Kiteworks

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

CHIFFRES CLÉS

Outils de communication utilisés	5%	Plus de 7
	7%	6
	37%	5
	21%	4
	12%	3
	9%	2
	5%	1
Échange de contenu sensible avec des tiers	7%	Plus de 5 000
	40%	2 500 à 4 999
	19%	1 000 à 2 499
	16%	500 à 999
	19%	Moins de 499
Types de données les plus préoccupantes (Top 3)	58%	PII
	50%	PI
	46%	Documents financiers
	42%	Échanges juridiques
	35%	LLMs de GenAI
	23%	PHI
	23%	CUI et FCI
	23%	Fusions & Acquisitions
Top 2 des priorités sur la confidentialité et la conformité	49%	CMMC
	44%	Lois des États américains
	37%	HIPAA
	35%	Exigences SEC
	23%	RGPD
	12%	Lois propres à chaque pays
	0%	PCI DSS
Top 2 des certificats de sécurité les plus importants	63%	NIST 800-171/CMMC 2.0
	60%	ISO 27001, 27017, 27018
	33%	FedRAMP Moderate
	19%	SOC 2 Type II
	16%	IRAP (Australie)
	7%	Directive NIS 2
Nombre de piratages des communications de contenu sensible	5%	Plus de 10
	51%	7 à 9
	14%	4 à 6
	14%	2 à 3
	2%	1
	14%	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 l'enseignement supérieur. Ce brief reprend les principales conclusions du rapport concernant l'enseignement supérieur ; 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

Près de la moitié (49 %) des établissements d'enseignement supérieur utilisent au moins cinq outils de communication pour envoyer et partager des contenus sensibles, ce qui est légèrement inférieur à la moyenne de l'ensemble de la cohorte (53 %). 19 % d'entre eux déclarent pouvoir suivre et contrôler les données sensibles envoyées et partagées en interne, et 14 % lorsque ces données sont échangées en externe. Ces chiffres sont nettement inférieurs aux moyennes de l'ensemble de la cohorte (51 % pour les échanges de données internes et 43 % pour les échanges de données externes).

L'enseignement supérieur est beaucoup plus exposé que les autres secteurs d'activité. En dehors des données personnelles (PII et PHI), l'enseignement supérieur envoie et partage des données ultra-confidentielles telles que la propriété intellectuelle et les secrets nationaux, notamment avec la R&D pour le ministère de la défense américain. Les risques sont réels au vu des résultats catastrophiques obtenus par le secteur en matière de gouvernance.

La prévention des litiges longs et coûteux est citée dans 63 % des cas comme la première ou la deuxième priorité. La prévention des fuites de propriété intellectuelle et de secrets d'entreprise arrive en deuxième (56 %). Ces deux réponses reflètent la multiplication des réglementations sur le traitement des données personnelles et la nécessité de protéger les informations confidentielles, dont celles échangées par les établissements d'enseignement supérieur.

Évaluer le risque tiers pour les contenus sensibles

Les risques liés aux tiers représentent une faille importante dans l'enseignement supérieur, puisque 47 % des répondants déclarent échanger des contenus sensibles avec plus de 2500 interlocuteurs différents (une proportion légèrement supérieure à celle de la cohorte mondiale de 44 %) et 66 % avec plus de 1000 (identique à la moyenne des répondants). 31 % des répondants indiquent pouvoir suivre et contrôler plus des trois quarts des contenus sensibles lorsqu'ils quittent une application. C'est un des secteurs les plus matures sur ce point.

Évaluer le niveau de conformité pour les contenus sensibles

84 % des établissements d'enseignement supérieur 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 %.

En raison de leur implication dans les questions relatives à la base industrielle de défense (DIB), de nombreux établissements d'enseignement supérieur interrogés ont cité la CMMC 2.0 comme leur première ou deuxième priorité (49 %). Viennent ensuite les lois sur la confidentialité des données propres à chaque État américain (44 %), ce qui témoigne de la nécessité de protéger les informations personnelles identifiables.

En ce qui concerne les normes et certificats de sécurité, les répondants de l'enseignement supérieur privilégient le NIST 800-171 (63 %), probablement en raison de la quantité d'échanges de données avec le gouvernement fédéral. Les normes ISO 27001, 27017 et 27018 suivent de près (60 %).

Évaluer les risques liés à la sécurité des contenus sensibles

86 % des établissements d'enseignement supérieur interrogés déclarent que leur management des risques associés aux communications sensibles doit être amélioré de manière significative ou partielle. 2 % supplémentaires ont indiqué qu'ils n'avaient rien mis en place aujourd'hui. Ces deux chiffres sont similaires à l'ensemble de la cohorte.

56 % des répondants de l'enseignement supérieur ont indiqué avoir subi au moins sept violations de leur contenu sensible. Ce chiffre est assez préoccupant, car il est nettement plus élevé que celui de l'ensemble de la cohorte (32 %). L'enseignement supérieur est certainement la cible privilégiée des acteurs malveillants; le DBIR de Verizon a révélé que l'enseignement supérieur était le secteur le plus ciblé et subissait plus de violations de données que n'importe quel autre.[1]

Les répondants de l'enseignement supérieur affirment utiliser des outils de sécurité avancés (chiffrement, authentification multifactorielle, suivi et contrôle de la gouvernance) pour les communications internes sensibles dans une proportion plus élevée que les autres secteurs d'activité (65 % comparé aux 59 % de l'ensemble de la cohorte).

Évaluer le coût de la sécurité et de la conformité

Les violations de données dans l'enseignement supérieur coûtent cher en frais de contentieux; près de la moitié des personnes interrogées ont déclaré que leur organisation dépensait plus de 5 millions de dollars par an. Un chiffre plus élevé que n'importe quel autre secteur d'activité. Le risque est d'autant plus grand que 19 % des établissements d'enseignement supérieur interrogés ont indiqué ne pas connaître ce montant.

Connaissance et classification des types de données

De nombreuses personnes interrogées dans l'enseignement supérieur ont déclaré étiqueter et classer plus de 50 % de leurs données non structurées (79 %). Contrairement à d'autres secteurs, elles pensent qu'une petite partie des données non structurées ont besoin d'être étiquetées et classées (seulement 14 % ont indiqué que plus de 60 % des données devaient être étiquetées et classées).

Urgence absolue à protéger les contenus sensibles dans l'enseignement supérieur

Le rapport Kiteworks 2024 souligne l'importance de la gestion des risques et de la conformité pour les communications de contenu sensible dans l'enseignement supérieur.

La protection des données personnelles des étudiants, des enseignants et du personnel relève certainement de la responsabilité des établissements. Il n'est donc pas surprenant que les répondants aient cité les informations personnelles identifiables (PII) en tête de leurs priorités (58 % les ont citées en premier ou en second). Et la protection des données de propriété intellectuelle et des secrets d'entreprise en seconde (50 %).

En pratique, les répondants passent beaucoup de temps à compiler les journaux d'audit générés par les nombreux outils de communication de contenus sensibles. 58 % doivent en réconcilier plus de 11 (contre 48 % en moyenne), et 9 % ne savent même pas combien il y en a. L'enseignement supérieur consacre plus de temps à compiler des journaux pour les rapports de conformité que les autres : 49 % y consacrent 2 000 heures par an.

[1]"2024 Data Breach Investigations Report", Verizon, Mai 2024.

Accéder au rapport complet