LIVRE BLANC

Comment sécuriser les données du conseil d'administration ?

La digitalisation du conseil d'administration en toute sécurité

UNE PUBLICATION DE DILITRUST

Sommaire

Avant-propos

Avec l'omniprésence d'Internet ainsi que l'augmentation du nombre de personnes, des objets connectés et des échanges numériques au sein des organisations, **les risques associés à l'informatique n'ont jamais été aussi forts**.

La transformation digitale des organisations a fait apparaître de nouveaux outils et moyens de communication permettant d'améliorer l'efficacité, la performance et par ailleurs favoriser l'internationalisation. Cependant, **ce processus a rendu les organisations plus vulnérables à une fuite de données sensibles**.

La société Uber a subi une cyberattaque à grande échelle et 57 millions de données clients ont été piratées.

Deloitte, l'un des plus grands cabinets de conseil en technologie et d'audit au monde, a subi une cyberattaque compromettant des documents sensibles et des emails entre la société et plusieurs de ses clients.

La société d'évaluation de côte de crédit Equifax a été victime d'une attaque informatique qui a touché 143 millions de clients américains, canadiens et britanniques.

Les risques informatiques

La nécessité d'adresser les risques informatiques et d'instaurer de **véritables politiques de sécurité** est donc indispensable pour éviter de graves conséquences que ce soit sur le plan financier ou en termes de réputation et d'image.

Le conseil d'administration dans son application d'une bonne gouvernance a pour responsabilité la **surveillance de la gestion des risques**. Les systèmes d'information ont pris une place stratégique au sein des entreprises, ainsi les risques associés doivent être compris par les administrateurs. Ces derniers, en occupant le plus haut niveau d'autorité de l'organisation, doivent **faire preuve d'exemplarité en adoptant de bonnes pratiques de sécurité informatique**.

Dans ce livre blanc, nous allons introduire la sécurité informatique, observer le rôle du conseil d'administration dans la gestion des risques informatiques et les risques au sein même du conseil ainsi que **les solutions pour les prévenir**.

Qu’est-ce que la sécurité informatique ?

Introduction à la sécurité informatique

Physiquement, la sécurité est l'état d'une situation présentant le minimum de risque.

Psychiquement, la sécurité est l'état d'esprit d'une personne qui se sent tranquille et confiante.

Pour l'individu ou un groupe, c'est le sentiment (bien ou mal fondé) d'être à l'abri de tout danger et risque.

« La sécurité est un métier. C'est notre métier. »

Nadim Baklouti
Chief Technology Officer de DiliTrust

Sécuriser un système d'information signifie la mise en place d'un dispositif de gestion des risques qui englobe l'identification du risque, son évaluation et sa compréhension, puis, la mise en place de mesures pour le prévenir, le minimiser ou l'éliminer.

La sécurité légale

La sécurité contractuelle définit le **périmètre de protection des informations** ainsi que les moyens mis en place pour **garantir la propriété intellectuelle** comme le dépôt de brevets.

LE PATRIOT ACT

Le Patriot Act est une loi qui s'inscrit dans la lutte contre le terrorisme et qui a été adoptée par les États-Unis après le 11 septembre 2001. Elle permet aux **services de sécurité américains d'accéder à tout moment et sans autorisation judiciaire aux données informatiques** des individus et entreprises liés aux États-Unis ainsi que les serveurs qui hébergent leurs données ou celles de leurs clients.

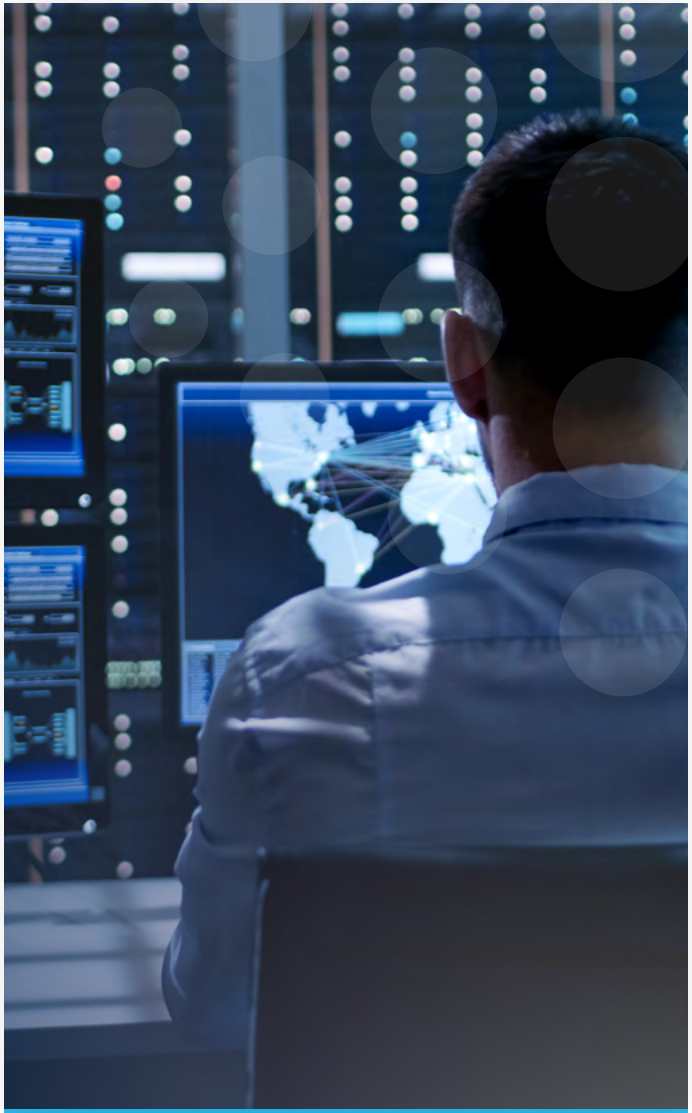
En 2014, on constate la première décision juridique à aborder la question de la portée du Patriot Act. En effet, un juge américain impose au géant de l'informatique, Microsoft (société de droit américain), de **remettre aux autorités américaines les informations privées de l'un de ses clients** malgré l'hébergement des données en Europe (Irlande).

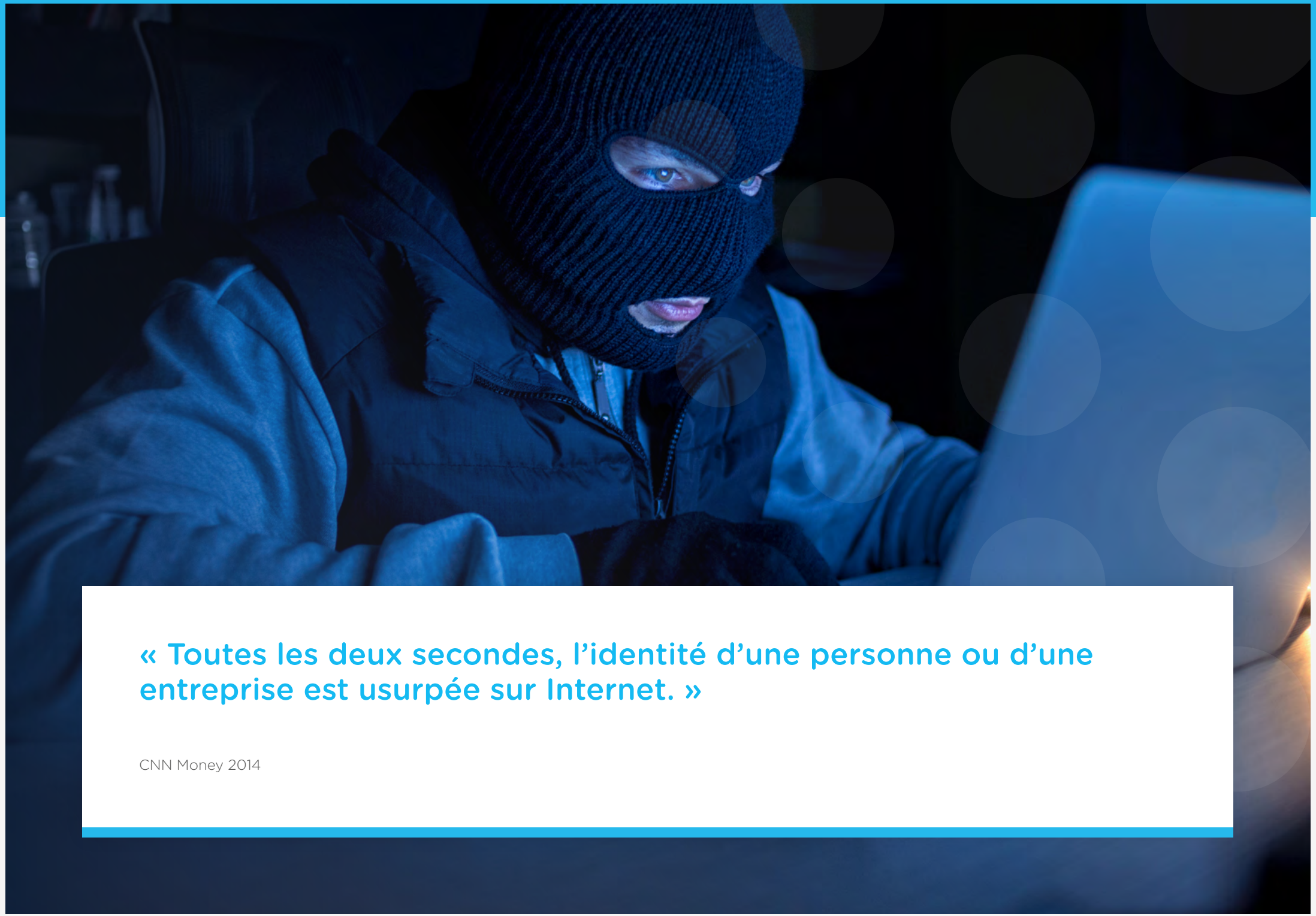
Pour éviter l'assujettissement à des programmes de surveillance tel que le **Patriot Act**, il faut contrôler toute la chaîne de fournisseurs en relation avec le traitement et le stockage des données. Si un seul élément de cette chaîne fait que les données se trouvent sur des serveurs sur le sol américain, dans le « cloud » ou stockées par un hébergeur de nationalité américaine, toute la chaîne sera soumise au Patriot Act.

La sécurité « anti-intrusion »

De nombreux risques pèsent sur les informations confidentielles des organisations. Il y a des risques physiques comme un incendie ou une inondation sur le lieu de stockage, une défaillance du matériel, un cambriolage… ainsi que des menaces virtuelles liées à la **cybercriminalité** (on note un large éventail de types d'attaques : virus, logiciels malveillants, vol d'identité, harcèlement, extorsion de fonds, espionnage industriel, manipulation boursière…).

Les pirates informatiques développent des attaques de plus en plus sophistiquées et discrètes qui exploitent les technologies de l'information et ces nouvelles formes d'interactivité. Leur but ? **Voler les données confidentielles** des organisations, **les secrets industriels et commerciaux**, pour les revendre sur un marché mondial et hyperconcurrentiel.





« Toutes les deux secondes, l'identité d'une personne ou d'une entreprise est usurpée sur Internet. »

CNN Money 2014

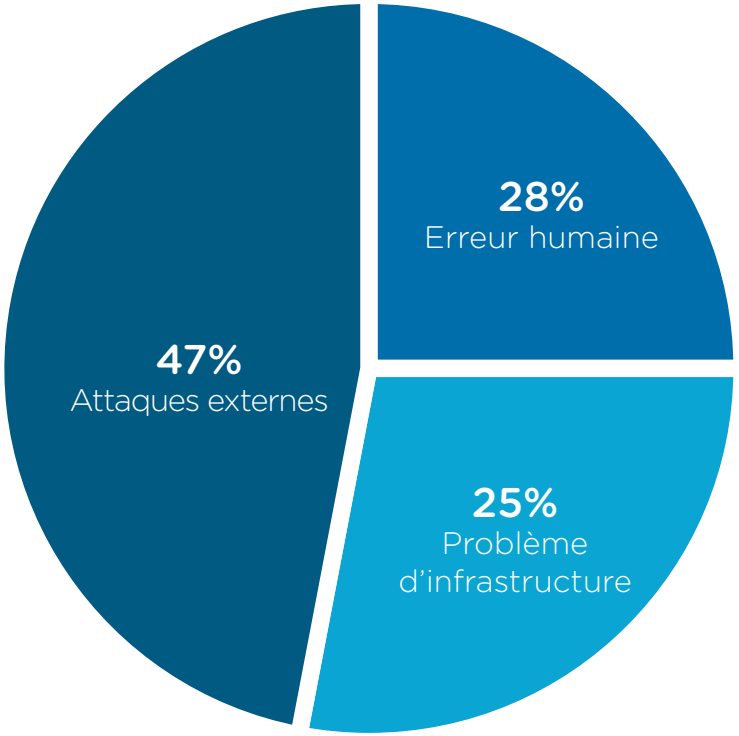
La sécurité des processus

Les risques en termes de sécurité informatique sont souvent traités comme des questions strictement technologiques, pourtant, **la sécurisation des données doit impérativement placer au cœur du processus le facteur humain**.

La sensibilisation des collaborateurs passe par une politique relative à la sécurité avec une **charte informatique** qui ne doit pas être perçue comme une contrainte mais comme une nécessité pour protéger le capital informationnel de l'entreprise ainsi que leurs propres données personnelles.

Pour atteindre une vision commune sur l'importance de la sécurité informatique et éviter toute forme d'imprudence, **la communication est primordiale**.

Répartition des sources d'incidents de sécurité (en %)



Source : Ponemon Institute - 2017 Cost of a data breach

Quel rôle le conseil d'administration joue-t-il en matière de sécurité ?

Le conseil et la gestion des risques

Pour déterminer le rôle du conseil d'administration dans la gestion des risques, le Code de Commerce donne une définition simple et claire de cette entité :

CODE DE COMMERCE - ARTICLE L225-35 (FRANCE)

« Le conseil d'administration détermine les orientations de l'activité de la société et veille à leur mise en œuvre. Sous réserve des pouvoirs expressément attribués aux assemblées d'actionnaires et dans la limite de l'objet social, **il se saisit de toute question intéressant la bonne marche de la société et règle par ses délibérations les affaires qui la concernent**. [...]

Le conseil d'administration procède aux contrôles et vérifications qu'il juge opportuns. Le président ou le directeur général de la société est tenu de communiquer à chaque administrateur tous les documents et informations nécessaires à l'accomplissement de sa mission. »

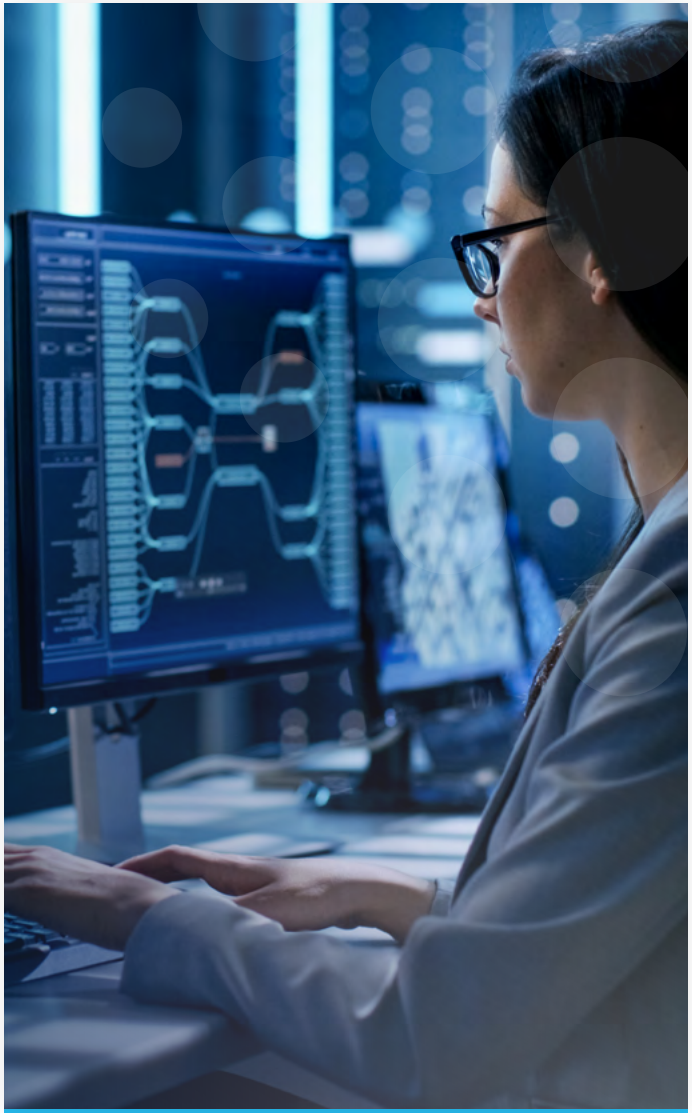
L'Union Européenne a adopté le **RGPD, Règlement Général sur la Protection des Données**, qui sera instauré en mai 2018 et concerne toutes les entreprises situées en Europe, ou qui collectent des informations personnelles de citoyens européens. Si ce règlement n'est pas respecté par les entreprises, celles-ci s'exposent à **des amendes pouvant aller jusqu'à 4% de leurs chiffre d'affaires annuels**.

La surveillance de la gestion des risques

Le conseil d'administration est responsable d'appliquer la bonne gouvernance. Le conseil occupe un rôle de surveillance de la mise en œuvre du plan stratégique et de la Direction Générale.

Les administrateurs jouent un rôle de premier plan dans la supervision de la mise en place d'un système de gestion de ces risques avec un suivi pour assurer le bon fonctionnement de ce processus (par la remontée d'information et d'indicateurs clés par la Direction Générale).

Aujourd'hui, **de nombreux membres de conseils d'administration réalisent la gravité des risques informatiques** et estiment que la sécurité informatique est une question qu'ils doivent traiter au sein du conseil.



« Seules 39% des entreprises se déclarent confiantes en leur capacité d'identifier les sources des cyberattaques. »

Source : Global State of Information Security survey 2018 - PwC (France)

Une compréhension de la sécurité informatique

Le conseil d'administration doit comprendre la sécurité informatique et les risques liés à l'utilisation des nouvelles technologies. Le conseil doit se doter des compétences nécessaires soit par l'ajout d'un administrateur expert soit par l'organisation de formations.

Une fois la compréhension globale acquise sur la sécurité informatique ainsi qu'une vue d'ensemble des systèmes d'informations et un suivi du cadre réglementaire, le conseil peut traiter de manière éclairée ce sujet et **contrôler l'efficacité du programme de gestion des risques en place**.

La gestion des risques de la sécurité informatique doit être à l'ordre du jour des réunions du conseil d'administration au moins une fois par an. Aux côtés du directeur général, **le directeur des systèmes d'information devient l'interlocuteur privilégié du conseil** qui peut lui exiger de présenter des rapports réguliers afin de mesurer la performance du dispositif de gestion de ces risques. **Les rôles de chaque acteur dans la sécurité informatique doivent être définis** et des moyens suffisants alloués pour assurer le développement de bonnes pratiques.

Les risques au sein des conseils d'administration

Avec ce grand nombre de documents nécessaires pour la tenue des réunions du conseil, l'utilisation de supports papier est un processus long, incommodant et dispendieux. **Ces multiples papiers très confidentiels ne sont pas sécurisés**; un document peut tomber ou être oublié dans un lieu public, pire être volé. L'organisateur doit donc s'assurer qu'un messager sécurisé délivre les documents aux membres du conseil et les récupère après la réunion.

Certaines organisations ont choisi de communiquer par email pour éliminer le papier. Cependant, **avec l'utilisation de services de messagerie, les données qui y transitent ne sont pas chiffrées**. Ainsi, une grande quantité d'information pourrait être **vulnérable au piratage et à des failles de sécurité**.

« Les conseils d'administration produisent en moyenne 12 358 pages de documents par an pour la préparation et la tenue des réunions. »

Source : The Evolving Role of the Global Board : étude réalisée par Thomson Reuters en 2014

L'externalisation de la sécurité des données

Au sommet de l'organisation, le conseil doit montrer l'exemple en matière de gestion des risques. Cependant ces entités utilisent parfois des outils archaïques, des supports papier et des emails non sécurisés ; ce qui présentent des **risques majeurs pour les informations les plus confidentielles**. Seuls les outils de dématérialisation proposent aujourd'hui une sécurité satisfaisante, néanmoins certains administrateurs refusent leur utilisation par simple résistance au changement, mettant ainsi en péril les données sensibles de l'organisation.

Équiper le conseil d'administration d'un portail dématérialisé permet de mettre à disposition des administrateurs et du conseil, une plateforme simple et pratique pour optimiser la gestion du conseil, introduire les nouvelles technologies avec des fonctionnalités efficaces et des outils pratiques tout en **renforçant la sécurité des données**.

Confier cette partie de son système d'information à un prestataire de services permet de **profiter d'une expertise technique et d'un accompagnement** tout au long de l'utilisation de la solution.

La sécurité est un critère de sélection prioritaire

Une vigilance accrue est obligatoire lors du choix du prestataire. **Le prestataire doit prouver ses engagements en matière de sécurité** avec une politique stricte de mots de passe, la réalisation de tests d'intrusion, un chiffrement des données et la réalisation d'audits externes.

« Un conseil digitalisé permet d'assurer un suivi de l'information et d'en contrôler l'accès offrant donc une meilleure sécurité des données du conseil à l'interne comme à l'externe. »

Yves Garagnon
Directeur Général de DiliTrust

Un portail digitalisé pour le conseil d'administration permet de **regrouper toutes les opérations de gestion, les réunions et les documents dans un espace sécurisé**. Toute communication se déroule à l'intérieur de la plateforme ; ainsi **le risque de perte ou de vol d'un papier confidentiel est éliminé**. **Les données sont disponibles et protégées dans toutes les circonstances** (comme lors d'une panne de courant ou de catastrophes naturelles).

À propos de DiliTrust Exec

UN PORTAIL DIGITALISÉ DÉDIÉ AUX CONSEILS D'ADMINISTRATION

DiliTrust Exec est une **solution permettant la gestion digitalisée des conseils d'administration et des instances** à travers un portail hautement sécurisé. Certifiée ISO 27001, **elle réduit considérablement les risques liés aux pertes et fuites de données** en garantissant les meilleurs standards de sécurité.

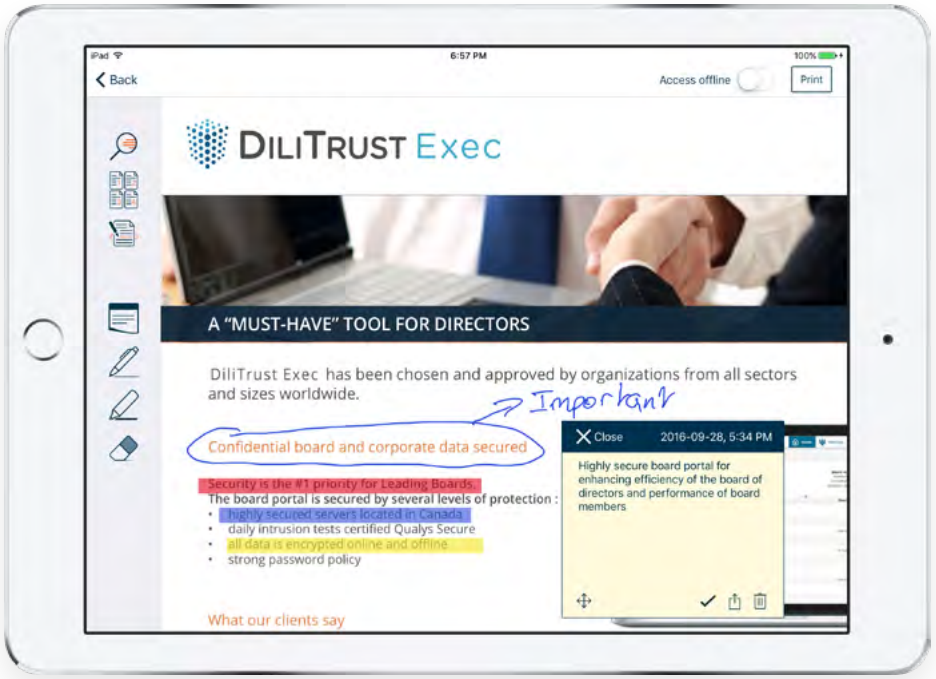
- **Création d'ordres du jour**
  rapports, procès verbaux...
- **Accès instantané et illimité**
  aux réunions et aux archives
- **Protection de la confidentialité**
  des données grâce à l'hébergement en France
- **Optimisation des échanges**
  avec les administrateurs

TÉLÉCHARGER LA FICHE

DEMANDER UNE DÉMO

À propos de DiliTrust Exec

Simple, **sécurisé** et **efficient**, le portail multiplateforme permet l'organisation des réunions et une gestion électronique des documents ainsi que des archives. La solution inclut des fonctionnalités de collaboration efficaces, dont une prise de notes numérique et un outil de recherche. Ainsi, **le portail aide les administrateurs à accomplir leurs devoirs de diligence** par un accès en temps réel à l'information en tout temps et où qu'ils soient.



Lancé en 2008, le portail digitalisé DiliTrust Exec a été choisi et **approuvé par de nombreuses entreprises ou organisations** de tous les secteurs et de toutes les tailles à travers le monde.

Download on the App Store

GET IT ON Google Play

Get it from Microsoft

DILITRUST

LE LEADER DES SOLUTIONS DE GOUVERNANCE

DÉCOUVRIR LE SITE

DiliTrust - Les Collines de l'Arche - 76 route de la Demi-Lune - 92057 Paris La Défense Cedex - France

+33 (0)1 42 91 92 00

contact@dilitrust.com

www.dilitrust.com