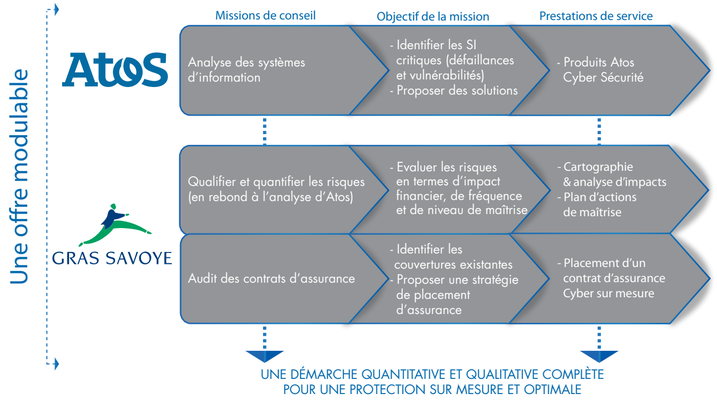
Gras Savoye & Atos, une nouvelle vision des Risques Cyber

Une réponse concrète aux Cyber Risques

Gras Savoye et Atos se sont alliés et ont conçu une offre complète, innovante, modulable avec pour objectif de VOUS proposer des missions de Conseil suivies de Prestations de services uniques sur le marché :



Bénéficiez d'une offre, de Conseil et de Services, qui s'articule autour de trois actions majeures :

- Apprécier les politiques de sécurité informatique
- Mesurer les enjeux financiers liés à une attaque ou intrusion
- Déterminer l'existence et le montant des garanties d'assurance en adéquation avec votre niveau d'exposition aux Risques Cyber

Nos experts sont à votre disposition pour vous informer sur notre nouvelle offre

GRAS SAVOYE | CONSEIL & COURTAGE EN ASSURANCES

Cyber Risques :
l'innovation au service des entreprises

Infos pratiques

Pour souscrire ou avoir plus d'informations, récupérez nos contacts proche de chez vous sur notre site internet **www.grassavoye.com**

Contacts

Laure Zicry
+ 33 (1) 41 43 51 82 - + 33 (6) 68 98 52 84
laure.zicry@grassavoye.com

Hervé Marzal
+ 33 (0) 1 41 43 53 11 - + 33 (6) 10 15 06 99
herve.marzal@grassavoye.com

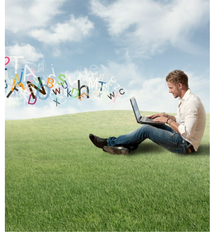
Gras Savoye et Atos : un partenariat stratégique pour prévenir, gérer et assurer les Cyber Risques.

GRAS SAVOYE

Société de courtage d'assurance et de réassurance
Siège Social : Immeuble Quai 33, 33/34 quai de Dion-Bouton, CS 70001, 92814 Puteaux Cedex. Tél : 01 41 43 50 00. Télécopie : 01 41 43 55 55. http://www.grassavoye.com. Société par actions simplifiée au capital de 1 432 600 euros. 311 248 637 RCS Nanterre. N° FR 61311248637. Intermédiaire immatriculé à l'ORIAS sous le n° 07 001 707 (http://www.orias.fr).
Gras Savoye est soumis au contrôle de l'ACPR (Autorité de Contrôle Prudentiel et de Résolution) 61 rue Taitbout 75436 Paris Cedex 9.

GRAS SAVOYE Willis
YOUR WORLDWIDE PARTNERS

La maîtrise du risque Cyber…
… un défi au quotidien !



Les enjeux auxquels vous êtes confrontés

Quelle entreprise aujourd'hui n'a pas son activité stratégique reliée à son Système d'Information ?

Les Systèmes d'Information font partie de notre quotidien et procurent des bénéfices mesurables :

- **Productivité, rentabilité…**
- **Parts de marché gagnées**
- **Temps de travail optimisé**
- **Stockage des données professionnelles et stratégiques**

Notre confiance dans les Systèmes d'Information est telle que les processus d'externalisation des données et l'ouverture aux nouvelles technologies se déploient de façon exponentielle. Ainsi toute l'organisation, le fonctionnement et les échanges d'une entreprise reposent sur un socle à multiples facettes :

L'entreprise est aujourd'hui confrontée à la nécessité d'un développement rapide des Nouvelles Technologies de l'Information pour développer son activité, et à la difficulté d'identification de l'ensemble des risques liés à ces NTI et de leurs conséquences financières.

Telle est la dichotomie à laquelle chaque entreprise doit faire face…

Avez-vous mesuré…
… les impacts financiers ?

Un défi au quotidien

Aujourd'hui, les entreprises sont la proie d'organisations criminelles qui, elles aussi, se sont adaptées pour tirer profit des failles des entreprises, pas toujours conscientes qu'elles sont des cibles ou que leurs données ont de la valeur !

La cybercriminalité, une réalité des temps modernes et aucune entreprise ne peut y échapper :

En 2013, ont subi une intrusion informatique : 78 % des grandes entreprises, 63 % des PME.

** Information Security Breach Survey 2013 (PWC & InfoSecurity)*

Grands comptes, ETI ou PME-PMI, les dirigeants doivent s'organiser pour faire face aux risques et aux conséquences des cyber-attaques.

La protection des systèmes d'information à 100 % n'existe pas

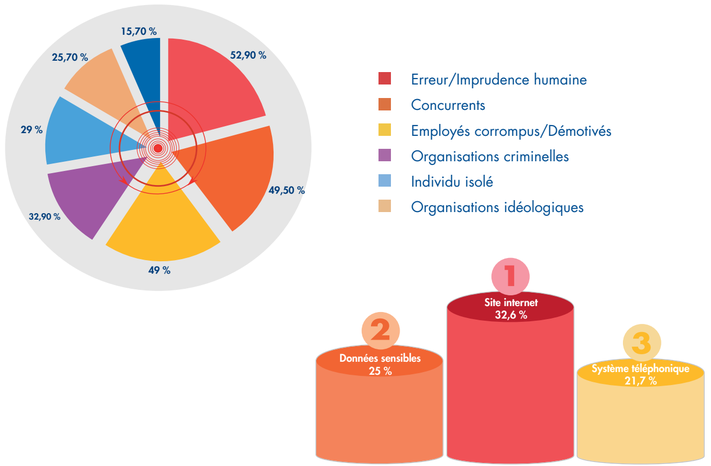
Ne sous estimez pas les impacts d'une attaque !

- **84% réussissent en moins d'une journée,**
- **28,3% ont un impact financier,**
- **25% ternissent l'image de l'entreprise.**

Des chiffres éloquents qui devraient interpeler, alors même que **84 % des dirigeants déclarent « avoir confiance dans l'efficacité de la sécurité informatique de leurs systèmes ».**

(Global State of Information Security Survey® 2014 • PWC)

Chiffres inquiétants lorsque nous savons que les menaces sont nombreuses tant au niveau DES AUTEURS QUE DES CIBLES



Autant d'enjeux de risques qu'il ne faut pas négliger, car leurs conséquences financières pourraient mettre en péril la pérennité des actifs de votre entreprise.

Une prise de conscience

- **44% des entreprises craignent d'être victimes d'un acte de cybercriminalité dans les 24 mois à venir [4]**

C'est pourquoi : 32,5% des entreprises ont pour projet de réaliser un audit de sécurité de leurs systèmes d'information à court terme et 33,5% d'entre-elles souhaitent renforcer la protection de leurs données*.

Il apparait clairement que le risque d'attaque n'est plus considéré comme un événement exceptionnel, mais un fait tangible et probable.

La question n'est pas de savoir si vous allez vous faire pirater….. mais quand !!!

Face à ce phénomène, les entreprises doivent mettre en place des actions concrètes : cartographie, audit des systèmes, calcul de l'exposition au risque…

En d'autres termes, les « cyber risques » doivent être intégrés dès aujourd'hui dans un processus de gestion des risques.

4 Global Economic Crime Survey (PwcC 2014)

** Enquête Usine Nouvelle – Orange Business Services réalisée en ligne du 11 au 19 décembre 2014*