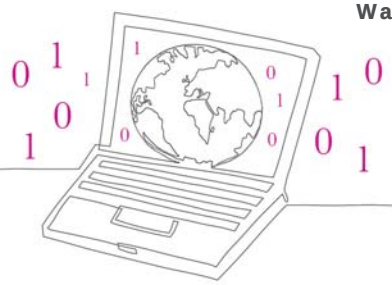
“Il faut 20 ans pour construire une réputation et

5 minutes pour la détruire”

Warren Buffett



Notre experience

- Presence aux Etats-Unis depuis 2004 (marché précurseur)
- Plus de 3.000 polices en portefeuille
- Plus de 1000 ‘data breach’ gérés
- Gestion des data breach : 80% de notre indemnisation

Pourquoi :

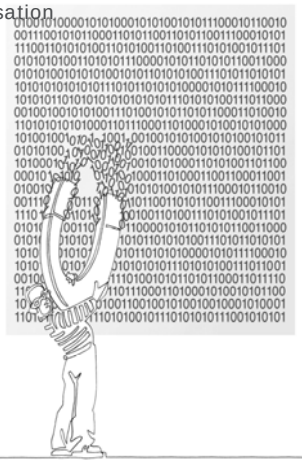
- Dématérialisation des données
- Recours aux nouvelles technologies

Evolution des risques :

- Cyber criminalité
- Facteur humain

Impacts :

- Evolution du contexte législatif
- Conséquences financières
- Impact sur la réputation



beazley

Les opérateurs d'importance vitale

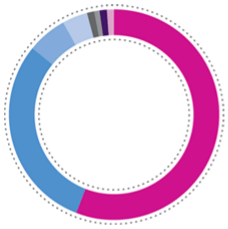
- **Définition Art. L1332-1 du Code de la Défense :** «*Les opérateurs publics ou privés (…) dont l'indisponibilité risquerait de diminuer d'une façon importante le potentiel de guerre ou économique, la sécurité ou la capacité de survie de la nation, sont tenues de coopérer à leurs frais (…) à la protection desdits établissements, installations et ouvrages contre toute menace, notamment à caractère terroriste* ».
- **Désignation par l'Autorité Administrative compétente (désignée par Décret 2006-212 du 23 avril 2006)**
- **Le « Plan Particulier de Protection », Art. L1332-3 du Code de la Défense** : «*Ces mesures comportent des dispositions efficaces de surveillance, d'alarme et de protection matérielle* ».
- **Procédure contraignante pour forcer l'OIV à respecter le Plan Particulier de Protection :**
  - **Mise en demeure, Art. L1332-4 du Code de la Défense :** « *En cas de refus des opérateurs de préparer leur plan particulier de protection, l'autorité administrative met, par arrêtés, les chefs d'établissements ou d'entreprises assujettis en demeure de l'établir dans le délai qu'elle fixe* ».
  - **Sanctions pénales, Art. L1332-7 du Code de la défense :** 150.000€ d'amende même envers les dirigeants qui auraient « *omis d'entretenir en bon état les dispositifs de protection* ».

Les opérateurs d'importance vitale

- **La Loi de Programmation Militaire 2014-2019 :** Débat parlementaire devant l'Assemblée Nationale, suite de la discussion générale en 2ème séance le 27 novembre 2013.
- **Orientation OIV / Risques Cyber :**
  - Le Premier Ministre fixera les règles de sécurité nécessaires à la protection des systèmes d'information des OIV.
  - Information « sans délai » des OIV au Premier Ministre des incidents survenus (Art. 1333-13 Code de la Défense)
  - Contrôle des systèmes d'information et de leur niveau de sécurité effectué par l'ANSSI
- **Nouvelle sanction pénale** (amende de 150.000€) étendue à la personne morale complice du dirigeant (Art. L1332-7 du Code de la Défense)
- **Place de l'assurance :** élément naturel du plan de prévention

D'où viennent les risques ?

Cas de pertes de donnees



Piratage et attaques malveillantes (attaques venues de l'extérieur, attaques malveillantes ou logiciels espion)	56%
Périphérique amovible (perte, disparition ou vol d'ordinateur portable, tablette, smartphone, clé USB, CD, disque dur, cartouches de données, etc.)	30%
Menace interne (personne disposant légitimement des accès et détournant intentionnellement les informations, comme par exemple un employé, sous-traitant, etc.)	6%
Divulgation non-intentionnelle (information sensible mise en ligne ou rendue publique sur internet, ou email, fax, courrier envoyé au mauvais destinataire.)	4%
Périphérique non-amovible (perte, disparition ou vol de périphérique non-amovible, tel qu'un serveur ou une unité centrale.)	1%
Fraude à la carte bancaire (fraude impliquant des cartes de crédit ou de débit, (hors hacking) par le biais de terminaux compromis)	1%
Perte physique (vol, perte ou disparition de documents non-électroniques, tels que des documents papiers.)	1%
Autre raison ou raison inconnue	1%

Source: Privacy Rights Clearinghouse, 10/18/2012

beazley

Chiffrer l'impact

•Plus de 21 Millions d'individus auraient été affectées par une perte de données dans le secteur de la santé *(Office of Civil Rights, organe dépendant du Ministère de la Santé et des Services Sociaux Américain – 2009)*

•70% des Européens s'inquiètent d'une utilisation abusive de leurs données personnelles *(Eurobaromètre 2012)*

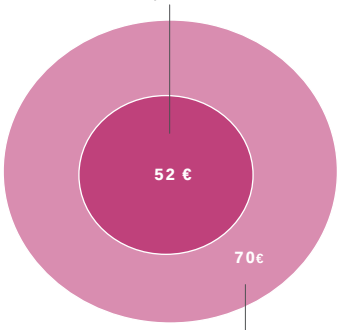
•19,7 Millions de données ont été vendues illégalement en ligne au premier semestre 2012 *(Experian)*

•Plus de 500 Millions d'individus affectés *(Privacy Right Clearinghouse)*

•Sur les deux dernières années, les attaques ciblées ont globalement augmenté de 42% mais ont plus que doublé pour les PME de moins de 250 salariés *(Symantec)*

•122 € serait le prix d'une donnée perdue

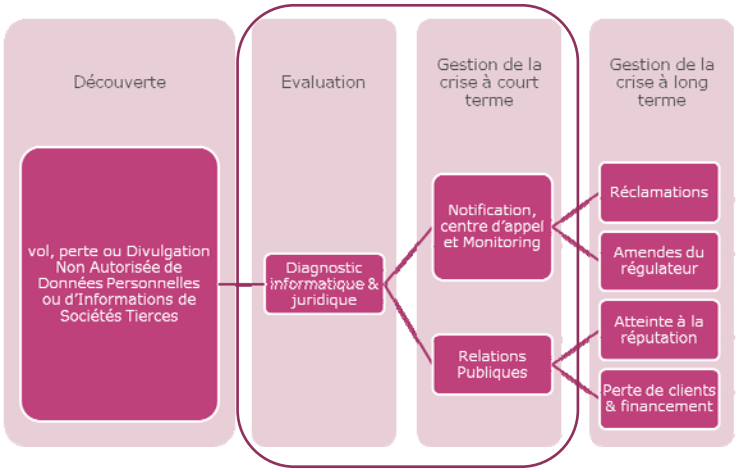
Pertes Directes
- o Notification
- o Centre d'appel
- o Identity Monitoring
- o Forensics
- o Reconstitution
- o Temps de travail



© Ponemon Institute 2011

Pertes Indirectes
- o Mesures correctives
- o Réclamations
- o Amendes
- o Perte de clients
- o Perte de financement

Transfert de la gestion de la crise



Conclusion : le service avant tout