Data | Insurance | Risk

CYBER-RISQUES & ASSURANCE

Conférence – Débat. Paris, le 08 Novembre 2016

Verbatim & Extrait des supports

COMETH CO CONSULTING

LES CYBER-RISQUES DANS L'ASSURANCE … AGENDA DÉTAILLÉ

Discours d'ouverture
David METHEL – Directeur Général, **COMETH Consulting**

Présentation des cyber-risques
Laure ZICRY – Responsable Institutions Financières et Cyber Risks, **GRAS SAVOYE**

Comment réagir face à une cyberattaque ?
Olivier CHOWANIAK – Directeur des Risques, **MUTUELLE FAMILIALE**

Les collecteurs de données face à la menace
Raimi ADET – Fondateur de la start-up **ACTUDATA**

Les solutions proposées par les assureurs
Pauline VACHER & Sophie PARISOT – Responsable Institutions Financières & Responsable Produits Cyber, **AIG**

LES CYBER-RISQUES DANS L'ASSURANCE

1- Discours d'ouverture et animation de la conférence
David METHEL, Directeur Général du cabinet **COMETH Consulting**

Verbatim – Ce qu'il faut retenir :

- *« En tant qu'assureur, vous êtes doublement concernés par les cyber-risques : d'une part en tant que cible privilégiée, et d'autre part en tant qu'acteur d'un nouveau marché à travers l'assurance cyber »*

- *« La donnée est le véritable moteur de la relation client individualisée. Toutes les données en lien avec les individus sont devenues une matière première très recherchée ; et les assureurs, de part leur activité, disposent d'un véritable actif dans leurs systèmes d'information. »*

- *« L'analyse des cyber-risques doit s'inscrire dans une stratégie globale des risques, incluant notamment une approche transversale au sein de l'entreprise, l'adhésion du COMEX et une forte sensibilisation des Collaborateurs et des Clients ».*

LE CYBER-RISQUE…UNE CROISSANCE EXPONENTIELLE

« L'ECONOMIE DU SAVOIR »

BIG DATA

Digital Marketing with specialty in Marketing Analytics

bitcoin

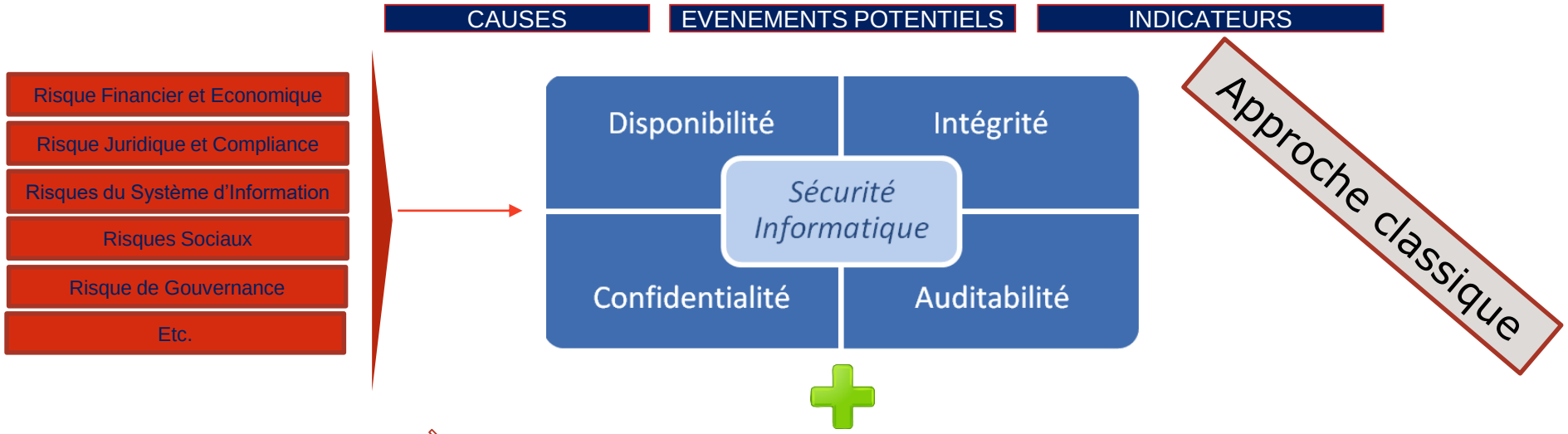
Cloud

The INTERNET of THINGS

BLOCKCHAIN

COMETH CO CONSULTING

LE CYBER-RISQUE…COMMENT S'EN PRÉMUNIR ?



- Politique globale de gestion des risques
- Approche transversale dans l'entreprise
- Identification dans la cartographie des risques
- Evaluation périodique plus rapprochée
- Mise sous contrôle des partenaires
- Contractualisation d'une assurance cyber
- Sensibilisation du COMEX, des Collaborateurs et des Clients

2- Présentation des cyber-risques

Laure ZICRY – Responsable Institutions Financières et Cyber Risks, **GRAS SAVOYE**

Verbatim - Ce qu'il faut retenir :

- *« Il existe une hiérarchie dans la valorisation des données sur le Dark web. Les données les plus recherchées sont les données médicales car elles sont rares et pour la plupart invariantes. »*

- *« En matière de cyber-risques, le risque zéro n'existe pas. »*

- *« En 2018, les entreprises connaîtront une forte montée en puissance des sanctions financières à travers le RGPD. Ces sanctions seront appliquées ou atténuées en fonction des dispositifs préventifs de sécurité déployées par les entreprises. »*

- *« Les arguments clés pour convaincre une DG d'investir dans la protection contre les cyberattaques sont la menace que cela représente pour le développement de l'activité, l'importance financière du risque règlementaire et l'engagement de la responsabilité civile personnelle du dirigeant. »*

Qu’entend-on par Cyber risques?

Définition : les conséquences d’une atteinte aux données numériques détenues et/ou gérées par l’entreprise, que celles-ci lui appartiennent ou qu’elles lui soient confiées par des tiers, ainsi que les conséquences d’une atteinte au système informatique.

Les atteintes aux données numériques

- **Vos données** nécessaires à l’activité,
- **Les données appartenant aux Tiers**,
- Les données de vos collaborateurs,
- Les données des clients,
- Les données des fournisseurs, sociétés partenaires…
- **L’atteinte à la réputation** : diffamation, atteinte à la protection de la vie privée, atteinte aux droits à l’image, atteinte aux droits de propriété intellectuelle d’un tiers

Les atteintes au système informatique

- **Intrusion** dans les systèmes informatiques,
- **Interruption** des systèmes informatiques.
- **Contamination** des systèmes (virus, bombe logique…)
- **Utilisation illégale** des systèmes et du réseau.
- **L’atteinte à la réputation** : pertes de chiffre d’affaires, atteinte à l’image de la société…

Impact du Règlement Général sur la Protection des Données pour l'entreprise : vos futures obligations dès Mai 2018

Avec le futur Règlement Général sur la Protection des Données (RGPD), toutes les entreprises européennes qui collectent, détiennent ou gèrent des données sur les citoyens de l'Union européenne devront respectées les obligations découlant du RGDP.

Vos obligations :

72h pour notifier à la CNIL les atteintes aux données

Notification individuelle à toutes les personnes concernées (clients, consommateurs, employés) s'il y a un risque pour les droits et libertés des personnes physiques.

Sanctions : 4% du CA ou 20 M€ en cas de manquement à leur obligation de sécurisation des données

Pourtant :

Seuls **52 %** des entreprises françaises sont inquiètes à l'idée de subir une fuite de données dans le futur.

alors que :

Seuls **24 %** des entreprises françaises croient qu'une atteinte à la sécurité des données risquerait de leur faire perdre des clients.

55 % des entreprises françaises ne savent pas qu'il existe des produits de cyber-assurance visant à fournir une couverture et des services aux entreprises qui subissent une atteinte à la sécurité des données.

GRAS SAVOYE
Willis Towers Watson

3- Comment réagir face à une cyberattaque ?
Olivier CHOWANIAK– Directeur des Risques, **MUTUELLE FAMILIALE**

Verbatim - Ce qu'il faut retenir :

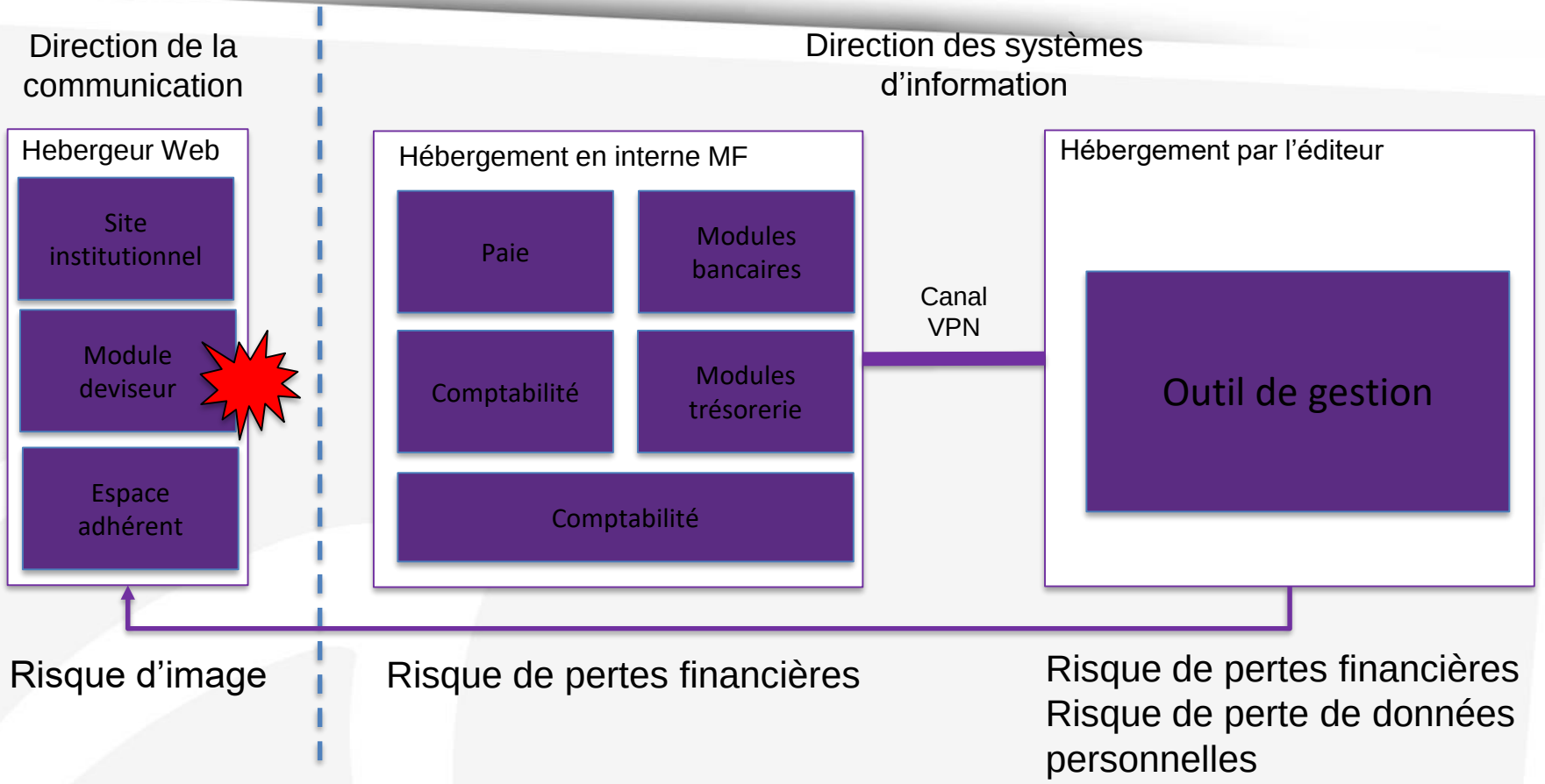
- *« On peut être une cible intéressante pour les pirates informatiques, même sans être une entreprise du CAC 40 ; l'important sont les données que vous possédez ! ».*

- *« Le cœur de notre activité assurantielle et nos données financières étaient bien protégés. L'attaque a eu lieu sur une activité considérée comme non sensible car nous pensions que le site Internet était limité à un risque d'image »*

- *« Désormais, nous pratiquons de manière systématique des audits de sécurité à chaque évolution de notre SI et nous pratiquons régulièrement des campagnes de sensibilisation auprès des collaborateurs de la mutuelle. »*

Une cartographie des risques simple

Cyberattaque



Conclusion

Le piratage informatique touche tout le monde et peut prendre plusieurs formes

- Ne pas sous estimer les probabilités de ce risque en fonction des pertes potentielles de l'entreprise – les motivations des pirates peuvent être multiples

- Risque à traiter globalement et non pas uniquement par l'informatique – l'alerte peut être levée par tout collaborateur et/ou un collaborateur peut être exploité pour s'introduire dans le système (par exemple cas des cryptolocker)

4- Les collecteurs de données face à la menace

Raimi ADET – Fondateur **ACTUDATA**, start-up spécialisée en analyse de portefeuille

Verbatim - Ce qu'il faut retenir :

- *« Notre plan marketing avait délivré beaucoup d'informations sur les réseaux sociaux. Cela a donc attiré les hackers qui recherchaient de la donnée à récupérer ; l'attaque a eu lieu dès le premier jour du lancement de notre site Internet. »*

- *« Notre activité nécessite la récupération et le stockage de données issues de différentes sources, y compris de nos clients, nous avons donc privilégié la sécurisation de notre infrastructure plutôt qu'une croissance trop rapide ».*

- *« Il faut que les assurances contre les cyber-attaques soient adaptées aux start-ups, c'est-à-dire, il faut privilégier les actions de prévention et d'audit préalable car les coût de réparation et de restauration suite à une attaque sont importants pour une TPE. »*

Etude de Cas
Attaque de type Injection SQL nor

Contexte de l'attaque : Injection de requêtes SQL www.actudata.fr

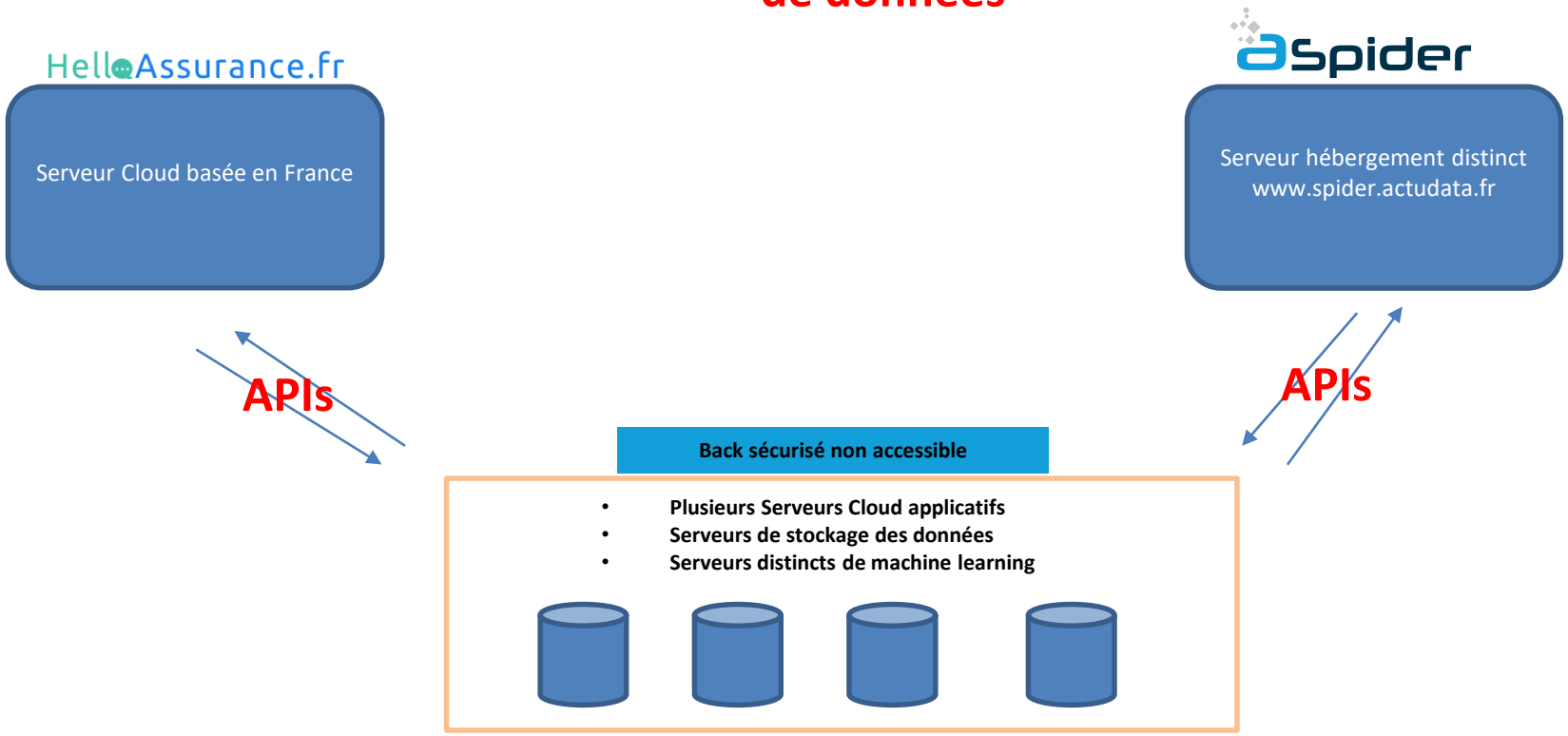
- En janvier 2016, lors du lancement de notre site web institutionnel www.actudata.fr , **plusieurs milliers de requêtes Sql** de remplissage automatique ont été effectué sur nos formulaire de devis
- Des **milliers de requêtes Sql** sur notre formulaire de devis actudata spider afin de récupérer la base de données des tarifs du marché
- **Objectif:** Nous soupçonnons que l'utilisateur pensait pouvoir récupérer accéder à nos bases de données clients ou tarifaires**.**

– ……

Etude de Cas
Exemple d'architecture de sécurité

Architecture de protection: cloisonnement + APIs

Règle fondamentale: séparation entre les applications et les bases de données



5- Les solutions proposées par les assureurs

Pauline VACHER & Sophie PARISOT – Responsable Institutions Financières & Responsable Produits Cyber, **AIG**

Verbatim - Ce qu'il faut retenir :

- *« Les produits d'assurance cyber se sont d'abord développés aux Etats-Unis, et ensuite quelques années après, en France. L'une des raisons est qu'aux Etats-Unis, les actionnaires ont la possibilité de lancer des « class action » à l'encontre des dirigeants en cas de suspicion de négligence. »*

- *« L'offre CyberEdge intègre un volet Prévention très complet incluant des services offerts et d'autres tarifés. Par exemple, il est possible d'effectuer un audit de la sécurité informatique de l'entreprise à distance. »*

- *« La prime d'assurance cyber est principalement évaluée selon le type de données à protéger, la localisation géographique de l'activité, la maturité de la sécurité informatique au sein de l'entreprise et selon la part d'acceptation du risque souhaitée par le souscripteur. »*

CyberEdge

Notre expertise à votre service

Prévention des risques cyber

CyberEdge® aide dans un premier temps à prévenir une cyber attaque, grâce à une multitude de services que nous vous proposons (scan de vulnérabilité, analyse de portefeuille, service de blocage des menaces...).

Coûts de récupération et de restauration des données/Pertes d'exploitation

Lorsqu'une atteinte à la sécurité se produit, nous vous aidons à informer et soutenir les personnes impactées, à gérer votre communication de crise, et déterminer ce qui est précisément arrivé. Nous prenons également en charge les frais de gestion et d'atténuation de l'incident Cyber et compensons les pertes et coûts d'exploitation liés à cette attaque.

Perte et coûts réglementaires des tiers

En cas d'attaque Cyber et suite à des réclamations de tiers ou fournisseurs, nous sommes à vos côtés. Une assistance est également fournie en réponse à toutes les actions réglementaires générées dans le cadre d'une violation, ou l'omission de dévoiler l'attaque.

Extorsion

Si un pirate informatique tente d'extorquer votre entreprise en menaçant l'accessibilité de votre réseau informatique ou en divulguant et détruisant des informations, nous pouvons vous aider. Nous dépêchons une équipe spécialisée dans la négociation de cas d'extorsion et prenons en charge les coûts associés suite à la menace et les frais d'enquête pour déterminer sa cause.

L'exposition médiatique en ligne

Si un contenu est divulgué par erreur sur le site Web d'une entreprise, nous la protégeons contre toute atteinte liée aux droits d'auteurs, à la contrefaçon, la diffamation, et l'atteinte à la vie privée.

Assistance d'urgence 24/7

Si une cyber-attaque ou une violation de données est considérée comme étant en cours, nous obtenons alors immédiatement le soutien technique d'un expert informatique. Nos experts sont disponibles 24 heures / 24, tous les jours de l'année, pour identifier immédiatement la menace (un pirate à l'intérieur d'un réseau, par exemple) et commencer la restauration et le processus de récupération des données dès que possible.

AIG

Exemples de sinistres

Perte d'ordinateur portable

Contexte: Un préposé de l'assuré a oublié son ordinateur portable contenant des données confidentielles non cryptées
Assurance: Prise en charge des frais d'expert informatique, de restauration des données et d'assistance juridique
Coût: 25.000 €

Perte d'exploitation

Contexte: Des hackers mettent hors service le site internet de vente en ligne qui représente 80% du chiffre d'affaires

Assurance: Prise en charge des frais d'expert informatique, de la perte de chiffre d'affaires sur la période d'arrêt du site et les honoraires du consultant en gestion de crise
Coût: 110.000 €

AIG

COMETH CO CONSULTING

Data | Insurance | Risk

Pour en savoir plus, n'hésitez pas à nous contacter :

94 rue de Courcelles 75008 Paris

Tél : 01 40 54 83 81

E-mail: contact@cometh-consulting.com

www.cometh-consulting.com