Rapport sur les défis pour la propriété intellectuelle 2025

Sécurité proactive contre les violations de la propriété intellectuelle

Introduction : Un monde en mutation rapide et à haut risque

La réputation d'une entreprise est très étroitement liée à la façon dont elle est représentée en ligne. Cet état de fait offre aux fraudeurs la possibilité de détourner des marques renommées, que ce soit en créant des sites Internet trompeurs, en copiant des produits ou des logos, ou en créant, sur les réseaux sociaux, de faux profils qui ressemblent à ceux de la marque.

Les barrières à l'entrée pour les usurpateurs d'identité ont été considérablement réduites, ce qui a facilité plus que jamais les violations de la propriété intellectuelle (PI). Les violations de la propriété intellectuelle sont de plus en plus difficiles à identifier et à réprimer, et les lettres de mise en demeure arrêtent peu souvent les auteurs de ces violations.

Pour relever ces défis, les entreprises ont tout intérêt à mettre en œuvre diverses stratégies visant à renforcer l'application des dispositions relatives à la propriété intellectuelle et à protéger leurs marques, leurs droits d'auteur et autres droits de propriété intellectuelle.

À une époque où les ressources des équipes juridiques sont toujours plus restreintes, comment doivent-elles collaborer plus étroitement avec les équipes marketing, informatiques et de sécurité pour hiérarchiser les efforts en matière de protection de la propriété intellectuelle et s'assurer que les budgets sont alloués à bon escient ?

« La capacité des fraudeurs à commettre des violations de la propriété intellectuelle évolue à un rythme tel qu'il serait dans l'intérêt de tous d'être mieux informés de ce qui se passe, de privilégier davantage les technologies et de renforcer la collaboration entre les équipes chargées des noms de domaine, explique Ian McConnel, directeur juridique de CSC. Qu'on le veuille ou non, la gestion des noms de domaine est un élément clé des stratégies de cybersécurité, qui ne se limite pas à la protection des noms de domaine les plus précieux. »

NOS EXPERTS

Ian McConnel
Directeur juridique de CSC

Ihab Shraim
Directeur de la technologie, division Digital Brand Services de CSC

Elliott Champion
Directeur produit mondial de CSC, Brand Protection and Anti-Fraud

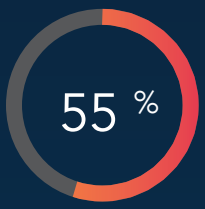
Mary Jo Murphy
Cheffe de produit de CSC, Brand and Fraud Services

Principaux points à retenir de notre étude

Nous avons interrogé 300 juristes chevronnés au 2e trimestre 2025 et nous avons constaté que :

Le taux de violation de la propriété intellectuelle en ligne augmente et que cette tendance devrait se poursuivre

La grande majorité des personnes interrogées (91 %) s'est dite préoccupée par la menace des violations de la propriété intellectuelle en ligne.



Plus de la moitié (55 %) a confié s'attendre à une augmentation significative des violations de la propriété intellectuelle en ligne au cours des trois prochaines années.

Voici le classement des trois principaux types de violations de propriété intellectuelle en ligne rencontrées par les répondants :

Contrefaçon

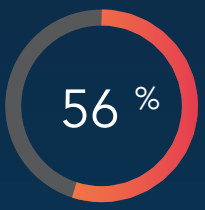
Abus des marques

Usurpation d'identité

L'IA joue un rôle important dans l'augmentation des violations de la propriété intellectuelle

Une majorité (88 %) a déclaré que les systèmes reposant sur l'intelligence artificielle (IA) entraînent une augmentation de la fréquence des violations.

Les répondants sont conscients des avantages liés à l'externalisation de la surveillance en ligne des violations de la propriété intellectuelle.



Plus de la moitié (56 %) a confié externaliser actuellement certaines activités de surveillance des violations de la propriété intellectuelle en ligne, mais envisage sérieusement d'en externaliser davantage.

La plupart des équipes juridiques collaborent déjà avec les équipes informatiques et de sécurité pour comprendre précisément les risques de violation de la PI

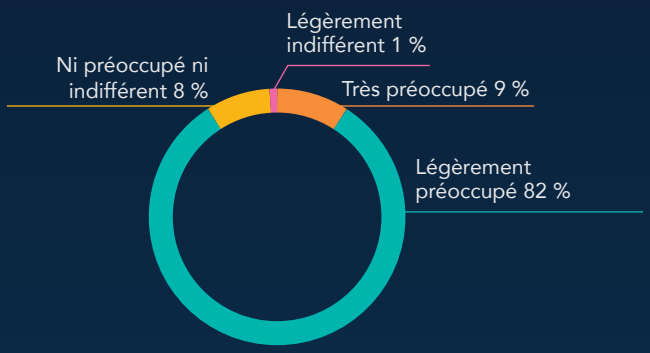
Près des deux tiers (64 %) ont évalué leur collaboration avec leurs collègues chargés de la sécurité informatique comme étant solide (quatre points sur cinq), **tandis que 22 %** ont déclaré travailler en étroite collaboration avec leur équipe chargée de la sécurité informatique.

La fréquence des violations de la propriété intellectuelle continue d'augmenter

Au cours des dernières années, plusieurs facteurs ont contribué à bouleverser profondément le monde de la contrefaçon de PI.

Cette diversité de facteurs comprend l'essor des outils Caas (« crimeware-as-a-service »), l'augmentation continue du coût de la vie et la croissance soutenue des achats en ligne, qui encouragent les violations de propriété intellectuelle et nuisent ainsi à la réputation et aux bénéfices des entreprises.

Chiffre révélateur, plus de 90 % des répondants à l'enquête mondiale menée par CSC ont déclaré être préoccupés par la menace que représentent les violations de la propriété intellectuelle en ligne pour les organisations comme la leur.



Un quart des répondants a indiqué avoir constaté une augmentation « significative » des violations de la propriété intellectuelle en ligne auxquelles leur organisation a été confrontée au cours des 12 derniers mois ; environ un tiers (35 %) a déclaré avoir constaté une augmentation « significative » au cours des trois dernières années.

Voici les trois principales ressources exploitées indiquées par les répondants :

- Contenu Internet ou contenu des marques (indiqué par 45 %)
- Applications mobiles (30 %)
- Places de marché en ligne (17 %)

« Les consommateurs sont toujours à la recherche de produits moins chers, qu'il s'agisse de médicaments, de pièces automobiles ou de biens de consommation, et les fraudeurs savent parfaitement en tirer profit », explique Mary Jo Murphy, cheffe de produit de CSC, Brand and Fraud Services.

La plupart des répondants (89 %) ont déclaré s'attendre à une augmentation des violations de la propriété intellectuelle au cours des trois prochaines années. Neuf sur dix (90 %) s'attendent également à une augmentation au cours des 12 prochains mois.

Parmi les types de violation de propriété intellectuelle en ligne suivants, lesquels préoccupent le plus votre organisation ?

- Contrefaçon
- Abus des marques
- Usurpation d'identité
- Abus des droits de conception
- Abus des droits d'auteur

« Votre perception de ces types de violation dépend de votre point de vue, ajoute Ian McConnel. « Si j'étais une entreprise grand public, je m'inquiéterais surtout des contrefaçons, mais si j'étais une société spécialisée dans les services financiers, je m'inquiéterais davantage d'un fraudeur détournant une marque déposée pour mener une attaque de hameçonnage ou une cyberattaque contre un client. »

> Votre réputation dépend de votre présence en ligne ; il vous faut donc aujourd'hui la protéger autrement que par le passé. On assiste à une explosion du nombre de vecteurs de menaces visant les entreprises, les cibles les plus faciles étant les noms de domaine et les adresses IP. Les choses ont changé : autrefois, les fraudeurs envoyaient des centaines de milliers d'e-mails de hameçonnage dans l'espoir que 2 ou 3 % des destinataires y répondent, tandis qu'aujourd'hui, les attaques frauduleuses sont plus ciblées et ont un taux de réussite beaucoup plus élevé.
>
> **– Ihab Shraim, directeur de la technologie, division Digital Brand Services de CSC**

L'IMPORTANCE DE LA PROTECTION DES NOMS DE DOMAINE DANS LA LUTTE CONTRE LE VOL DE PROPRIÉTÉ INTELLECTUELLE

« Les noms de domaine sont un élément central des interactions et des échanges quotidiens entre les individus. Ils sont si courants que les gens ne se rendent même pas compte qu'ils interagissent avec un nom de domaine et tiennent pour acquis le fait qu'ils sont à l'abri de tout danger. Pourtant, les noms de domaine frauduleux sont souvent le point de départ de violations graves de la propriété intellectuelle, et il n'a jamais été aussi facile pour les fraudeurs d'enregistrer le nom de domaine de leur choix », explique Elliott Champion, directeur produit mondial de CSC, Brand Protection and Anti-Fraud.

« Avez-vous remarqué que dans certains restaurants, vous utilisez désormais un code QR pour passer votre commande ? Lorsque vous le scannez, il vous redirige directement vers un nom de domaine et vous n'avez aucune idée de là où il vous mène. Vous lui faites simplement confiance, explique Elliot Champion. Cet exemple illustre l'importance cruciale des noms de domaine dans notre expérience numérique quotidienne. Nous leur faisons tous confiance et interagissons avec eux, même s'il suffit de quelques minutes pour créer un faux nom. Par conséquent, les barrières à l'entrée pour ce type d'activité frauduleuse sont désormais remarquablement faibles. »

L'IA joue un rôle de plus en plus important dans les violations de la propriété intellectuelle.

En un rien de temps, l'IA est devenue un sujet incontournable dans le monde des affaires et de la productivité au niveau mondial. En revanche, du côté de la fraude et des risques, l'IA est déjà utilisée pour créer des actifs de propriété intellectuelle très réalistes et sophistiqués, tels que des logos, des images et du contenu d'entreprise. À l'heure où l'IA et les capacités qu'elle offre continuent de progresser à grands pas, les équipes juridiques se demandent comment détecter au mieux les risques et garder une longueur d'avance.

Sans surprise, environ neuf répondants sur dix (88 %) à notre enquête ont déclaré que les systèmes basés sur l'IA sont à l'origine d'une augmentation de la fréquence des incidents.

La majorité des répondants (93 %) a également déclaré craindre que les capacités de l'IA à créer de faux actifs puissent avoir un impact significatif sur leur activité.

« Aujourd'hui, il est très facile d'utiliser un outil basé sur l'IA pour créer des documents fictifs qui peuvent être exploités très facilement, confie Ian McConnel. Le temps où il fallait s'asseoir et coder tout un tas de fausses pages Web est révolu, et à mesure que les outils se perfectionnent, les possibilités pour les cybercriminels moins aguerris sur le plan technique continueront de se multiplier. Les fraudeurs ne sont limités que par leur imagination. »

Les entreprises sont confrontées aux nouveaux défis en constante évolution posés par l'IA. Neuf répondants sur dix ont également déclaré craindre que les outils d'IA utilisent les données ou la propriété intellectuelle de leur organisation pour former des modèles susceptibles de générer du contenu exploitable par leurs concurrents. Cependant, la majorité des répondants partageant cette crainte estime disposer des protections adéquates.

Point positif, de nombreuses entreprises reconnaissent la menace croissante que représente l'IA et renforcent leurs mesures de protection grâce à des programmes de formation interne et d'autres initiatives.

Près de 70 % des répondants estiment que la qualité des directives ou politiques internes mises en place par leur organisation concernant l'utilisation de l'IA pour la création d'actifs de propriété intellectuelle est bonne, tandis que 20 % la jugent excellente.

À l'avenir, la formation devrait jouer un rôle de plus en plus important dans la gestion des menaces liées à l'IA au sein des entreprises.

DÉMÊLER LE VRAI DU FAUX DEVIENT DE PLUS EN PLUS DIFFICILE

L'une des trois principales préoccupations des répondants en matière de violation de la propriété intellectuelle est l'usurpation d'identité, notamment les reproductions réalistes de cadres supérieurs générées par l'IA qui peuvent être utilisées pour demander des fonds aux employés.

« On trouve suffisamment de contenu sur les PDG, notamment des discours, des publications et des vidéos, pour que les fraudeurs puissent créer en quelques heures des reproductions par IA susceptibles de tromper de nombreuses personnes au sein d'une organisation, explique Ian McConnel. Un jour, nous serons confrontés à une reproduction en ligne d'une personne qui ressemblera exactement à celle avec laquelle nous interagissons régulièrement et nous serons incapables de démêler le vrai du faux.

Ce n'est pas encore pour aujourd'hui, car on constate encore des anomalies dans les fausses conversations vidéo, mais les progrès sont si rapides et exponentiels qu'honnêtement, ce n'est qu'une question de temps.

De fait, les organisations devront mettre en place des processus et des systèmes qui ne reposent pas uniquement sur l'individu pour authentifier les communications, que ce soit par téléphone, vidéo ou e-mail. D'ici cinq ans, aucune formation ne permettra d'arrêter ces fraudeurs.

Pour contrer ce phénomène, il faut commencer par supprimer les noms de domaine susceptibles de diffuser ce type de communications et mettre en place les protocoles adéquats pour vérifier d'où proviennent les communications illicites. »

Les budgets augmentent, mais les dépenses ne sont pas toujours hiérarchisées

Dans un monde où le nombre et la nature des risques et des vecteurs de risque ne cessent d'augmenter, comment les budgets consacrés aux services informatiques ont-ils évolué pour relever ce défi ?

Notre étude a révélé que les budgets consacrés à la lutte contre les violations de la propriété intellectuelle et à la protection des marques sont en augmentation : deux tiers (67 %) des répondants ont déclaré s'attendre à une augmentation « significative » au cours des trois prochaines années, tandis qu'un peu moins de la moitié (46 %) prévoit une augmentation « significative » au cours de l'année à venir.

Les répondants s'attendent à ce que les domaines suivants bénéficient d'investissements supplémentaires au cours des 12 prochains mois :

72 %	69 %	68 %
Technologie en interne	Augmentation des effectifs de l'équipe chargée de la gestion de la PI	Croissance des effectifs du service juridique au sens large

Près de la moitié (44 %) prévoit une augmentation de l'externalisation vers des tiers spécialisés dans la propriété intellectuelle, comme CSC.

Cette augmentation des investissements soulève une question importante : où les ressources doivent-elles être allouées pour avoir le plus grand impact ? Plutôt que d'essayer de couvrir tous les canaux ou variantes potentiels d'un nom de domaine, les entreprises doivent privilégier les dépenses qui auront le plus d'impact.

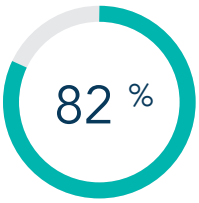
« Il ne s'agit pas seulement d'augmenter les budgets, mais aussi de déterminer comment ces budgets sont dépensés, explique Ian McConnel. Combien dépensez-vous pour rester au fait des enjeux liés à l'IA ? Combien dépensez-vous pour mobiliser les ressources adéquates afin d'atténuer correctement les risques ? »

L'émergence rapide de nouveaux risques, combinée au nombre croissant de canaux utilisés pour commettre des violations de la propriété intellectuelle, montre que la réduction des risques ne peut être un effort ponctuel, mais nécessite une analyse et une surveillance continues. Les organisations se tournent de plus en plus vers des partenaires externes qui les aideront à relever ce défi.

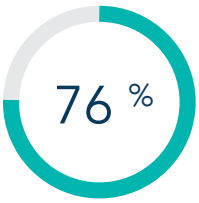
> Les plateformes évoluent à un rythme effréné. Ce dont nous dépendons aujourd'hui est déjà en train d'être remplacé par ce qu'utilisent les jeunes publics, et c'est ce que nous utiliserons demain. La feuille de route évolue constamment et nous sommes toujours un peu à la traîne. C'est un aspect qui mérite une attention particulière et qui nécessite d'être proactif plutôt que réactif.
>
> **– Elliott Champion, directeur produit mondial de CSC,Brand Protection and Anti-Fraud**

La lutte contre les violations de la propriété intellectuelle nécessite une approche globale et interfonctionnelle

Les répondants à notre enquête ont déclaré avoir un niveau de confiance relativement élevé dans leurs stratégies de surveillance et de gestion des noms de domaine, et la plupart (86 %) affirment travailler en étroite collaboration avec d'autres équipes, notamment les services informatiques et de sécurité.



des répondants ont déclaré avoir « extrêmement » ou « assez » confiance dans les systèmes internes de surveillance des violations de la propriété intellectuelle de leur organisation.



ont déclaré que leur organisation avait mis en place une stratégie de gestion des noms de domaine et 12 % ont indiqué être en train d'en élaborer une.

En revanche, seulement 16 % ont indiqué que leurs équipes juridiques avaient une visibilité « totale » sur la gestion du portefeuille de noms de domaine de leur organisation.

« Les organisations ont besoin de cette approche cohérente pour traiter les problèmes de sécurité du back-end, en particulier lorsque le service marketing prévoit de lancer une campagne spécifique avec son propre nom de domaine, explique Mary Jo Murphy. Elles doivent s'assurer que les équipes juridiques, de sécurité et informatiques en soient informées afin qu'elles puissent l'ajouter à leur liste de surveillance. »

L'ÉMERGENCE DES ÉQUIPES DE GOUVERNANCE NUMÉRIQUE

Les organisations qui ont adopté une approche efficace et proactive pour lutter contre les violations de la propriété intellectuelle sont plus susceptibles d'avoir réuni une équipe officielle de gouvernance numérique, composée de représentants des domaines juridique, marketing, informatique et de la sécurité.

« Dans de nombreuses grandes organisations, le responsable du service juridique côtoie rarement le responsable du service informatique, confie Elliott Champion. Ils ne comprennent pas le monde de l'autre. La première chose que nous recommandons aux nouveaux clients est de réunir tout le monde dans une même pièce afin d'aborder ce problème sous différents angles.

Si j'avais un message à faire passer, ce serait le suivant : les différentes équipes doivent se parler. Il n'est pas nécessaire de mettre en place un processus formel, une seule réunion mensuelle suffit, mais il est essentiel de s'informer mutuellement. »

Utilisation accrue des services d'externalisation, notamment la surveillance des noms de domaine

À l'heure où le nombre de violations de la propriété intellectuelle ne cesse d'augmenter, les efforts nécessaires pour surveiller les noms de domaine et autres activités deviennent de plus en plus difficiles à gérer en interne. Ces activités relèvent souvent de la responsabilité de l'équipe juridique, qui est parfois déjà trop débordée.

Un peu plus de la moitié (56 %) des répondants ont déclaré qu'ils externalisaient actuellement au moins certaines activités de surveillance, mais qu'ils envisageaient sérieusement d'en externaliser davantage.

Travailler en partenariat avec un spécialiste reconnu, établi et impliqué allège non seulement la charge de travail des équipes juridiques, mais traduit également un engagement à protéger les clients et à respecter les normes réglementaires. Autre élément important, ces partenariats peuvent apporter une valeur ajoutée considérable en renforçant les protocoles et les mesures de protection, tout en donnant accès à de nouveaux outils et applications innovants.

« Si vous vous retrouvez dans une affaire de violation de marques déposées, les tribunaux ne vous seront pas favorables si vous n'avez pas surveillé les utilisations abusives de vos marques déposées dans le passé, explique Mary Jo Murphy. Aujourd'hui, vous pouvez souligner le fait que vous travaillez avec un partenaire tel que CSC, capable d'analyser les marchés, de prévenir les violations et de contrer autant que possible les acteurs malveillants ; ainsi, vous démontrez clairement que vous mettez tout en œuvre pour protéger votre propriété intellectuelle. »

> CSC est à la pointe de la fourniture d'outils assurant une veille proactive des menaces qui pèsent sur les noms de domaine, et qui risquent de servir de point de départ à une attaque. La capacité de CSC à agir rapidement et de manière proactive dans le monde entier aide les entreprises à se protéger des violations de propriété intellectuelle qui commencent par des noms de domaine frauduleux.
>
> « Une entreprise responsable qui fait face à des risques de violation de la propriété intellectuelle doit adopter une approche proactive et multicouche en matière de cybersécurité. Disposer d'un pare-feu ne suffit pas. Si vous n'avez pas encore envisagé d'externaliser la surveillance des violations de propriété intellectuelle et les stratégies de gestion des noms de domaine, vous passerez à côté d'une grande opportunité. »
>
> **– Ian McConnel, directeur juridique de CSC**

BUREAUX D'ENREGISTREMENT DE DÉTAIL ETBUREAUX D'ENREGISTREMENT D'ENTREPRISE : QUELLE EST LA DIFFÉRENCE ?

Il est essentiel de comprendre les différences entre les bureaux d'enregistrement de détail et les bureaux d'enregistrement d'entreprise pour déterminer comment surveiller et protéger les noms de domaine. Ihab Shraim pointe cinq différences clés.

1. **La capacité de mise en œuvre :** Les bureaux d'enregistrement d'entreprise garantissent une mise en œuvre (ou un démantèlement) mondiale, efficace et intelligente, alors que les bureaux d'enregistrement de détail ne disposent pas des outils et de l'expertise nécessaires pour y parvenir.
2. **L'orientation commerciale :** Les bureaux d'enregistrement de détail ont pour mission principale de vendre des noms de domaine, en tant qu'intermédiaires, tandis que les bureaux d'enregistrement d'entreprise se consacrent à la gestion et à la protection des noms de domaine ainsi qu'à l'atténuation des risques à l'échelle mondiale.
3. **La sécurité de l'infrastructure d'hébergement :** Les bureaux d'enregistrement de détail peuvent proposer des serveurs pour héberger des domaines, mais ceux-ci sont souvent mal gérés et peuvent reposer sur une infrastructure partagée peu sécurisée.
4. **La stratégie de sécurité :** Les bureaux d'enregistrement d'entreprise disposent de mesures de sécurité plus robustes pour protéger les portefeuilles de noms de domaine de leurs clients, mesures que les bureaux d'enregistrement de détail ne peuvent égaler.
5. **La portée de la surveillance :** Les bureaux d'enregistrement d'entreprise surveillent les sites de commerce électronique et d'enchères dans le monde entier afin de détecter toute utilisation abusive des noms de domaine, tandis que les bureaux d'enregistrement de détail n'interviennent généralement que lorsqu'un problème a été identifié.

« Les fraudeurs ciblent les propriétaires de marques à l'aide de trois tactiques principales : l'utilisation abusive de la marque, l'usurpation d'identité et la contrefaçon de produits », fait remarquer Ihab Shraim. « Pour lutter efficacement contre ces menaces, vous avez besoin d'un bureau d'enregistrement d'entreprise disposant d'un service chargé de la mise en œuvre. Ce n'est ni plus ni moins que le minimum requis. »

Agir avant qu'il ne soit trop tard

Le volume et la diversité des attaques visant la propriété intellectuelle des organisations ne cessent d'augmenter. Les barrières à l'entrée pour les fraudeurs sont nettement moins élevées du fait de technologies telles que l'IA et les outils CaaS. Notre étude montre que les juristes sont généralement convaincus qu'ils ont mis en place les politiques et les pratiques de travail collaboratif adéquates pour faire face à ces risques. Cependant, sans une stratégie proactive et multicouche en matière de cybersécurité, il sera de plus en plus difficile de faire face à la multiplication des menaces.

Travailler avec un tiers de confiance à la mise en place d'une stratégie de sécurité proactive trace une voie claire et efficace à la protection de la propriété intellectuelle, tout en garantissant aux clients et aux parties prenantes que des mesures de protection adéquates sont en place.

« En vous montrant proactif, vous démontrez que vous accordez de l'importance à vos actifs et à votre propriété intellectuelle, affirme Mary Jo Murphy. Sur le long terme, cela se révèle payant. En effet, cela permet non seulement de détecter et de surveiller les violations, mais aussi de garantir la mise en place de mécanismes juridiques appropriés de mise en œuvre et de démantèlement. »

Une approche proactive, notamment via la collaboration avec un partenaire expérimenté, est également plus efficace en termes de temps et de ressources.

« Si l'on n'agit pas de manière proactive, il faudra déployer davantage d'efforts pour remédier aux problèmes, conclut Elliott Champion. Ce qui prendrait cinq minutes lors d'une discussion avec CSC pourrait vous prendre cinq mois et entraîner des frais supplémentaires pour récupérer un nom de domaine sans l'aide d'un fournisseur qui travaille avec les entreprises. »

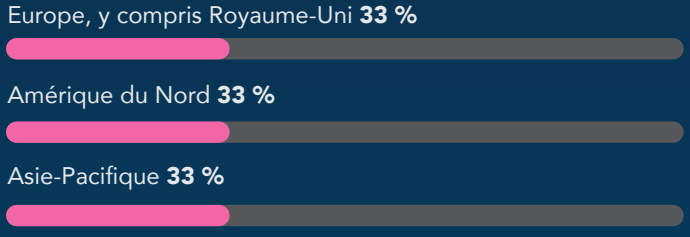
Enfin, Ihab Shraim souligne le lien entre la protection de la propriété intellectuelle et les risques pour les finances et la réputation des entreprises.

« La PI est indissociable de la réputation, car votre réputation repose désormais sur votre présence en ligne. Aujourd'hui, elle doit être protégée autrement que par le passé, compte tenu de l'afflux massif des nouveaux types de menaces. »

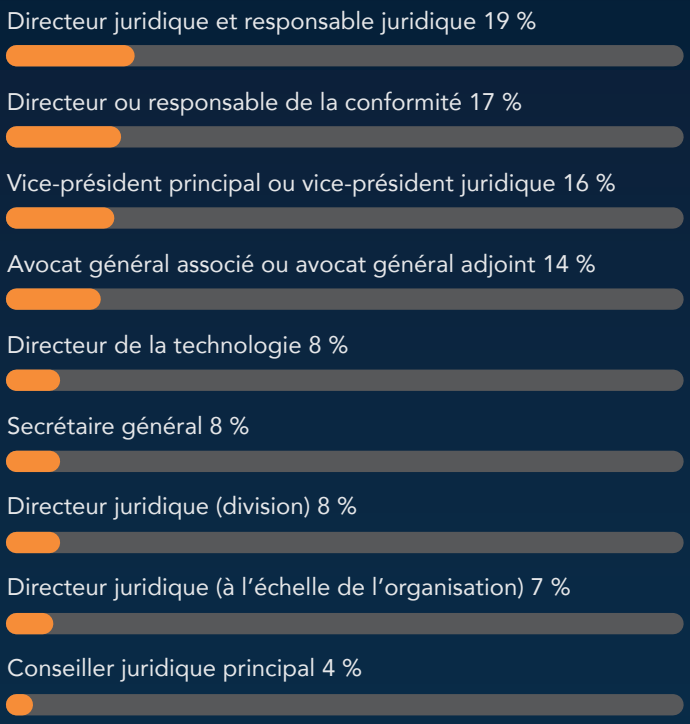
Aperçu de nos répondants

Nombre d'entreprises par secteur vertical

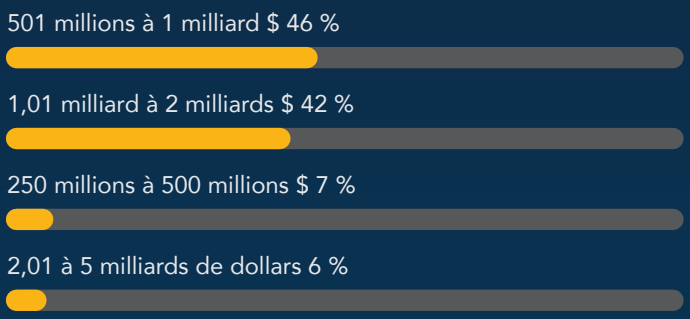
Sièges sociaux des entreprises par région



Fonction des répondants



Chiffre d'affaires annuel des entreprises



Discutons

1 800 927 9800 | cscdbs.com

À propos de CSC

CSC est le partenaire de confiance des entreprises du classement Forbes Global 2000 (Interbrand®) et 100 Best Global Brands en matière de sécurité et de veille sur les menaces et propose des solutions de gestion de la sécurité des domaines et, de protection des marques en ligne et contre la fraude. Les entreprises internationales investissent considérablement dans leur stratégie de sécurité. C'est la raison pour laquelle notre plateforme DomainSecSM peut les aider à identifier leurs failles en matière de cybersécurité et leur permettre de protéger leurs actifs numériques et leurs marques en ligne. En s'appuyant sur la technologie exclusive de CSC, les entreprises peuvent consolider leur stratégie de sécurité pour se protéger contre les vecteurs de cybermenaces qui pèsent sur leur patrimoine numérique, et éviter les pertes de revenus catastrophiques et les atteintes à la réputation de leurs marques. CSC propose également une protection de la marque en ligne (une combinaison de la surveillance de la marque en ligne et des activités de mise en œuvre) et une vue multidimensionnelle des différentes menaces à l'extérieur du pare-feu ciblant des noms de domaine spécifiques. Des services de protection contre la fraude, qui luttent contre l'hameçonnage dès les premiers stades de l'attaque, viennent compléter nos solutions. Basée à Wilmington, dans le Delaware (États-Unis), depuis 1899, CSC possède des bureaux à travers les États-Unis, le Canada, l'Europe et la région Asie-Pacifique. CSC est une entreprise d'envergure mondiale, ce qui nous permet d'intervenir là où sont nos clients en mettant à leur disposition nos équipes d'experts dans chacune de nos activités. Visitez cscdbs.com.

DBS10222025