

Faire face aux menaces cyber

Présentation AMRAE

13 janvier 2017



Rapport du Lloyd's: Faire face aux menaces cyber

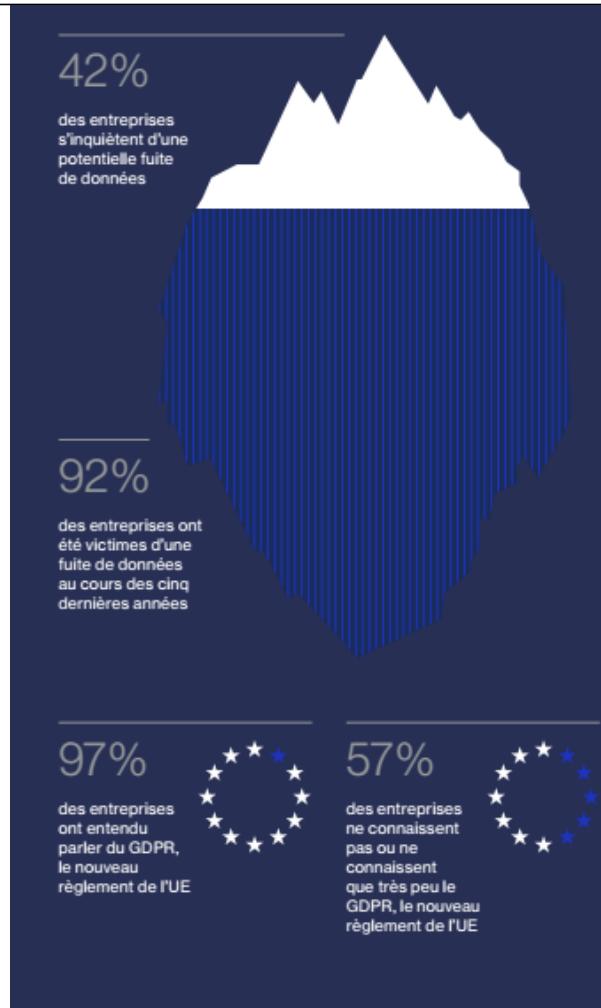
Contexte

- Dépendance des entreprises aux technologies numériques
- Ouverture sur les marchés vs plus grande vulnérabilité face aux attaques cyber
- En 2018, introduction du règlement général de l'Union Européenne sur la protection des données (GDPR)

Objectif de l'étude du Lloyd's

- Comprendre les mesures de sécurité mises en place par les entreprises européennes
 - Comprendre comment ces dernières se préparent à l'entrée en vigueur du GDPR
-

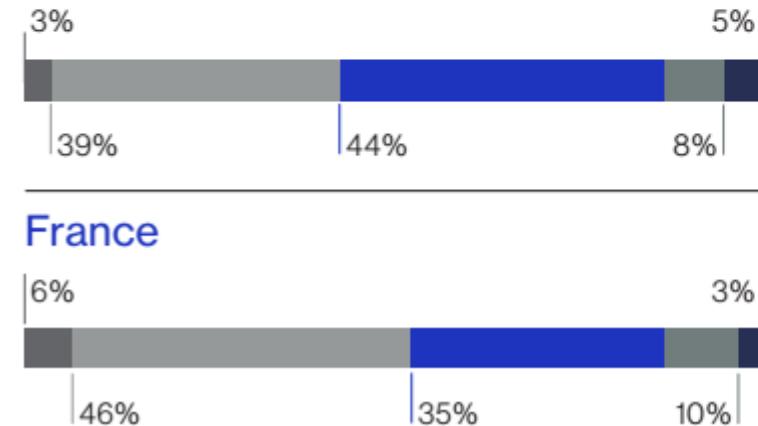
Rapport du Lloyd's: Faire face aux menaces cyber



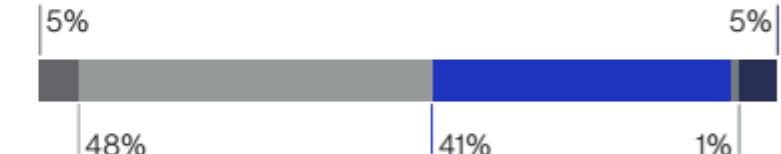
Êtes-vous inquiet de la survenue d'une fuite de données dans votre entreprise ?

- Pas du tout inquiet
- Assez inquiet
- Peu inquiet
- Très inquiet
- Pas d'avis

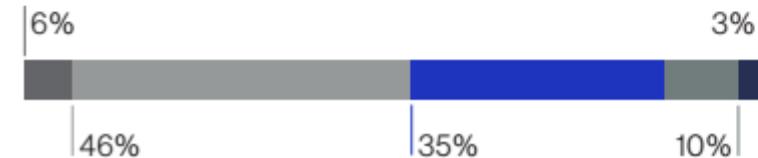
Total



Royaume-Uni



France



Allemagne



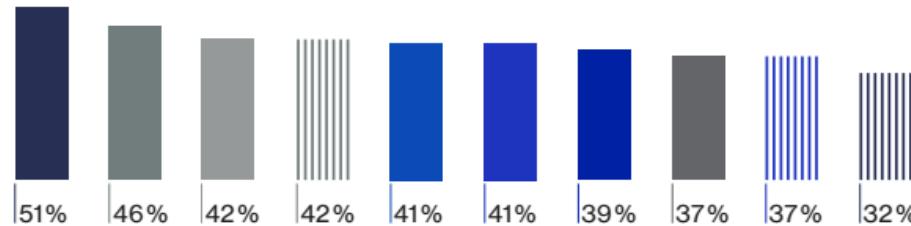
Rapport du Lloyd's: Faire face aux menaces cyber

Menaces externes et internes

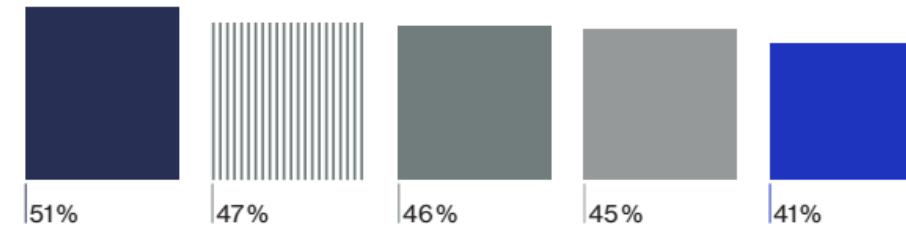
- Piratage informatique («hacking») – gain financier
- Piratage informatique («hacking») – concurrent
- Piratage informatique («hacking») – motivations politiques
- Erreur humaine/divulgation involontaire
- Phishing

- Équipements perdus, jetés ou volés
- Ransomware («ransomware»)
- Logiciel malveillant
- Perte physique de documents papier ou de matériel non électronique
- Collaborateur divulguant intentionnellement des informations

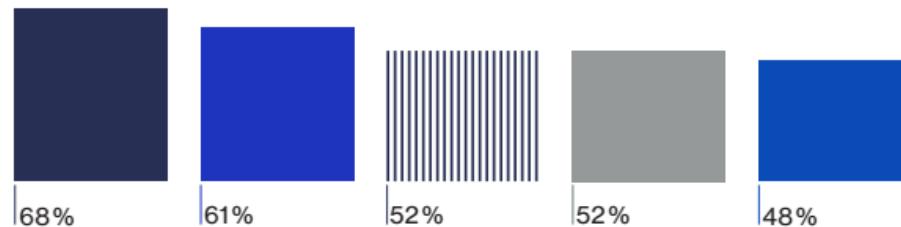
Total



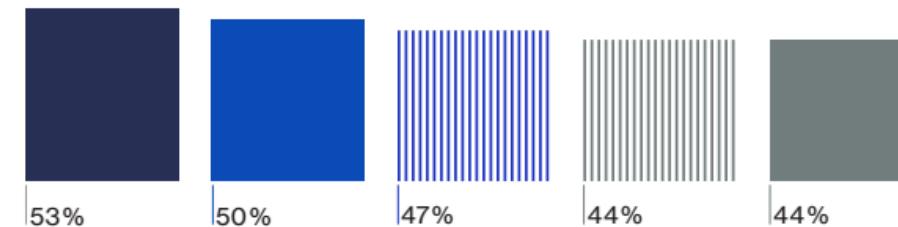
Royaume-Uni



France



Allemagne



Rapport du Lloyd's: Faire face aux menaces cyber

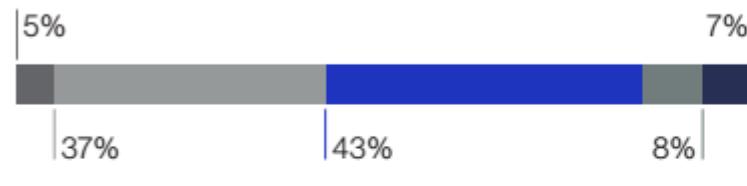
Approche sectorielle

Êtes-vous inquiet de la survenue d'une fuite de données dans votre entreprise ?

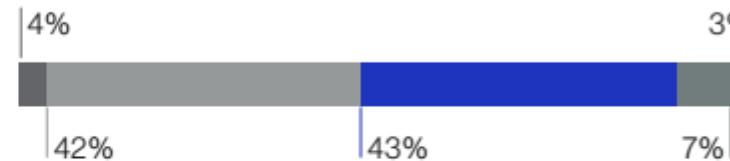
- Pas du tout inquiet
- Peu inquiet
- Pas d'avis

- Assez inquiet
- Très inquiet

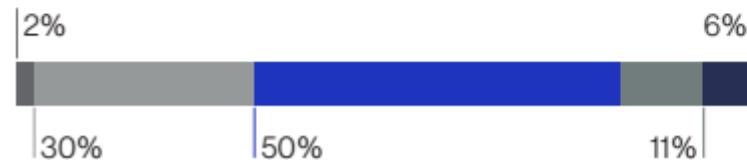
Distribution



Banque et finance



Santé/médical



Ces résultats montrent

- soit que les entreprises font confiance aux mesures de sécurité informatique qu'elles ont mises en place
- soit qu'elles se satisfont de leur résilience aux attaques cyber

Rapport du Lloyd's: Faire face aux menaces cyber

Préparation et riposte

93 %

des entreprises se disent «prêtes» ou «bien préparées» à intervenir en cas de crise

89 %

se disent «prêtes» ou «bien préparées» à agir en cas d'atteinte à la réputation

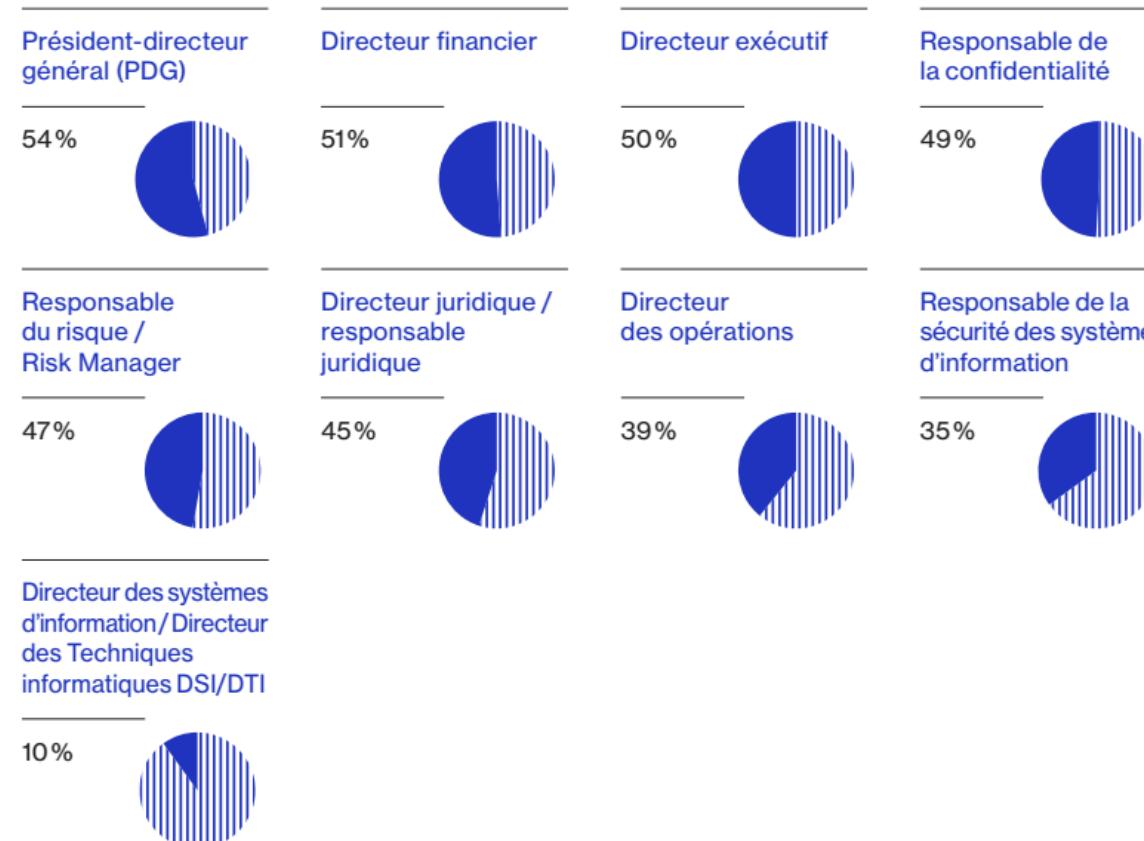
87 %

prennent en compte les implications réglementaires

Rapport du Lloyd's: Faire face aux menaces cyber

Responsabilité

Qui dans votre entreprise prend les décisions concernant la protection et la planification des actions en cas de violation de données?



Rapport du Lloyd's: Faire face aux menaces cyber

GDPR

Qu'est-ce que le règlement général sur la protection des données (GDPR)?

- Harmonisation des lois sur la protection des données existant au sein de l'UE
- Exigence de reporting à l'organisme de contrôle compétent et aux personnes impactées
- Mise en place de sanctions y compris des amendes pouvant se chiffrer jusqu'à 4 % du chiffre d'affaires annuel mondial ou à 20 millions d'euros, ainsi que des dommages et intérêts en cas de pertes financières ou de préjudice moral.
- Entrée en vigueur le 25 mai 2018 dans tous les États membres de l'UE
- Applicable à toute entreprise menant des activités touchant des citoyens de l'UE, indépendamment de sa localisation.

L'étude montre que la principale inquiétude des grandes entreprises européennes est l'incidence financière du GDPR en cas de fuite de données. L'attaque cyber contre TalkTalk, par exemple, a coûté à l'entreprise 60 millions de livres sterling et a entraîné une chute de 10 % du cours de l'action le jour où l'événement a été annoncé.

Rapport du Lloyd's: Faire face aux menaces cyber

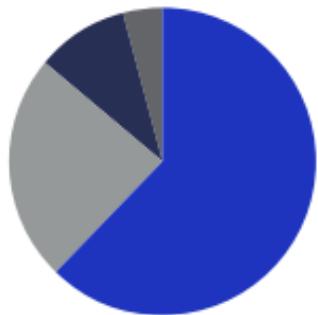
GDPR

Connaissez-vous les nouvelles règlementations ou les changements de règlementations liés à la protection des données?

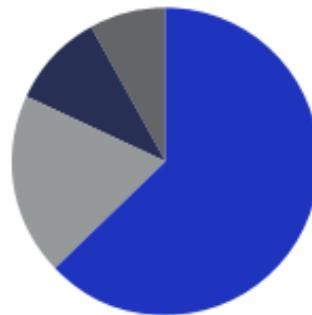
■ Ne sait pas
■ Non

■ Oui – autre
■ Oui – règlement général sur la protection des données (GDPR) de l'UE

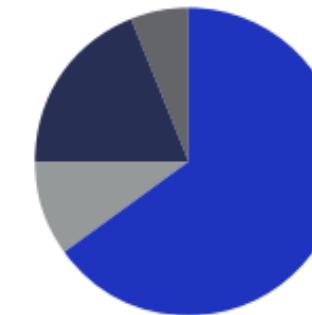
Total



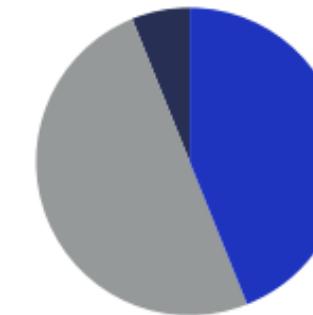
Royaume-Uni



France



Allemagne

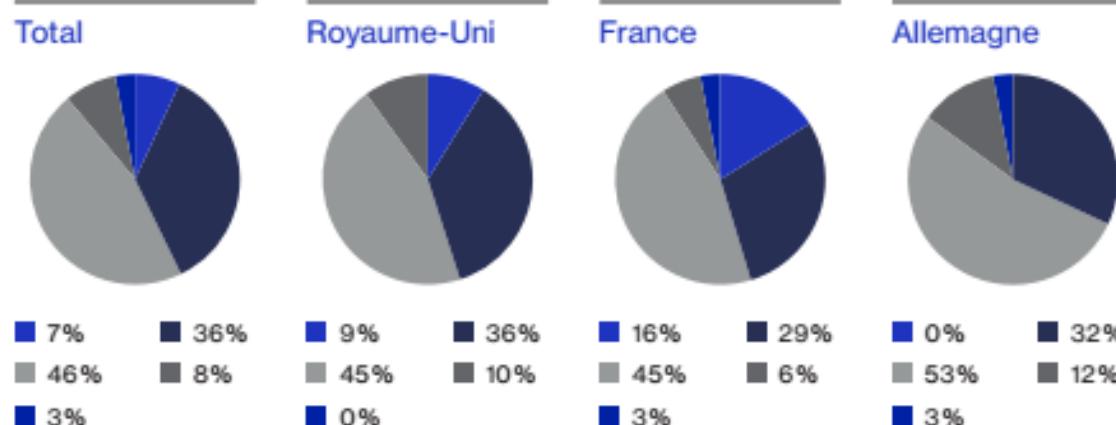


Rapport du Lloyd's: Faire face aux menaces cyber GDPR

Prise de conscience et compréhension du GDPR

Dans quelle mesure connaissez-vous le règlement général sur la protection des données (GDPR) de l'UE?

- | | |
|---|--|
| <ul style="list-style-type: none">█ Je connais très bien le GDPR de l'UE█ J'ai entendu parler du GDPR de l'UE mais je n'en connais pas tous les détails█ Je n'ai pas entendu parler du GDPR de l'UE et je n'en connais rien | <ul style="list-style-type: none">█ Je connais assez bien le GDPR de l'UE█ J'ai entendu parler du GDPR de l'UE mais je n'en connais pas du tout les détails |
|---|--|



97 %

des personnes interrogées
ont entendu parler du GDPR

57 %

admettent connaître «peu»
ou «pas du tout» le GDPR

Rapport du Lloyd's: Faire face aux menaces cyber GDPR

Quelles sont les incidences que le GDPR est susceptible d'avoir sur votre entreprise?

64%

enquête
réglementaire

58%

sanctions financières
ou amendes

57%

impact sur les profits/
le cours des actions

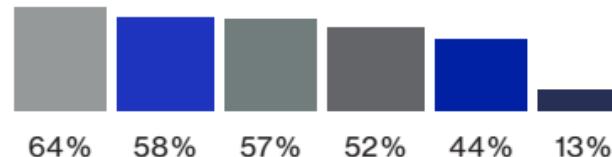
13%

perte
de clients

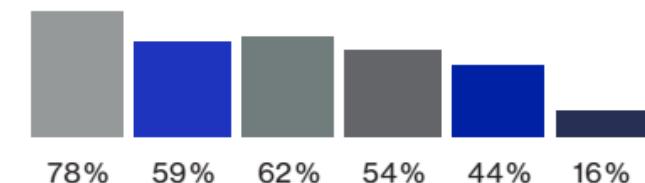
- Enquête par un organisme de contrôle
- Sanction financière/amende
- Impact sur les profits/le cours des actions

- Impact sur la marque/la réputation
- Réduction du temps de réponse
- Perte de clients

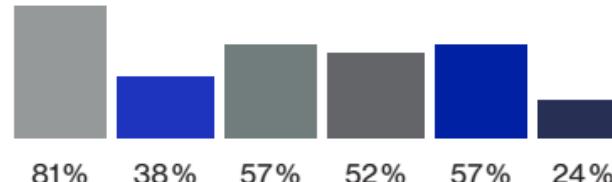
Total



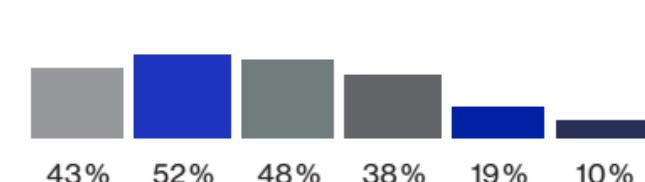
Royaume-Uni



France



Allemagne



Rapport du Lloyd's: Faire face aux menaces cyber

Conclusion

La question est de savoir « quand » et non pas « si » une entreprise va être victime d'un piratage informatique.

Il est donc essentiel de

- 1 Identifier les risques spécifiques auxquels vous êtes confronté**

 - 2 Informer sur la menace cyber et la réglementation dans toute votre entreprise**

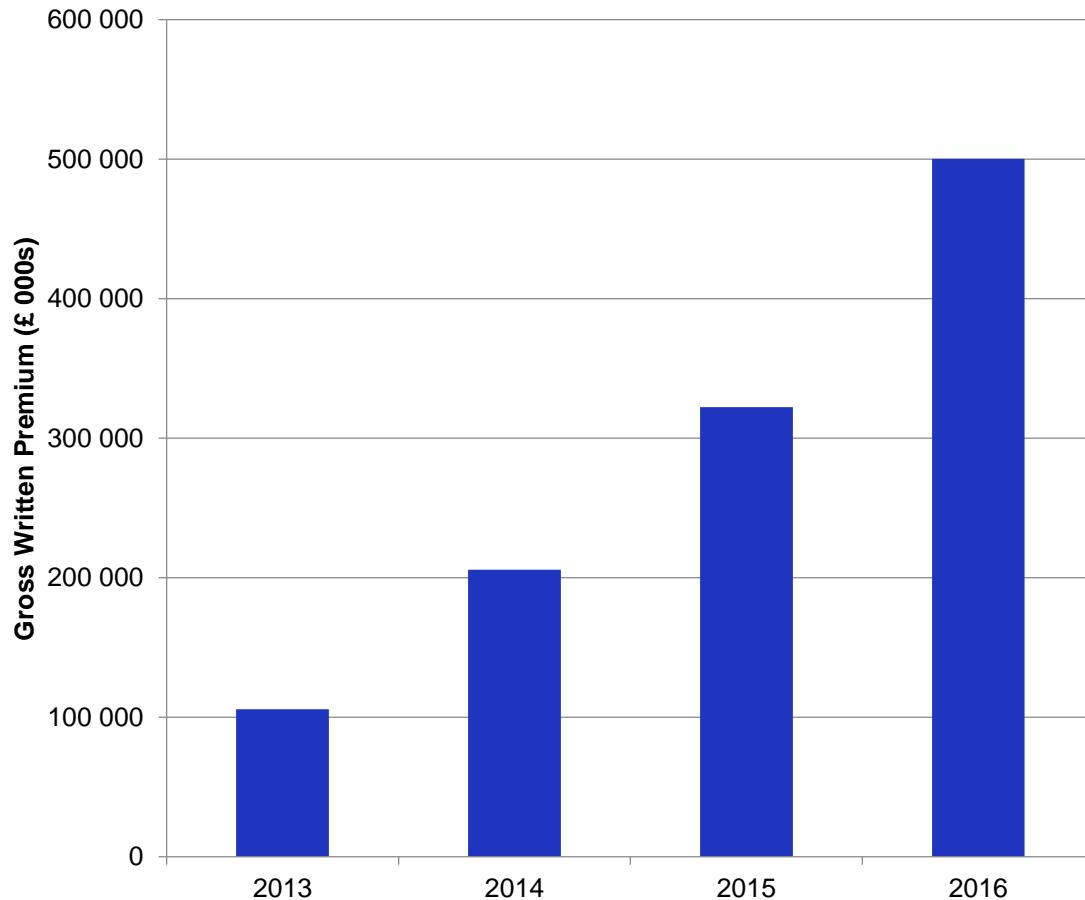
 - 3 Ne jamais cesser de se former sur le sujet**
-

Rapport du Lloyd's: Faire face aux menaces cyber

Conclusion : le rôle de l'assurance cyber

- 73 % des dirigeants d'entreprise ont une connaissance limitée de l'assurance cyber et 50 % d'entre eux ne savent pas qu'il existe des garanties en cas de fuites de données.
- L'assurance cyber donne accès à des **indemnisations** mais aussi des **conseils d'experts** afin d'améliorer la sécurité et l'assistance sur site pendant la période de crise.
- Les polices cyber couvrent généralement deux types de coûts : les coûts de l'enquête technique et juridique, ainsi que les coûts de communication aux clients et d'interruption des activités.
- Travailler avec des assureurs spécialisés est un **avantage pour la stratégie de l'entreprise**. En accompagnant les entreprises dès le départ, les assureurs les aide à réduire la probabilité d'une atteinte à la protection des données.
- L'assurance cyber contribue non seulement à la **protection des bilans de l'entreprise**, mais aussi à la **augmentation de la sécurité informatique** et à une **meilleure gestion du risque**.

L'assurance cyber au Lloyd's



77 syndicats en 2016

Environ 25% de l'assurance cyber mondiale est souscrite au Lloyd's

Capacité maximum par risque ~£500m

Modélisation et cumul de risques

- En terme de modélisation, utilisation de modèles Cat mais peu d'informations actuarielles.
 - En tant que marché, le Lloyd's a mis en place une procédure de déclaration des souscriptions pour le calcul de cumuls éventuels.
-

Estimation des capacités et budgets

Grands comptes

- Les produits d'assurance incluent de plus en plus d'assistance spécialisée
 - Certains grands groupes n'hésitent pas à avoir des franchises importantes
-

Innovation

Exemple de garantie innovante en matière de risque cyber:

Perte d'exploitation / perte de revenus suite à une malveillance chez un sous-traitant



Questions

LLOYD'S