Kiteworks

Analyse 2024 des communications de contenu sensible dans le secteur financier : les tendances en matière de sécurité et de conformité

CHIFFRES CLÉS

Outils de communication utilisés	16%	Plus de 7
	21%	6
	29%	5
	16%	4
	13%	3
	3%	2
	0%	1
Échange de contenu sensible avec des tiers	13%	Plus de 5 000
	30%	2 500 à 4 999
	27%	1 000 à 2 499
	10%	500 à 999
	20%	Moins de 499
Types de données les plus préoccupantes (Top 3)	50%	Documents financiers
	46%	PHI
	44%	PII
	43%	LLMs de GenAI
	39%	PI
	37%	Échanges juridiques
	23%	CUI et FCI
	17%	Fusions & Acquisitions
Top 2 des priorités sur la confidentialité et la conformité	53%	Lois des États américains
	44%	RGPD
	31%	HIPAA
	29%	Exigences SEC
	19%	Lois propres à chaque pays
	16%	CMMC
	9%	PCI DSS
Top 2 des certificats de sécurité les plus importants	53%	NIST 800-171/CMMC 2.0
	50%	ISO 27001, 27017, 27018
	36%	SOC 2 Type II
	37%	IRAP (Australie)
	21%	FedRAMP Moderate
	11%	Directive NIS-2
Nombre de piratages des communications de contenu sensible	10%	Plus de 10
	20%	7 à 9
	37%	4 à 6
	16%	2 à 3
	9%	1
	9%	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 la finance. Ce brief reprend les principales conclusions du rapport concernant le secteur financier ; 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

66 % des établissements financiers utilisent au moins cinq outils de communication pour envoyer et partager des contenus sensibles, plus que les 53 % des personnes interrogées au niveau mondial. 57 % d'entre eux déclarent pouvoir suivre et contrôler les données sensibles envoyées et partagées en interne, tandis que 49 % 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 et la réduction des frais de contentieux sont les deux priorités citées par les établissements financiers (57 %). Tous secteurs confondus, ces deux priorités sont citées dans le même ordre, mais à des taux inférieurs (56 % et 51 %). En revanche, l'impact négatif sur l'image de marque est la motivation la moins souvent citée par les répondants du secteur financier (15 %).

Évaluer le risque tiers pour les contenus sensibles

La gestion des risques tiers est une préoccupation majeure des établissements financiers. 43 % d'entre eux échangent des contenus sensibles avec plus de 2 500 interlocuteurs. Étonnamment, 70 % d'entre eux comptent plus de 1 000 interlocuteurs dans leur supply chain (contre 66 % pour l'ensemble des secteurs d'activité).

Cette situation est inquiétante dans la mesure où seuls 44 % des répondants ont indiqué pouvoir suivre et contrôler environ la moitié des contenus sensibles qui quittent une application.

Évaluer le niveau de conformité pour les contenus sensibles

82 % des établissements financiers ont indiqué que leur système de management de la conformité des communications sensibles nécessitait des améliorations plus ou moins importantes. Ce chiffre est inférieur à celui de l'ensemble des répondants : 88 %.

Les établissements financiers ont cité les lois sur la protection des données de chaque État américain en tête de leurs priorités (53 % en premier ou deuxième). Avec l'adoption de 18 lois nationales, ce n'est pas une grande surprise. Le RGPD arrive en deuxième position, avec 44 % des organisations qui le citent parmi leurs priorités. La norme PCI DSS arrive loin derrière, avec 9 % des répondants seulement qui la placent en première ou en deuxième position.

Pour ce qui est des certifications de sécurité, les établissements financiers sont plus nombreux que les autres secteurs à s'en soucier. Par exemple, 53 % ont cité NIST 800-171/CMMC 2.0 comme l'un de leurs deux premiers choix, et 50 % pour ISO 27001, 27017 et 27018. La directive NIS 2, qui entrera en vigueur fin 2024, est la moins citée avec 9 %. La présence de la norme NIST 800-171 en tête de liste est quelque peu surprenante, car elle s'applique principalement aux organisations opérant pour le compte du gouvernement fédéral et du DoD (ministère de la défense américain).

Évaluer les risques liés à la sécurité des contenus sensibles

88 % des établissements financiers déclarent que leur management des risques associés aux communications sensibles doit être amélioré de manière significative ou partielle (résultat identique à l'ensemble de la cohorte).

57 % des établissements financiers ont indiqué avoir subi au moins cinq violations de leur contenu sensible (30 % déclarent en avoir subi plus de sept). Près d'un répondant sur dix issu de la finance admet ne pas connaître avec certitude le nombre de violations de données subies par son entreprise.

Les outils de sécurité avancés (chiffrement, authentification multifactorielle, suivi et contrôle de la gouvernance) ne sont utilisés que partiellement dans 36 % des établissements financiers, dont 4 % indiquant n'en utiliser aucun et 60 % y avoir recours de façon systématique. Ces résultats sont en décalage avec les réponses de l'ensemble de la cohorte, et révèlent une lacune majeure du secteur financier.

Évaluer le coût de la sécurité et de la conformité

Comme la plupart des secteurs d'activité, l'enquête montre que la finance est très exposée aux violations de données, 30 % des répondants déclarant avoir subi au moins sept violations de données en 2023. Un chiffre est légèrement supérieur à la moyenne mondiale de 32 %. De plus, 37 % affirment avoir subi entre quatre et six attaques.

Du point de vue financier, 36 % des établissements financiers interrogés ont déclaré avoir dépensé plus de 5 millions de dollars par an en frais de contentieux. Ce chiffre est supérieur à la moyenne mondiale de 25 %. En outre, 55 % des répondants du secteur financier ont déclaré avoir dépensé plus de 3 millions de dollars, contre seulement 45 % au niveau mondial.

Connaissance et classification des types de données

19 % des établissements financiers ont indiqué étiqueter et classer moins de 25 % des données non structurées ; 23 % ont admis étiqueter et classer moins de la moitié des données. Ces pourcentages correspondent aux moyennes mondiales : 20 % étiquettent et classent moins d'un quart des données.

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. 20 % des établissements financiers ont déclaré que plus de 80 % des données avaient besoin d'être classées et 23 % plus de 60 %. Autrement dit, 43 % déclarent que plus de 60 % des données ont besoin d'être classées. Ces chiffres révèlent un écart, surtout si on les compare aux moyennes mondiales, où 22 % des répondants étiquettent et classifient moins d'un quart des données et 35 % entre 40 et 60 %.

Urgence absolue à protéger les contenus sensibles dans le secteur financier

Le rapport Kiteworks 2024 souligne l'importance de la gestion des risques et de la conformité pour les communications de contenu sensible dans les établissements financiers. Les documents financiers ressortent comme le type de données le plus exposé (par 50 % des répondants), bien que d'autres types de données soient fréquemment cités. Les établissements financiers sont assurément la cible des acteurs malveillants, puisque deux tiers d'entre eux ont subi plus de cinq violations de données l'année dernière.

En pratique, ils passent beaucoup de temps à compiler les journaux d'audit générés par les nombreux outils de communication de contenus sensibles. Près de la moitié (48 %) des répondants doivent en réconcilier plus de 11, et 8 % d'entre eux ne savent même pas combien il y en a. Cela représente un engorgement considérable : 11 % des personnes interrogées y consacrent au moins 2 500 heures par an et 20 % plus de 2 000 heures.

Accéder au rapport complet