Kiteworks

Analyse 2024 des communications de contenu sensible dans l'industrie : les tendances en matière de sécurité et de conformité

CHIFFRES CLÉS

Outils de communication utilisés	17%	Plus de 7
	8%	6
	27%	5
	20%	4
	17%	3
	11%	2
	2%	1
Échange de contenu sensible avec des tiers	11%	Plus de 5 000
	23%	2 500 à 4 999
	32%	1 000 à 2 499
	20%	500 à 999
	15%	Moins de 499
Types de données les plus préoccupantes (Top 3)	79%	Documents financiers
	46%	PI
	46%	Échanges juridiques
	44%	LLMs de GenAI
	35%	PII
	23%	Fusions & Acquisitions
	15%	CUI et FCI
	13%	PHI
Top 2 des priorités sur la confidentialité et la conformité	52%	Lois des États américains
	36%	RGPD
	33%	Exigences SEC
	29%	CMMC
	21%	HIPAA
	18%	Lois propres à chaque pays
	11%	PCI DSS
Top 2 des certificats de sécurité les plus importants	58%	ISO 27001, 27017, 27018
	37%	IRAP (Australie)
	33%	SOC 2 Type II
	29%	NIST 800-171/CMMC 2.0
	29%	FedRAMP Moderate
	9%	Directive NIS 2
Nombre de piratages des communications de contenu sensible	14%	Plus de 10
	12%	7 à 9
	23%	4 à 6
	29%	2 à 3
	23%	1
	0%	Ne sait pas

Le rapport Kiteworks 2024 sur la confidentialité et la conformité des communications de contenu sensible fournit une analyse détaillée des problématiques et des pratiques dans différents secteurs d'activité, et notamment dans l'industrie. Ce brief reprend les principales conclusions du rapport concernant le secteur industriel ; outils utilisés pour échanger des données sensibles, problèmes de cybersécurité, risques dans les échanges avec des tiers, menaces spécifiques et conséquences sur la conformité règlementaire.

Gestion de tous les outils de communication de contenu sensible

52 % des industriels utilisent au moins cinq outils de communication pour envoyer et partager des contenus sensibles, plus que les 53 % des personnes interrogées au niveau mondial. 52 % d'entre eux déclarent pouvoir suivre et contrôler les données sensibles envoyées et partagées en interne, tandis que seulement 39 % indiquent être en mesure de le faire lorsqu'elles sont échangées en externe.

La prévention des fuites de propriété intellectuelle et de secrets d'entreprise (61%) et le fait d'éviter les pannes opérationnelles et pertes de revenus (44%) sont les deux priorités citées par les industriels. Ces chiffres contrastent avec ceux de l'ensemble des répondants qui ont cité la prévention des fuites de propriété intellectuelle et de secrets d'entreprise (56 %) et l'atténuation des litiges longs et coûteux (51 %). En revanche, l'impact négatif sur l'image de marque est la motivation la moins souvent citée par les répondants du secteur industriel (15 %).

Évaluer le risque tiers pour les contenus sensibles

La gestion des risques tiers est une préoccupation majeure des industriels. 34 % d'entre eux échangent des contenus sensibles avec plus de 2500 interlocuteurs. 66 % ont plus de 1000 interlocuteurs dans leur supply chain, un chiffre identique à celui de la cohorte. Il y a de bonnes nouvelles concernant le suivi et le contrôle des communications de contenu sensible dans

l'industrie ; un pourcentage plus élevé (79 %) que tout autre secteur a déclaré être capable de suivre et contrôler plus des trois quarts des contenus sensibles qui quittent une application.

Évaluer le niveau de conformité pour les contenus sensibles

94 % des industriels ont indiqué que leur système de management de la conformité des communications sensibles nécessitait des améliorations plus ou moins importantes. Ce chiffre est nettement supérieur à celui de l'ensemble des répondants (88 %). Le seul secteur qui affiche un retard supérieur est celui des professions libérales (96 %).

Les industriels ont cité les lois sur la protection des données de chaque État américain en tête de leurs priorités (52 % l'ont classé en premier ou en deuxième). Avec l'adoption de 18 lois au niveau des États, ce n'est pas une grande surprise. Le RGPD arrive en deuxième position, avec 36 % des organisations qui le citent parmi leurs priorités. La norme PCI DSS arrive loin derrière, avec 11 % des répondants qui la placent en première ou en deuxième position.

Pour ce qui est des certifications de sécurité, 58 % des industriels ont cité les normes ISO 27001, 27017 et 27018 comme l'un de leurs deux premiers choix. L'IRAP (Information Security Registered Assessors Program), supervisé par le gouvernement australien pour évaluer de manière indépendante leur posture de cybersécurité, a étonnamment été cité le plus souvent par 37 % des industriels, soit plus que SOC 2 Type II (33 %).

Évaluer les risques liés à la sécurité des contenus sensibles

98 % des industriels déclarent que leur management des risques associés aux communications sensibles doit être amélioré de manière significative ou partielle (contre 88 % pour l'ensemble des répondants). Cette différence est considérable et signe d'une lacune majeure à corriger.

Les outils de sécurité avancés (chiffrement, authentification multifactorielle, suivi et contrôle de la gouvernance) ne sont utilisés que partiellement pour 42 % des industriels (contre 39 % pour l'ensemble des secteurs). Ce chiffre révèle une autre lacune importante qui touche ce secteur.

Évaluer le coût de la sécurité et de la conformité

Comme la plupart des secteurs, l'enquête montre que les industriels sont très exposés aux violations de données, même si les résultats sont meilleurs. Plus précisément, 49 % des industriels ont déclaré avoir subi au moins cinq violations de leur contenu sensible, et 24 % au moins sept. C'est mieux que l'ensemble des répondants à l'enquête : 32 % au moins sept et 55 % au moins quatre.

Du point de vue financier, les fabricants s'en sortent mieux que la plupart des autres secteurs : 18 % ont indiqué avoir dépensé plus de 5 millions de dollars par an en frais de contentieux, contre 25 % pour la moyenne mondiale.

Connaissance et classification des types de données

Près de la moitié (49 %) des industriels ont indiqué étiqueter et classer plus des trois quarts des données non structurées et 30 % plus de la moitié des données. Ces pourcentages sont proches des chiffres mondiaux, où 48 % déclarent étiqueter et classer les trois quarts ou plus de leurs données non structurées.

Mais toutes les données non structurées n'ont pas besoin d'être classées, du moins c'est ce qu'ont indiqué la plupart des répondants. 18 % des industriels interrogés ont déclaré que 80 % ou plus des données non structurées avaient besoin d'être classées et 58 % moins de 60 %.

Urgence absolue à protéger les contenus sensibles dans l'industrie

Le rapport Kiteworks 2024 souligne l'importance de la gestion des risques et de la conformité pour les communications de contenu sensible dans le secteur industriel. Les documents financiers ressortent comme le type de données le plus exposé (par 79 % des répondants), plus que tous les autres secteurs.

En pratique, les industriels passent beaucoup de temps à compiler les journaux d'audit générés par les nombreux outils de communication de contenus sensibles. La moitié des personnes interrogées doivent en réconcilier plus de 11. Cela représente un engorgement considérable : 11 % y consacrent au moins 2 500 heures par an et 21 % plus de 2 000 heures.

Accéder au rapport complet