claranet
security

# Panorama de la sécurité

11 Janvier 2018

claranet
hosting | applications | networks

helping our customers
do amazing things

# Objectifs de ce cours

- Introduction/sensibilisation à la problématique de la sécurité
- Panorama des différentes composantes de cette problématique
- Identification et maîtrise des concepts et techniques de base

# LA CYBERCRIMINALITE

claranet
hosting | applications | networks

helping our customers
do amazing things

# La cybercriminalité

La cybercriminalité est le terme employé pour désigner l'ensemble des infractions pénales qui sont commises via les réseaux informatiques, notamment, sur le réseau Internet.

– Les atteintes aux biens :

- Fraude à la carte bleue sur Internet
- Vente par petites annonces ou aux enchères d'objets volés ou contrefaits
- Encaissement d'un paiement sans livraison de la marchandise
- Piratage d'ordinateur; gravure pour soi ou pour autrui de musiques, films ou logiciels.

# La cybercriminalité

– Les atteintes aux personnes :
  - Diffusion d'images pédophiles, de méthodes pour se suicider, de recettes d'explosifs ou d'injures à caractère racial
  - Diffusion auprès des enfants de photographies à caractère pornographique ou violent
  - Atteinte à la vie privée.

Tous ces faits sont punis d'une peine d'emprisonnement (5 ans maximum) et d'une amende (375 000 euros maximum).

# Cible: les entreprises

Ex **Target** : Chaine de distribution américaine

<u>Vol de données clients :</u>

- 110 Millions de données personnelles
- 40 Millions de Numéros de CB

<u>Préjudice :</u>

- Bourse : -13% en 1 mois (Soit 3 Milliards de $)

**Le groupe Target victime d'un vol géant de données bancaires**

Le Monde.fr avec AFP et Reuters | 11.01.2014 à 11h19 • Mis à jour le 11.01.2014 à 12h28

Abonnez-vous à partir de 1 € Réagir Classer Partager

# Cible: les entreprises

Ex **Home Depot** : Chaine de bricolage américaine

<u>Vol de données clients :</u>

- 56 Millions de Numéros de CB

<u>Préjudice :</u>

- Bourse : -7%
- Env. 80 Millions de $ de perte immédiate

Great Speculations

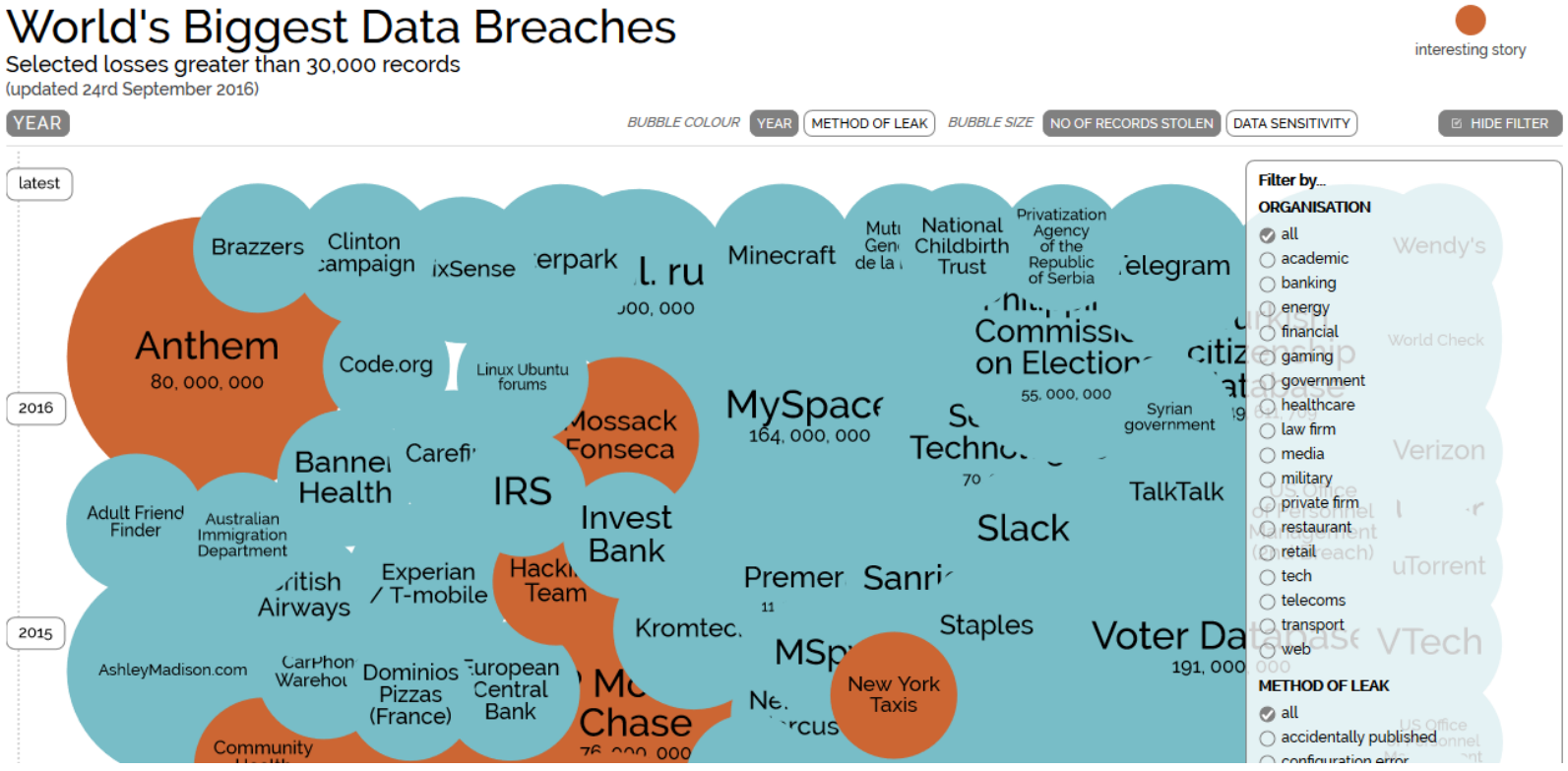
INVESTING 9/24/2014 @ 1:39PM | 8 526 views

## Home Depot: Could The Impact Of The Data Breach Be Significant?

Trefis Team , Contributor

+ Comment Now + Follow Comments

# World’s Biggest Data Breaches



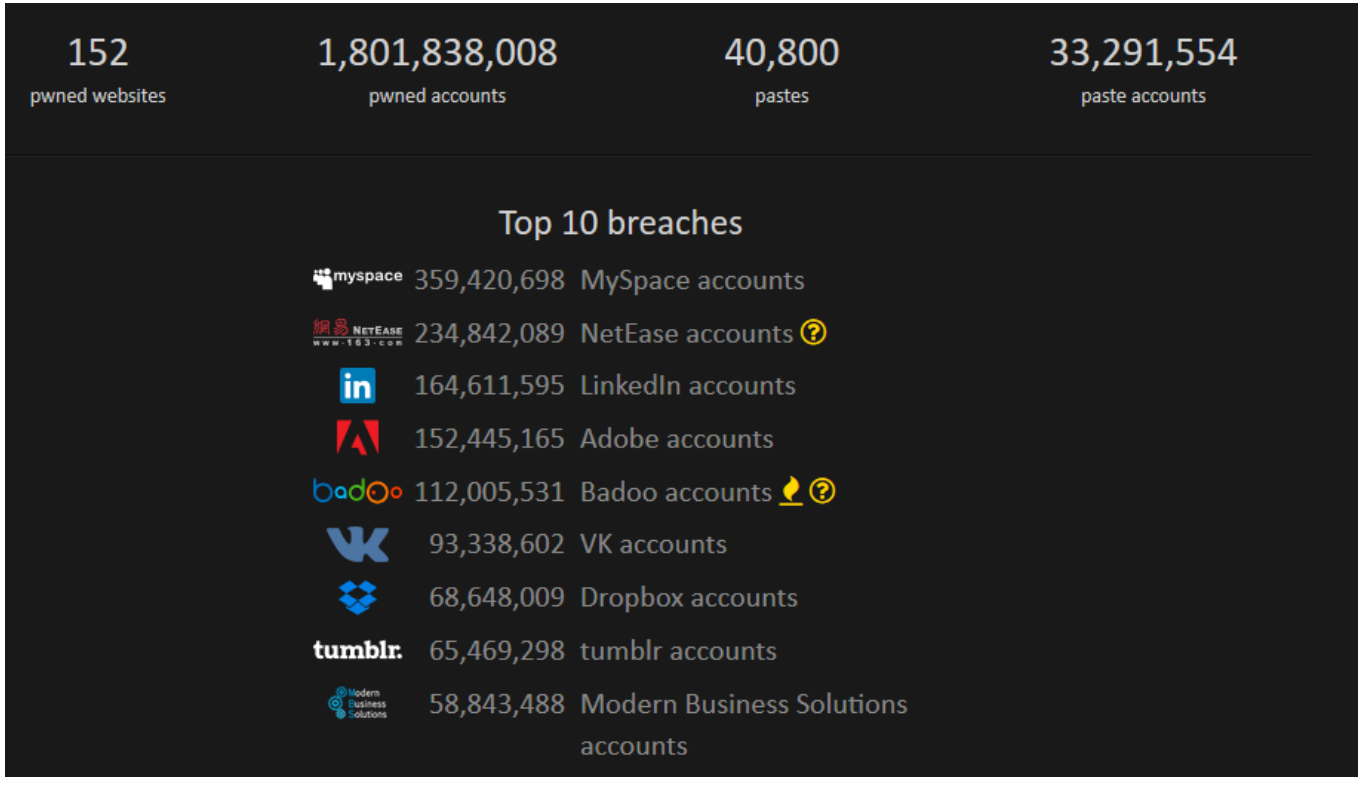

http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/

# Cible: les particuliers

- 78% des voleurs utilisent les réseaux sociaux avant de vous cambrioler
- 120000 personnes se font voler leur identité chaque année
- Chaque seconde 18 personnes se font pirater
  - 1080 par minute
  - 64.800 par heure (2x la population de Lens)
  - 1.555.200 par jour (Population de Lyon et sa banlieue)

# Compte compromis ?

https://haveibeenpwned.com/



# Dans quel but?

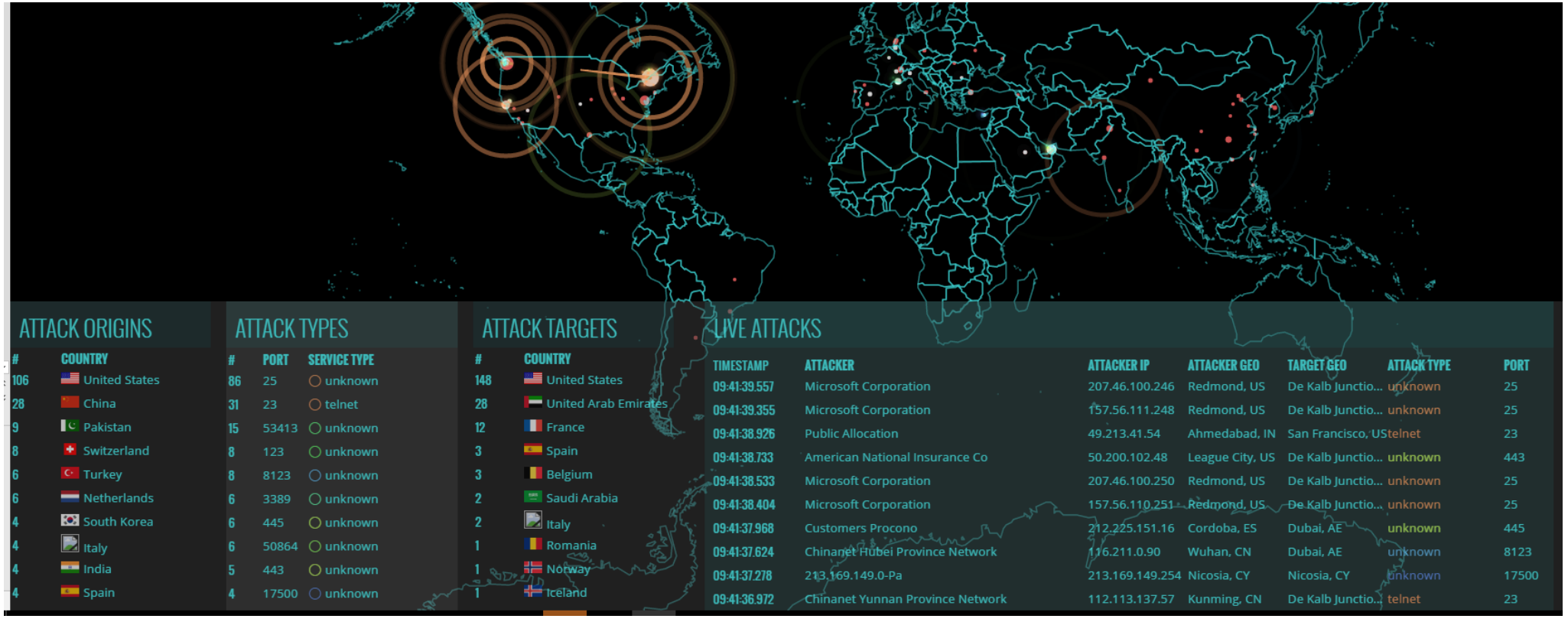
La cybercriminalité coûte 445 Milliards

de Dollars par an à l'économie mondiale.

# CYBERTHREAT REAL-TIME MAP


https://cybermap.kaspersky.com/#

# CYBERTHREAT REAL-TIME MAP




http://map.norsecorp.com/#/

# Création d’une politique

Mise en place indispensable d’une politique de prise en compte des risques et de sécurisation du SI

# LE R.S.S.I

## Responsable de la Sécurité des Systèmes d'Information

claranet
hosting | applications | networks

helping our customers
do amazing things

# RSSI

Définition que donne Internet :

- « Le RSSI est chargé de la définition et de la mise en œuvre de la politique de sécurité de l'entreprise »
- « Il possède en outre un rôle stratégique d'information, de conseil et d'alerte de la direction générale sur les risques en matière de sécurité informatique »
- « La fonction de RSSI est essentiellement managériale et consiste à encadrer une équipe d'ingénieurs et de techniciens d'exploitation, dont il organise et contrôle le travail »

# RSSI

Ses compétences:

- « Le RSSI doit avoir des connaissances pointues sur les réseaux, les systèmes et la sécurité des systèmes d'information »
- « Par ailleurs, étant donnée ses fonctions d'encadrement, il doit posséder des qualités relationnelles et avoir une expérience de conduite de projets »

# RSSI

Ses études:

- « Il existe quelques études (niveau licence généralement) conduisant au métier, mais une expérience personnelle et une passion dans le domaine sont tout autant de qualités indispensables »

Son salaire:

- « Le salaire d'un RSSI peut varier entre 26 k€ et 40k€ par an, selon l'expérience selon la taille et la complexité du site à administrer »

# LA S.S.I

## Sécurité des Systèmes d'Information

claranet
hosting | applications | networks

helping our customers
do amazing things

# Qu'est-ce que la sécurité d'un SI ?

Elle tourne autour des 5 critères principaux suivants :

- La disponibilité (D) des services,
- L'intégrité des données (I),
- La confidentialité (C) de l'information et des échanges,
- L'authentification des utilisateurs
- La non répudiation des transactions.

# Disponibilité

- La **disponibilité** d'une ressource est relative à la période de temps pendant laquelle le service offert est opérationnel. Le volume potentiel de travail susceptible d'être prit en charge durant la période de disponibilité d'un service, détermine **la capacité** d'une ressource à être utilisée (serveur ou réseau par exemple)

- Il ne suffit pas qu'une ressource soit disponible, elle doit pouvoir être utilisable avec des temps de réponses acceptables.

# Intégrité

- Le critère **d'intégrité** des ressources physiques et logiques (équipements, données, traitements, transactions, services) est **relatif au fait qu'elles n'ont pas été détruites** (altération totale) **ou modifiée** (altération partielle) à l'insu de leurs propriétaires tant de manière intentionnelle qu'accidentelle.

# Confidentialité

- « La **confidentialité** est le **maintien du secret** des informations.. » (Le Petit Robert). Transposée dans le contexte de l'informatique et des réseaux, la notion de confidentialité peut être vue comme la « protection des données contre une divulgation non autorisée »

- Il existe deux types d'actions complémentaire permettant d'assurer la confidentialité des données:

  - limiter et contrôler les accès
  - les rendre inintelligibles en les chiffrant

# Identification et authentification

- Des procédures d'identification et d'authentification peuvent être mises en œuvres pour contribuer à réaliser des procédures de contrôles d'accès et des mesures de sécurités assurant:

- **La confidentialité et l'intégrité des données:** seuls les ayant droits identifiés et authentifiés peuvent accéder aux ressources et les modifier s'ils sont habilités à le faire.

- **La non-répudiation et l'imputabilité:** seules les entités identifiées et authentifiées ont pu réaliser une certaine action (preuve de l'origine d'un message par ex) . L'identification et l'authentification permet d'imputer la responsabilité de la réalisation d'une action à une entité.

# Non-répudiation

- La **non-répudiation** est le **fait de pouvoir nier ou rejeter** qu'**un évènement** (action, transaction) a eu lieu. A ce critère de sécurité, peuvent être associés les notions d'imputabilité, de traçabilité ou encore d'auditabilité.

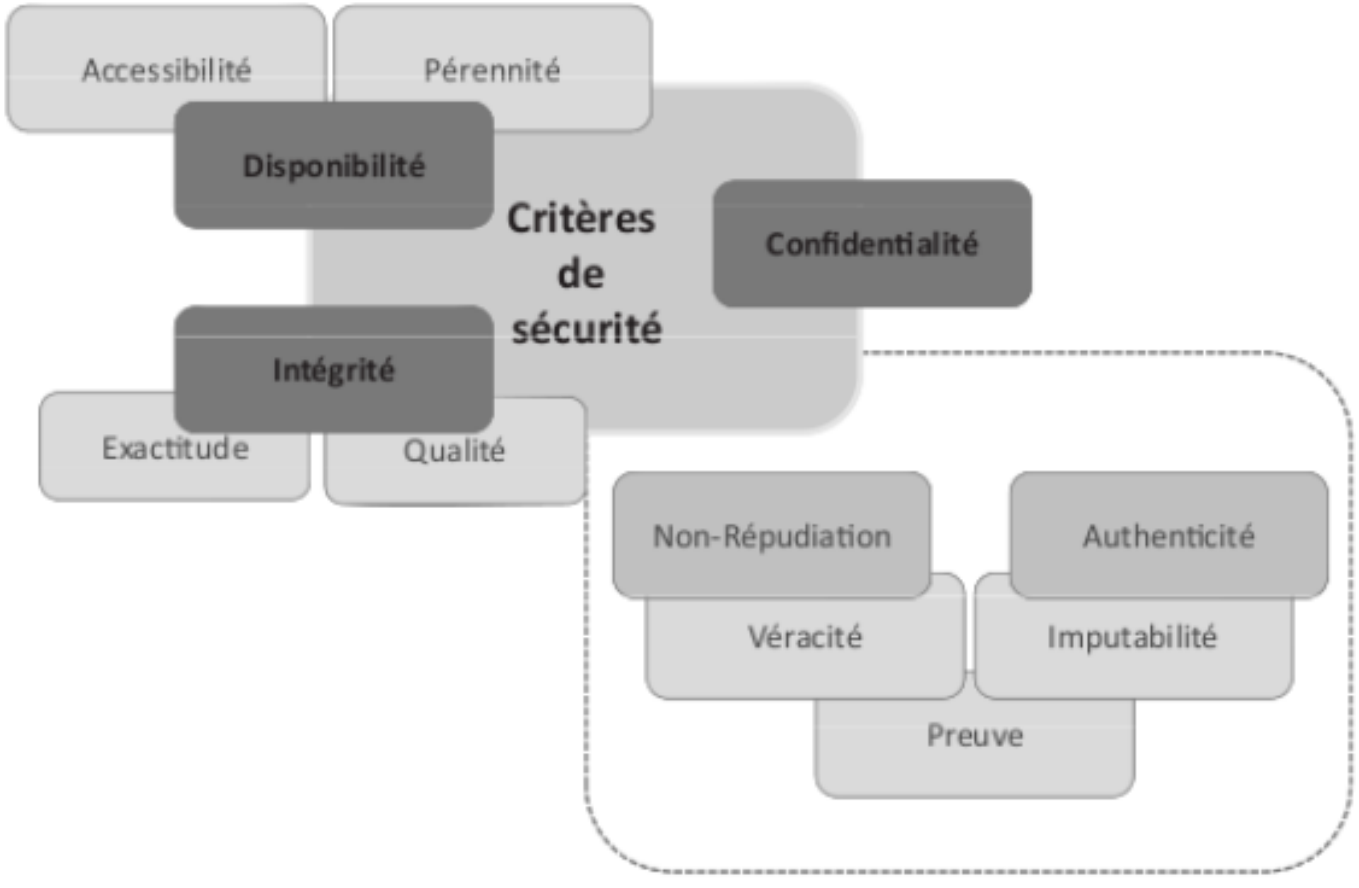
- L'imputabilité se définit par l'attribution d'une action (événement) à une entité déterminée (ressource, personne). Elle peut être réalisée par un ensemble de mesures garantissant l'enregistrement fiable d'informations pertinents par rapport à une entité et à un événement

# Traçabilité et auditabilité

- La traçabilité des événements est une fonction indispensable qui permet de grader la mémoire des actions survenues à des fins d'analyse pour reconstituer et comprendre ce qui s'est passé.

- L'auditabilité se définit par la capacité d'un système à garantir la présence d'informations nécessaires à une analyse ultérieur d'un événement (courant ou exceptionnel) effectué dans le cadre de procédures de contrôles spécifiques ou d'audit.

# Critères de sécurité



# Pourquoi ?

Le système d'information représente un patrimoine essentiel de l'organisation, qu'il convient de protéger :

- Infrastructures matérielles de traitement ou de communication
- Les logiciels
- Les données
- Les utilisateurs
- Etc…

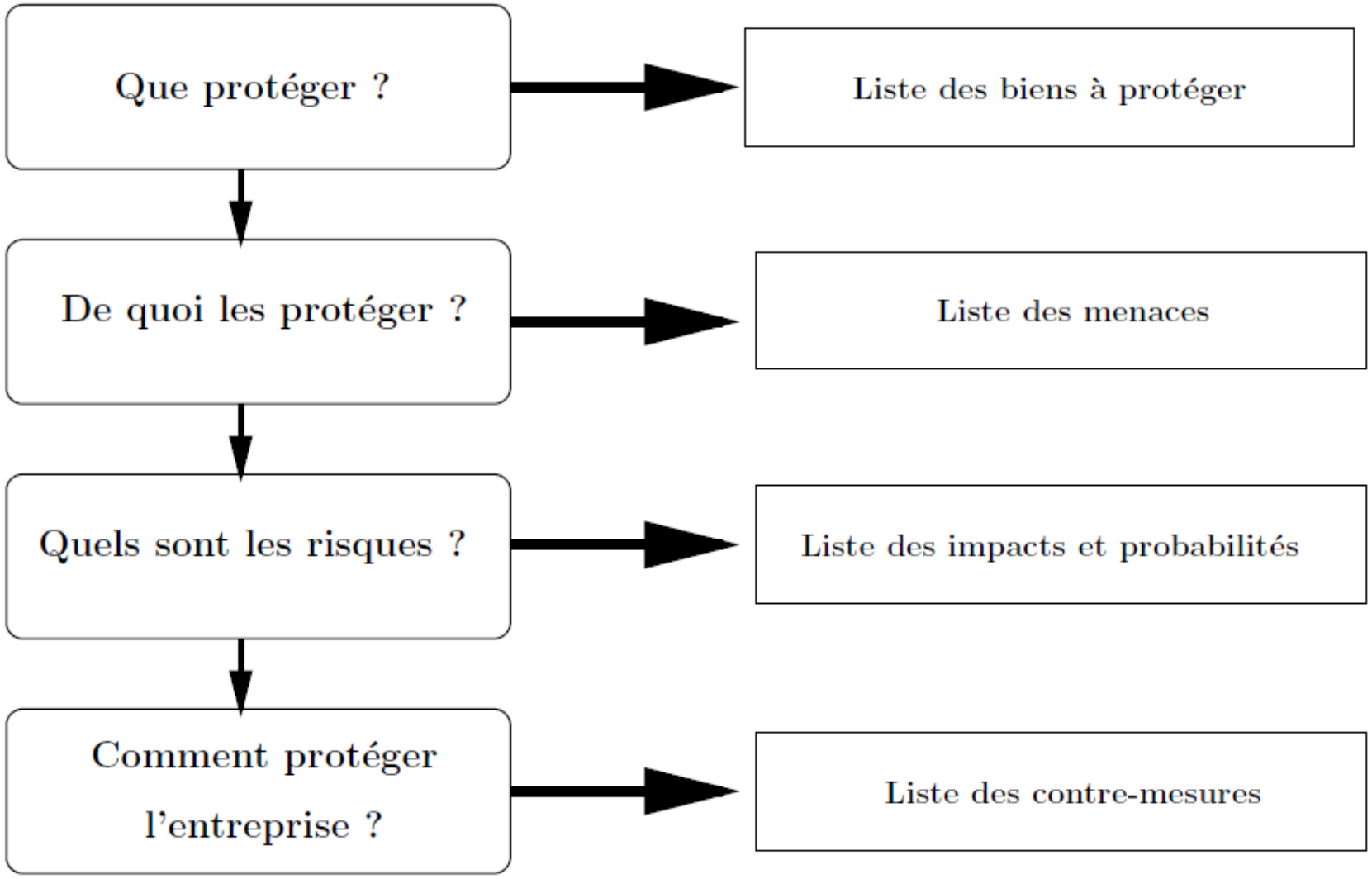
# Problématique

- **Risques auxquels il faut faire face :**
  - **Destruction** : Incendie, inondation, tempête, etc…
  - **Vol** : D'informations, de biens, etc…
  - **Piégeage logiciel** : Virus, Ver, cheval de Troie, etc…
  - **Saturation du SI** : Perturbation, disponibilité, « Pourriel », etc…
  - **Abus de droit** : Droits systèmes, droits réseau, etc…
  - **Usurpation de droits** : Utilisation de privilèges illégitimement obtenus
  - **Usurpation d'identité** : utilisation des codes d'un autre utilisateur
  - **Hors la loi** : Non respect de la CNIL, utilisation de logiciels sans licence,etc…
  - **Etc… etc… etc…**
- **Des risques de deux catégories**
  - Financiers
  - Image de marque

# Conséquences des risques

- Panne/Arrêt
- Diminution de la qualité de service
- Perturbation interne de l'entreprise
- Perte d'image
- Retard de la mise sur le marché d'un produit
- Fuite de technologie
- ...

# Se questionner



# Exercice

***Par groupe de 3 personnes, citer moi quelques exemples en vous inspirant du tableau précédent.***

# Une demarche générique

**Evaluer les risques et leur criticité :**

- Quels risques, quelles menaces ?
- Sur quelles données, sur quelle activité ?
- Avec quelles conséquences ?

**Rechercher et sélectionner les parades**

- Quoi sécuriser ?
- Comment ?
- Quand ?

# Une demarche générique

**Mise en œuvre**

- « Y’a plus qu’à ! »

**Vérification**

- Audit régulier des solutions implémentées

# Une demarche générique

**Raison d’être**

- Réduire les risques identifiés à un niveau acceptable

**Le moyen d’y arriver**

- La PSSI

# Dans quel but ?

Définir, mettre en place et animer une

**Politique de Sécurité**,

afin de permettre

une déclinaison opérationnelle

**pragmatique, efficace, progressive et**

**en adéquation avec les enjeux** de l'entreprise

# LA P.S.S.I

## Politique de Sécurité des Systèmes d'Information

claranet
hosting | applications | networks

helping our customers
do amazing things

# Définition

- La politique de sécurité permet de transcrire le travail effectué pour comprendre les risques et leurs impacts, en des mesures de sécurité.

- Elle donne de la cohérence à la gestion et contribue à adopter vis-à-vis des risques, une attitude proactive et réactive.

- Une bonne définition et une réalisation pertinent de la politique de sécurité autorisent une certaine maîtrise des risques informatiques, tout en réduisant leur probabilité d'apparition.

# Objectifs

- Fournir aux dirigeants une stratégie d'entreprise en matière de Sécurité de l'Information, au service de l'amélioration de la performance de l'organisation.

- Permettre de garantir la continuité des activités métiers les plus critiques, et de limiter les impacts d'incidents ou d'accidents liés à la sécurité de l'information

# Ne pas perdre de vue

- Un bon gestionnaire de la sécurité, même en anticipant et en prévenant certains accidents volontaires ou non, n'est pas devin !

- Ne pouvant anticiper toutes les menaces mais sachant qu'elles exploitent les vulnérabilités des systèmes en place, le gestionnaire s'emploiera à réduire les vulnérabilités de l'environnement afin de minimiser la réalisation de menaces

- Aucune politique de sécurité, aussi perfectionné soit-elle, ne tient si l'intégrité des personnes se trouvent mise en cause. En effet, le maillon faible de la sécurité est bien souvent l'humain.

# Concrètement ?

- Continuité des activités critiques
- Développer la culture sécurité
- Respect de la règlementation
- Accès et habilitations
- Architectures adaptées (cloisonnement, etc…)
- Traçabilité / Authentification
- Etc…

# Mise en oeuvre

- La définition de la politique de sécurité doit être

  - ✓ Simple et compréhensible
  - ✓ Aisément réalisable
  - ✓ De maintenance facile
  - ✓ Vérifiable et contrôlable
  - ✓ Adoptable par un personnel préalablement sensibilité, voire formé

# Contexte

- Une politique de sécurité ne doit pas être statique mais périodiquement évaluée, optimisée et adaptée à la dynamique du contexte dans laquelle elle s'inscrit.

- Elle doit être évolutive et suivre les modifications du contexte (risques, systèmes, environnement, personnes, réglementations). Elle doit donc prendre en compte la dimension temporelle des besoins de sécurité qui peuvent varier.

- Elle doit prendre aussi en compte une dimension spatiale en tenant compte par exemple des employés qui travaillent à leur domicile ou qui sont en déplacement.

claranet secops

# METHODES ET NORMES

## Contribuant à la définition d'une P.S.S.I

claranet
hosting | applications | networks

helping our customers
do amazing things

# Dans un premier temps

- Il faut pouvoir identifier les risques avant d'identifier les parades à mettre en place.

- S'appuyer sur une méthode qui facilite l'identification des points principaux à sécuriser *(notion de check list)*, ou sur des normes ou sur un ensemble reconnu de bonnes pratiques *(best practises).*

- Toutes peuvent servir de guide à l'élaboration de politique de sécurité. Elles sont utilisées plus ou moins complètement et le plus souvent adaptées à un contexte particulier en fonction de l'entité qui les met en œuvre.

# Quelques méthodes

- **EBIOS** : Expression des Besoins et Identification des Objectifs de Sécurité développée par l'ANSSI
- **MEHARI** : Méthode Harmonieuse d'Analyse des Risques développée par le CLUSIF
- **OCTAVE** : Opérationaly Critical Threat, Asset, and Vulnérability Evaluation développée par l'université de Carnegie Mellon (USA)
- Vous trouverez également un bon guide dans la norme **ISO 27002 –** Les bonnes pratiques
- Commission Nationale Informatique et Liberté

# MEHARI

- Les méthodes préconisées par le **Clusif** sont historiquement **Marion** ( *Méthode d'analyse des Risques Informatiques et Optimisation par Niveau*) et **Méhari** (*Méthode Harmonisée d'Analyse des Risques*)

- Existe en langue française et en anglais, elle est utilisée par de nombreuses entreprises publiques ainsi que par le secteur privé.

- Logiciel Risicare disponible pour faciliter le travail

# EBIOS

- EBIOS (Expression des Besoins et Identification des Objectifs de Sécurité) permet d'identifier les risques d'un SI et de proposer une politique de sécurité adaptée aux besoin de l'entreprise (ou d'une administration). Elle a été créée par la **DCSSI** (Direction Centrale de la Sécurité des Systèmes d'Information), du **Ministère de la Défense** (France). Elle est destinée avant tout **aux administrations françaises et aux entreprises**.

- La méthode EBIOS se compose de 5 guides (Introduction, Démarche, Techniques, Outillages) et d'un logiciel permettant de simplifier l'application de la méthodologie explicitée dans ces guides.

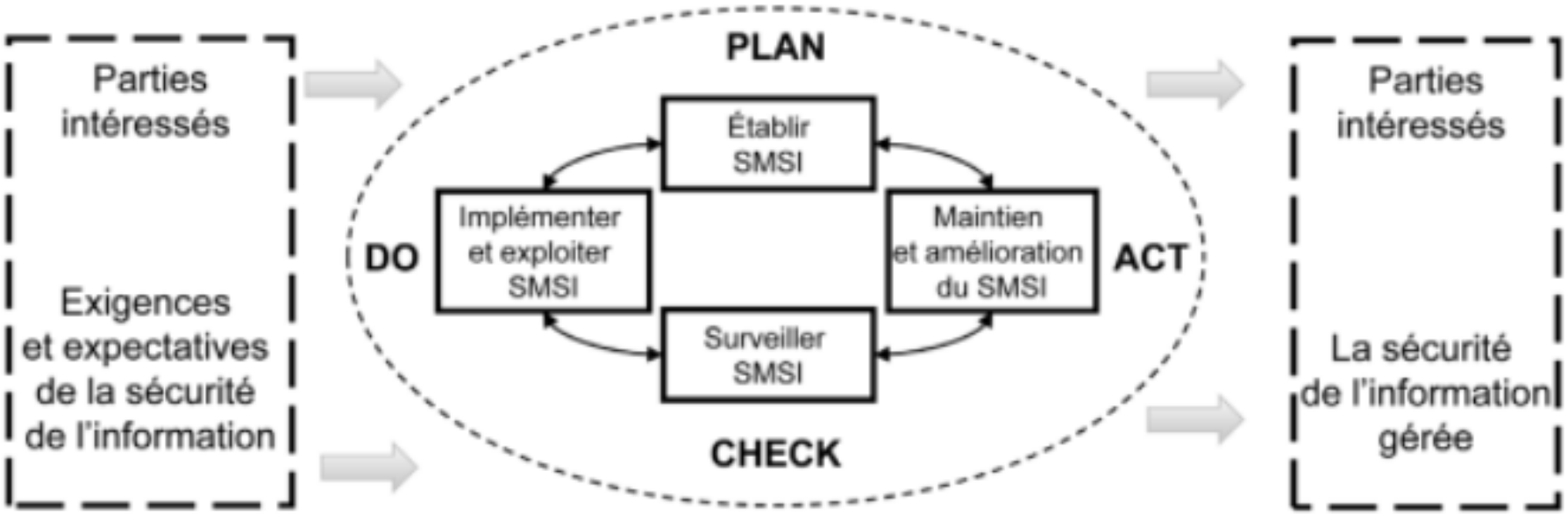
# La Norme ISO 27001

- La norme iso 27001 propose un modèle pour établie, implémenter, exploiter, surveiller, maintenir le système de management de la sécurité de l'information (**SMSI : Système de mangement de la sécurité de l'information**)

- Le norme 27001 se focalise sur l'implémentation d'un système de management de la sécurité basé sur une structure formalisée et des contrôles à effectuer

- La norme **se base** sur un modèle dit **modèle PDCA** (Plan, Do, Check, Act) – Planifier – Développer – Contrôler – Agir qui **reprend le concept de la roue de Deming**

# Norme ISO 27001




***Le modèle PDCA (adapté à partir de le norme iso 27001)***

# Norme ISO 27001

Appréhender la sécurité sous la forme d'un modèle PDCA contribue à:

- **Comprendre** les exigences de sécurité et les besoins de la politique de sécurité
- **Implémenter** et effectuer des contrôles pour gérer le risque informationnel
- **Surveiller** et revoir la performance du SMSI
- **Proposer** des améliorations basées sur des mesures d'efficacité du SMSI

# Avantages et inconvénients de l'utilisation d'une méthode

| Avantages | Inconvénients |
|---|---|
| Gain en termes d'efficacité en réutilisant le savoir-faire transmis par la méthode. Capitalisation des expériences.<br><br>Langage commun, référentiel d'actions, structuration de la démarche, approche exhaustive.<br><br>Être associé à des groupes d'intérêts. Partage d'expérience, de documentation, formation possible. | Bien qu'elles puissent faire l'objet de révision (nouvelles versions), les normes ou méthodes n'évoluent pas au même rythme que les besoins ou les technologies.<br><br>Une norme ou une méthode est générale. Il faut savoir la spécifier en fonction de besoins particuliers de l'organisation.<br><br>Prolifération des méthodes : difficulté de choix.<br><br>Disposer des compétences nécessaires. Efforts financiers, durée, coûts. Difficultés à maîtriser la démarche qui peut s'avérer lourde et nécessiter des compétences externes. |

# Questions

claranet
hosting | applications | networks

helping our customers
do amazing things