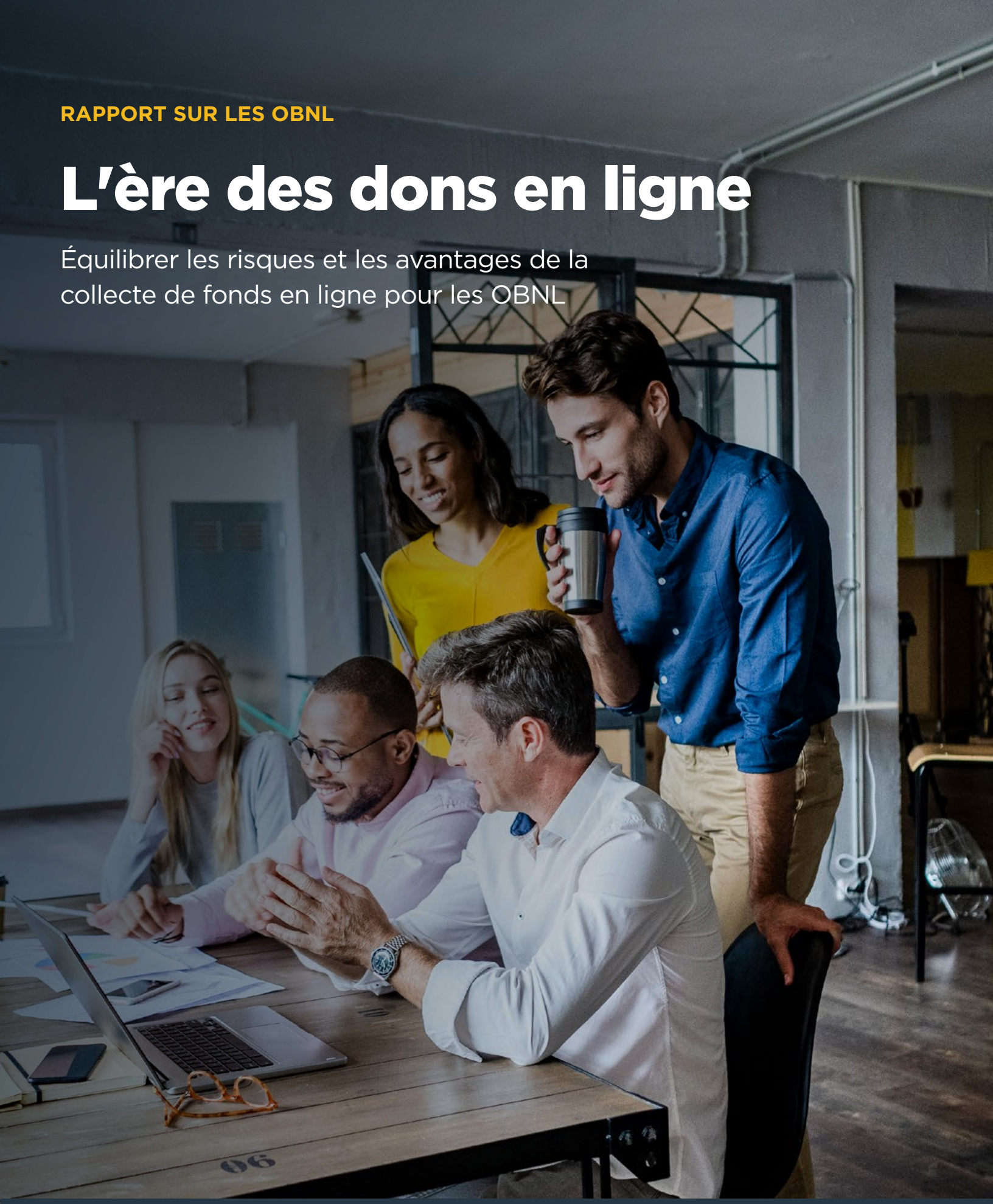
RAPPORT SUR LES OBNL

L'ère des dons en ligne

Équilibrer les risques et les avantages de la collecte de fonds en ligne pour les OBNL



Les dons en ligne se développent rapidement et deviennent essentiels dans les efforts de collecte de fonds des OBNL. Au-delà de la simple collecte de contributions, les organisations tirent parti des plateformes numériques pour susciter l'engagement des donateurs et les inciter à soutenir leurs causes. Cette évolution a permis aux OBNL d'atteindre davantage de bienfaiteurs, de rationaliser le processus de don et d'enregistrer une croissance constante des dons en ligne. Le nombre de donateurs canadiens qui font des dons en ligne et le montant total par don en ligne ont connu une croissance à deux chiffres entre 2019 et 2023[1], et 84 % des donateurs canadiens qui ont fait des dons en ligne dans le passé ont indiqué qu'ils prévoyaient de continuer à le faire à l'avenir[2].

En raison des tendances en matière de dons en ligne, 67 % des OBNL dans le monde acceptent aujourd'hui les dons en ligne[3]. Ce chiffre ne fera qu'augmenter, car de plus en plus d'OBNL adoptent la collecte de fonds numérique; cependant, les organisations doivent s'assurer qu'elles peuvent offrir aux donateurs une expérience sûre et efficace.

Principales vulnérabilités des OBNL en matière de collecte de fonds numérique

La collecte de fonds numérique offre de nombreux avantages aux OBNL, mais elle présente également une série de risques. Parmi ceux-ci figurent les menaces en matière en matière de cybersécurité, les problèmes de confidentialité des données des donateurs et les répercussions juridiques et financières liées aux questions de droits d'auteur si le contenu de la collecte de fonds numérique est utilisé sans les autorisations ou licences appropriées.

Les conséquences de l'un ou l'autre de ces incidents peuvent être dévastatrices pour un OBNL. Outre le coût financier — en moyenne près de 7,1 millions $ par violation de données en 2024[4] — l'atteinte à la réputation peut gravement compromettre la capacité d'un OBNL à gagner la confiance des donateurs, à attirer des fonds et à mener à bien sa mission.

Comprendre le risque cybernétique

L'un des plus grands risques pour les OBNL qui utilisent des méthodes de collecte de fonds numériques est la violation de données ou la cybercriminalité. Les OBNL sont devenus des cibles majeures pour les cybercriminels en raison de la quantité de données sensibles sur les donateurs qu'ils conservent et de leur utilisation des canaux numériques pour le traitement des fonds. En outre, de nombreux OBNL ne disposent pas des ressources nécessaires pour protéger correctement leurs systèmes technologiques, 68 % d'entre eux ayant déclaré avoir subi une violation de données au cours des trois dernières années[5].

Les OBNL sont tenus, en vertu des lois sur la protection des données, des réglementations sectorielles et des accords contractuels avec des tiers, de protéger toutes les données personnelles collectées, transmises ou stockées lors des

Étude de cas

Un OBNL spécialisé dans le travail avec les jeunes à risque a contacté HUB, craignant d'être victime d'une attaque de rançongiciel, exposant les données sensibles des patients et des résidents. HUB a immédiatement mis en place un plan d'action pour minimiser l'accès aux courriels et autres informations personnelles. Après avoir fait appel à un avocat spécialisé dans les violations de données et à des enquêteurs en informatique légale, il a été déterminé qu'aucune donnée n'avait été volée au cours de l'événement.

Le client était non seulement soulagé que les répercussions aient été minimes et que la réclamation ait été inférieure à 85 000 $, mais l'organisation a également profité de l'occasion pour former son personnel afin qu'il soit mieux préparé à l'avenir.

[1]CanadaHelps.org, « The Giving Report 2024 : From Disconnection to Collective Action », 17 avril 2024.
[2]Pay Pal Giving Fund Canada, « Future of Giving : Online Across Generations », 21 juin 2022.
[3]Nonprofitsource.com, « The Ultimate List Of Charitable Giving Statistics For 2024, » consulté le 21 janvier 2025.
[4]IBM, « Escalating Data Breach Disruption Pushes Costs to New Highs », 30 juillet 2024.
[5]CyberPeaceInstitute.org, « Cyber-poor, target-rich: The crucial role of cybersecurity in nonprofit organizations », 25 mars 2024.

transactions. Ces données stockées peuvent exposer les OBNL. Même si un OBNL fait appel à un tiers pour traiter les paiements par carte de crédit et que ces fournisseurs sont responsables du stockage des informations relatives aux donateurs, l'OBNL peut être tenu responsable en cas d'accès à des informations personnelles identifiables ou de vol de celles-ci.

Les OBNL doivent évaluer soigneusement la sécurité et les contrats des fournisseurs de paiement tiers pour s'assurer qu'ils n'assument pas une responsabilité excessive, tout en prenant des mesures pour protéger correctement toutes les informations personnelles identifiables qui transitent par l'organisation.

Des erreurs coûteuses en matière de droits d'auteur

Alors que de plus en plus OBNL adoptent une approche numérique pour leurs opérations et leurs activités de collecte de fonds et que les jeunes donateurs se tournent vers les dons en ligne, 91 % des OBNL disposent désormais d'un site Web et 87 % intègrent systématiquement les médias sociaux dans leurs stratégies de marketing numérique et de collecte de fonds[6].

Si l'engagement des donateurs par le biais d'un site Web et d'un contenu de médias sociaux attrayants est un élément essentiel de la collecte de fonds numérique, les OBNL doivent également s'assurer qu'ils ne publient pas de matériel protégé par les droits d'auteur ou de contenu sous licence qu'ils n'ont pas l'autorisation d'utiliser. Cela inclut, sans s'y limiter, les photographies, la musique, les logos, les œuvres d'art ou tout autre type de contenu/information utilisé par d'autres sites Web ou plateformes de médias sociaux.

Les OBNL peuvent être sanctionnés pour violation des droits d'auteur et être tenus responsables des honoraires d'avocats et des frais juridiques liés aux plaintes pour violation des droits d'auteur[7].

Une utilisation prudente de l'intelligence artificielle

Les OBNL misent de plus en plus sur l'intelligence artificielle (IA) pour améliorer leurs opérations et leur communication avec les donateurs. L'IA peut également contribuer grandement aux efforts de collecte de fonds, 67 % des OBNL canadiens déclarant qu'ils utilisent actuellement l'IA dans le cadre de leur stratégie de collecte de fonds[8]. Parmi les OBNL mondiaux, 70 % de ceux qui utilisent l'IA pensent qu'elle les aidera à atteindre les objectifs de développement durable de leur organisation en améliorant la productivité, en facilitant l'accès à l'information et en renforçant la sensibilisation afin de susciter des changements de politique[9].

Cependant, les OBNL doivent prendre des mesures pour atténuer les risques liés à l'utilisation de l'IA.

Les documents générés par l'IA peuvent entraîner des risques juridiques, notamment des plaintes pour dommages personnels, violation de droits d'auteur ou de marques et plagiat, ce qui pourrait entraîner des amendes coûteuses et des atteintes à la réputation.

D'un autre point de vue, les OBNL doivent être conscients que l'IA permet aux cybercriminels de mettre en œuvre des plans de cybercriminalité plus élaborés et plus sophistiqués par le biais d'attaques d'hameçonnage et de rançongiciel. Les hypertrucages (*deepfakes*) générés par l'IA, où l'IA imite la voix ou le visage de personnes réelles, sont utilisés pour autoriser des virements bancaires frauduleux, diffuser des informations erronées, usurper l'identité de donateurs ou manipuler des employés pour qu'ils divulguent des informations sensibles.

[6]NonprofitTechforGood.com, « 2023 Nonprofit Tech for Good Report, » 1er février 2023.
[7]Canada.ca, « Violation de droit d'auteur », consulté le 7 mars 2025.
[8]Ontario Nonprofit Network, « AI, Income Performance, and Innovation: Key Fundraising Trends in 2024 », 10 septembre 2024.
[9]McKinsey & Co., « AI for social good: Improving lives and protecting the planet », 10 mai 2024.

Une stratégie proactive de gestion des risques

Compte tenu des divers risques liés à la collecte de fonds numérique, il est essentiel de disposer d'une assurance adéquate et d'un plan de gestion des risques éprouvé pour atténuer les conséquences potentielles sur le plan financier et sur le plan de la réputation.

Les OBNL peuvent réduire leur exposition et préserver leur mission et leur viabilité à long terme en adoptant les stratégies suivantes :

- **Soyez sélectif en ce qui concerne les tiers fournisseurs.** Ne choisissez que des fournisseurs disposant de solides contrôles de sécurité des données, qui comprennent et respectent les exigences réglementaires en matière de protection des données personnelles sensibles.

- **Transférez contractuellement les risques qui devraient être couverts par des fournisseurs externes ou des parties prenantes.** Les OBNL doivent examiner attentivement les contrats afin de s'assurer qu'ils ne sont pas responsables si les données des clients sont compromises à la suite d'une faille informatique du fournisseur de services.

- **Sensibilisez et formez le personnel et les bénévoles.** Il est important de former les employés pour les aider à identifier les escroqueries potentielles de piratage psychologique ou les tentatives d'hameçonnage qui pourraient conduire à un accès non autorisé aux réseaux ou à des activités frauduleuses.

- **Mettez en place des politiques et des procédures écrites à l'intention du personnel et des donateurs concernant les transferts de fonds.** Ces procédures devraient notamment exiger que le personnel confirme les transferts de fonds dépassant un certain montant par un appel téléphonique au demandeur.

- **Maintenez les protocoles du site Web et des médias sociaux.** Les OBNL doivent examiner le contenu prévu et les actifs médiatiques pour confirmer qu'ils sont correctement autorisés, et surveiller régulièrement l'activité en ligne pour s'assurer qu'elle est conforme aux politiques de l'entreprise.

Étude de cas

Une personne se faisant passer pour un donateur a tenté de faire un don de 14 000 $ à la campagne de financement d'une organisation par l'intermédiaire de son site Web. Le donateur présumé a effectué trois transactions distinctes et a ensuite contacté l'organisation pour lui dire que les multiples tentatives de dons avaient été faites par erreur. Les transactions ayant été effectuées pendant le week-end, elles sont apparues comme étant en cours de traitement et l'organisation a procédé au remboursement de deux des trois dons, pour un montant total de plus de 30 000 $. Une fois les remboursements effectués, les transactions initiales ont toutes été rejetées par la banque, laissant l'organisation privée de 30 000 $ à la suite de l'escroquerie. Une solide stratégie de gestion des risques peut aider les organisations à évaluer leurs processus de transfert de fonds et à remédier aux vulnérabilités potentielles, afin qu'elles ne deviennent pas la proie de manœuvres frauduleuses.

Considérations relatives à la couverture d'assurance

Les polices d'assurance responsabilité civile générale standard des OBNL peuvent ne pas couvrir les cyberrisques d'aujourd'hui. En fonction de la portée de leur travail, les OBNL peuvent envisager différentes couvertures, notamment :

- **Assurance cyber :** Couvre les violations de données, les rançongiciels et les litiges avec des tiers découlant de ces types d'incidents. Certaines polices peuvent également inclure une couverture pour les crimes électroniques, bien que certains risques liés à la fraude puissent être traités de manière plus efficace dans le cadre d'une police d'assurance vol et détournements traditionnelle.

- **Assurance vols et détournements commerciale :** Couvre les fraudes commises par des employés ou des tiers. Elle peut également inclure le piratage psychologique. Il est important que les assureurs sachent que l'assuré est un OBNL, afin d'inclure une clause relative aux donateurs.

- **Assurance responsabilité civile des médias :** Protège contre les réclamations liées à l'utilisation du contenu numérique, telles que la violation des droits d'auteur, la reproduction ou la distribution non autorisée de contenu médiatique. Les polices médias et cyber peuvent être souscrites ensemble ou séparément.

Facteurs clés à prendre en compte lors de la sélection d'un courtier

Un courtier de confiance offre une expertise en matière de produits d'assurance et devient un partenaire précieux dans la gestion des risques complexes. Les OBNL doivent rechercher un courtier capable d'offrir des solutions personnalisées en matière de gestion des risques et de produits, y compris des réponses aux situations de crise, et de fournir des services consultatifs continus, tels que la révision régulière des polices et des systèmes afin de les adapter à l'évolution des risques. En donnant la priorité à l'expérience, à la personnalisation et au soutien continu, les OBNL peuvent construire une base solide pour protéger leur mission, leurs actifs et leur réputation dans un paysage numérique en constante évolution.

Pour en savoir plus sur la protection de votre OBNL dans ce monde numérique, contactez dès aujourd'hui les spécialistes en assurance des OBNL de HUB International.

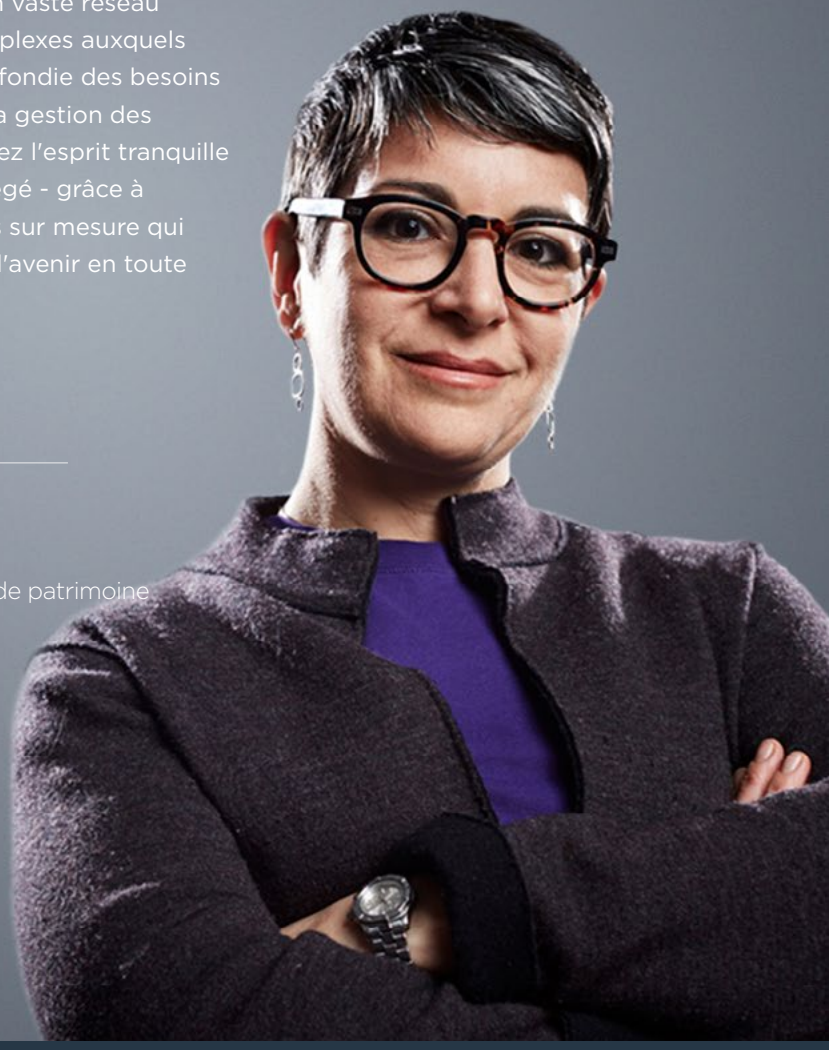
Un soutien stratégique qui vous permet de garder le contrôle.

Lorsque vous travaillez avec HUB, vous êtes au centre d'un vaste réseau d'experts qui offrent des solutions créatives aux défis complexes auxquels vous êtes confrontés. Nous avons une connaissance approfondie des besoins des organisations caritatives et une approche globale de la gestion des risques, des talents et de la réputation. Avec HUB, vous avez l'esprit tranquille en sachant que ce qui compte le plus pour vous sera protégé - grâce à une défense sans relâche de vos intérêts et à des solutions sur mesure qui soutiennent votre mission et vous permettent de planifier l'avenir en toute confiance.

hubinternational.com

Prêt pour demain.

Risque et assurance | Avantages sociaux | Retraite et gestion de patrimoine



HUB