Kiteworks

Analyse 2024 des communications de contenu sensible du gouvernement fédéral : les tendances en matière de sécurité et de conformité

CHIFFRES CLÉS

Outils de communication utilisés	28%	Plus de 7
	3%	6
	28%	5
	7%	4
	24%	3
	10%	2
	0%	1
Échange de contenu sensible avec des tiers	28%	Plus de 5 000
	10%	2 500 à 4 999
	24%	1 000 à 2 499
	7%	500 à 999
	31%	Moins de 499
Types de données les plus préoccupantes (Top 3)	61%	Échanges juridiques
	50%	PI
	44%	LLMs de GenAI
	33%	PII
	33%	PHI
	33%	Documents financiers
	28%	Fusions & Acquisitions
	17%	CUI et FCI
Top 2 des priorités sur la confidentialité et la conformité	55%	Lois propres à chaque pays
	45%	RGPD
	28%	Lois des États américains
	24%	Exigences SEC
	21%	CMMC
	14%	HIPAA
	14%	PCI DSS
Top 2 des certificats de sécurité les plus importants	48%	ISO 27001, 27017, 27018
	45%	NIST 800-171/CMMC 2.0
	34%	FedRAMP Moderate
	31%	SOC 2 Type II
	24%	IRAP (Australie)
	17%	Directive NIS 2
Nombre de piratages des communications de contenu sensible	17%	Plus de 10
	10%	7 à 9
	17%	4 à 6
	34%	2 à 3
	17%	1
	3%	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 pour le gouvernement fédéral. Ce brief reprend les principales conclusions du rapport concernant le gouvernement fédéral ; 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

59 % des agences fédérales utilisent au moins cinq outils de communication pour envoyer et partager des contenus sensibles, ce qui est plus que la moyenne de l'ensemble de la cohorte (53 %). En ce qui concerne le suivi et le contrôle des contenus sensibles, 59 % des répondants ont déclaré pouvoir suivre et contrôler les données sensibles envoyées et partagées en interne, et autant lorsqu'elles sont échangées en externe. Ces chiffres sont légèrement supérieurs aux moyennes de 51 % et 43 % de l'ensemble des répondants. Cela s'explique sans doute par les différents contrôles et normes de sécurité appliqués au niveau des administrations fédérales.

La prévention des fuites de propriété intellectuelle et de secrets d'entreprise est de loin la priorité des répondants fédéraux (69 % l'ont citée comme première ou deuxième priorité). Hormis les cabinets d'avocats, c'est le taux de réponse le plus élevé enregistré, contre 56 % pour l'ensemble de la cohorte. Éviter les sanctions pour non-respect des règlementations est la deuxième priorité la plus fréquemment citée, probablement en raison des différentes normes imposées aux agences fédérales (par exemple, CMMC 2.0 ou encore Executive Order 14028).

Évaluer le risque tiers pour les contenus sensibles

La gestion des risques liés aux tiers est une préoccupation majeure des agences fédérales, 38 % d'entre elles déclarant échanger des contenus sensibles avec plus de 2 500 interlocuteurs différents et 60 % avec plus de 1 000 (contre 44 % et 66 % pour l'ensemble des répondants). En ce qui concerne le suivi et le contrôle des contenus sensibles lorsqu'ils quittent une application, le secteur fédéral est l'un des secteurs industriels les plus matures : 62 % des répondants indiquent pouvoir suivre et contrôler plus des trois quarts des données qui quittent une application.

Évaluer le niveau de conformité pour les contenus sensibles

86 % des répondants fédéraux ont indiqué que leur système de management de la conformité des communications sensibles nécessitait des améliorations plus ou moins importantes. Ce chiffre est légèrement inférieur à celui de l'ensemble des répondants : 88 %.

Le gouvernement en général est très attentif à la protection de la vie privée de ses citoyens et résidents. Dans notre étude, les lois sur la confidentialité des données propres à chaque pays sont le plus citées par les répondants fédéraux (55 %), ce qui est nettement supérieur à la moyenne de 21 % pour l'ensemble des répondants. Le RGPD arrive en deuxième position (45 %).

En ce qui concerne les normes et certificats de sécurité, les personnes consultées au niveau fédéral ont cité les normes ISO 27001, 27017 et 27018 comme leur priorité absolue (48 %), suivies de la norme NIST 800-171/CMMC 2.0 (45 %). Les normes de sécurité gouvernementales s'appliquent non seulement au secteur privé, mais aussi au secteur public, et l'on s'attend donc à une augmentation constante de ces chiffres.

Évaluer les risques liés à la sécurité des contenus sensibles

80 % des agences fédérales ont déclaré que leur management des risques associés aux communications sensibles devait être amélioré de manière significative ou partielle, et 20 % indiquent qu'ils n'ont besoin d'aucune amélioration. Ce dernier chiffre est plus élevé que dans la plupart des autres secteurs d'activité. Toutefois, comme le révèlent les données relatives aux violations de données, un niveau de confiance plus élevé n'est pas forcément synonyme de moins de risques.

44 % des répondants fédéraux ont admis avoir subi au moins quatre violations de leur contenu sensible et 27 % au moins sept. Ces chiffres sont inférieurs à ceux des autres secteurs (55 % et 32 %). C'est peut-être le signe que les agences fédérales gèrent mieux les risques que leurs homologues du privé. Sachant qu'elles sont dans le viseur des pirates informatiques, c'est une bonne nouvelle (un point à surveiller dans l'enquête de l'année prochaine).

Les outils de sécurité avancés (chiffrement, authentification multifactorielle, suivi et contrôle de la gouvernance) ne sont que partiellement utilisés par 52 % des agences fédérales. C'est nettement mieux que les 41 % de l'ensemble des personnes interrogées. 39% ont admis en utiliser quelques-uns et 2% n'en utiliser aucun. Encore une fois, cela révèle une plus grande maturité en matière de sécurité dans le secteur fédéral par rapport à l'ensemble des personnes interrogées.

Évaluer le coût de la sécurité et de la conformité

Les frais engagés suite à des violations de données sont aussi élevés dans le secteur public que dans le privé. 35 % des répondants de l'administration fédérale ont déclaré que les violations de données leur avaient coûté plus de 3 millions de dollars par an, et 45 % que les frais de contentieux s'élevaient à plus de 3 millions de dollars par an. 7 % des répondants fédéraux ont admis ne pas connaître ces coûts annuels.

Connaissance et classification des types de données

45 % des répondants fédéraux ont déclaré étiqueter et classer plus des trois quarts des données non structurées ; ce chiffre est légèrement inférieur à celui de l'ensemble des répondants (48 %). Lorsqu'on les interroge sur la proportion de données non structurées qui doivent être étiquetées ou classées, une divergence apparaît, 41 % répondant 80 % ou plus.

Urgence absolue à protéger les contenus sensibles du gouvernement fédéral

Le rapport Kiteworks 2024 souligne l'importance de la gestion des risques et de la conformité pour les communications de contenu sensible du gouvernement fédéral.

Les personnes du gouvernement fédéral interrogées ont indiqué que les échanges juridiques constituaient leur principale préoccupation en matière de données (61 %), suivis par la propriété intellectuelle (50 %). Compte tenu des attaques incessantes contre les secrets nationaux, cette réponse est logique. Ces réponses contrastent néanmoins avec celles de la cohorte, où les documents financiers sont cités à 55 % et les échanges juridiques à 44 %.

En pratique, les répondants passent beaucoup de temps à compiler les journaux d'audit générés par les nombreux outils de communication de contenus sensibles. 48 % doivent en réconcilier plus de 11 (identique à la moyenne de l'ensemble des personnes interrogées), et 10 % ne savent même pas combien il y en a. Cela représente un engorgement considérable, bien qu'à un taux inférieur à celui du secteur privé ; 21 % des répondants fédéraux y consacrent au moins 2 000 heures par an et 56 % plus de 1 500 heures.

Accéder au rapport complet