Kiteworks

Les 11 principales violations de données

Informations exploitables et recommandations grâce à l'indice d'exposition aux risques de Kiteworks

Rapport du 1er semestre 2024

Table des matières

Introduction

Chers lecteurs,

Alors que nous naviguons dans le paysage complexe de la cybersécurité en 2024, la fréquence croissante et la gravité des violations de données sont indéniables. Rien que durant la première moitié de cette année, les cybercriminels ont compromis plus d'un milliard d'enregistrements, touchant de multiples secteurs, y compris les télécommunications, la santé, la finance et le gouvernement. Ces incidents ont non seulement exposé les vulnérabilités au sein de nos infrastructures numériques, mais ont également souligné le besoin urgent de stratégies de cybersécurité robustes pour protéger les données sensibles.

Le rapport « Les 11 principales violations de données au 1er semestre 2024 » utilise l'indice d'exposition aux risques de Kiteworks pour fournir une analyse détaillée des violations les plus significatives survenues durant la première moitié de l'année. Nos découvertes révèlent plusieurs tendances alarmantes, de la prévalence croissante des attaques par rançongiciel aux vulnérabilités associées aux interactions avec des tiers et aux erreurs internes. Ce rapport souligne l'importance cruciale de la gestion des communications de contenu sensible dans tous les secteurs, surtout à mesure que les organisations s'appuient de plus en plus sur de multiples outils de communication et services tiers, ce qui peut créer de nombreux points d'entrée pour les menaces cybernétiques.

Chez Kiteworks, nous nous engageons à aider les organisations à atténuer ces risques en fournissant des informations exploitables et des recommandations. L'indice d'exposition aux risques, présenté dans ce rapport, est un outil stratégique conçu pour aider les organisations à évaluer et à prioriser les violations de données en fonction de leur gravité et de leur impact potentiel. En employant ce cadre complet, les organisations peuvent mieux allouer leurs ressources, renforcer leurs postures de sécurité et améliorer leur résilience globale contre les violations futures.

Nous espérons que ce rapport vous fournira des conseils précieux alors que vous continuez de protéger vos informations sensibles. Ensemble, nous pouvons construire un avenir numérique plus sûr.

Cordialement,

Patrick Spencer

Patrick E. Spencer, Ph.D.
Vice President of Corporate Marketing & Research
Kiteworks

Aperçu des violations de données au premier semestre 2024

La première moitié de 2024 a vu une augmentation significative du nombre et de l'ampleur des violations de données, reflétant la sophistication et la détermination croissantes des cybercriminels dans le monde. Selon les données du Centre de Ressources sur le Vol d'Identité (ITRC),[1] les 10 principales violations de données durant cette période ont compromis plus d'un milliard de dossiers dans divers secteurs, y compris les télécommunications, la santé, la finance, la technologie et les agences gouvernementales. Ces incidents vont des attaques par rançongiciel et les vulnérabilités de la chaîne d'approvisionnement aux fuites de données accidentelles, soulignant les tactiques diverses employées par les cybercriminels et les vulnérabilités répandues à travers différents secteurs. Le top 10 de l'ITRC n'a pas inclus la violation de données publiques nationales, qui a exposé jusqu'à 2,9 milliards d'enregistrements de données associés à 1,3 million de personnes. Ainsi, nous avons ajouté les données publiques nationales à notre rapport.

Les découvertes dans le rapport 2024 de Kiteworks sur la confidentialité et la conformité des communications de contenu sensible soulignent davantage la nature critique de la gestion des données sensibles dans tous les secteurs.[2] Le rapport met en évidence les défis auxquels les organisations sont confrontées pour protéger le contenu sensible alors qu'elles dépendent de plus en plus de multiples outils de communication et d'interactions avec des tiers, ce qui peut créer de nombreuses vulnérabilités. Par exemple, le rapport a trouvé que ceux disposant de 10 outils de communication ou plus ont subi 3,55 fois plus de violations de données que la moyenne rapportée par l'ensemble des répondants.

Tendances clés en matière de violations de données

Lorsqu'on examine en détail les 11 principales violations de données du premier semestre 2024, plusieurs conclusions se dégagent:

1. **Attaques par rançongiciel:** Le ransomware continue d'être une méthode d'attaque répandue, ciblant les organisations de divers secteurs. Des violations de grande envergure, telles que celles impliquant Change Healthcare et MediSecure, montrent l'impact dévastateur que le ransomware peut avoir, non seulement en perturbant les opérations, mais aussi en compromettant des données sensibles. Ces attaques ont entraîné des pertes financières importantes et des perturbations opérationnelles, soulignant la nécessité de stratégies de défense robustes contre les ransomwares.

2. **L'ampleur massive de l'exposition des données:** Le volume de données exposées lors de violations a augmenté, avec des incidents impliquant des millions de dossiers devenant plus fréquents. Par exemple, AT&T a subi deux violations majeures qui ont compromis ensemble plus de 180 millions de dossiers clients, y compris des informations personnelles et des journaux d'appels. De même, la violation chez Snowflake a affecté plusieurs entreprises et exposé des centaines de millions de dossiers, illustrant la menace considérable des attaques de la supply chain dans le paysage numérique interconnecté d'aujourd'hui (corroboré par les conclusions du Rapport d'enquête sur les violations de données 2024 de Verizon où 15 % de toutes les attaques de l'année passée étaient liées à la chaîne d'approvisionnement).[3]

3. **Vulnérabilités dans plusieurs secteurs:** Les violations de données ne se limitent pas à un seul secteur ; elles touchent une large gamme d'industries, chacune confrontée à des vulnérabilités uniques. Les secteurs tels que la santé, la finance et la technologie sont particulièrement à risque en raison de la nature sensible des données qu'ils traitent et sont bien représentés dans le top 10 des violations de données du rapport ITRC

pour le premier semestre 2024. Le manque de suivi de la gouvernance et de contrôles ainsi que l'absence de fonctions de sécurité avancées sont des raisons clés. Par exemple, le rapport de Kiteworks souligne que 57 % des organisations ne peuvent pas suivre, contrôler et générer des reportings sur les envois et partages de contenu externe.

4. **Menaces émergentes liées aux risques tiers et aux erreurs internes:** Au-delà des attaques externes, les risques associés aux tiers et les erreurs internes sont également apparus comme des menaces significatives. Les violations chez Kaiser et USPS, où des informations sensibles ont été partagées par inadvertance avec des annonceurs, soulignent l'inquiétude croissante concernant la gouvernance interne des données et les risques liés aux interactions avec des tiers. Suivre et contrôler le flux de données échangées avec tous les tiers est difficile, les deux tiers des organisations déclarant échanger du contenu sensible avec plus de 1 000 tiers.[4]

Détails sur les violations de données

Violation de données	Risk Exposure Index	Indice d'exposition aux risques	Impact commercial total estimé (USD)	Type de données converties	Violations de la conformité réglementaire	Ransomware Demand
Change Healthcare	**9,46**	100 000 000	17 900 000 000 $	Informations personnelles, médicales, de facturation	HIPAA, HITECH Act, California CMIA, Texas Medical Records Privacy Act, Règle de sécurité HIPAA, Règle de confidentialité HIPAA	Oui, montant payé inconnu
National Public Data	**9,46**	2 900 000 000	501 700 000 000 $	Numéros de sécurité sociale personnels	Loi FTC, RGPD, diverses lois sur la protection des données privées des États américains telles que la CCPA	Non
AT&T (two breaches)	**9,37**	110 000 000	19 690 000 000 $	Numéros de téléphone, registres d'appels, informations personnelles	Règlementations de la FCC (CPNI), Loi FTC, CCPA, Loi NY SHIELD, RGPD, Loi sur les télécommunications	Oui, montant non divulgué
Synnovis	**9,11**	300 000 000	53 700 000 000 $	Données d'interaction avec les patients	Loi sur la protection des données 2018 au Royaume-Uni, RGPD, Règlements NIS, Trousse à outils de sécurité et de protection des données du NHS au Royaume-Uni	Oui, 50 millions de dollars demandés
Ticketmaster	**8,79**	560 000 000	100 240 000 000 $	Noms complets, adresses, adresses électroniques, numéros de téléphone, données relatives aux cartes de paiement	PCI DSS, FTC Act, CCPA, Loi de notification des violations de données du Massachusetts, RGPD	Non
Kaiser	**7,60**	13 400 000	2 398 600 000 $	Termes de recherche sur le site, informations médicales	HIPAA, HITECH Act, California CMIA, FTC Act, RGPD (si des résidents de l'UE sont concernés)	Non
MediSecure	**7,56**	13 000 000	2 327 000 000 $	Données personnelles et médicales	Loi australienne sur la protection de la vie privée, Loi sur les identifiants de santé, réglementations spécifiques aux États sur les données de santé	Oui, montant inconnu
USPS	**7,31**	62 000 000	11 098 000 000 $	Adresses postales, données de suivi	CCPA, Loi FTC, diverses lois étatiques sur la notification des violations de données, RGPD (si applicable)	Non
Evolve Bank	**6,83**	7 600 000	1 360 400 000 $	Informations personnelles	CCPA, GLBA (Gramm-Leach-Bliley Act), Règle de protection de la FTC, lois étatiques sur la protection des données financières	Oui, montant inconnu
Cencora	**6,23**	1 000 000	179 000 000 $	Données de santé	HIPAA, réglementations de la FDA, lois sur la confidentialité médicale spécifiques à chaque État (par exemple, CMIA de Californie, Texas Medical Records Privacy Act)	Non
Infosys McCamish Systems	**6,23**	6 078 263	1 074 000 000 $	Numéros de sécurité sociale, informations médicales, données financières	CCPA, GLBA, Loi FTC, lois étatiques sur la protection des données d'assurance, HIPAA (si applicable)	Oui, montant inconnu

Table 1: Détails de la violation de données.

Coût des violations de données

L'augmentation de la fréquence et de la gravité des violations de données souligne l'urgence pour les organisations d'adopter des mesures de cybersécurité avancées. Le rapport 2024 d'IBM sur le coût d'une violation de données révèle que le coût moyen mondial d'une violation de données a augmenté de 10 % au cours de l'année écoulée, atteignant 4,88 millions de dollars.[5]

L'impact financier des violations de données sur les entreprises va au-delà des coûts immédiats liés à la détection, à l'escalade et à la notification. Il existe des coûts directs significatifs, tels que les amendes réglementaires, les règlements juridiques, les enquêtes judiciaires et les dépenses de notification des clients. Les organisations qui ne se conforment pas aux réglementations sur la protection des données, comme le Règlement Général sur la Protection des Données (RGPD) ou la loi sur la portabilité et la responsabilité en matière d'assurance maladie (HIPAA), peuvent faire face à des amendes substantielles. Par exemple, au 1er mars 2024, le montant total des amendes RGPD enregistrées s'élevait à environ 4,48 milliards d'euros (4,96 milliards de dollars), soit une augmentation de 1,71 milliard d'euros par rapport à l'année précédente.[6] En même temps, le coût moyen d'une violation du RGPD est passé d'environ 500 000 euros en 2019 à 4,4 millions d'euros (4,4 millions de dollars) en 2023.

En plus de ces réglementations mondiales ou nationales, des réglementations régionales ou étatiques sur la confidentialité des données, telles que le California Consumer Protection Act (CCPA), ajoutent une complexité et des défis supplémentaires pour les entreprises opérant dans ces zones.

Facteurs de risque liés aux violations de données

Volume et type de données exposées

Les facteurs de risque associés aux violations de données sont fortement influencés par le volume et le type de données exposées. Au premier semestre 2024, les violations ont varié considérablement en termes de types de dossiers compromis. Les données personnelles sont certainement une cible majeure, Verizon rapportant que près de 60 % des violations de données impliquaient des informations personnelles identifiables (PII), y compris les noms, adresses, numéros de sécurité sociale et informations financières telles que les détails de carte de crédit.[7] Les dossiers médicaux, y compris les informations sensibles des patients, ont également été fortement ciblés, en particulier lors de violations touchant les organisations de santé où l'exposition d'informations médicales protégées (PHI) ajoutait une couche supplémentaire de risque en raison des exigences réglementaires comme la HIPAA.

Nombre de victimes

L'ampleur de l'impact d'une violation de données est souvent déterminée par le nombre de personnes et d'entités touchées. Au cours du premier semestre 2024, plusieurs violations ont affecté des millions de personnes dans divers secteurs. Par exemple, les violations dans les secteurs des télécommunications et de la santé ont eu des effets considérables, touchant des dizaines de millions de clients et de patients.

Sensibilité des données exposées

Le niveau de sensibilité des données exposées est un facteur crucial pour déterminer la gravité et l'impact d'une violation de données. Les données à haute sensibilité, telles que les numéros de sécurité sociale, les dossiers médicaux et les informations financières, présentent un risque plus élevé que les données à faible sensibilité

comme les adresses e-mail ou les informations commerciales générales. Les violations impliquant des données à haute sensibilité sont plus susceptibles d'entraîner des conséquences graves, telles que le vol d'identité, la fraude financière et d'autres activités malveillantes. Dans les cas où des informations financières sensibles ou des dossiers médicaux sont concernés, les actions réglementaires qui en découlent et les coûts de remédiation plus élevés dus aux exigences strictes en matière de protection des données pour ces types de données sont beaucoup plus importants.

Méthodes de violation

Les méthodes utilisées dans les violations de données ont évolué, reflétant la sophistication croissante des tactiques des cybercriminels. Les méthodes courantes incluent les attaques par ransomware, les campagnes de phishing, les menaces internes et l'exploitation des vulnérabilités dans les services ou logiciels tiers. Le ransomware reste un vecteur d'attaque répandu, où les attaquants chiffrent les données et exigent une rançon pour leur libération, provoquant souvent des perturbations opérationnelles significatives et des pertes financières.

Les attaques de phishing continuent également d'être une cause majeure de violations, utilisant des techniques d'ingénierie sociale pour tromper les employés afin qu'ils divulguent des informations sensibles ou accordent un accès non autorisé. L'exploitation des vulnérabilités dans les services tiers ou les attaques de la chaîne d'approvisionnement est une tendance croissante. Plus précisément, les violations provenant de vulnérabilités tierces peuvent avoir des impacts étendus, car elles impliquent souvent plusieurs organisations et affectent l'ensemble des réseaux de partenaires commerciaux et de clients. Cette tendance souligne la nécessité de pratiques robustes de gestion des risques tiers et d'évaluations régulières des vulnérabilités.

Développement de l'indice d'exposition aux risques

Présentation de l'indice d'exposition aux risques

L'Indice d'Exposition au Risque est un outil stratégique développé pour évaluer et hiérarchiser les violations de données en fonction de leur gravité et de leur impact potentiel. À une époque où les violations de données deviennent de plus en plus fréquentes et complexes, les organisations font face à des défis importants pour évaluer le risque que chaque violation représente pour leurs opérations, leur réputation et leur conformité réglementaire. L'Indice d'Exposition au Risque vise à fournir un cadre standardisé pour quantifier et comparer les risques associés à différentes violations de données. En utilisant cet indice, les organisations peuvent prioriser leurs mesures de cybersécurité, allouer leurs ressources plus efficacement et améliorer leur posture de sécurité globale en se concentrant sur les menaces les plus critiques.

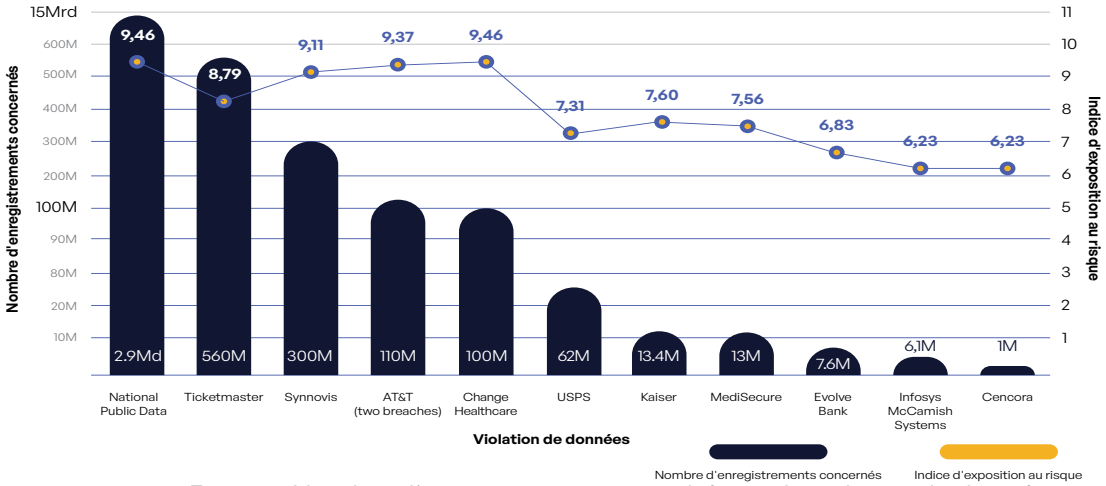


Figure 1: Nombre d'enregistrements touchés par la violation de données

Comment fonctionne l'indice d'exposition aux risques

L'indice d'exposition aux risques va au-delà des mesures traditionnelles telles que le nombre de dossiers exposés ou le coût financier encouru. Il intègre plutôt une gamme de facteurs pour offrir une compréhension plus nuancée de la gravité des violations. Ces facteurs peuvent inclure le type de données compromises, l'étendue de l'exposition, le potentiel de sanctions réglementaires et l'impact à long terme sur la réputation de la marque. En agrégeant ces éléments en un score unique, l'indice permet aux organisations d'évaluer objectivement la gravité de chaque violation et de prendre des décisions éclairées sur les efforts d'atténuation à privilégier.

Méthodologie de l'indice d'exposition aux risques

La méthodologie de calcul de l'indice d'exposition au risque repose sur plusieurs critères, chacun contribuant au score global de risque d'une violation. Ces critères sont soigneusement sélectionnés pour offrir une vue d'ensemble des risques associés à une violation et incluent les éléments suivants ::

1. **Nombre de dossiers exposés :** Ce critère évalue le volume de données compromises lors d'une violation. Plus le nombre de dossiers exposés est élevé, plus le score de risque est important, car les violations de grande ampleur entraînent généralement des conséquences plus graves, notamment un risque accru de vol d'identité, de fraude et d'atteinte à la réputation.

2. **Estimation de l'impact financier :** Ce critère évalue les pertes financières potentielles résultant d'une violation, y compris les coûts directs tels que les amendes, les frais juridiques et les dépenses de remédiation, ainsi que les coûts indirects comme la perte d'activité et l'atteinte à la réputation. Les violations avec un impact financier estimé plus élevé reçoivent un score plus élevé, reflétant le fardeau économique significatif qu'elles imposent aux organisations.

3. **Implication des ransomwares :** Compte tenu de la menace croissante des attaques par ransomware, ce critère prend spécifiquement en compte les violations impliquant des ransomware. Les attaques par ransomware sont particulièrement perturbatrices, provoquant souvent des interruptions opérationnelles importantes et nécessitant des efforts de récupération considérables. Les violations impliquant des ransomware obtiennent un score plus élevé en raison de la complexité et de la gravité de la réponse requise.

4. **Sensibilité des données :** La sensibilité des données exposées lors d'une violation est un facteur crucial pour déterminer son niveau de risque. Les violations impliquant des données hautement sensibles, telles que les informations médicales protégées (PHI) ou les dossiers financiers, se voient attribuer des scores plus élevés. Cela reflète le risque accru de sanctions réglementaires, d'actions en justice et la nécessité d'efforts de remédiation approfondis pour protéger les personnes concernées.

5. **Gravité de la violation :** Ce critère prend en compte l'impact global de la violation sur l'organisation concernée, y compris la perturbation opérationnelle, la confiance des clients et l'atteinte à la réputation à long terme. La gravité est évaluée en fonction de l'étendue de la violation, des données impliquées et de l'efficacité de la réponse de l'organisation. Les violations plus graves se voient attribuer des scores plus élevés pour refléter leurs implications plus larges.

6. **Number of Regulations Impacted:** Ce critère évalue le paysage réglementaire affecté par la violation. Les violations qui enfreignent plusieurs réglementations, telles que le RGPD, la HIPAA ou le CCPA, obtiennent des scores plus élevés. Cela reflète la complexité de la gestion de la conformité à travers différentes juridictions et le potentiel de multiples amendes et actions en justice.

Processus de normalisation et ajustement des scores

Pour s'assurer que l'indice d'exposition au risque fournit une mesure juste et cohérente de la gravité de la violation, un processus de normalisation est appliqué pour ajuster les scores sur une échelle normalisée de 1 à 10. Ce processus comporte plusieurs étapes :

1. **Collecte des données et notation initiale :** Chaque violation est évaluée selon les six critères mentionnés ci-dessus, et un score initial est attribué à chaque critère en fonction de plages prédéfinies. Par exemple, les violations exposant plus de 10 millions de dossiers peuvent recevoir le score maximum pour le critère « Nombre de dossiers exposés ».

2. **Attribution de poids :** Chaque critère se voit attribuer un poids en fonction de son importance relative dans la détermination du niveau de risque global. Par exemple, la "Sensibilité des données" et "l'Impact financier estimé" peuvent être pondérés plus lourdement que le "Nombre de dossiers exposés" pour refléter leur impact critique sur la posture de sécurité de l'organisation et les exigences de conformité.

3. **Agrégation des scores :** Les scores pondérés pour chaque critère sont agrégés pour calculer un score de risque total pour chaque violation. Ce score total représente la gravité globale de la violation en fonction de la combinaison de tous les facteurs de risque.

4. **Normalisation :** Les scores totaux sont ensuite normalisés pour s'inscrire dans une échelle standardisée de 1 à 10. Cela est réalisé en appliquant une formule mathématique qui ajuste les scores en fonction des scores maximum et minimum observés dans l'ensemble des violations. Le processus de normalisation garantit que l'indice offre une mesure cohérente et comparable de la gravité des violations, indépendamment des données sous-jacentes.

5. **Note finale:** Les scores normalisés sont examinés et validés pour garantir leur exactitude et leur cohérence. Chaque violation se voit ensuite attribuer un indice d'exposition au risque final sur une échelle de 1 à 10, les scores plus élevés indiquant des violations plus graves nécessitant une attention et une action immédiates.

En appliquant cette méthodologie rigoureuse, l'Indice d'Exposition aux Risques offre un cadre fiable et concret pour évaluer et gérer les risques de violation de données, permettant ainsi aux organisations d'améliorer leurs stratégies de cybersécurité et de mieux protéger leurs données sensibles contre les menaces en constante évolution..

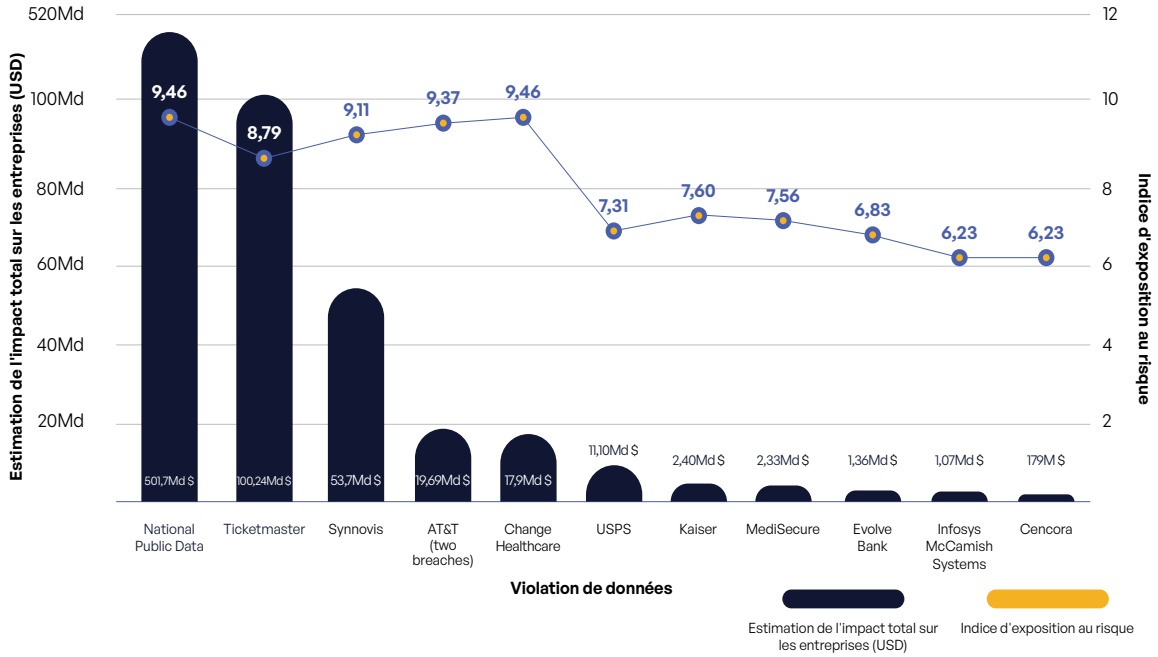


Figure 2: Estimation de l'impact total sur les entreprises d'une violation de données.

Analyse des 11 principales violations de données basée sur l'indice d'exposition aux risques

Voici le classement corrigé des 11 principales violations de données au premier semestre 2024, basé sur leur indice d'exposition au risque.

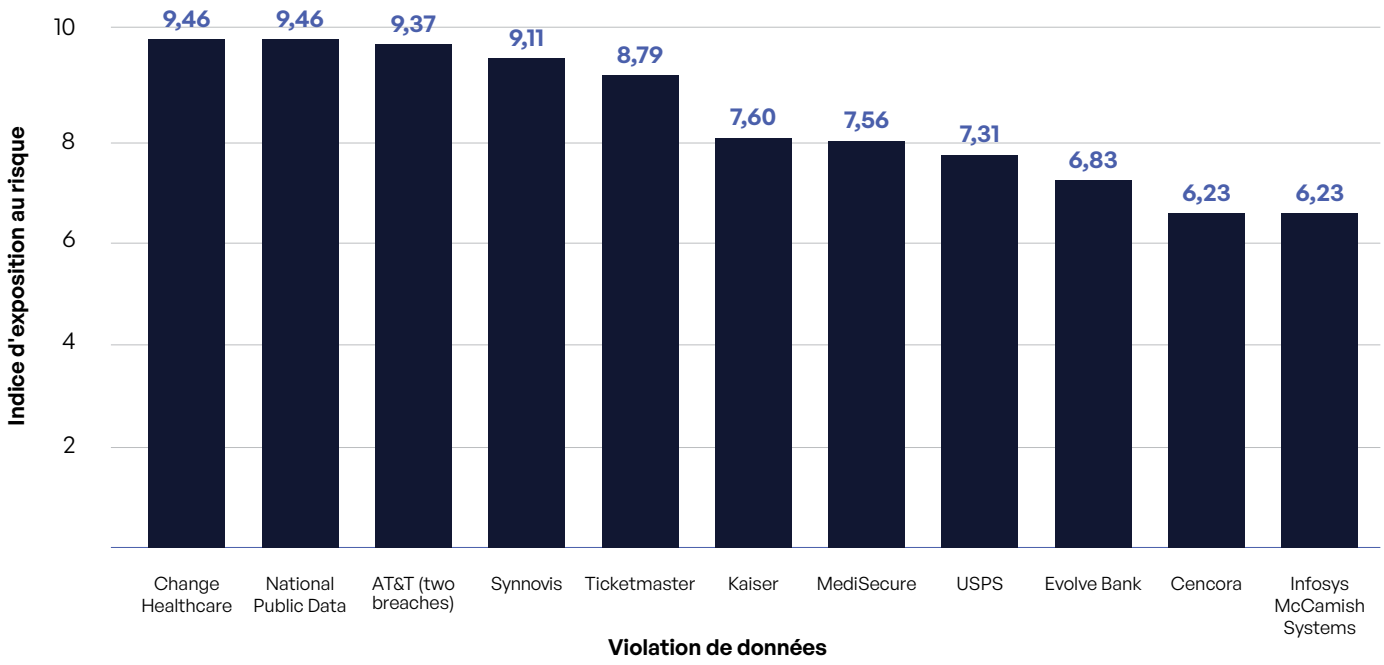


Figure 3: Score d'exposition au risque des 11 principales violations de données au cours du premier semestre 2024.

1. Change Healthcare (Exposition au risque: 9.46)

Description de l'incident : Change Healthcare a subi une attaque par ransomware qui a entraîné le vol de données de santé sensibles, y compris des informations personnelles, médicales et de facturation, touchant 100 millions de dossiers..

Analyse d'impact : La violation a eu un impact financier sévère, avec des coûts liés aux paiements de rançon, à la restauration des systèmes et aux frais juridiques. Les perturbations opérationnelles ont été importantes, affectant les soins aux patients dans divers établissements de santé. L'atteinte à la réputation a été considérable, entraînant une perte de confiance parmi les patients et les partenaires.

Décomposition de l'Exposition aux Risques:

Dossiers exposés:
100 000 000

Estimation de l'impact financier:
17 900 000 000 $

Sensibilité des données(1-5): 5

Impact financier (1-5): 4

Conformité réglementaire (1-5): 5

2. National Public Data (Exposition au risque: 9.46)

Description de l'incident : La violation a eu lieu le 23 décembre 2023. National Public Data, un courtier en données spécialisé dans les vérifications de dossiers et les services de prévention de la fraude, a indiqué que 2,9 milliards de dossiers appartenant à 1,3 million de personnes ont été compromis.

Analyse d'impact: Les informations violées comprenaient des numéros de sécurité sociale, des noms, des adresses électroniques, des numéros de téléphone et des adresses postales.

Décomposition de l'Exposition aux Risques:

Dossiers exposés:
2 900 000 000

Estimation de l'impact financier:
501 700 000 000 $

Sensibilité des données (1-5): 5

Impact financier (1-5): 5

Conformité réglementaire (1-5): 4

3. AT&T (Exposition au risque: 9.37)

Description de l'incident : Cette violation a entraîné le vol de 110 millions de dossiers clients, y compris des numéros de téléphone, des enregistrements d'appels et des informations personnelles, en raison d'un accès non autorisé.

Analyse d'impact: Des coûts financiers importants ont résulté des amendes réglementaires et des dépenses liées à la notification des clients. La violation a entraîné des impacts opérationnels, notamment des interruptions de service et un examen accru des pratiques de gestion des données d'AT&T. L'atteinte à la réputation a conduit à une diminution de la confiance des clients et à une augmentation du taux de désabonnement.

Pour la deuxième violation de données chez AT&T, bien que le nombre exact de dossiers de données ne soit pas explicitement mentionné, il est raisonnable d'estimer que le nombre total de dossiers de données compromis lors des deux violations dépasse largement les 110 millions, potentiellement atteignant des milliards, compte tenu de la nature des enregistrements d'appels et de messages sur une période de six mois pour une base de clients aussi vaste.

Décomposition de l'Exposition aux Risques:

Dossiers exposés:
110 000 000

Estimation de l'impact financier:
19 690 000 000 $

Sensibilité des données (1-5): 3

Impact financier (1-5): 5

Conformité réglementaire (1-5): 5

4. Synnovis (Exposition au risque: 9.11)

Description de l'incident : Synnovis, un laboratoire de pathologie au Royaume-Uni, a été la cible d'une attaque par ransomware, compromettant les données relatives à 300 millions d'interactions avec des patients et perturbant les services médicaux.

Analyse d'impact : L'impact financier comprenait les coûts de restauration des services et les amendes réglementaires potentielles. L'impact opérationnel a été considérable, avec de nombreuses procédures médicales reportées, provoquant un incident critique dans le secteur de la santé. L'atteinte à la réputation a affecté la confiance au sein de la communauté médicale.

Décomposition de l'Exposition aux Risques:

Dossiers exposés:
300 000 000

Estimation de l'impact financier:
53 700 000 000 $

Sensibilité des données (1-5): 1

Impact financier(1-5): 5

Conformité réglementaire (1-5): 4

5. Ticketmaster (Exposition au risque : 8.79)

Description de l'incident : La violation chez Snowflake, touchant Ticketmaster, a exposé 560 millions de dossiers clients, incluant les noms complets, adresses, adresses e-mail, numéros de téléphone et données de cartes de paiement.

Analyse d'impact : Les impacts financiers comprenaient les coûts de remédiation et les poursuites judiciaires potentielles. Les impacts opérationnels ont entraîné des perturbations des services clients et une surveillance de sécurité renforcée. L'atteinte à la réputation a touché Snowflake et ses clients, soulevant des inquiétudes concernant la sécurité du cloud.

Décomposition de l'Exposition aux Risques:

Dossiers exposés:
560,000,000

Estimation de l'impact financier:
100 240 000 000 $

Sensibilité des données (1-5): 2

Impact financier (1-5): 5

Conformité réglementaire (1-5): 5

6. Kaiser (Exposition au risque : 7.60)

Description de l'incident: Kaiser a involontairement partagé les informations médicales protégées de 13,4 millions de dossiers de patients avec des annonceurs en raison de codes de suivi utilisés sur son site Web.

Analyse d'impact: Les impacts financiers incluaient des amendes réglementaires et des règlements juridiques. Les impacts opérationnels ont nécessité une refonte des pratiques de gouvernance des données et de protection de la vie privée. La violation a causé une atteinte significative à la réputation et a soulevé des préoccupations concernant la confidentialité des données.

Décomposition de l'Exposition aux Risques:

Dossiers exposés:
13 400 000

Estimation de l'impact financier:
2 398 600 000 $

Sensibilité des données (1-5): 5

Impact financier (1-5): 4

Conformité réglementaire (1-5): 5

7. MediSecure (Exposition au risque : 7.56)

Description de l'incident: MediSecure, un fournisseur australien de prescriptions, a subi une attaque par ransomware compromettant les données personnelles et médicales de près de 13 millions d'Australiens.

Analyse d'impact: Les coûts financiers comprenaient les paiements de rançon et les frais juridiques. Les impacts opérationnels ont été considérables, perturbant les services de santé et menant à l'insolvabilité. L'atteinte à la réputation a érodé la confiance des clients et des partenaires.

Décomposition de l'Exposition aux Risques:

Dossiers exposés:
13 000 000

Estimation de l'impact financier:
2 327 000 000 $

Sensibilité des données (1-5): 5

Impact financier (1-5): 4

Conformité réglementaire (1-5): 3

8. USPS (Exposition au risque : 7.31)

Description de l'incident: USPS a partagé les adresses postales des utilisateurs connectés avec des annonceurs tels que Meta, LinkedIn et Snap via des codes de suivi.

Analyse d'impact: La violation a entraîné des coûts financiers dus aux amendes et aux règlements. Les impacts opérationnels ont inclus des modifications des pratiques de gouvernance des données. L'atteinte à la réputation a conduit à un examen accru et à des préoccupations concernant les pratiques de confidentialité.

Décomposition de l'Exposition aux Risques:

Dossiers exposés:
62 000 000

Estimation de l'impact financier:
11 098 000 000 $

Sensibilité des données (1-5): 1

Impact financier (1-5): 4

Conformité réglementaire (1-5): 5

9. Evolve Bank (Exposition au risque : 6.83)

Description de l'incident: Evolve Bank, un fournisseur de services bancaires en tant que service, a subi une attaque par ransomware compromettant les informations personnelles de plus de 7,6 millions de personnes.

Analyse d'impact: Les impacts financiers comprenaient des paiements de rançon et des amendes réglementaires. Les perturbations opérationnelles ont été importantes, affectant les services clients et entraînant des mesures de sécurité renforcées. L'atteinte à la réputation a été considérable, affectant la confiance des clients.

Décomposition de l'Exposition aux Risques:

Dossiers exposés:
7 600 000

Estimation de l'impact financier:
1 360 400 000 $

Sensibilité des données (1-5): 3

Impact financier (1-5): 3

Conformité réglementaire (1-5): 3

10. Infosys McCamish Systems (Exposition au risque : 6.23)

Description de l'incident: La violation a entraîné l'exposition de numéros de sécurité sociale, d'informations médicales et de données financières, affectant 6,1 millions de dossiers.

Analyse d'impact: Les impacts financiers comprenaient des amendes réglementaires et les coûts liés à la notification des violations. Les impacts opérationnels impliquaient des mesures de sécurité renforcées et des pratiques améliorées de protection des données. L'atteinte à la réputation a affecté la confiance des clients et les relations avec les partenaires.

Décomposition de l'Exposition aux Risques:

Dossiers exposés:
6 078 263

Estimation de l'impact financier:
1 074 000 000 $

Sensibilité des données (1-5): 5

Impact financier (1-5): 2

Conformité réglementaire (1-5): 5

11. Cencora (Exposition au risque : 6.23)

Description de l'incident: La violation de données a entraîné l'exposition de données de santé sensibles, y compris des dossiers médicaux de patients et d'autres données médicales confidentielles, impactant environ 1 million de dossiers. Cette attaque sur la supply chain a affecté les enregistrements de données d'au moins 27 entreprises pharmaceutiques et biotechnologiques.

Analyse d'impact: La violation a entraîné des coûts financiers importants, y compris des amendes réglementaires et les dépenses liées à la notification des personnes concernées et à la mise en œuvre de mesures de cybersécurité supplémentaires pour prévenir de futures violations. Les implications financières se sont également étendues aux frais juridiques et aux éventuels règlements avec les parties impactées.

Décomposition de l'Exposition aux Risques:

Dossiers exposés :
1 000 000

Estimation de l'impact financier :
179 000 000 $

Sensibilité des données (1-5): 5

Impact financier (1-5): 2

Conformité réglementaire (1-5): 5

Utilisation de l'indice d'exposition aux risques

Notre Indice d'Exposition au Risque prend en compte bien plus que le simple nombre de dossiers exposés ou le nombre de victimes touchées. Cette approche offre une compréhension plus claire de la véritable gravité et de l'impact potentiel de chaque violation. Bien qu'un nombre élevé de dossiers exposés puisse indiquer une violation importante, cela ne signifie pas nécessairement que l'exposition au risque est plus élevée. Plusieurs facteurs contribuent au score de risque d'une violation, ce qui peut parfois entraîner un score de risque plus élevé pour une violation avec moins de dossiers que pour une avec plus de dossiers.

1. Nature et sensibilité des données concernées

Le type de données compromises est un facteur déterminant influençant l'indice d'exposition au risque. Par exemple, la violation chez Change Healthcare, qui a impliqué 100 millions de dossiers, a principalement touché des informations personnelles, médicales et de facturation. Ce type de données est hautement sensible, entraînant des conséquences graves, telles que la perte irréversible de données de santé, ce qui augmente l'exposition au risque malgré un nombre de dossiers inférieur par rapport à d'autres violations. De même, la violation chez Cencora, avec seulement 1 million de dossiers exposés, a également obtenu un score élevé sur l'échelle des risques en raison de la sensibilité des données de santé impliquées, démontrant que la nature des données est souvent plus cruciale que le volume de données.

2. Implications en matière de réglementation et de conformité

Les implications réglementaires peuvent avoir un impact significatif sur l'exposition globale au risque d'une violation. Par exemple, la violation chez AT&T, qui a impliqué 110 millions de dossiers, présentait une exposition au risque substantielle non seulement en raison du nombre de dossiers, mais aussi en raison des violations potentielles de plusieurs réglementations, y compris les réglementations de la FCC, la loi FTC et le CCPA. Ces violations réglementaires peuvent entraîner des amendes et des sanctions importantes, augmentant ainsi le score de risque global de la violation. En revanche, une violation impliquant un plus grand nombre de dossiers, comme celle de Ticketmaster avec 560 millions de dossiers, pourrait avoir une exposition au risque plus faible si les données compromises n'entraînent pas de conséquences réglementaires aussi sévères.

3. Impact potentiel au-delà des pertes immédiates

Les conséquences à long terme d'une violation de données, telles que l'usurpation d'identité, la fraude financière ou l'atteinte à la réputation, sont également prises en compte dans l'indice d'exposition au risque. La violation de Synnovis, qui concernait 300 millions d'enregistrements de données d'interaction avec les patients, est un exemple où l'impact à long terme sur les services aux patients et la confiance a donné lieu à un score de risque élevé. Même si le nombre d'enregistrements était inférieur à celui de la violation de Ticketmaster, la possibilité d'un préjudice durable pour les patients et les services de santé a considérablement augmenté l'exposition au risque. Cet exemple montre que l'indice tient compte des conséquences plus larges d'une violation, au-delà de la perte immédiate de données.

4. Ransomware et facteurs d'extorsion

La présence de demandes de rançon peut également augmenter le score de risque d'une violation, quel que soit le nombre d'enregistrements exposés. La faille de Synnovis, par exemple, a fait l'objet d'une demande de rançon de 50 millions de dollars, ce qui a contribué à l'obtention d'un score de risque élevé. Même si le nombre d'enregistrements concernés est inférieur à celui de Ticketmaster, les coûts et les risques supplémentaires associés aux demandes de rançon, y compris la possibilité d'une double extorsion et les frais de récupération, augmentent l'exposition globale au risque de la violation.

5. L'impact de la sensibilité des données et le risque d'usurpation d'identité

L'impact de la sensibilité des données est évident dans les violations telles que celles subies par des entreprises comme Change Healthcare et Synnovis, où les types de données concernées comprenaient des informations médicales et personnelles très sensibles. Le potentiel d'utilisation abusive, comme l'usurpation d'identité et la fraude financière, contribue de manière significative à l'exposition à un risque plus élevé de ces violations, même par rapport aux violations impliquant un volume plus important de données moins sensibles, comme celle subie par Ticketmaster.

Réflexions finales

Notre analyse des 11 principales violations de données au cours du premier semestre 2024 révèle plusieurs informations essentielles sur l'évolution du paysage des menaces de cybersécurité :

1. **Diversité des vecteurs d'attaque et sophistication croissante :** Les cybercriminels continuent d'utiliser diverses méthodes d'attaque, allant des ransomwares et des accès non autorisés au partage involontaire de données, chacune ayant des implications uniques pour les stratégies de sécurité. Cette diversité des vecteurs d'attaque souligne l'importance pour les organisations d'adopter une approche de sécurité multicouche qui couvre un large éventail de menaces potentielles.
2. **L'impact significatif des rançongiciels :** Les attaques par ransomware, en particulier celles visant des secteurs de grande valeur comme la santé et la finance, se révèlent à la fois perturbatrices et coûteuses. Des violations telles que celles impliquant Change Healthcare et Synnovis ont démontré les graves dommages opérationnels, financiers et d'atteinte à la réputation qui peuvent en résulter. Les organisations doivent prioriser des défenses robustes contre les ransomwares, incluant la détection avancée des menaces, des capacités de réponse rapide et des stratégies de sauvegarde de données efficaces.
3. **Sensibilité et volume élevés des données exposées:** Les violations de données impliquant de grands volumes d'informations sensibles, en particulier les données personnelles et financières, ont systématiquement entraîné des scores de risque plus élevés en raison de leur potentiel de vol d'identité, de fraude financière et de sanctions réglementaires. Cela souligne la nécessité de renforcer les mesures de protection des données, notamment pour les organisations, telles que National Public Data, qui traitent des données sensibles à travers plusieurs outils et plateformes de communication.
4. **Vulnérabilités des tiers et de la chaîne d'approvisionnement :** Plusieurs violations, comme celles touchant AT&T et Ticketmaster, ont mis en lumière les vulnérabilités liées aux fournisseurs tiers et aux partenaires de la supply chain. Cela souligne la nécessité cruciale d'une surveillance continue et d'une gestion robuste des relations avec les tiers pour atténuer les risques associés aux réseaux étendus.
5. **Conformité réglementaire et répercussions juridiques :** L'analyse montre que les violations de données entraînent souvent des infractions à plusieurs réglementations, ce qui conduit à des amendes substantielles et à des conséquences juridiques. Les organisations doivent renforcer leurs cadres de conformité et leurs pratiques de gouvernance des données pour éviter les infractions réglementaires et les pénalités financières associées.
6. **Évaluation globale des Risques:** Les conclusions du rapport soulignent l'importance de prendre en compte plusieurs facteurs lors de l'évaluation de l'exposition au risque d'une violation de données. Il ne s'agit pas uniquement du nombre de dossiers compromis ou du coût financier immédiat ; le véritable risque est souvent déterminé par une combinaison d'éléments, notamment la sensibilité des données compromises, le potentiel de violations réglementaires et les implications plus larges pour l'atteinte à la réputation à long terme.
7. **Impact contextuel du type de violation et de la sensibilité des données :** Les conclusions soulignent que le type de violation et la sensibilité des données impliquées sont des facteurs critiques influençant l'exposition globale au risque. Par exemple, une violation impliquant un petit nombre de dossiers hautement sensibles, tels que des numéros de sécurité sociale ou des dossiers médicaux, peut avoir des conséquences plus graves qu'une violation impliquant un grand volume de données moins sensibles. Cela démontre que les organisations doivent évaluer le contexte et le contenu des données violées, et pas seulement la quantité, pour comprendre pleinement les impacts potentiels.

Recommandations pratiques

1. **Adopter des postures de sécurité renforcées :** Les organisations doivent renforcer leurs cadres de cybersécurité avec des mesures de sécurité durcies, adaptées pour protéger les communications de contenu sensible. Cela inclut le déploiement de fonctions de sécurité avancées telles que des systèmes de détection et de prévention des intrusions, des canaux de communication sécurisés, et une surveillance continue des menaces pour empêcher tout accès non autorisé et atténuer les violations potentielles.

2. **Mettre en œuvre des techniques de cryptage avancées :** Pour garantir la confidentialité et la sécurité des données sensibles, les organisations doivent utiliser des méthodes de chiffrement avancées pour les données au repos, en transit et en cours d'utilisation. Le chiffrement des communications de contenu sensible aide à prévenir l'accès non autorisé et les violations de données, assurant ainsi la conformité aux exigences réglementaires et protégeant les informations sensibles.

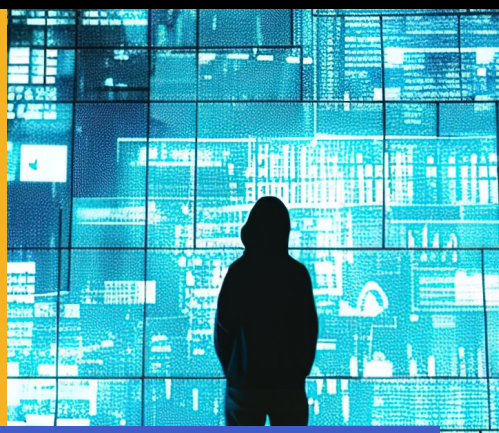
3. **Déployer une gestion des droits numériques (DRM) de nouvelle génération :** Les organisations doivent mettre en place des stratégies solides de gestion des droits numériques pour contrôler et surveiller l'accès aux contenus sensibles. Cela inclut la définition des droits d'accès, le suivi de l'utilisation des documents et l'application de contrôles pour empêcher le partage non autorisé ou l'utilisation abusive d'informations sensibles, réduisant ainsi le risque de violations de données et garantissant la conformité aux réglementations en matière de protection des données.

4. **Améliorer les pratiques de gestion des risques des tiers :** Évaluez et surveillez régulièrement les pratiques de sécurité des fournisseurs et partenaires tiers pour atténuer les risques liés aux réseaux étendus. Cela inclut l'application de strictes exigences de sécurité pour les interactions avec des tiers et la mise en œuvre de protocoles de communication sécurisés pour protéger les données sensibles partagées avec des entités externes.

5. **Priorité à la sensibilité des données et à la conformité :** Renforcez les pratiques de protection des données en priorisant la sécurité des informations hautement sensibles grâce à des contrôles d'accès, du chiffrement et une surveillance rigoureuse. Assurez la conformité aux réglementations en matière de protection des données personnelles en auditant régulièrement les pratiques de gestion des données et en maintenant des cadres de gouvernance solides pour protéger les communications de contenu sensible.

Perspectives d'avenir

Alors que les cybermenaces continuent d'évoluer en complexité et en ampleur, les organisations doivent rester vigilantes et proactives dans leurs efforts de cybersécurité. La dépendance croissante aux plateformes numériques et aux services tiers augmentera probablement la surface d'attaque, rendant la gestion des risques plus cruciale que jamais. En utilisant des outils comme l'Indice d'Exposition aux Risques et en adoptant une approche prospective de la cybersécurité, les organisations peuvent mieux se protéger contre les futures violations et minimiser les impacts potentiels.



Annexe

Algorithme de l'indice d'exposition aux risques

Critères de notation

1. **Nombre de dossiers exposés :**
   - Plus de 100 000 000 : 6 points
   - 10 000 001 - 100 000 000 : 5 points
   - 1 000 001 - 10 000 000 : 4 points
   - 100 001 - 1 000 000 : 3 points
   - 10 001 - 100 000 : 2 points
   - 1 - 10 000 : 1 point
2. **Estimation de l'impact financier :**
   - Plus de 10 000 000 000 $: 6 points
   - 1 000 000 001 $ - 10 000 000 000 $: 5 points
   - 100 000 001 $ - 1 000 000 000 $: 4 points
   - 10 000 001 $ - 100 000 000 $: 3 points
   - 1 000 001 $ - 10 000 000 $: 2 points
   - 1 - 1 000 000 $: 1 point
3. **Implication des ransomwares :**
   - Oui : 1 point
   - Non : 0 points
4. **Sensibilité des données :**
   - **5 points (Données extrêmement sensibles) :** Les violations impliquant des informations hautement confidentielles telles que les numéros de sécurité sociale, les dossiers médicaux, les données biométriques ou les données d'entreprise très confidentielles qui pourraient causer des dommages graves ou irréparables si elles étaient divulguées.
   - **4 points (Données hautement sensibles) :** Les violations impliquant des informations plus sensibles telles que des détails financiers (numéros de carte de crédit, détails de compte bancaire), des informations médicales, ou des données pouvant mener à un vol d'identité ou à une fraude.
   - **3 points (Données sensibles):** Les violations impliquant des informations personnelles identifiables (PII) telles que les adresses e-mail, les numéros de téléphone ou d'autres détails personnels pouvant potentiellement être utilisés pour le phishing ou le spam.
   - **2 points (Sensibilité modérée):** Les données qui incluent des informations non publiques et moins sensibles telles que les noms, adresses ou coordonnées, qui peuvent être facilement obtenues mais ne présentent pas de risque significatif en cas d'exposition.
   - **1 point (Faible sensibilité):** Les violations impliquant des données non sensibles ou publiquement disponibles, telles que des ensembles de données génériques ou anonymisés ne contenant aucune donnée personnelle identifiable (PII) ou donnée personnelle sensible.

5. **Sévérité:**
   - **5 points (Impact critique):** Impact catastrophique avec de graves répercussions financières, des risques majeurs pour la santé publique, un vol d'identité généralisé, ou une atteinte à la réputation sévère entraînant une perte de confiance durable.
   - **4 points (Fort impact):** Conséquences importantes, notamment des vols d'identité massifs, des cas de fraude, des pertes financières considérables ou des amendes réglementaires.
   - **3 points (Impact modéré):** Préjudice modéré, tel que des pertes financières limitées ou une atteinte à la réputation, certains cas de vol d'identité, ou un examen réglementaire modéré.
   - **2 points (Faible impact):** Perturbations mineures, impact financier limité ou exposition restreinte sans préjudice significatif pour les individus ou les opérations de l'organisation.
   - **1 point (Impact minimal):** Violations ayant peu ou pas d'impact sur l'organisation ou les individus, peut-être en raison d'une maîtrise rapide ou de l'absence d'exposition de données précieusese.

6. **Nombre de règlements concernés:**
   - 5 règlementations ou plus : 5 points
   - 4 règlementations : 4 points
   - 3 règlementations : 3 points
   - 2 règlementations : 2 points
   - 1 règlementation : 1 point

Détails de l'algorithme

1. Récapitulez les points des six critères.
2. Diviser la somme par 2,8 pour normaliser le score sur une échelle de 1 à 10.
3. Arrondir le résultat à deux décimales.

Score final = (Points relatifs aux enregistrements + Points relatifs à l'impact financier + Point relatif aux rançongiciels + Sensibilité des données + Gravité + Points relatifs à la réglementation)

2.8 *(NOTE: Score brut maximal possible: 28 points; score brut minimal possible: 5 points)*

1. "2023 Data Breach Report," Identity Theft Resource Center, Janvier2024.
2. "Cost of a Data Breach Report 2024," IBM, Juillet 2024.
3. "2024 Data Breach Investigations Report," Verizon, Avril 2024.
4. "Privacy in Practice 2024," ISACA, Janvier 2024.
5. "Cost of a Data Breach Report 2024," IBM, Juillet 2024.
6. "Enforcement Tracker Database," CMS, consulté le 2 septembre 2024.
7. "2024 Data Breach Investigations Report," Verizon, Mai 2024.