Diligent

ÉVALUATION DE VOTRE CYBER-RISQUE

Une meilleure évaluation et analyse du risque grâce à un tableau de bord Cyber-risque

L’importance de la sensibilisation au cyber-risque

Les menaces de cybersécurité sont bien réelles et en constante évolution. Les dégâts financiers et structurels, ainsi que l’atteinte à l’image de marque causés par une cyber-violation, sont difficiles à réparer. Pour les conseils d'administration, la vigilance est de mise.

Sans les outils adéquats, il est quasiment impossible de rester à niveau. Indépendamment du secteur ou du lieu d’activité, la cybersécurité est une question critique pour l'entreprise et les conseils d'administration vont devoir la mettre au rang de leurs priorités dans les mois et les années à venir.

En effet, d’après l’enquête de Gartner sur les conseils d'administration en 2020 (2020 Board of Directors survey), d’ici 2025 quelques 40 % des conseils d'administration auront créé un comité dédié à la cybersécurité (moins de 10 % aujourd’hui). Ce chiffre indique clairement les changements organisationnels à haut niveau qui se produisent déjà « en réponse au risque accru créé par l’étendue de l’empreinte numérique des organisations pendant la pandémie [de Covid-19] ».

Alors que les entreprises avancent vers un avenir gouverné par le numérique, les conseils d'administration doivent veiller à mettre en place les mesures adéquates pour assurer une transition aussi douce que possible. Ils doivent être conscients de toutes les vulnérabilités, des violations potentielles de données aux partenariats avec des tiers, susceptibles de représenter un risque si des mesures préventives ne sont pas prises.

Une approche correcte de la gestion du cyber-risque exige une meilleure connaissance de plusieurs facteurs, notamment :

- la transformation numérique, qui comporte la réalisation d’opérations par des moyens techniques et, parallèlement, le remisage des processus manuels hérités à base de papier ;
- l’augmentation très nette du télétravail, qui montre combien la sécurité de la collaboration et de la communication est importante dans un environnement de travail virtuel ;
- une vigilance accrue de la part des investisseurs, des attentes plus pressantes du côté des consommateurs et un nombre croissant de considérations relatives aux parties prenantes qui doivent être prises en compte ;
- le ciblage de la réglementation dans la surveillance des tierces parties ;
- l’impact du risque pour l’image de marque et ses conséquences.

À l'heure actuelle, il est donc très important pour les conseils d'administration d'être parfaitement conscients des cyber-risques.

> « Au XXIe siècle, il n'existe pas une seule décision importante qui n’inclue pas des aspects de cybersécurité. La cybersécurité doit être intégrée dans l’ensemble du processus, de la R+D à la fabrication, en passant par les relations publiques. Le message à propos de la cybersécurité ? Nous sommes tous concernés. »
>
> **Larry Clinton**
> Président, Internet Security Alliance

Une surveillance efficace du risque commence au sommet de la hiérarchie.

Pour qu'une stratégie de lutte contre le cyber-risque soit efficace, les administrateurs doivent pouvoir accéder aux données de cybersécurité pertinentes, présentées sous un format intuitif qui permette de les évaluer rapidement et de prendre des décisions éclairées, afin d'améliorer la situation dans ce domaine.

Cette fonctionnalité est incluse dans les tableaux de bord Cyber-risque, en particulier lorsqu'ils accompagnent le portail pour conseils d'administration, avec lequel les administrateurs sont déjà familiarisés. Des données claires et succinctes aident les administrateurs à détecter les informations utiles et à les employer pour prendre leurs décisions, qu'il s'agisse de prendre des mesures pour renforcer la cybersécurité ou que cela concerne le niveau de préparation face à une cyberattaque ou, tout simplement, à créer une compréhension commune au sein de l'organisation et à susciter des échanges productifs à tous les niveaux.

> « [Aujourd'hui], il n'existe pas une seule décision importante qui n'inclue pas les aspects de cybersécurité. [Ils devraient] être intégrés dans l'ensemble du processus. »
>
> **Larry Clinton**
> Président,
> Internet Security Alliance

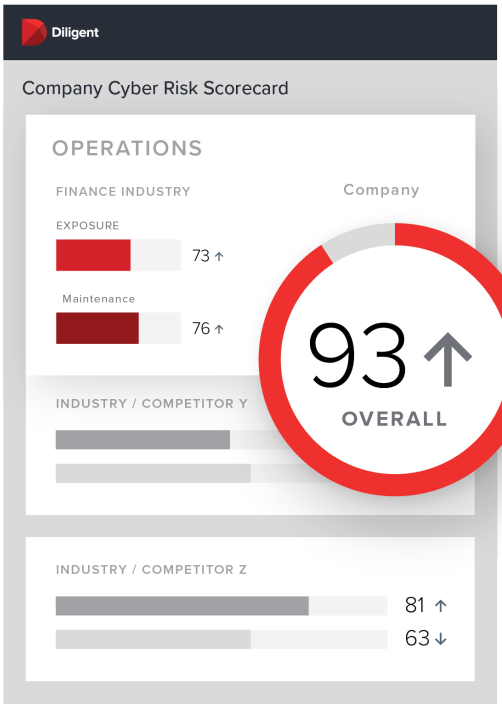
La lutte contre le cyber-risque : les meilleures pratiques pour les conseils d'administration

- ☐ Encouragez la cohérence dans toute l'organisation, de la sécurité juridique à la sécurité technologique, sans oublier la sécurité des données. Une approche intégrée au niveau du conseil et en dessous entraînera une réaction plus rapide et efficace en cas de menace.
- ☐ Un bon conseil d'administration donne l'exemple et veille à ce que ses propres communications soient sécurisées et protégées. En intégrant la cybersécurité dans ses processus, le conseil montre l'importance d'une telle approche dans l'ensemble de l'organisation. La cybersécurité doit être considérée comme une question de gestion du risque à l'échelle de l'entreprise et non pas seulement comme un problème relevant du service informatique.
- ☐ Mettez en œuvre une solution permettant d'évaluer et de communiquer le cyber-risque. Cette mesure est indispensable dans un paysage de risque de plus en plus complexe. L'utilisation d'un tableau de bord contenant toutes les données liées au risque, présentées de manière rationnelle et au même endroit, permet de se concentrer sur ce point et de produire des rapports fiables.
- ☐ Assurez-vous qu'en cas d'incident de cybersécurité, un plan détaillé, solide et éprouvé a été mis en place. Plus l'intervention sera rapide, moins il y a aura de possibilités de causer des dommages à long terme.
- ☐ Dirigez depuis le sommet de la hiérarchie. Le conseil d'administration, grâce à sa propre gouvernance et à sa propre maîtrise de la cybersécurité, peut donner le ton au reste de l'organisation. La cybersécurité est-elle un point qui revient constamment dans l'ordre du jour ou simplement un phénomène ponctuel ? La stratégie et la gestion du risque se situent au tout début de la liste des priorités d'un grand nombre de conseils d'administration. Les discussions les concernant ne devraient pas se produire sans mettre l'accent sur la technologie et la sécurité.

Suivre un tableau de bord Cyber-risque conduit à une meilleure gestion du cyber-risque

En matière de cybersécurité, les évaluations, graphiques et drapeaux de couleurs sont des éléments de surveillance qui permettent aux membres du conseil d'administration de poser des questions plus pertinentes :

- **Quelles sont les failles de notre système de cybersécurité ?**
- **Y a-t-il chez le prestataire de services avec qui nous envisageons de travailler des vulnérabilités qui pourraient comporter un risque pour notre entreprise ?**
- **Quel est le niveau de risque de nos prestataires actuels ?**
- **Comment nos défenses en matière de cybersécurité se situent-elles par rapport à celles de la concurrence ?**
- **Comment le conseil d'administration peut-il savoir si l'entreprise est en train de renforcer sa cybersécurité et sa conformité ?**
- **L'entreprise que nous sommes sur le point de racheter a-t-elle des problèmes de cybersécurité qui pourraient influencer la transaction ?**



Les risques de cybersécurité évoluent en permanence. Néanmoins, à des fins de reporting et de planification, les informations les plus utiles prennent souvent la forme d'une note, simple et facile à comprendre. Une note de cyber-risque comporte de nombreux avantages. Grâce à un système simple de notation dans l'ordre hiérarchique, composé de lettres ou de chiffres, elle améliore le reporting au niveau de la direction pour renforcer la cybersécurité et l'aligner sur les besoins de l'entreprise. Le conseil d'administration, muni de cette notation et de la visibilité qu'elle offre, est en mesure de prendre plus rapidement des décisions mieux informées en matière de cybersécurité.

4 scénarios exigeant un tableau de bord Cyber-risque

1 ÉVALUATION DU CYBER-RISQUE DE L'ENTREPRISE

Un tableau de bord Cyber-risque doit évaluer le risque de sécurité de l'organisation en utilisant des indicateurs continuellement actualisés, basés sur les données, qui mettent en évidence les failles des contrôles de sécurité et les vulnérabilités potentielles dans tout l'écosystème de la chaîne d'approvisionnement.

Munis de ces connaissances, les conseils d'administration peuvent mettre en œuvre les changements qui corrigeront les points faibles. De plus, le suivi continu d'un tel système de notation permet aux conseils d'administration de voir où les progrès ont lieu et de mesurer l'impact de ces progrès à l'échelle de l'organisation.

Un conseil d'administration qui exploite la visibilité d'un tableau de bord Cyber-risque est en mesure de gérer de manière proactive les risques de sécurité et de les hiérarchiser, ainsi que de prendre des décisions éclairées basées sur les données.

La réalité d'une violation de la cybersécurité

SolarWinds, une grande société d'informatique qui fournit des logiciels à des entités allant de sociétés listées au Fortune 500 au gouvernement des États-Unis, a récemment fait l'objet d'une attaque massive de cybersécurité qui s'est propagée à ses clients. Cette violation de la sécurité est restée indétectée pendant des mois. Environ 18 000 clients de SolarWinds ont, à leur insu, installé des mises à jour de logiciels qui incluaient un code piraté, exécuté si furtivement que certaines des victimes pourraient ne jamais savoir si elles ont été ou non contaminées. Des sommes astronomiques seront nécessaires pour sécuriser de nouveau les systèmes concernés et cela pourrait prendre des années.

2 COMPARAISON AVEC LES PAIRS

La capacité à évaluer rapidement la sécurité des pairs et des concurrents dans leur secteur permet aux conseils d'administration de savoir exactement où ils se situent par rapport aux autres dans le même domaine, ce qu'ils pourraient mieux faire et où ils sont mieux placés que la concurrence. Pouvoir creuser les problèmes spécifiques de sécurité d'un groupe de pairs est un moyen instantané de comparer et de contraster sa propre préparation en matière de cybersécurité.

Les organisations analysent régulièrement les indicateurs de rendement clés (ICR), relatifs aux ventes, aux bénéfices et à la rentabilité d'autres sociétés et améliorent par conséquent leur performance interne en réallouant des ressources et en accordant la priorité à certains objectifs. L'application des mêmes processus à l'analyse du cyber-risque peut être avantageuse. Le fait de connaître la position de vos concurrents aide non seulement à remédier aux failles de sécurité dans votre organisation, mais aussi à encourager l'innovation et à faire avancer les processus. L'utilisation de ces données peut aider à dresser un plan d'action et à fixer des objectifs à court et long terme pour parvenir au même niveau de cybersécurité que ses concurrents les plus performants, voire le dépasser.

3 L'EXERCICE DE DUE DILIGENCE

Le rapport de Gartner, Innovation Insight for Security Rating Services (L'innovation pour les services de notation de sécurité) affirme que, d'ici 2022, « les notations de sécurité auront pris autant d'importance que les notations de crédit lors de l'évaluation du risque dans les relations commerciales ». Une due diligence complète exige de connaître l'état de cybersanté de tout fournisseur ou société avec qui l'organisation du conseil d'administration a l'intention d'avoir des échanges, qu'il s'agisse de partenaires ou de fournisseurs existants ou potentiels, ou de prospects pour rachat.

Avoir la capacité d'identifier, de suivre et de gérer sans discontinuer le risque que présente l'écosystème des fournisseurs est un facteur fondamental de pérennité de la réussite. Après tout, la cybersécurité d'une organisation est aussi forte que le maillon le plus faible de son réseau.Une vulnérabilité dans cette chaîne d'approvisionnement, où qu'elle se trouve, non seulement augmente le risque de l'entreprise mais met aussi en danger sa productivité, sa rentabilité et sa réputation.

Dans le même ordre d'idée, investir dans une société, créer un partenariat avec elle ou la racheter implique la prise en charge de ses opérations numériques, ce qui peut entraîner de nouveaux risques de cybersécurité susceptibles de modifier la transaction. À moins que ces cybermenaces ne soient détectées et corrigées au début du processus, elles ont le potentiel d'affecter négativement la valeur prévue de la transaction.

La violation de données dans l'organisation d'un tiers peut faire des ravages dans toutes les organisations qui lui sont liées. En 2018, quand les serveurs du prestataire de services de facturation d'Atrium Health, AccuDoc Solutions ont été attaqués, les données de plus de 2,65 millions de patients ont été violées. Un autre exemple : les données personnelles d'au moins 30 000 travailleurs du ministère américain de la Défense ont été exposées lorsqu'un prestataire de services de voyages a été piraté.

> « [D'ici 2022], les notations de sécurité deviendront aussi importantes que les notations de crédit lors de l'évaluation du risque dans les relations commerciales. »
>
> « Innovation Insight for Security Rating Services »,
> Gartner

4 LA GESTION DES RISQUES POUR L'IMAGE DE MARQUE

Le risque pour l'image de marque est peut-être le pire de tous les risques. Alors que certains risques peuvent être atténués, gérés et souvent traités en interne, une entreprise peut passer des années à reconstruire une image de marque ternie. Il est donc indispensable que les sociétés gèrent soigneusement leur image de marque.

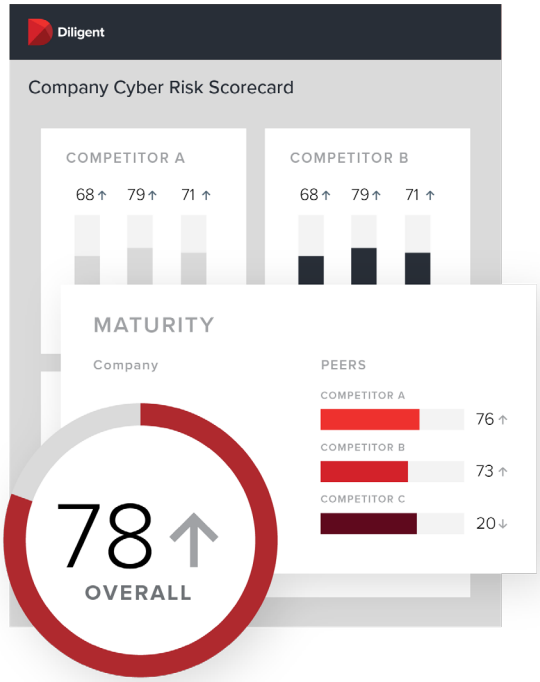
Un tableau de bord Cyber-risque offre une visibilité homogène des menaces et vulnérabilités qui pourraient perturber les opérations commerciales. Il permet aux organisations de détecter les failles de sécurité potentielles tout en s'assurant que les tierces parties avec qui elles collaborent sont en conformité avec les réglementations applicables.

En 2017, Verizon a racheté Yahoo pour 3,73 milliards €. L'opération a pourtant été à deux doigts d'avorter à cause du scandale déclenché par deux violations de données qui ont été découvertes au cours des négociations. La société Yahoo a révélé qu'elle avait subi deux violations de données qu'elle n'avait pas rendues publiques. Verizon a malgré tout racheté Yahoo, mais en a profité pour rabaisser le prix d'achat de 300 millions €. Verizon a également accepté de partager avec Yahoo la responsabilité juridique des violations. Le legs a été coûteux et, ajouté à la baisse du prix, il a nui à la valeur de l'opération d'innombrables façons.

Le tableau de bord Cyber-risque de Diligent donne une instantanée complète de la cybersanté de l'entreprise

Une approche proactive de la gestion du cyber-risque est impérative pour que la réussite organisationnelle perdure.

Le tableau de bord Cyber-risque de Diligent offre aux membres des conseils d'administration un niveau de visibilité qu'ils n'avaient pas auparavant. Le tableau est toujours à jour et accessible. C'est un élément indispensable en matière de cyber-risque. Les informations qu'il comporte sont faciles à assimiler et elles permettent de mieux comprendre, de dresser des rapports plus précis et d'améliorer l'analyse. Il mesure la cybersécurité de manière intuitive, en tirant ses données et informations de plusieurs points de contact et en compilant ses conclusions sous forme d'affichage visuel cohérent. Le tableau de bord Cyber-risque de Diligent propose des évaluations de sécurité précises qui contribuent à la détection des problèmes critiques au sein de l'organisation et chez les pairs, progressivement et en fonction de facteurs clés qui déterminent la notation. Les organisations qui choisissent d'aller plus loin peuvent accéder à un niveau d'information encore plus profond concernant les relations avec les fournisseurs, les fusions et acquisitions, les opérations de financement privé, la souscription de crédits, la vente d'actifs financiers et les échanges.



Avec le tableau de bord Cyber-risque de Diligent, basé sur la technologie SecurityScorecard, reconnue par le Forum économique mondial, les administrateurs peuvent surfer sur un paysage numérique changeant et complexe et :

- accéder à leur notation de cyber-risque et la comparer à celle de leurs pairs et de groupes concurrents gérés par Diligent ;
- connaître leur position en matière de cybersécurité par rapport aux indices du secteur et comprendre les trois principaux facteurs de sécurité qui déterminent cette notation ;
- accorder des priorités aux mesures à prendre et identifier les infrastructures et les logiciels qui doivent en faire l'objet ;
- gérer les risques pour l'image de marque de leur société, identifier des tendances et accéder à leurs notations historiques du cyber-risque.

L'ORGANISATION VUE DE L'EXTÉRIEUR

Le tableau de bord Cyber-risque de Diligent contribue à détecter les vulnérabilités et les failles actives ainsi que les cybermenaces avancées, le tout d'un point de vue « extérieur ». Les conseils d'administration voient ce qu'un hacker voit. Grâce à une meilleure visibilité et à un accès direct à l'information, les conseils d'administration peuvent suivre le rythme et rester informés.

Le tableau de bord Cyber-risque note les sociétés sur une échelle qui va de A à Z. Les entreprises ayant la notation « F » ont 7,7 fois plus de chances de subir une violation des données que celles qui bénéficient de la notation « A ». Ces notations, lorsqu'elles font partie d'une stratégie de supervision complète du risque, peuvent exposer efficacement les vulnérabilités de la cybersécurité et contribuer à éviter les violations de données.

Pour offrir l'aperçu le plus complet possible, les notations sont calculées à partir d'un grand nombre de facteurs, notamment la santé des DNS, la réputation IP, la sécurité des applications Web, la sécurité du réseau, les fuites d'informations, les discussions de pirates, la sécurité des points d'accès et la cadence des correctifs. Malgré sa clarté et la simplicité visuelle de l'information qu'il fournit, le tableau de bord Cyber-risque contient une mine de données, d'analyses humaines et d'apprentissage machine lui permettant d'évaluer plus de 1,6 million de sociétés.

Le tableau de bord Cyber-risque de Diligent surveille continuellement la sécurité de votre organisation et affiche les problèmes liés aux principaux risques que votre société encourt, classés par ordre de gravité. Il crée automatiquement un plan de mesures correctives recommandées qu'il renseigne à l'aide des objectifs et procédures de votre organisation, vous aidant ainsi à mettre les meilleurs processus en place.

Lexique de la cybersécurité

- **Sécurité du réseau :** parmi les exemples de piratage de réseau, on peut citer l'exploitation des vulnérabilités telles que les points d'accès ouverts, les certificats SSL non sécurisés ou mal configurés, ou encore les vulnérabilités des bases de données et les failles de sécurité qui peuvent provenir d'un manque de mesures de sécurité adéquates.
- **Santé des DNS :** cela fait généralement référence aux mesures des paramètres de configuration des systèmes de noms de domaine (DNS) ainsi qu'à la présence de configurations recommandées.
- **Cadence des correctifs :** elle mesure comment une société apporte des correctifs à ses systèmes d'exploitation, services, applications, logiciels et matériel, et si elle le fait en temps voulu.
- **Sécurité des points d'accès :** la sécurité des points terminaux fait référence à la protection des ordinateurs, portables et de bureau, des appareils mobiles et de tous les dispositifs que les employés utilisent pour accéder au réseau de la société.
- **Réputation IP :** le tableau de bord Cyber-risque intègre des millions de signaux de malware provenant d'infrastructures de commandement (C2) réquisitionnées dans le monde entier. Les adresses IP entrantes infectées sont alors traitées et attribuées à des entreprises au moyen d'un algorithme d'attribution d'IP. La quantité et la durée des infections par malware sont utilisées comme facteur déterminant de ces calculs, fournissant un point de données pour l'évaluation globale de la réputation IP d'une organisation.
- **Discussion de hackers:** le tableau de bord Cyber-risque collecte continuellement plusieurs flux de discussions clandestines, y compris de forums de hackers difficiles d'accès ou privés. Les organisations et les IP qui font l'objet de ces discussions ou qui y sont ciblées sont identifiées.
- **Fuite d'information :** le tableau de bord Cyber-risque identifie les informations sensibles qui sont exposées dans le cadre d'une violation ou d'une fuite de données, d'un vidage de keylogger, de pastebin ou de base de données et via d'autres dépôts d'informations. Ces informations sont ensuite cartographiées sur les sociétés à qui les données appartiennent.

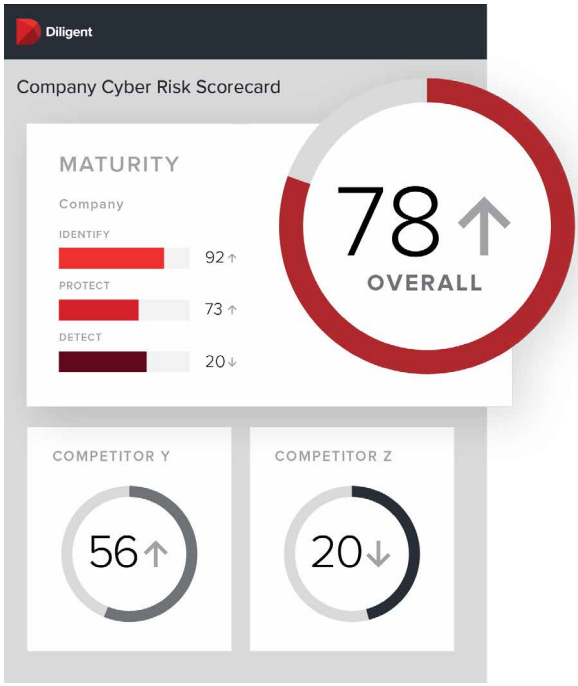
Le tableau de bord Cyber-risque et l'écosystème général de la gouvernance

Une solution bien gérée des cybermenaces établies et entrantes est seulement l'une des facettes de l'approche moderne de la gouvernance d'entreprise. La cybersécurité exige, par nature, une solution numérique.

De plus, les conseils d'administration passant à de nouveaux styles de supervision, ils adoptent de nouveaux canaux d'information. Le concept de « tableau de bord des risques » existe depuis un certain temps déjà, les conseils d'administration doivent maintenant demander à y accéder. Le tableau de bord Cyber-risque propose cette fonctionnalité intuitive.

Le tableau de bord Cyber-risque fonctionne en synergie avec le reste de la plateforme de gouvernance moderne de Diligent, créant une entreprise plus solide, plus sûre et numériquement plus robuste, prête à prospérer. Grâce au tableau de bord Cyber-risque, les entreprises bénéficient des atouts suivants :

- Sécurité continue et résilience numérique
- Renforcement des connaissances sur les questions importantes, de la gestion des données à la sécurité de la chaîne d'approvisionnement.
- Stabilité organisationnelle
- Potentiel d'investissement futur
- Prospérité à long terme



Les administrateurs, les dirigeants et les professionnels de la gouvernance font face à un impératif de gouvernance moderne. Ils doivent résoudre les complexités et prendre rapidement des décisions difficiles. Une suite de solutions qui atténuent le risque, améliorent les opérations et maintiennent les dirigeants informés est non seulement essentielle pour la pérennité de la sécurité et la résilience numérique mais aussi pour le potentiel futur et la stabilité opérationnelle.

Souhaitez-vous voir un tableau de bord Cyber-risque en pleine action ? Demander une démo

DEMANDER UNE DÉMO

Diligent

Une entreprise de
GOUVERNANCE
DANS L'AIR DU TEMPS

À propos de Diligent

Diligent est le pionnier de la gouvernance moderne. Nos applications de confiance, basées dans le cloud, rationalisent le travail quotidien des membres et des comités des conseils d'administration, assurent la sécurité de la collaboration, gèrent les données des filiales et des entités et fournissent des informations qui permettent aux dirigeants de société de prendre de meilleures décisions dans le paysage complexe d'aujourd'hui. Plus de 19 000 organisations et de 700 000 dirigeants, dans plus de 90 pays, font confiance à Diligent, qui possède le plus grand réseau international d'administrateurs et de dirigeants d'entreprises. Avec un service client primé dans le monde entier, Diligent est au service de plus de 50 % des entreprises du Fortune 1000, de 70 % de celles du FTSE 100 et de 65 % de celles de l'ASX.

Plus de 700 000 dirigeants et de 19 000 organisations dans le monde nous font confiance.

mastercard · BARCLAYS · Marriott · General Mills · Domino's · Liberty Mutual

Les plus hautes normes de sécurité

- Chiffrage 256 bits
- Verrouillage à distance
- Authentification à deux facteurs

Une assistance leader dans le secteur

- Assistance 24 h/24, 7 j/7, 365 j/an
- Un service haut de gamme
- Formation illimitée des utilisateurs

Certificats de conformité

- Audits ASEA 18
- Certification ISO
- Tests de sécurité de tiers

Pour obtenir davantage d'informations ou demander une démonstration :

Tél. : **+33 (0)6 29 26 57 42** | E-mail : **info@diligent.com** • Web : **www.diligent.com/fr/**