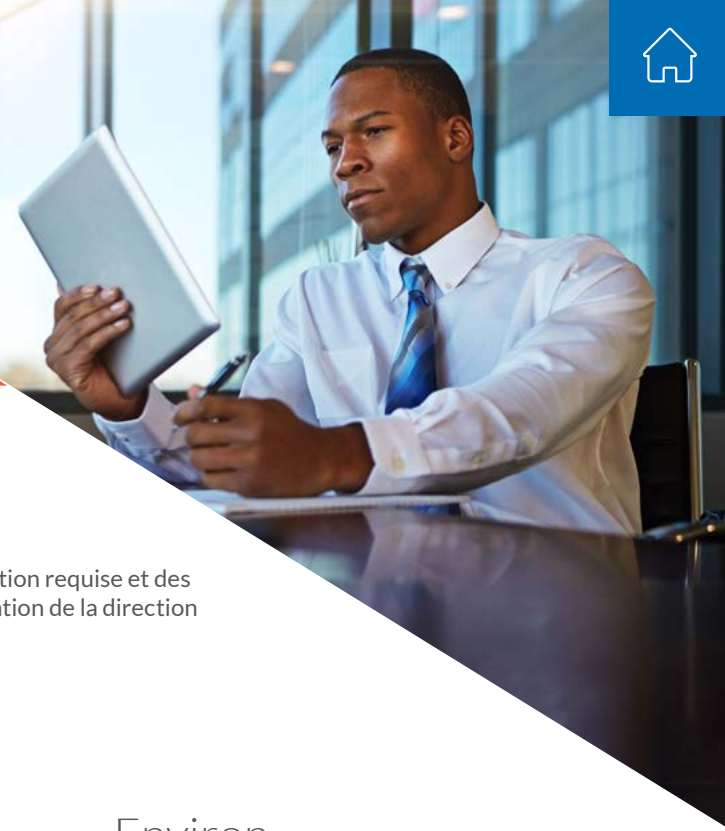
ENTREPRISES

conviennent que la durabilité environnementale est un facteur primordial lorsqu'il s'agit de décider avec quelle entreprise s'associer

25 % DE

EMPLOYÉS TRAVAILLANT HORS SITE

jettent les documents imprimés à la poubelle ou au bac de recyclage malgré le fait qu'ils contiennent potentiellement des informations privées



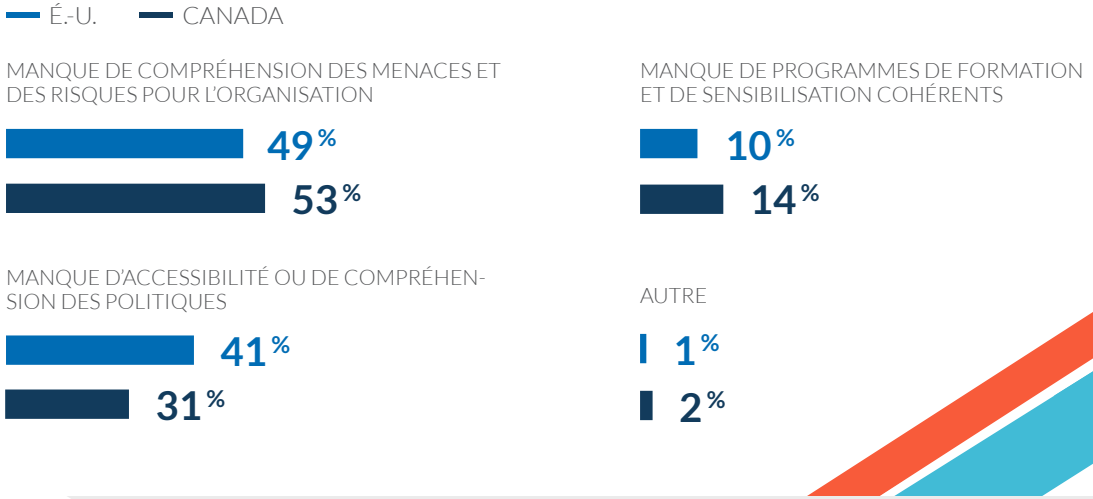
Malgré les politiques et la formation, les employés ont de la difficulté à mettre les apprentissages en pratique

Bien que les politiques et la formation soient un élément essentiel de la stratégie de protection de l'information d'une entreprise, il est également important que les employés soient conscients de l'importance de comprendre les menaces d'une violation de données et de suivre les politiques. De nombreuses entreprises réalisent qu'elles ne peuvent pas le faire seules. Dans tous les secteurs sondés, les trois quarts des chefs d'entreprise aux États-Unis ont embauché un expert en sécurité tiers pour évaluer les pratiques de sécurité. Cela est également vrai avec les réponses du DPR de 2020.

Environ la moitié des chefs d'entreprise nord-américains (49 % États-Unis et 53 % Canada) indiquent que le manque de compréhension des menaces et des risques pour l'organisation est le plus grand obstacle pour les employés suivi par les politiques de sécurité de l'information. Cela est suivi d'un manque d'accessibilité ou de compréhension des politiques (41 % aux États-Unis et 31 % au Canada) comme le prochain obstacle le plus important.

Les deux tiers des employés canadiens et la moitié des employés étatsuniens travaillant pour des entreprises ayant des politiques de cybersécurité croient que la formation requise et des rappels périodiques aideront les employés à respecter les politiques de sécurité de l'information. Bien que la moitié des employés étatsuniens croient que la communication de la direction améliorera l'observance, seulement un Canadien sur quatre est d'accord.

Obstacles les plus importants pour les employés qui suivent les politiques et procédures de sécurité de l'information



Environ

50 %

DE

CHEFS D'ENTREPRISE

interrogés indiquent que le manque de compréhension des menaces et des risques pour l'organisation est le plus grand obstacle pour les employés suivi par les politiques de sécurité de l'information

RECOMMANDATIONS

Comme les résultats du sondage l'ont indiqué, les entreprises doivent investir dans la sécurité des données maintenant ou faire face aux conséquences. Bien que le paysage soit en constante évolution, les entreprises peuvent s'assurer que leurs données sont protégées en restant informées des lois et réglementations, en comprenant le type de données qu'elles collectent et en favorisant une culture d'entreprise axée sur la sécurité.

Connaître les règles : Restez informé des lois sur la confidentialité et la sécurité des consommateurs

Comme l'a souligné les observations précédentes, les consommateurs votent avec leurs portefeuilles, travaillant avec des entreprises qui accordent la priorité au maintien de la confidentialité et de la sécurité de leurs données. Au cours de la dernière décennie, les lois et règlements sur la protection des données ont subi une évolution radicale non seulement pour dissuader les criminels, mais aussi pour contraindre les organisations à agir. Les deux facteurs sont l'impulsion pour les entreprises de prendre des mesures ou de faire face à des érosions de la confiance des consommateurs, ainsi que des conséquences juridiques et financières potentiellement lourdes.

Bien que certains pays aient une législation fédérale sur la protection des renseignements personnels et des données, les États-Unis utilisent une approche état par état. Cependant, les récentes lois sur la protection des données des consommateurs dans plusieurs États peuvent rapprocher le gouvernement fédéral d'un point de basculement. Les grandes entreprises nationales et mondiales s'efforceront probablement d'adopter une loi nationale, car le coût de la conformité et de la gestion de 50 lois différentes sur la protection de la vie privée et des données sera intenable. Par conséquent, il est essentiel pour les entreprises de se tenir au courant de la législation sur la protection des données. Les organisations doivent tenir compte des éléments suivants pour rester en tête :

Soyez prêt pour la nouvelle législation aux États-Unis.

Trois États, y compris la Californie, le Colorado et la Virginie, ont mis en place des lois qui régissent la façon dont les organisations doivent protéger les renseignements personnels des consommateurs et établir les droits à la vie privée des individus. D'autres sont susceptibles de suivre.

Soyez également prêt à faire face aux changements au Canada.

La Loi sur la protection des renseignements personnels et les documents électroniques du Canada, ou LPRPDE, devrait être remplacée par la Loi sur la protection de la vie privée des consommateurs. Les ébauches de cette nouvelle législation comprennent des sanctions pécuniaires pouvant aller jusqu'à 5 % des revenus mondiaux pour les violations. Il décrit également le droit des consommateurs à « être oublié » du point de vue des données.

Pensez à l'échelle mondiale.

Les exigences légales qui comprennent le Règlement général sur la protection des données (RGPD) s'appliquent à toutes les organisations qui recueillent, traitent ou utilisent les renseignements personnels des personnes qui vivent dans l'Union européenne (UE), peu importe où se trouve l'entreprise ou les données. Par exemple, si une entreprise située à l'extérieur de l'UE fournit des biens ou des services et traite des données personnelles ou surveille le comportement des personnes de l'UE, elle est soumise au RGPD.

Surveiller les exigences en matière de souveraineté des données.

De nombreuses nations continuent d'exiger que les organisations conservent certains types de renseignements, y compris diverses formes de données personnelles, sur des serveurs situés à l'intérieur de leurs frontières.

Connaissez vos données : C'est payant d'être conscient

Compte tenu des risques et des ressources financières ainsi que des coûts de réputation et d'exploitation associés à une violation de données, il est essentiel de se préparer pour minimiser l'impact. N'oubliez pas qu'une violation de données peut avoir des répercussions plus importantes que de simples paiements de rançongiciels ou de pertes d'affaires.

Alors, que peuvent faire les entreprises pour se protéger? La première étape consiste à connaître vos données. Demandez-vous quelles sont les données que nous avons, où les conservons-nous et avec qui les partageons-nous? Répondre à ces questions est la première étape pour prendre des décisions intelligentes, à la fois dans la création d'un plan de sécurité des données efficace et dans les investissements nécessaires pour le mettre en œuvre. Tenez compte des éléments suivants lorsque vous protégez vos données :

Élaborez un plan complet qui couvre toutes les données.

Tenez compte des documents électroniques et papier dans vos balayages de sécurité. Toutes les données doivent être détruites régulièrement conformément aux directives et aux pratiques exemplaires légales. Les mêmes attentes en matière de conservation et de destruction des documents doivent être exigées des partenaires et des entrepreneurs et doivent être incluses comme exigence pour toutes les demandes de propositions et de contrats.

Utiliser une stratégie de minimisation des données.

Assurez-vous de ne recueillir, d'utiliser, de traiter ou de stocker que les renseignements dont vous avez besoin pour mener vos activités. Mettre en place un plan de gestion des dossiers. Ne conservez que ce dont vous avez besoin tant que vous devez le conserver.

Évaluez votre infrastructure et vos pratiques TI.

Accédez à la bonne expertise en TI. Peu d'organisations informatiques possèdent l'expertise nécessaire à l'interne pour surveiller le paysage actuel des menaces en évolution rapide ou les outils et la technologie nécessaires pour lutter contre un éventail sans cesse croissant de cybermenaces. Pour de nombreuses organisations, les services de sécurité et de protection des données par abonnement sont une solution éprouvée pour les équipes TI à ressources limitées.

Adoptez le nuage.

Les fournisseurs de nuage réputés ont mis en place les solutions de sécurité les plus avancées et déploient des ressources de sécurité qui éclipsent celles des entreprises les plus avancées. Étant donné que la plupart des atteintes à la protection des données se produisent dans les centres de données, les réseaux ou les systèmes sur place, assurez-vous de tout sauvegarder et de le faire fréquemment. Les solutions de reprise après sinistre et de sauvegarde d'aujourd'hui tirent parti de l'élasticité inhérente du cloud et permettent des instantanés fréquents de l'ensemble de données complet à des intervalles choisis par le client.

Chiffrer les données importantes sur place, dans le nuage et en transit.

L'utilisation d'un chiffrement conforme aux normes actuelles de l'industrie protégera souvent une organisation contre les litiges civils, même si les données des consommateurs sont compromises.

Investir dans une technologie de détection et de réponse des points d'extrémité (EDR).

Investir dans la technologie EDR protège la périphérie du réseau, souvent son point le plus vulnérable. Plus important encore, déployez une solution de surveillance de réseau qui alerte les TI des activités suspectes en temps réel et prenez des mesures. Vous ne pouvez pas combattre ce que vous ne pouvez pas voir.

Préparez-vous à agir : Les politiques ne sont pas suffisantes; la protection des données est un sport d'équipe

La meilleure ligne de défense d'une entreprise commence à l'intérieur. Le fait d'équiper les employés des outils et des connaissances appropriés leur permettra de devenir des ambassadeurs de la sécurité de l'information, encourageant les autres à faire de même. Les entreprises doivent également s'assurer de savoir ce que font les fournisseurs pour protéger leurs renseignements. Pour créer une ligne de défense solide pour prévenir une violation de données, les entreprises doivent :

Créer une culture d'entreprise axée sur la sécurité pour les meilleures pratiques de protection des données.

Les données sont l'élément vital de toute organisation et la protection sont un sport d'équipe. Il est important que les employés comprennent l'impact global d'une violation. Non seulement une violation a-t-elle une incidence sur les activités quotidiennes, mais elle pourrait avoir une incidence sur la sécurité de leur emploi.

Instituer des politiques accompagnées d'une formation basée sur les rôles.

Les entreprises doivent mettre en œuvre des politiques pour assurer la sécurité des renseignements de l'entreprise, la confidentialité des données des consommateurs, les directives de sécurité réglementaires (telles que celles de HIPAA dans les soins de santé et la loi Gramm-Leach-Bliley dans les services financiers) et la sécurité physique des données dans tous les formulaires, y compris les documents électroniques et imprimés. Cependant, afin qu'une politique soit efficace, les entreprises devraient offrir des programmes de formation pour aider les employés à mettre l'information en pratique afin d'assurer leur compréhension et leur respect.

Évaluez vos politiques de protection des données.

Les entreprises doivent mettre en place des politiques pour s'assurer que les employés comprennent les attentes en matière de traitement et de conservation des documents Les politiques, comme un bureau propre, un déchiquetage et un travail à distance, élimineront les devinettes de la manipulation sécurisée des documents et réduiront le risque d'erreur humaine. La politique doit clairement énoncer les attentes et les mesures qui seront prises en cas de violation.

Former les employés à être une première ligne de défense viable.

Les politiques ne sont que le début. Les employés doivent être formés, afin de s'assurer qu'ils comprennent et peuvent mettre en œuvre les attentes décrites dans la politique. Les entreprises peuvent utiliser diverses initiatives de formation, comme des simulations d'hameçonnage, pour encourager les employés à être vigilants et à promouvoir le respect. Les incitatifs peuvent également être utilisés pour récompenser les employés qui signalent des dangers pour la sécurité. L'enthousiasme qui en résulte pousse les programmes et les initiatives de protection des données vers l'avant.

Aborder les menaces internes.

Envisagez de mettre en œuvre une authentification à deux facteurs pour tous les utilisateurs lors de l'accès aux systèmes et applications critiques. Considérez également une approche de confiance zéro pour l'accès au réseau exigeant que tous les utilisateurs, que ce soit dans ou à l'extérieur du réseau de l'organisation, soient authentifiés, autorisés et validés pour la configuration de sécurité avant d'obtenir l'accès aux applications et aux données.

Avoir un plan d'intervention.

Démontrez votre compétence dans votre réponse à toute violation de données en vous préparant avec un plan d'intervention en cas d'incident. Assurez-vous d'avoir un plan d'atténuation et de communication qui vous permettra de vous déplacer rapidement. Les consommateurs perdent rapidement confiance aux marques et aux organisations qui ne les alertent pas d'une violation de la sécurité impliquant leurs données personnelles en temps opportun. Fournir aux clients une transparence sur ce qui s'est passé et sur la façon dont l'entreprise prend des mesures pour prévenir une violation de données à l'avenir.

Investir dans la cyberassurance et l'aide d'experts.

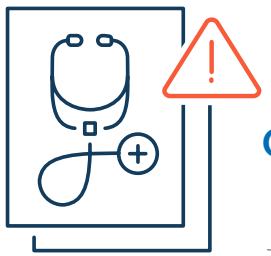
Ces services peuvent aider à couvrir le coût des services juridiques et des conseils ainsi que les services de gestion de crise. De plus, ils peuvent informer et préparer la réponse d'une entreprise à une violation de données, y compris la notification des parties concernées (clients commerciaux ou personnes dont les données ont été consultées ou acquises pendant la violation).

RENSEIGNEMENTS PROPRES À L'INDUSTRIE

Le DPR 2021 comprend un examen approfondi des pratiques propres à l'industrie dans les secteurs des soins de santé, des finances, des services professionnels, de l'assurance et de l'immobilier. En général, toutes les entreprises interrogées conviennent que la sécurité de l'information est importante pour leur entreprise. Pourtant, chacun fait face à un ensemble unique de réalités en ce qui concerne leur préparation à la protection des données.

Le meilleur médicament : La préparation de l'industrie des soins de santé combat les cyberattaques

En 2020, il y a eu une augmentation de 73 % du nombre de violations de données confirmées dans le secteur des soins de santé.1 Ces incidents ont exposé 12 milliards de renseignements médicaux protégés (RMP).1 Dans ce contexte, les organismes de soins de santé seraient bien avisés de continuer leur vigilance.



56 % DE **ORGANISATIONS DE SANTÉ**

J'ai déjà fait l'expérience d'une violation de données

29 % DE **ORGANISATIONS DE SANTÉ**

ont enquêté sur une atteinte à la protection des données survenue au cours des 12 derniers mois

Les organisations de soins de santé comprennent qu'il est important d'être préparé

75 %
La sécurité de l'information de l'État est très importante pour leur entreprise

62 %
Croire qu' une violation de données serait coûteuse*

54 %
Sentir une violation de données aurait un impact majeur sur leur réputation

61 %
Embauche d'un expert en sécurité tiers pour évaluer les pratiques de sécurité

* En termes d'argent et de temps pris pour corriger la situation.

Les organisations de soins de santé sont mieux équipées que les entreprises d'autres industries

Plus que toute autre industrie, 65 % des organisations de soins de santé affirment que leur organisation a accès aux outils et ressources de sécurité de l'information appropriés. Ils sont beaucoup plus susceptibles que toute autre industrie d'avoir un plan d'intervention en cas d'incident, ce qui accélère les temps de récupération des incidents que les autres industries.

Politiques et stratégies de protection

- **64 %** Utiliser une politique sur la sécurité des renseignements
- **48 %** Effectuer une vérification régulière de l'infrastructure
- **27 %** Avoir un service de déchiquetage papier pour se protéger contre les violations de données
- **85 %** Avoir une police d'assurance cybernétique
- **33 %** Effectuer des évaluations de vulnérabilité

Plan d'intervention

- **58 %** Avoir un plan d'intervention
- **35 %** Pris quelques semaines pour résoudre la plus récente violation de données

Faire le point : L'industrie financière excelle dans l'utilisation des politiques de sécurité de l'information

Des numéros de sécurité sociale et des rapports de crédit aux reçus de revenus mensuels et plus encore, les clients doivent soumettre de nombreuses informations personnellement identifiables (PII) lorsqu'ils travaillent avec des organisations financières. Si l'un de ces renseignements tombe entre de mauvaises mains, cela pourrait exposer les clients à un risque grave de vol d'identité ou de fraude. Bien que les organisations financières ne soient pas à l'abri des violations de données, elles investissent dans des ressources pour se protéger contre les violations futures.

52 % DE **ORGANISATIONS FINANCIÈRES**

J'ai déjà fait l'expérience d'une violation de données

42 % DE **ORGANISATIONS FINANCIÈRES**

ont enquêté sur une atteinte à la protection des données survenue au cours des 12 derniers mois

Les organisations financières comprennent qu'il est payant d'être préparé

40 %
La sécurité de l'information de l'État est très importante pour leur entreprise

47 %
Croire qu'une violation de données serait coûteuse*

49 %
Sentir une violation de données aurait un impact majeur sur leur réputation

80 %
Embauche d'un expert en sécurité tiers pour évaluer les pratiques de sécurité

*En termes d'argent et de temps pris pour corriger la situation.

Les organisations financières estiment qu'elles sont équipées

L'industrie financière a confiance en les mesures qu'elle a mises en place pour créer une culture d'entreprise axée sur la sécurité, car 62 % croient qu'ils ont accès aux outils et au soutien appropriés. Et, bien qu'ils excellent dans la mise en œuvre de politiques, la protection contre les violations de données physiques peut être améliorée avec un service de déchiquetage.

Politiques et stratégies de protection

- **72 %** Utiliser une politique sur la sécurité des renseignements
- **89 %** Avoir une police d'assurance cybernétique
- **43 %** Effectuer une vérification régulière de l'infrastructure
- **38 %** Effectuer des évaluations de vulnérabilité
- **13 %** Avoir un service de déchiquetage papier pour se protéger contre les violations de données

Plan d'intervention

- **40 %** Avoir un plan d'intervention
- **44 %** Pris quelques semaines pour résoudre la plus récente violation de données

Ajouter tout : Les Services professionnels repensent le partage des données avec les fournisseurs de services

Alors que les personnages néfastes deviennent plus sophistiqués dans leur approche, ils deviennent de plus en plus difficiles à repérer. Près de la moitié (41 %) des services professionnels interrogés sont plus susceptibles de dire que le partage de données avec des tiers est considéré comme un risque important pour la sécurité de l'information. Dans cette optique, les services professionnels doivent créer une culture d'entreprise axée sur la sécurité pour renforcer leur première ligne de défense contre les violations de données, leurs employés et fournisseurs de services.

51 % DE **SERVICES PROFESSIONNELS**

J'ai déjà fait l'expérience d'une violation de données

40 % DE **SERVICES PROFESSIONNELS**

ont enquêté sur une atteinte à la protection des données survenue au cours des 12 derniers mois

Les Services professionnels comprennent qu'il est important d'être préparé

55 %
La sécurité de l'information de l'État est très importante pour leur entreprise

40 %
Croire qu'une violation de données serait coûteuse*

35 %
Sentir une violation de données aurait un impact majeur sur leur réputation

69 %
Embauche d'un expert en sécurité tiers pour évaluer les pratiques de sécurité

* En termes d'argent et de temps pris pour corriger la situation.

Les services professionnels sont les plus préoccupés par les documents laissés à l'extérieur

Les services professionnels sont plus préoccupés par le fait que les employés laissent des documents confidentiels sur leur bureau (71 %), mais seulement un quart ont des services de déchiquetage papier. Étant donné que l'exposition aux documents physiques laisse les entreprises à risque, ces organisations devraient investir dans des stratégies de politique et de protection afin de réduire la possibilité d'une violation de données.

Politiques et stratégies de protection

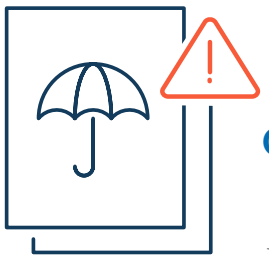
- **56 %** Utiliser une politique sur la sécurité des renseignements
- **69 %** Avoir une police d'assurance cybernétique
- **44 %** Effectuer une vérification régulière de l'infrastructure
- **36 %** Effectuer des évaluations de vulnérabilité
- **25 %** Avoir un service de déchiquetage papier pour se protéger contre les violations de données

Plan d'intervention

- **38 %** Avoir un plan d'intervention
- **30 %** A pris environ un mois pour résoudre la plus récente violation de données

Protection des protecteurs : L'industrie de l'assurance se tourne vers des experts en sécurité pour obtenir des conseils

Les organisations d'assurance sont connues pour stocker de grandes quantités de renseignements personnels identifiables (PII) sur leurs titulaires de police, ce qui en fait une cible pour la cybercriminalité. Et, par rapport aux autres industries sondées, l'assurance s'ajoute à ceux qui ont subi une violation de données.



75 % DE **ORGANISATIONS D'ASSURANCE**

J'ai déjà fait l'expérience d'une violation de données

65 % DE **ORGANISATIONS D'ASSURANCE**

ont enquêté sur une atteinte à la protection des données survenue au cours des 12 derniers mois

Les organisations d'assurance comprennent qu'il est important d'être préparé

44 %
La sécurité de l'information de l'État est très importante pour leur entreprise

39 %
Croire qu' une violation de données serait coûteuse*

43 %
Sentir une violation de données aurait un impact majeur sur leur réputation

84 %
Embauche d'un expert en sécurité tiers pour évaluer les pratiques de sécurité

* En termes d'argent et de temps pris pour corriger la situation.

Les organisations d'assurance sont plus préoccupées par les documents laissés à l'écart

Les compagnies d'assurance qui ont subi une violation comprennent l'importance de détruire des documents sensibles lorsqu'ils ne sont plus nécessaires pour améliorer les processus commerciaux et protéger les renseignements sensibles contre tout accès non autorisé. Pourtant, la majorité (85 %) des compagnies d'assurance interrogées sont préoccupées par le fait que les employés laissent du matériel confidentiel sur leur bureau. Les organisations d'assurance doivent revoir leur stratégie de protection des données contre les violations de données physiques, car la plupart d'entre elles ont signalé ne pas avoir de service de déchiquetage de papier.

Politiques et stratégies de protection

- **50 %** Utiliser une politique sur la sécurité des renseignements
- **25 %** Effectuer une vérification régulière de l'infrastructure
- **6 %** Avoir un service de déchiquetage papier pour se protéger contre les violations de données
- **90 %** Avoir une police d'assurance cybernétique
- **13 %** Effectuer des évaluations de vulnérabilité

Plan d'intervention

- **25 %** Avoir un plan d'intervention
- **49 %** A pris environ un mois pour résoudre la plus récente violation de données

Emplacement, emplacement, emplacement : Manque de planification des interventions en cas d'incident dans l'industrie immobilière

La réputation est essentielle à la fidélisation des clients dans l'industrie immobilière, et avec l'augmentation des attentes des consommateurs en matière de sécurité de l'information, elle comprend l'importance de protéger les renseignements.

69 % DE **ORGANISATIONS IMMOBILIÈRES**

J'ai déjà fait l'expérience d'une violation de données

58 % DE **ORGANISATIONS IMMOBILIÈRES**

ont enquêté sur une atteinte à la protection des données survenue au cours des 12 derniers mois

Les organisations immobilières comprennent qu'il est important d'être préparé

57 %
La sécurité de l'information de l'État est très importante pour leur entreprise

46 %
Croire qu'une violation de données serait coûteuse*

42 %
Sentir une violation de données aurait un impact majeur sur leur réputation

77 %
Embauche d'un expert en sécurité tiers pour évaluer les pratiques de sécurité

*En termes d'argent et de temps pris pour corriger la situation.

Les organisations immobilières estiment qu'elles sont équipées

Le secteur de l'immobilier a mis en place les mesures nécessaires pour créer une culture d'entreprise axée sur la sécurité, car 56 % pensent avoir accès aux outils et au soutien appropriés. Bien qu'ils excellent dans l'utilisation des politiques, la planification des interventions en cas d'incident peut être améliorée

Politiques et stratégies de protection

- **64 %** Utiliser une politique sur la sécurité des renseignements
- **88 %** Avoir une police d'assurance cybernétique
- **33 %** Effectuer une vérification régulière de l'infrastructure
- **19 %** Effectuer des évaluations de vulnérabilité
- **15 %** Avoir un service de déchiquetage papier pour se protéger contre les violations de données

Plan d'intervention

- **29 %** Avoir un plan d'intervention
- **47 %** Pris quelques semaines pour résoudre la plus récente violation de données

Conclusion : Investir maintenant ou payer plus tard

Le rapport de protection des données Shred-it 2021 confirme que les entreprises nord-américaines, petites et grandes, ne peuvent plus considérer la protection des données et la sécurité comme un investissement facultatif. Oui, le paysage actuel de la protection des données peut être accablant, mais il n'est pas impossible de le gérer. En s'éduquant, en s'assurant qu'ils sont équipés des bons services et de l'expertise, et en planifiant, avant la violation, chaque entreprise peut équilibrer les risques et les récompenses lorsqu'elle protège la santé et le bien-être de ses relations de confiance, de ses résultats et de sa marque.

> **En fait, les organisations qui vont au-delà de la simple conformité réglementaire peuvent bâtir la confiance avec les clients et se démarquer de la concurrence.**

Le DPR 2021 décrit les principales perspectives et recommandations pour vous aider à orienter votre cheminement vers l'avenir :

Comprendre les règles.

Actuellement, trois États ont mis en place des lois pour protéger les renseignements des consommateurs et ont établi des droits individuels en matière de confidentialité. Le Canada cherche à promulguer de nouvelles lois, la LPRPDE, pour remplacer la LRCR. À mesure que les exigences réglementaires continuent d'évoluer, il est essentiel que les entreprises restent à jour.

Connaissez vos données.

Une once de prévention vaut une livre de remède. Faites l'inventaire des types de données que vous recueillez, de la façon dont vous les stockez et avec qui vous les partagez. Ces détails sont essentiels à la mise en œuvre d'un plan de sécurité des données efficace.

Préparez-vous à agir.

Les politiques ne suffisent pas. La protection des données est un sport d'équipe. Équipez les employés des connaissances et des outils appropriés et fournissez des rappels et des incitatifs fréquents pour garder la sécurité des données à l'esprit. Il est payant d'avoir des stratégies d'atténuation et un plan d'intervention en place pour protéger votre marque et vos résultats.

Le besoin de protéger les données n'a jamais été aussi important

Se tenir au courant des règlements et des attentes des consommateurs est beaucoup à jongler, mais vous n'avez pas à le faire seul. Pour vous assurer d'avoir une visibilité sur le paysage des menaces en évolution rapide et les technologies disponibles pour le combattre, collaborez avec un fournisseur de services expert pour vous aider à combler les lacunes.

Choisissez le partenaire de sécurité de l'information qui peut vous aider à relever les défis croissants de votre organisation en matière de sécurité de l'information. Avec des services de sécurité de l'information de pointe, le service de destruction de documents Shred-it de Stericycle peut protéger la santé et le bien-être de votre entreprise, protégeant vos données et votre réputation.

Expertise en sécurité

Avec plus de 30 ans d'expertise en matière de destruction et une chaîne de possession sécurisée de bout en bout, notre objectif principal de sécurité des documents vous assure que vos renseignements confidentiels demeurent confidentiels.

Fiabilité du service

Que vous soyez une grande entreprise nationale ou une petite entreprise, vous pouvez mettre à votre service la puissance du plus grand parc de déchiquetage et de la plus grande empreinte de service en Amérique du Nord.

Expérience du client

D'une gamme d'options de libre-service et de solutions de destruction personnalisables, d'un service à la clientèle réactif et dévoué, nous nous engageons à assurer votre protection.

Apprenez-en plus sur la sécurité des renseignements et sur la façon dont nous pouvons vous aider à protéger votre organisation sur www.shredit.com ou appelez le 800 697-4733.

Nous protégeons ce qui compte.

À propos du sondage

Les répondants au sondage DPR 2021 comprenaient les consommateurs ainsi que les cadres (titres : propriétaire, cadre, cadre supérieur, vice-président, directeur des TI ou supérieur, défini par le nombre d'employés dans l'organisation) en Amérique du Nord (États-Unis et Canada). Ces entreprises représentaient les secteurs des soins de santé, des finances, des services professionnels (ingénierie, comptabilité et recherche), de l'assurance et de l'immobilier.

Les petites et moyennes entreprises ont été définies comme ayant de 20 à 499 employés et les grandes entreprises ont été définies comme ayant 500 employés ou plus. Les quotas devaient être représentatifs à l'échelle nationale en fonction du sexe, de l'âge et de la région géographique pour les États-Unis et le Canada séparément. De plus, seuls les employés et propriétaires d'entreprises qui connaissent les politiques et procédures de sécurité de l'information de l'entreprise ont été sondés.

400
CONSOMMATEURS

125
CADRES SUPÉRIEURS

139
PROPRIÉTAIRES DE PETITES ET MOYENNES ENTREPRISES

SOURCE

1. Rapport d'enquête sur la violation des données de 2021 de Verizon.
2. Ponemon Institute, IBM Security Cost of Data Breach Report, 2021.
3. Ponemon Institute, IBM Security Cost of Data Breach Report, 2018.
4. The Drum, l'état actuel des lois américaines sur la confidentialité des données, 26 avril 2021.
5. Sécurité basée sur le risque, rapport de fin d'année 2020.
6. Zendesk, Rapport sur les tendances en matière d'expérience client, 2020.

Shred-it®
Une Solution Stericycle®