Atelier B2

Digitalisation : quels impacts sur le profil de risque de l'entreprise ?

Atelier B2

Digitalisation : quels impacts sur le profil de risque de l'entreprise ?

Intervenants

Marc AYADI	EY	**Cyber (Security, technology and Data) leader for Western Europe and Maghreb**
Julien BLANCHEZ	Google	**Global Security & Compliance Strategist**
François BRISSON	Swiss Re Corporate Solutions	**Head Tech Cyber**

Modérateur

François BEAUME	BUREAU VERITAS	**Director, Risk and Insurance**

La Digitalisation, c’est quoi ?

Une définition ?

« La digitalisation est l'intégration des technologies digitales dans la vie de tous les jours par la numérisation de tout ce qui peut être numérisé. »

Un changement sociétal majeur

« La digitalisation représente la troisième révolution anthropologique majeure »

Michel Serres, membre de l'académie française, professeur à Stanford

1. **Passage de la transmission orale à l'écrit (-4 000 av JC)**
2. **Invention de l'imprimerie (XVéme siècle)**
3. **Digitalisation (XXI éme siècle)**

Pour l'Entreprise ?

Une opportunité

Numériser son offre et toute la chaîne de création de valeur

Des risques

Un environnement qui devient dynamique

Moins de contrôle des flux d'information la concernant

Une accélération du cycle d'innovation

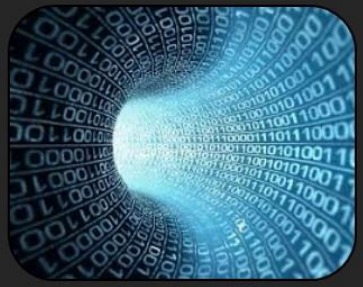
…/…

Stratégie

Sécurité, quel est le contexte actuel ?

La « digitalisation » modifie en profondeur les interactions avec les partenaires, les clients et les processus internes de l'entreprise

La sécurité des systèmes d'information et la protection de l'information ne peut pas être correctement appréhendée si on ne prend pas en compte les mutations profondes qui ont actuellement lieu : stratégie digitale, évolutions des usages, ruptures technologiques, etc.



Dans les trois prochaines années, le nombre d'utilisateurs de réseaux sociaux dans le monde dépassera 2,5 milliards

27%

27% du temps passé sur internet l'est sur les réseaux sociaux

De plus en plus de personnes se connectent pour la première fois chaque jour, développant la capacité d'innovation

217

Nouveaux usagers se connectent à l'internet mobile toutes les minutes *

Le nombre d'appareils connectés croît chaque jour et génère un volume de données gigantesque

50mds

d'objets connectés d'ici 2020, incluant capteurs, puces RFID, etc. **

La vitesse du changement ne faite que croitre, et de plus en plus vite

16

Nombre de jours pour Google Plus pour atteindre 10m de personnes ***

** Source: Ultralinx, **Source: Ericsson Vision 2020, ***Source: Google*

Evolution des menaces et des réponses aux menaces

La digitalisation, l'arrivée massive des objets connectés, l'évolution des réglementations et l'explosion de la cybercriminalité sont autant de facteurs qui contraignent les entreprises à faire évoluer leurs systèmes de protection.

1970	>1980	>1990	> 2000	> 2010
- Faire face aux dangers naturels - Mise en place de mesures concrètes (évacuation, premiers soins) - Recours à une assistance externe	- Recours à un nombre restreint de technologies émergentes - Récupération simple après une défaillance des systèmes	- Apparition de la gestion des risques dans l'ensemble de l'organisation - Généralisation de la conformité réglementaire - Plan de continuité d'activité - Développement des protections contre les virus	- Progrès en information et cybersécurité - Passage au 100% en ligne - Connexion de dispositifs - Management des identités et des accès	- Chocs globaux (terrorisme, changement climatique, crises politiques) - Externalisation avec des tiers (exemples : le cloud) - Résilience économique - Objets connectés - Infrastructures critiques - Cyberespionnage et cyberattaques menées par des Etats tiers
Unités centrales	**Client / serveur**	**Internet**	**E-commerce**	**Digital**

Au devant de la scène..

Le digital dans un contexte sensible très particulier

Médiatisation des incidents sécurité

- Une pression médiatique et légale,
- Un niveau de tolérance zéro sur la protection des données personnelles.

La sécurité comme argument commercial

- Nécessité d'un dispositif fiable et transparent à destination des partenaires.
- Essor des certifications des processus de contrôle interne (ISAE3402, SOCx) et organisations (ISO 27001).

Augmentation continue de l'exposition et des menaces

- Evolution permanente du profil d'exposition au risque de l'entreprise.
- Déploiement imposé des nouvelles technologies, des média sociaux et des solutions de mobilité.

Une implication de plus en plus pressante des métiers

- Transfert de la gouvernance du SI vers les métiers lié au changement de modèle des DSI (Cloud computing, mobilité …).
- Perte de maitrise des frontières et de la mise en œuvre des mesures de sécurité.

Un renforcement des textes réglementaires

- Professionnalisation de la filière de contrôle IT au sein des DSI, Directions de l'Audit Interne, Directions des Risques et Inspections Générales.
- Fortes attentes autour de la protection des données : Accès, disponibilité, confidentialité, traçabilité.

LA CYBER-CRIMINALITÉ FAIT PARTIE DU QUOTIDIEN - AVEC LE DIGITAL ENCORE PLUS


Les États-Unis secoués par le piratage géant de données chez Target

TECH & WEB > TECH & WEB Par Robin Korda | Mis à jour le 13/01/2014 à 18:05 | Publié le 13/01/2014 à 12:33


Cyber-sécurité : le smartphone, nouvelle cible de choix des attaques

SCIENCES AVENIR Par Sciences et Avenir avec AFP Voir tous ses articles | Publié le 29-02-2016 à 08h00 | A+ A-

44% des organisations ont le sentiment d'être vulnérables à cause de salariés non sensibilités

(Source : EY Global Information Security Survey 2015)

82 secondes suffisent à une campagne de phishing pour avoir un premier clic

(Source : Data Breach Investigations Report 2015)


Cybersécurité : les hackers-braqueurs ont les banques dans le collimateur


Piratage de TV5 Monde: une facture très salée

15/10/2015 à 06h12

317 millions de nouveaux programmes malveillants ont été créés en 2014

(Source : Symantec Internet Security Threat Report 2015)

5 grandes entreprises sur **6** ont été la cible d'une attaque en 2014

(Source : Symantec Internet Security Threat Report 2015)

92% des outils connectés à Internet sont vulnérables aux failles connues

(Source : Cisco 2016 Annual Security Report)


Les erreurs de Sony face à un piratage de données "sans précédent"

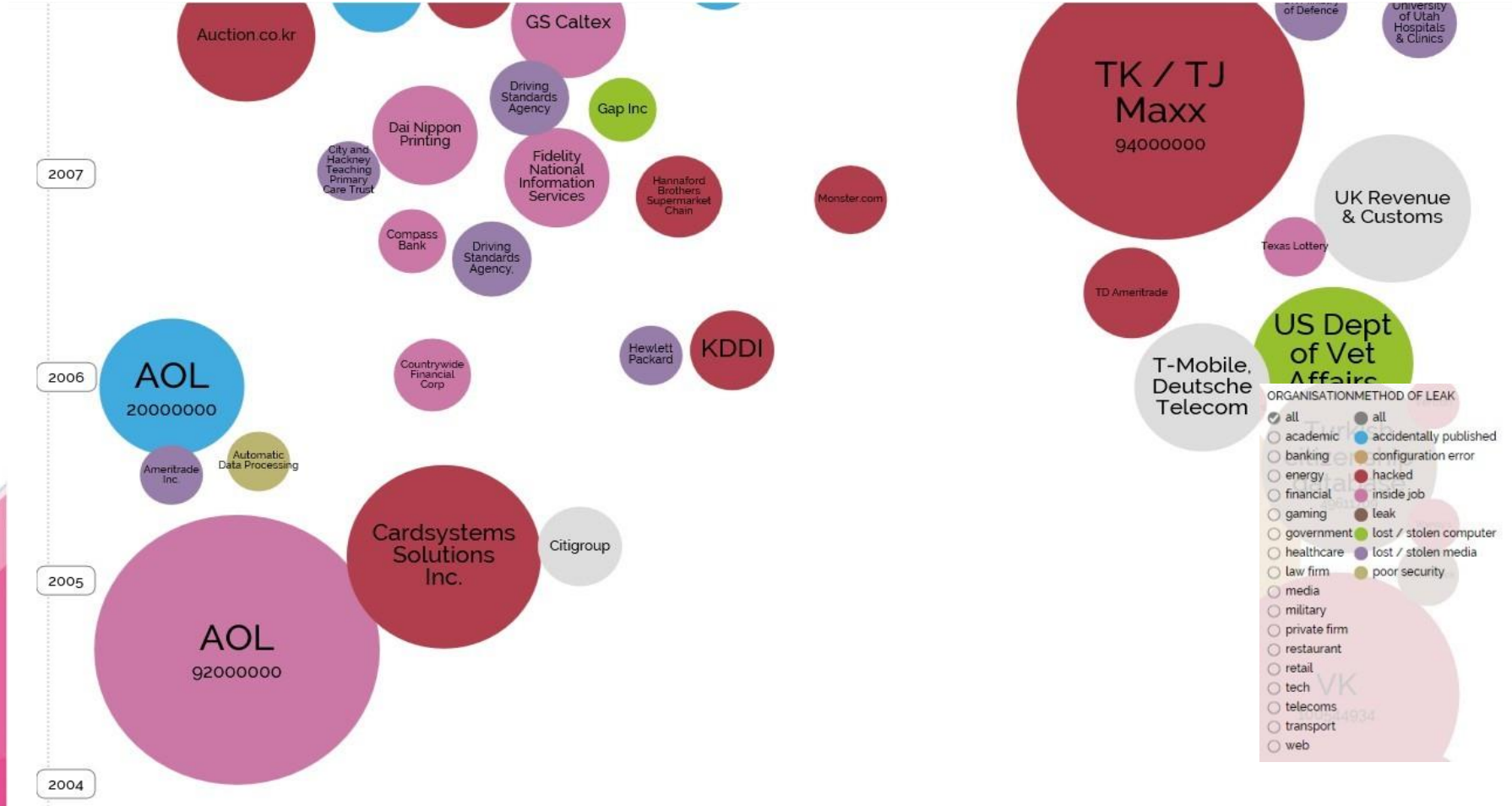
Les nouvelles formes de menaces

Des attaques de plus en plus sophistiquées … et organisées exploitant les nouvelles failles

1. **Les fuites de données sont inévitables**
2. Le cyber-espionnage continue et devient l'apanage d'Etat
3. Attaques DDOS via IOTs
4. Les logiciels malveillants sur mobiles continuent d'augmenter
5. Le phishing basé sur la collecte d'informations personnelles explose (spear phishing)
6. Les attaques par ingénierie sociale sont utilisées sur les réseaux sociaux
7. Les réseaux de zombies (machines piratées) infiltrent toujours les entreprises
8. Les notifications en cas de fuite de données deviennent la règle
9. Les infrastructures essentielles sont des cibles
10. Le code source des applications est analysé et toutes les vulnérabilités mises à nu

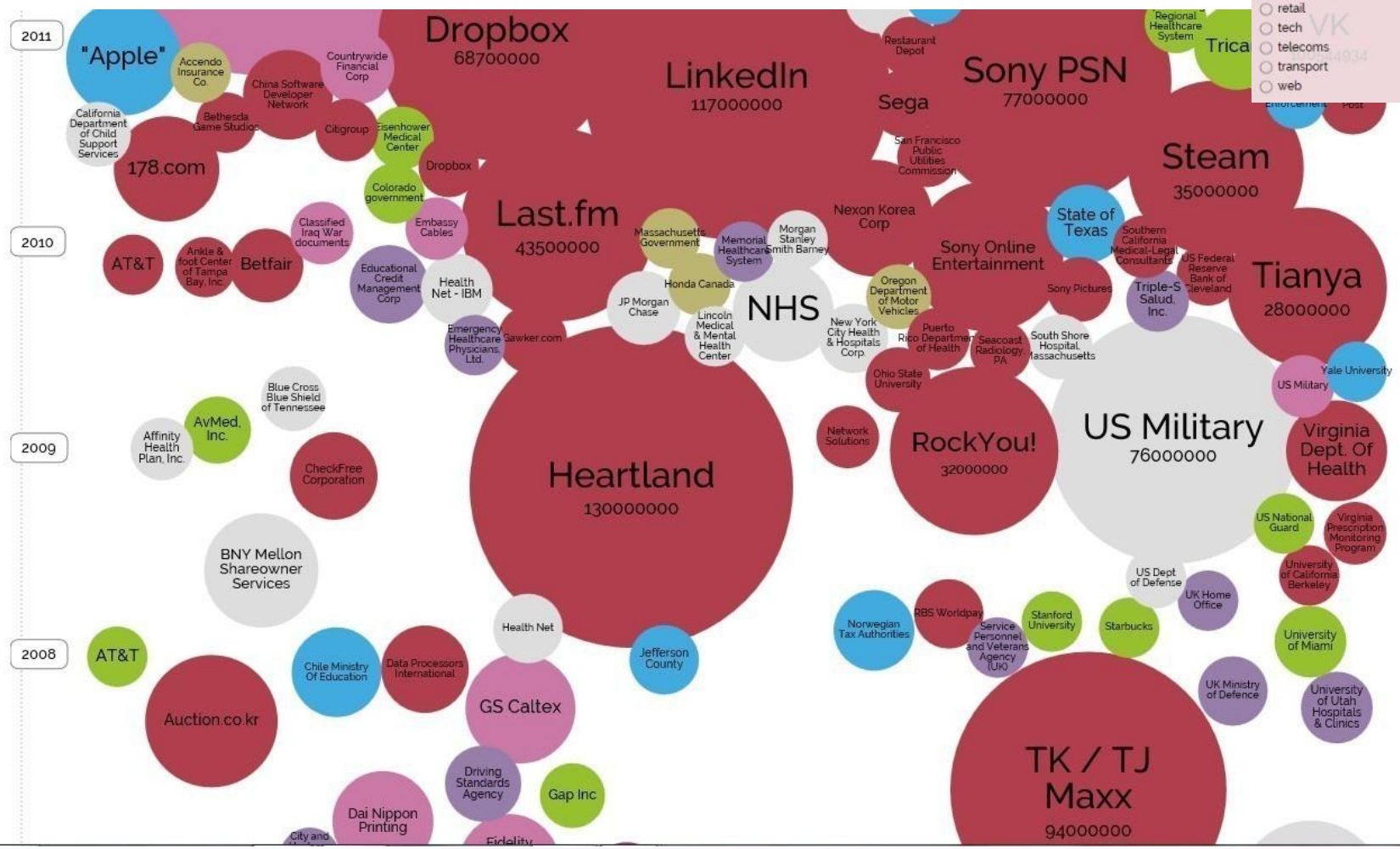
Les plus grosses fuites de données recensées à juillet 2016

Plutôt rares entre 2004 et 2008



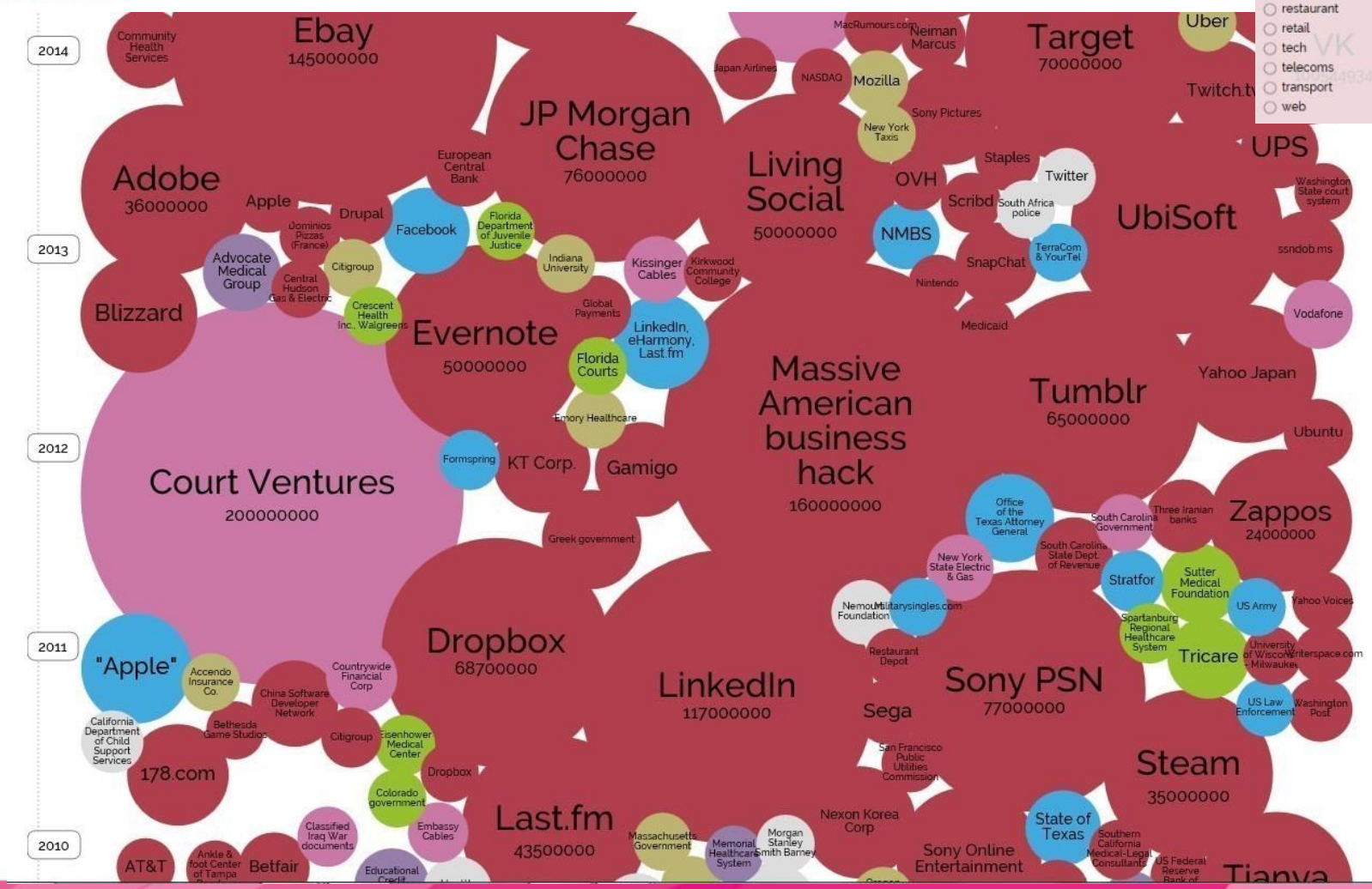
Les plus grosses fuites de données recensées à juillet 2016

Une accélération entre 2008 et 2011



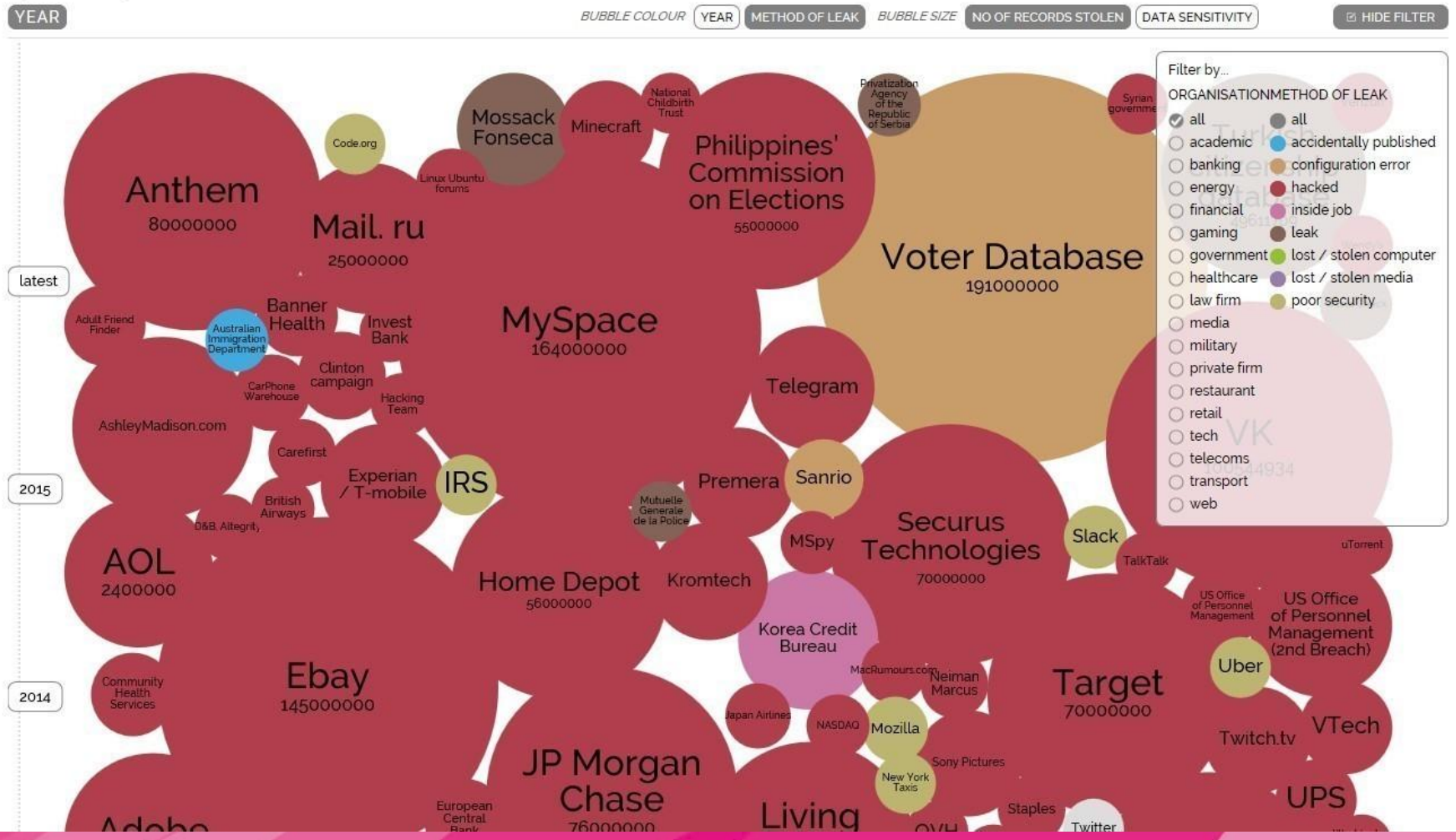
Les plus grosses fuites de données recensées à juillet 2016

Une explosion depuis 2011



Les plus grosses fuites de données recensées à juillet 2016

Des volumes de données de plus en plus importants



SE POSER LES BONNES QUESTIONS

La cyber-sécurité est l'affaire de tous – plus encore maintenant

*« Mon ordre du jour est **surchargé** »*

*« Cela relève de **l'informatique** »*

*« Ce n'est pas **notre problème** »*

*« C'est trop **technique** »*

*« Les risques sont difficiles à **évaluer** »*

*« Le retour sur **investissement** est difficile à percevoir »*

*« Notre sécurité est-elle centrée sur la **protection des actifs** qui génèrent du **revenu** ? »*

« Comment mesurer l'efficacité de notre programme de sécurité ? »

*« Nos investissements sécurité permettent-ils de couvrir nos **risques** et sait-on **anticiper** les nouvelles menaces ? »*

*« Comment notre sécurité prend t-elle en compte les **évolutions** de notre "operating model" et de notre écosystème SI »*

*« Notre dynamique de projets sécurité est-elle **adéquate** ? A-t-on le bon **rythme** et la bonne **priorisation** ? »*

CRÉER UNE STRATÉGIE CENTRÉE SUR LA PROTECTION DE L'INFORMATION

« La sécurité périmétrique va me permettre de protéger mes applications et mes services »

Il est vital de faire évoluer la stratégie de sécurité périmétrique vers une stratégie centrée sur la protection de l'information

2010

Protection périmétrique

Point de sécurité toujours d'actualité :

- Sécurité des PC/Laptops, etc.
- Sécurité des systèmes mobiles
- Contrôle des connexions Internet
- Protection contre les malwares, etc.

2016

Protection des informations critiques

Sécurité de l'information :

- Détection en quasi « temps-réel », réaction sur incidents, décontamination des systèmes infectés et correction des autorisations d'accès
- Industrialisation des contrôles de conformité

ÉVOLUER VERS DES STRATÉGIES DE SÉCURITÉ DITES « PROACTIVES »

Dès lors que la prévention a atteint ses limites, les entreprises doivent adopter une posture où elles sont prêtes à répondre à un incident de sécurité

*Compliquer « la vie » des assaillants et **RALENTIR** leur avancée*

*Définir et **EXÉCUTER** la stratégie de sécurité*

*Mettre en œuvre des moyens de **DÉTECTION***

*Prendre des mesure rapides et efficaces afin de répondre à une attaque, mettre en œuvre des corrections **STRUCTURANTES***

Technique

L'évolution vers le Cloud

Une situation reconnaissable
Des conséquences prévisibles

Mainframe	Mini	PC	Mobile	Cloud
1960-1975	*1975-1990*	*1990-2005*	*2005-2015*	*2015+*

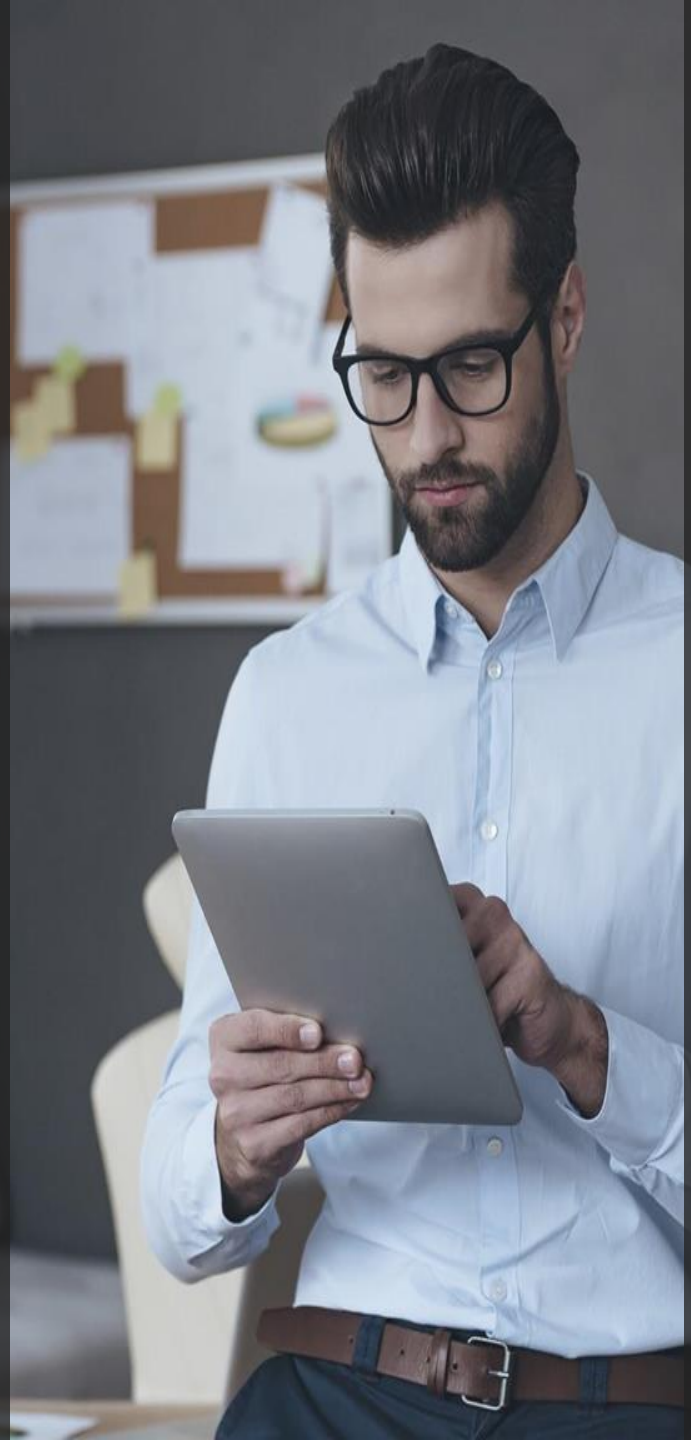
AMRAE LES RENCONTRES

Anticiper la menace

D'où vient le risque

- Lone-Wolves
- Script kiddies
- Malicious Insider
- Criminal Organizations
- Nation-state Actors
- ...

Quel est le maillon faible ?



99.%

63%

12%

** Verizon Data Breach Investigations Report 2016*

Google Cloud

Capacité d'anticipation

Les organisations prennent confiance dans leur capacité à anticiper les cybermenaces, mais des progrès restent à faire…

Trop peu d'organisations accordent le niveau d'attention requis aux principes élémentaires de cybersécurité. Ainsi chaque jour, elles placent leurs clients, leurs salariés et même leur propre avenir face à des risques considérables.

L'émergence des objets connectés et l'explosion du nombre de ces dispositifs accentuent les besoins d'anticipation des organisations et font émerger de nouveaux challenges.

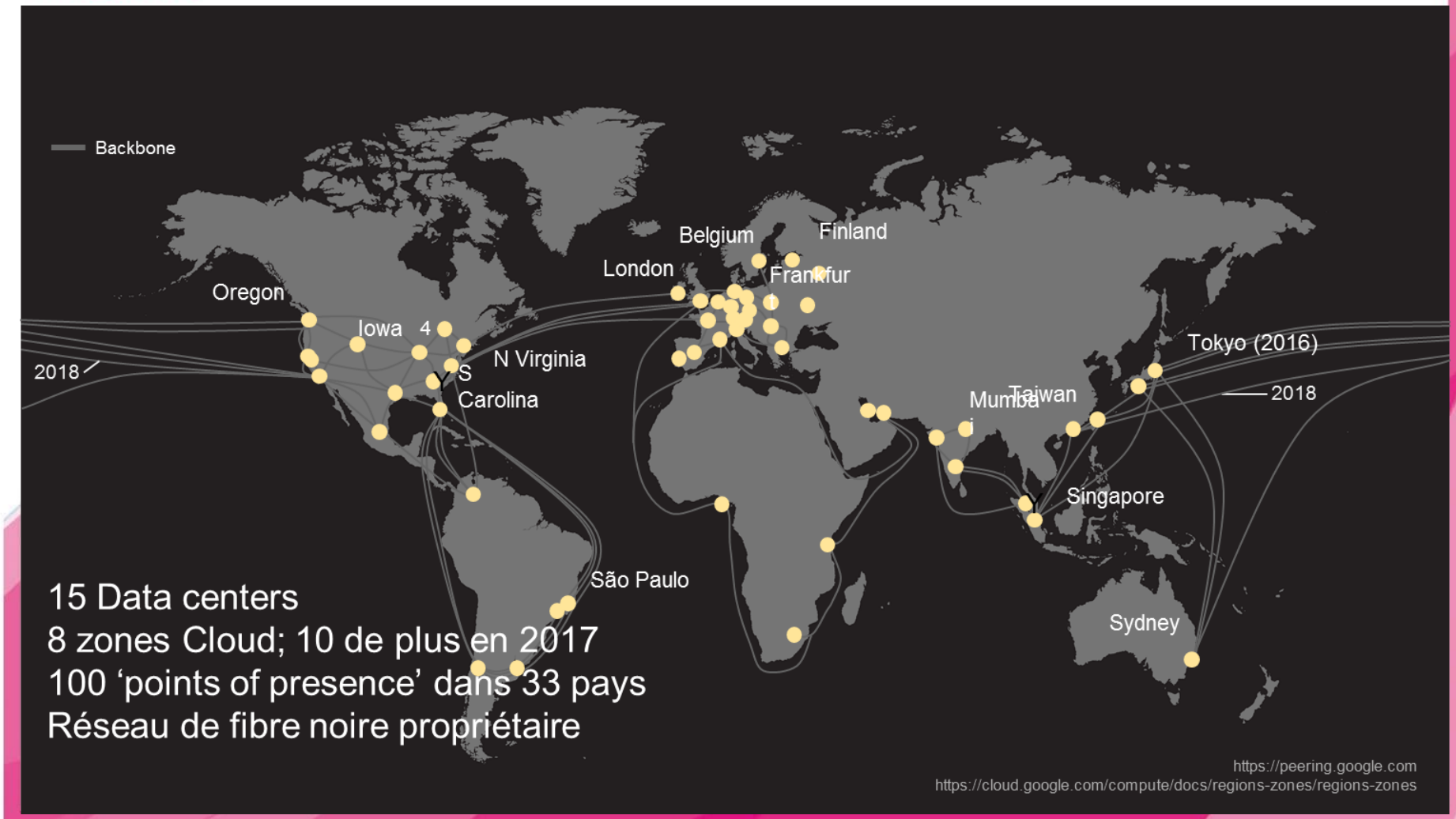
Le challenge du nombre de dispositifs : **73% se déclarent préoccupées par la faible connaissance qu'ont les usagers de leurs failles de sécurité potentielles**.

Le challenge des données : Les organisations doutent de leur capacité à traquer les trafics suspects au-delà de leurs réseaux (49%) ou à repérer les attaques «*zero day*» cachées ou inconnues (40%).

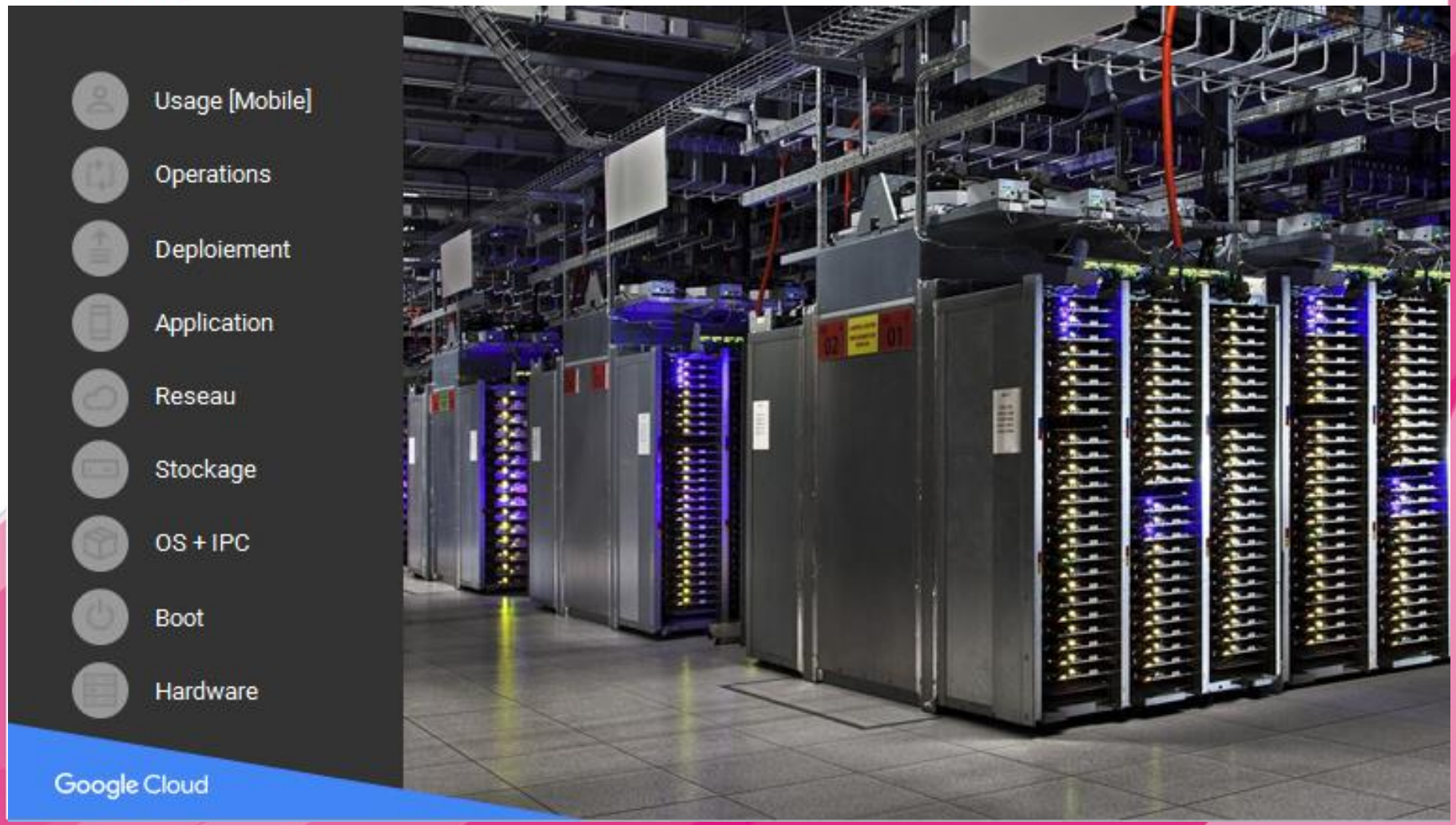
Le challenge de l'écosystème : De nombreuses organisations s'attendent à ce qu'il soit de plus en plus difficile de superviser l'ensemble de leur écosystème (34%).

Les outils techniques

Infrastructure Google Cloud



Sécurité sur toute la pile technologique



Capacités à résister

Si dans l'ensemble, les organisations ont amélioré leur capacité à résister, les cyberattaques ne cessent de se sophistiquer

Près de la moitié des répondants (48%) déclarent que l'obsolescence de leur système de protection est une importante source de vulnérabilité. Alors qu'elles affichaient un véritable optimisme en 2015, ils sembleraient qu'après une phase de rodage de leurs systèmes, les entreprises aient finalement véritablement pris conscience de la nature de la menace.

86%

des répondants déclarent que leur programme de cybersécurité ne répond pas pleinement aux besoins de leur organisation.

Au cours de ces 12 derniers mois, quelles menaces/vulnérabilités ont augmenté votre exposition au risque ?

57%

des répondants ont eu récemment un incident important de cybersécurité.

	2013	2014	2015	2016
Vulnérabilités				
Salariés non sensibilisés	53%	57%	44%	55%
Systèmes obsolètes	51%	52%	34%	48%
Accès sans autorisation	34%	34%	32%	54%
Menaces				
Logiciels malveillants	41%	34%	43%	52%
Phishing	39%	39%	44%	51%
Cyberattaques conçues pour voler des informations financières	46%	51%	33%	45%
Cyberattaques conçues pour voler des données ou de la propriété intellectuelle	41%	44%	30%	42%
Attaques en interne	28%	31%	27%	33%

METTRE EN PLACE UNE GESTION AVANCÉE DES MENACES : SMARTSOC

La création d'une stratégie de supervision et de contrôle sécurité doit s'appuyer sur les processus métiers et pas uniquement sur « l'infrastructure technique »

Collecte d'informations :

- Systèmes d'exploitation
- Applications
- Bases de données
- Gouvernement
- Santé
- Education
- Etc.

Flux de données en provenance de services commerciaux

Flux de données en provenance de services non commerciaux

Flux de données en provenance de réseaux sociaux

Information contextuelles liées aux technologies déployées

Analyses avancées des menaces, agrégation et corrélations

SMARTSOC

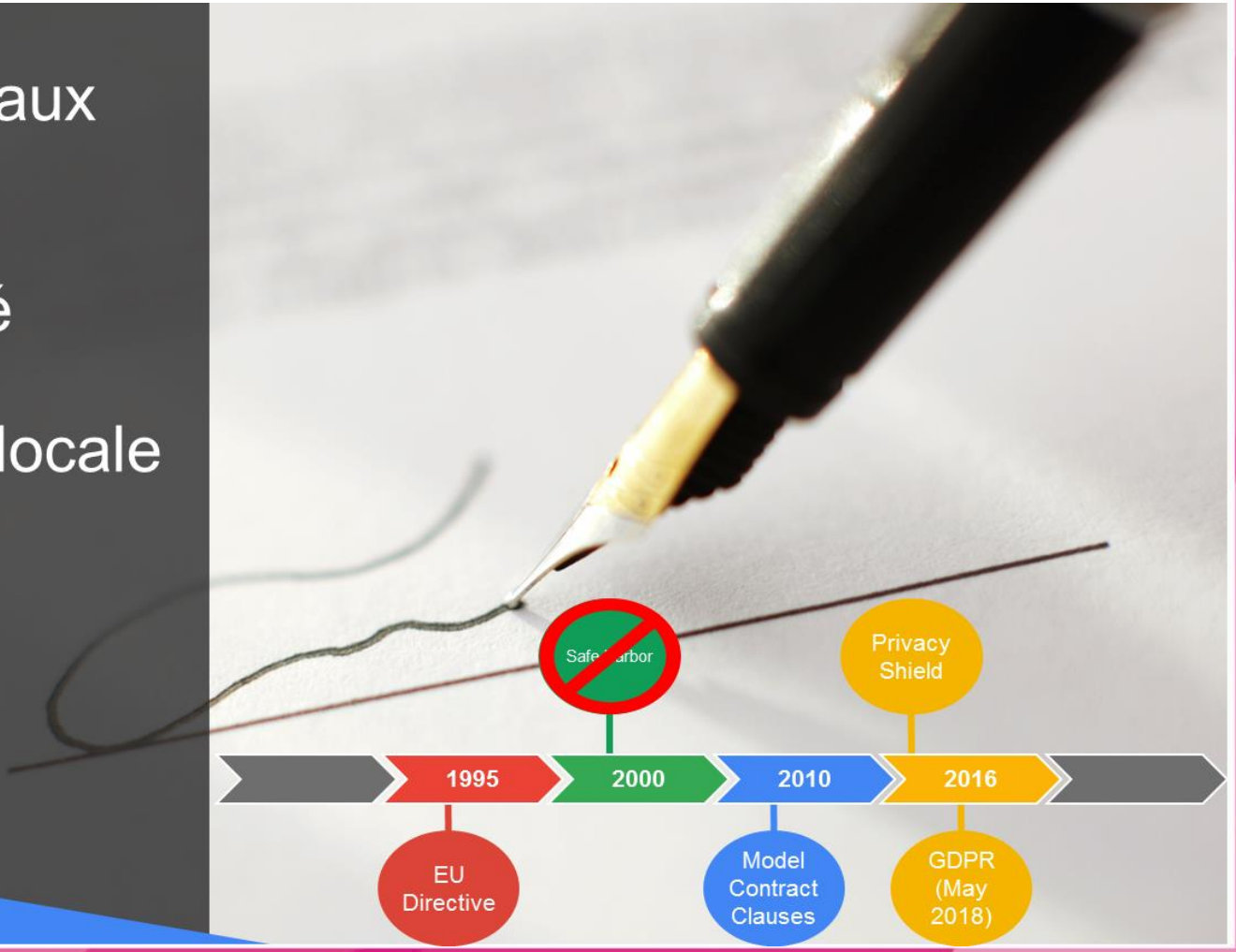
24/7

Information spécifiques à l'industrie et à la localisation géographique

Juridique

Les outils légaux

- Controle
- Conformité
- GDPR
- Guidance locale



Google Cloud

Compliance

Compliance

Privacy Shield Framework

HIPAA

FedRAMP

PCI DSS COMPLIANT

GOV.UK

DeNederlandscheBank

Le Risque Politique

Organisation

Rôle du Risk Manager ?

- Il doit appréhender le sujet dans toutes ses dimensions (techniques, juridiques, organisationnelles) pour :
  - Porter l'analyse de risque
  - Dynamiser la réduction des risques
  - Permettre le financement
  - Communiquer au top management sur ce risque (comme sur les autres)

7 points clés d'une organisation cyberrésiliente

Acquérir une fine connaissance de l'organisation pour mieux la mobiliser en cas d'attaque

Cartographier l'écosystème

Collaborer pour réduire les facteurs de risque

Les **7** points clés d'une organisation cyberrésiliente

Identifier les informations prioritaires et actifs stratégiques

Faire preuve d'un leadership exceptionnel dans l'encadrement de ses équipes

Instaurer une culture du changement

Mener des investigations formelles et préparer d'éventuelles poursuites judiciaires

La cyberrésilience : une dynamique lancée mais des efforts restent à faire

Etre capable de prévoir et de détecter les cybermenaces via une stratégie de veille et à une démarche de défense active.

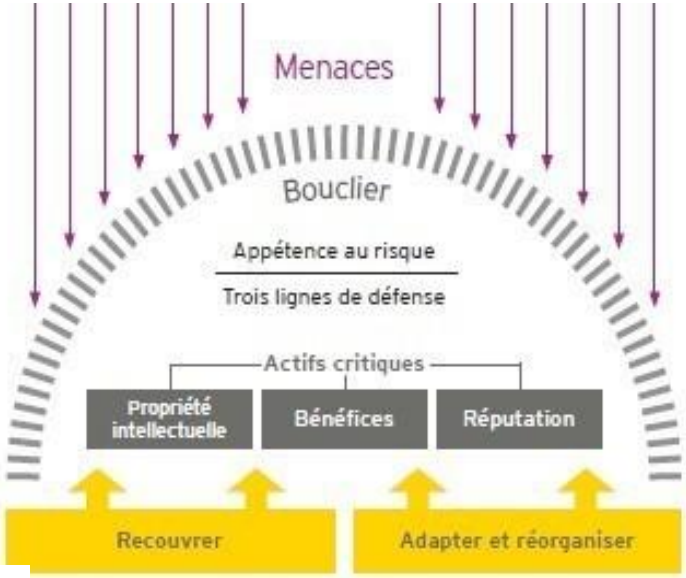
Anticiper

Mettre en place un bouclier efficace de protection conçu en fonction du niveau de risque que l'organisation.

Résister

Disposer d'une capacité de réponse adaptée et savoir gérer une crise (investigation post-incident et reprise d'activité).

Réagir



	Anticiper (Voir les menaces arriver)	Résister (Le bouclier de l'organisation)	Réagir (Se remettre de l'attaque)
Dans quels domaines les organisations placent-elles leurs priorités ?	Moyen	Fort	Faible
Dans quels domaines investissent-elles ?	Moyen	Fort	Faible
Engagement du comité exécutif et des C-Suites	Faible	Fort	Faible
Qualité du reporting à la direction ou au comité exécutif	Faible	Moyen	Faible

L'investissement des organisations présente encore des lacunes

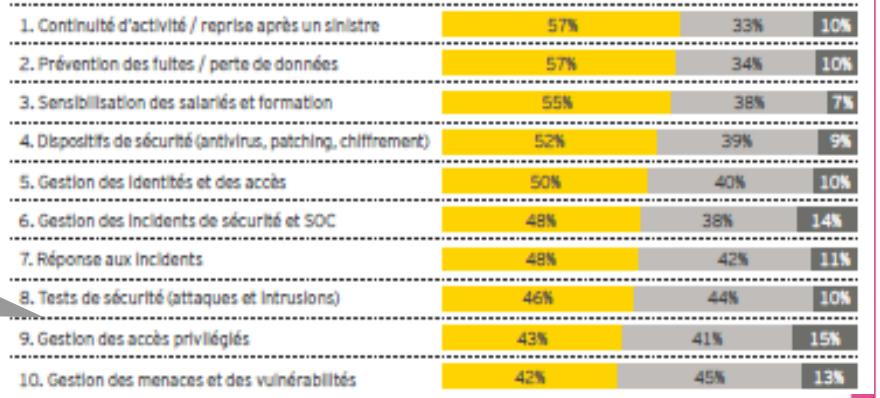
Capacité à réagir

Les organisations ont compris l'importance de renforcer leurs capacités de réaction aux cyberattaques

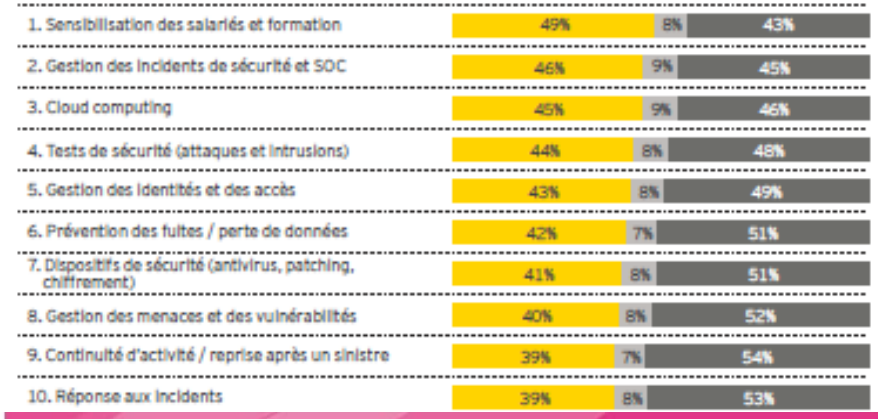
Savoir prioriser

Le plan de continuité d'activité (PCA) et les systèmes de gestion des informations font partie des priorités des organisations, preuve qu'elle ont compris l'importance de savoir réagir. Les systèmes de gestion des informations et des événements de sécurité (SIEM) combinés aux SOC sont aussi privilégiés par les entreprises.

Quel degré de priorité accordez-vous à chacun des domaines suivants (fort, moyen, faible) dans les 12 prochains mois ?



Votre entreprise a-t-elle cette année l'intention de dépenser plus, moins, ou relativement le même montant que l'année précédente dans les domaines suivants ?



Les investissements des organisations

Perception des priorités et choix d'investissement ne vont pas toujours de pair. Identifié comme une top priorité, le plan de continuité d'activité arrive ainsi en 9e position des priorités budgétaires. Les organisations ne semblent pas prêtes à investir dans de nouvelles compétences visant à adapter et/ou réorganiser leur système d'approche défensif

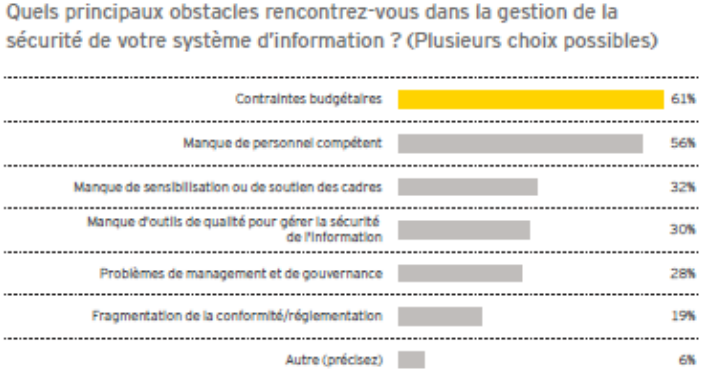
Cyberrésilience ou cyberagilité ?

Si chercher à être plus agile et investir en ce sens est important, la question de la résilience l'est tout autant : « êtes-vous cyberrésilients ? ».

La cyberrésilience est une composante de la résilience économique : elle mesure la résilience d'une organisation confrontée à une cybermenace au cours de trois phases clefs d'action : l'anticipation, la résistance et la réaction.

Années après années, l'enquête EY met en lumière les défis soulevés par la cybersécurité. Voici quelques résultats clés de l'enquête de cette année.

49% ne connaissent pas le préjudice financier potentiel d'une faille majeure de sécurité.



53% affirment que leur budget a augmenté au cours des 12 derniers mois.

des entreprises n'évaluent pas l'impact financier de chaque infraction significative.

49% des SOC collaborent et partagent leurs données avec d'autres acteurs du même secteur

des membres de comités exécutifs et des C-Suites ont des doutes sur le niveau de protection du dispositif de cybersécurité de leur organisation.

Synthèse de l’exposition

Exposition Digitale

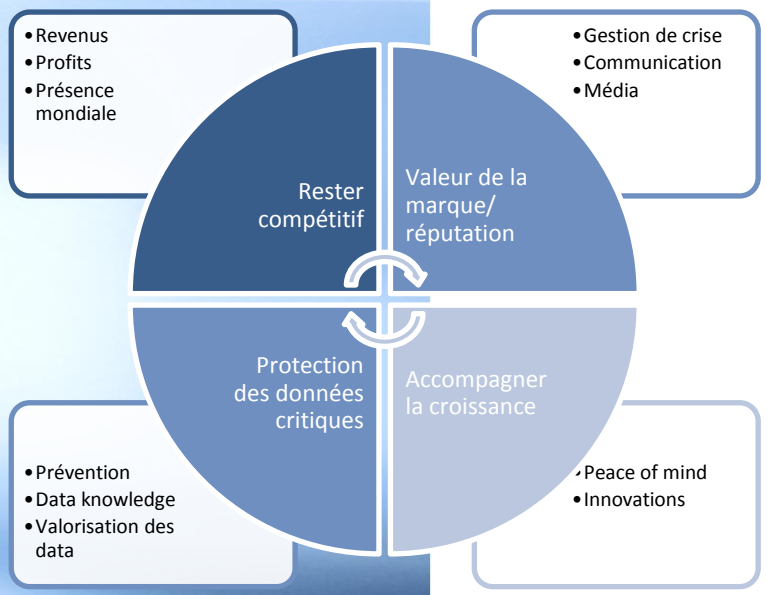
- Impacte toutes les entreprises (risques et opportunités)
- Evolue rapidement de même que le contexte technique et réglementaire
- Son analyse et son traitement nécessitent de mobiliser une pluralité d'expertises

Financement

Objectifs du transfert de risque

Pré-financer la réponse à incident de sécurité sur les données ou sur le réseau

- **Financer les frais de défense** face aux fournisseurs, clients et les entités publiques en cas d'incident
- Organiser sa capacité de **gestion de crise digitale**, former ses équipes et se tester
- Préparer un **accès privilégié à des expertises** peu disponibles part ailleurs (Forensique IT ultra spécialistes, expert en tentative d'extorsion, gestion médias et réseaux)
- **Anticiper et protéger** les profits futurs issus du Digital



La pluralité des transferts

- Assurance Cyber “stand alone”
  Le caractère Multi disciplinaire de la couverture

- Cyber Vs Garanties Traditionnelles
  Responsabilité Civile
  Dommages aux biens
  Pertes d’Exploitation

- Alternatives
  Garanties type “paramétriques”

Les challenges

Comprendre et couvrir les risques nouveaux

- Les Risques liés à **la disponibilité des réseaux**
- **Sabotage** de data
- Le risque d'**accumulation**
- **Vols massifs** de données
- Le cas particulier du “**cyberwar**”
- **La régulation 2.0**
- Les risques “silencieux”

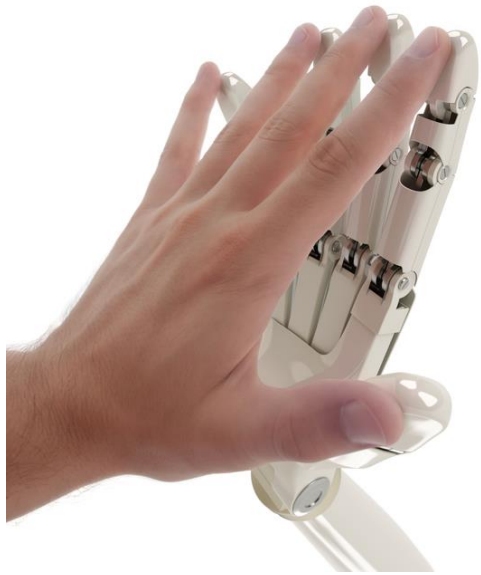
Les opportunités

Faire de l'innovation un moteur de croissance

- L'organisation des assureurs autour des **plateformes**
- L'utilisation massive des **smart datas et analytics**
- La création d'un droit des algorithmes « Ethics by design »
- La gestion des **sinistres 2.0**
- Le Machine learning et le Blockchain

Pour aller plus loin

- Big data et **actuariat**
- La disponibilité des **capacités d'investissement**
- **L'innovation** dans la chaine de valeur



Pour conclure

Pour conclure

Vision « Conseil »

1. Les attaques ne vont pas cesser. La digitalisation ouvre même la voie à plus d'exposition. Pour autant, il est plus que jamais important d'accompagner « lucidement » plutôt que de tenter de bloquer
2. Le facteur humain (collaboration et sensibilisation) est clé !!
3. Se connaître (force et faiblesses) par rapport à son exposition digitale permet de mieux doser les efforts
4. L'anticipation permet de mieux s'adapter et de résister
5. Une focalisation sur les actifs clés exposés permet de concentrer les efforts et une meilleure efficacité
6. Une surveillance adaptée complétée par des dispositifs de gestion des incidents sécurité / de crise efficaces permettent d'éviter les grandes crises
7. Envisager toutes les pistes en matière de traitement du risque (dispositifs technologiques, cyber-assurance, transfert de la gestion d'une partie de sac sécurité etc..)

Pour conclure

Vision « technique »

La technologie fait partie de la solution

Les rendements d'échelle , « internationale », seront importants dans la décision

La maturation du cadre légal va faciliter l'adoption

L'évolution de la discussion politique doit être observée avec précaution

Pour conclure

Vision « Assureur »

Le marché de l'assurance continue à s'adapter rapidement aux enjeux nouveaux des assurés, malgré la remise en question de la classification traditionnelle des risques et les résistances organisationnelles.

Le marché "cyber" a connu une phase expérimentale de développement basée sur la concentration des efforts en souscription sur l'analyse du niveau de sécurité de l'IT des assurés. Ce modèle doit s'adapter aux nouvelles méthodes de profilage de risques, aux technologies liées au Big Data ou au blockchain par exemple.

La complexité liée à la compliance peut être encadrée par un effort accru de « normalisation » et une collaboration en devenir entre le marché de l'assurance et les acteurs publics,

Pour conclure

Vision « Risk Manager »

Le Risk Manager est idéalement placé pour :

- mener à bien cette analyse de risque co-construite avec la DSI, le juridique, la stratégie, etc.
- en inclure les résultats dans la cartographie globale des risques,
- les partager avec les différents organes de Gouvernance,
- Adapter les modalités de financement aux spécificités des risques digitaux.

MERCI DE VOTRE ATTENTION !

AVANT DE PARTIR , N'OUBLIEZ PAS DE REMPLIR L'EVALUATION !

- Soit sur la feuille, à remettre à l'hôtesse à la sortie
- Soit directement sur la **WEB APPLI**

Merci : vous participez à l'objectif ZERO PAPIER !

Les slides seront en ligne dès la semaine prochaine sur www.amrae.fr