« CyberClear» by Hiscox, en bref

- **Hiscox, acteur leader dans l'assurance des risques informatiques :**
  Hiscox met à la disposition des professionnels français :
  - Une **expérience de 30 ans** dans le domaine des risques liés aux **technologies de l'information**
  - Un **recul de 7 ans** dans le domaine des **risques liés à la cybercriminalité** aux États-Unis (précurseurs en la matière).

- **Le contrat « CyberClear », c'est :**
  - Un **contrat d'assurance complet** qui vise à protéger l'entreprise contre les conséquences d'une cyber-attaque pour elle-même et pour des tiers.
  - Une **offre globale de services**, qui s'appuie sur un **réseau d'experts à la disposition des entreprises**, destinée à protéger les entreprises contre les risques liés à l'intégrité de leurs systèmes d'information et des données à caractère personnel et/ou sensibles, dont elles sont responsable.
  - Un moyen pour l'entreprise de **préserver** sa réputation et la pérennité de son activité **face aux menaces** que représentent les attaques de cyber-pirates ou l'imprudence de ses propres employés.

- **Le contrat « CyberClear» propose :**
  - Un **accompagnement pour prévenir et sensibiliser** les entreprises face aux risques liés à la gestion des données et à l'intégrité des systèmes d'information :
    - Audit possible des systèmes d'informations pour vérifier le niveau de sécurité
    - Publication régulière de documents d'aide à la prévention (livres blancs, livrets thématiques, articles)
    - Accès gratuit à notre solution d'information globale sur la protection des données personnelles via notre portail de ressources dédié (Hiscox eRisk HubTM)

  - Un engagement de services : la **mise en œuvre d'une réponse dans les 48 heures** en cas de sinistre, avec intervention immédiate d'un réseau de spécialistes, pour gérer au mieux les conséquences de l'incident, et ce quelle que soit la taille de l'entreprise assurée – notamment :
    - **Experts informatiques** pour déterminer l'origine de l'attaque, la circonscrire, identifier les données impactées, réparer la faille et mettre à jour le système,
    - **Avocats**, pour gérer les mises en causes et réclamations des régulateurs et des tiers,
    - **Spécialistes de la communication de crise**, pour contrôler les conséquences de l'attaque sur la réputation de l'entreprise (plans de communication dédiés, formations des porte-paroles…),
  - La **prise en charge en cas de sinistre** des frais engagés par l'entreprise (notification des attaques, négociation en cas de cyber-extorsion, remise en service des systèmes informatiques), de la perte de revenus qu'elle peut avoir subie, des sanctions assurables prononcées contre elle et des dommages et intérêts qu'elle peut être amenée à payer aux tiers dont les données ont été compromises.

- **Le contrat « CyberClear » couvre toutes tailles d'entreprises**, de la TPE/PME aux grands comptes (jusqu'à un milliard de chiffre d'affaires), avec une capacité maximum de **10 millions d'euros par sinistre et par an**, dans le **monde entier.**

- **Les appétits Hiscox « CyberClear » :**

Ce que nous couvrons (notamment)	Ce que nous ne couvrons pas
Métiers du tourisme	Banques, assurances et courtiers
Commerce de détails (y compris e-commerce)	Compagnies aériennes
Médias et marketing	Réseaux sociaux
Secteur de la santé	Paris et jeux d'argent
Métiers de l'informatique et télécommunications	Marketing direct
Professions du conseil : avocats, experts comptables…	Partenaires Hiscox

Enjeux sectoriels et risques majeurs

- **Une menace réelle avec la professionnalisation des cyber-attaques :**
  - **Industrialisation des attaques** avec automatisation de leurs processus et diminution des coûts.
  - En moyenne, il faut compter **plus de 150 jours pour détecter** une cyber-attaque[1].

- **Cela peut arriver à toutes les entreprises :**
  - Plus de **90% des entreprises** ont subi une cyber-attaque au cours des 12 derniers mois[2].
  - **88%** des virus fabriqués sur-mesure par les hackers ne sont **pas détectés par les anti-virus[3].**
  - **33%** des violations de données sont dues à l'**imprudence des employés** (vol, pertes d'appareils, etc.)[4].

- **Le risque principal : la non-assurance**
  - Un hacking **coûte cher : 351€**[5] par donnée piratée, jusqu'à 6M€ par violation de données.
  - **20% des entreprises piratées** ont subi des **pertes financières** (CA ou réputation).
  - Le hacking doit donc être **intégré dans la politique de gestion des risques d'une entreprise**, au même titre que l'incendie ou l'accident du travail.

- **La nouvelle réglementation européenne sur les données personnelles**
  - Le Règlement européen sur la protection des données personnelles (GDPR) du 27 avril 2016, qui entrera en vigueur en mai 2018, étend l'obligation de **notifier aux individus concernés et au régulateur** une violation de données personnelles à l'ensemble des entreprises, tous secteurs d'activité confondus.
  - Les **sanctions que la CNIL ou ses homologues européens pourront prononcer contre les entreprises** passent du montant actuel de 150.000€ (300.000€ en cas de récidive) à 10 millions d'euros / 2% du chiffre d'affaires mondial, voire 20 millions d'euros / 4% du chiffre d'affaires mondial.

Les porte-paroles

- **Astrid-Marie Pirson** – Responsable de marché Informatique et Cyber France
- **Louis Daviault** – Directeur Sinistres Hiscox France

Cas pratiques

- **Exemple de prime Hiscox:**

  Une entreprise de Telecom d'un CA de cent millions d'euros devrait payer, **après analyse de ses risques**, une prime d'environ 50.000 euros pour une garantie de cinq millions d'euros par sinistre.

- **Exemple de sinistres Hiscox :**

	Vol dans un bureau d'une association caritative d'un laptop contenant les données bancaires d'une centaine de donateurs	Vol par une employée des 45.000 données médicales et personnelles de patients pour les revendre
Montant total du sinistre	**76 000 €**	**305 000 €**
Frais de notification	49 000 €	42 000 €
Expertise informatique	17 000 €	5 000 €
Surveillance des numéros de CB (1 an)	8 500 €	220 000 €
Relation presse – image de marque	1 500 €	38 000 €

[1] Etude Trustwave 2012
[2] Etude Kaspersky 2013
[3] Etude TrustWave 2012 (18 pays étudiés dont la France)
[4] Étude Symantec 2012 (données françaises)
[5] Étude Symantec Mars 2014 (données françaises)

Q&A

- **Que couvre « CyberClear » ?**
  - **La réparation des dommages causés à l'assuré** par une cyber-attaque (coûts de notification, pertes de revenus, cyber-extorsion, pénalités PCI-DSS),
  - **La réparation des dommages causés à des tiers** du fait d'une violation de données personnelles subie par l'assuré,
  - **Les coûts de recours au réseau de spécialistes** d'Hiscox en cas de sinistre,
  - **Les coûts et conséquences d'enquêtes administratives** (CNIL ou équivalent),
  - Sur option et sous certaines conditions, la **cyber-fraude** et le **piratage de lignes téléphoniques**.

- **Pourquoi la certification PCI DSS est-elle un critère de qualité pour la sécurité des données ?**
  - Le **Payment Card Industry Data Security Standard** (PCI DSS) est un standard de sécurité des données pour les industries de carte de paiement créé par le comité PCI DSS pour les entreprises acceptant les transactions cartes bancaires. Il s'agit en réalité d'un guide de 12 règlements qui aident les entreprises émettrices de cartes de paiement **à protéger leurs données et à prévenir les fraudes.**
  - Les **membres fondateurs** sont American Express, Mastercard, Visa Inc, DFS, JCB International.
  - Il s'agit d'un **standard de qualité d'origine américaine, non obligatoire** mais devenu une référence mondiale. Il permet de s'assurer que les entreprises se conforment des normes de sécurité et de protection de leurs données, qui limitent les conséquences d'un incident et pourront, par exemple, leur permettre d'avoir des frais de notification ou des pénalités moindres.

- **Pourquoi faut-il crypter les données sensibles ?**
  - Le cryptage est un processus d'encodage de données, qui permet de **garantir que seules les parties autorisées peuvent les déchiffrer**. Il s'agit d'un processus très utilisé, par exemple pour les transactions financières en ligne : dans ce cas, une icône « cadenas » apparaît normalement dans la barre d'adresse web, ce qui signifie que la session du navigateur est cryptée.
  - Il s'agit d'un **élément essentiel dans l'appréhension et la bonne gestion des cyber-risques** : une violation de données cryptées est beaucoup moins onéreuse que dans le cas où les données compromises ne sont pas protégées – c'est aussi l'un des critères de déclenchement (ou non) de l'obligation de notification de chaque individu en cas d'incident.

- **Quelques questions à poser à vos clients :**
  - Connaissez-vous le **niveau de sécurité mis en place chez vos prestataires** pour protéger vos données ?
  - Connaissez-vous votre responsabilité quant aux **paiements par cartes bancaires** que vous acceptez ?
  - Savez-vous ce que vous devez faire en cas de **violation de données** pour en limiter les conséquences ?
  - Si **votre site internet est inaccessible pendant 2 jours**, comment gérez-vous vos ventes en ligne ?
  - Etes-vous en conformité avec les **standards et normes réglementaires** qui vous sont applicables ?
  - Savez-vous **à quel interlocuteur faire appel** en cas d'incident de cyber-sécurité ?

- **Quelle est la différence entre assurance RC Pro et cyber-assurance ?**

RC Pro	La responsabilité d'une entreprise peut être engagée en cas d'erreurs, d'omissions, d'oublis ou de négligences **dans l'exécution d'une prestation.** C'est dans ce cadre, qu'intervient l'assurance responsabilité civile professionnelle.
	Elle a pour objet de couvrir l'entreprise pour les conséquences pécuniaires qu'elle encourt du fait des dommages causés à des tiers **lorsque sa responsabilité est avérée**.
Cyber-assurance	La responsabilité de l'assuré est engagée **suite à l'utilisation par des tiers de données personnelles et/ou sensibles dont il avait la charge ou la garde** (responsable du traitement), que ces données soient sur un réseau, un serveur, une clé USB ou dans un dossier papier (ceci étant généralement exclu des contrats RC en l'absence de faute de sa part).
	Les **garanties** couvrent également les **dommages subis par l'entreprise elle-même**, ainsi que les frais d'expertises, de notification, de défense, d'upgrade de sécurité, d'extorsion, ou encore de maintien de réputation.