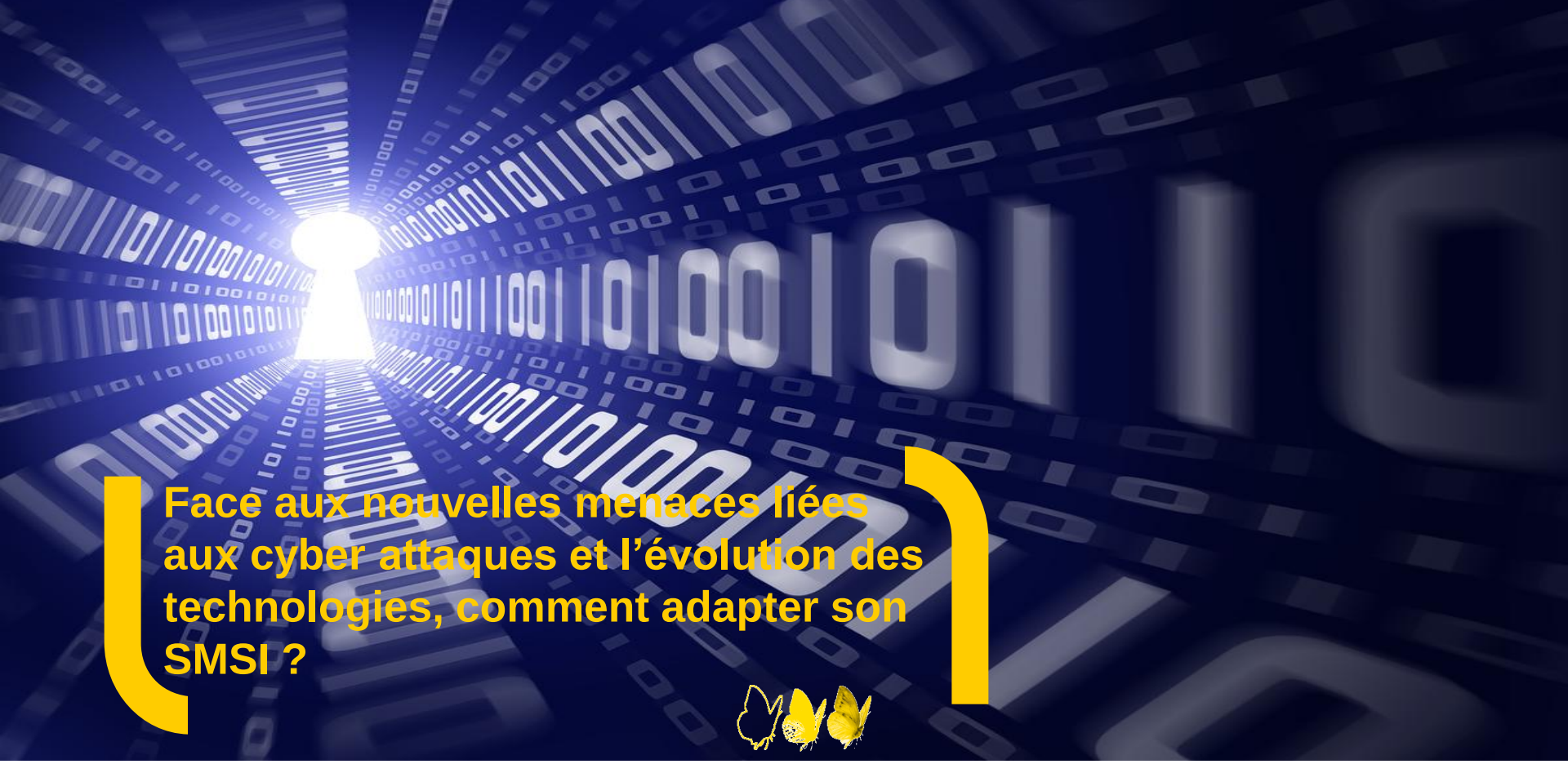


# Face aux nouvelles menaces liées aux cyber attaques et l'évolution des technologies, comment adapter son SMSI ?

**CLUB27001 – PARIS 22 novembre 2012**

CGI

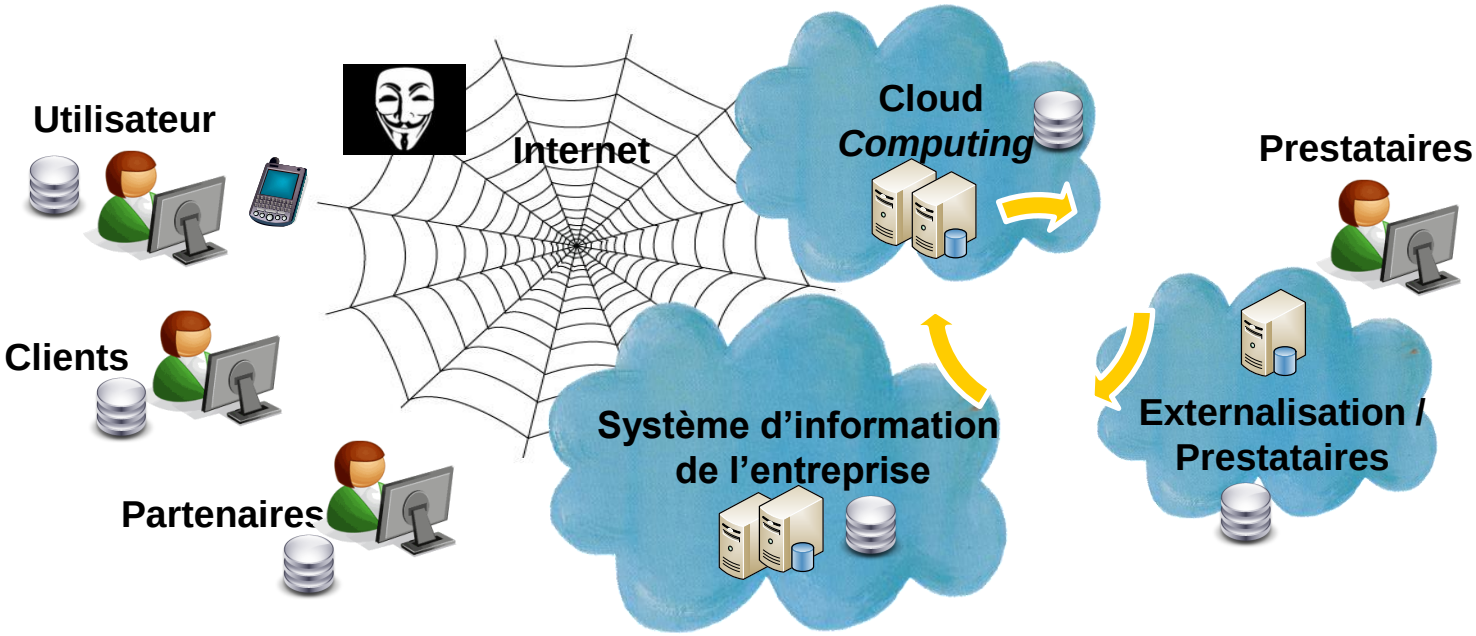
Logica Business Consulting
fait maintenant partie de CGI.

logica BUSINESS CONSULTING

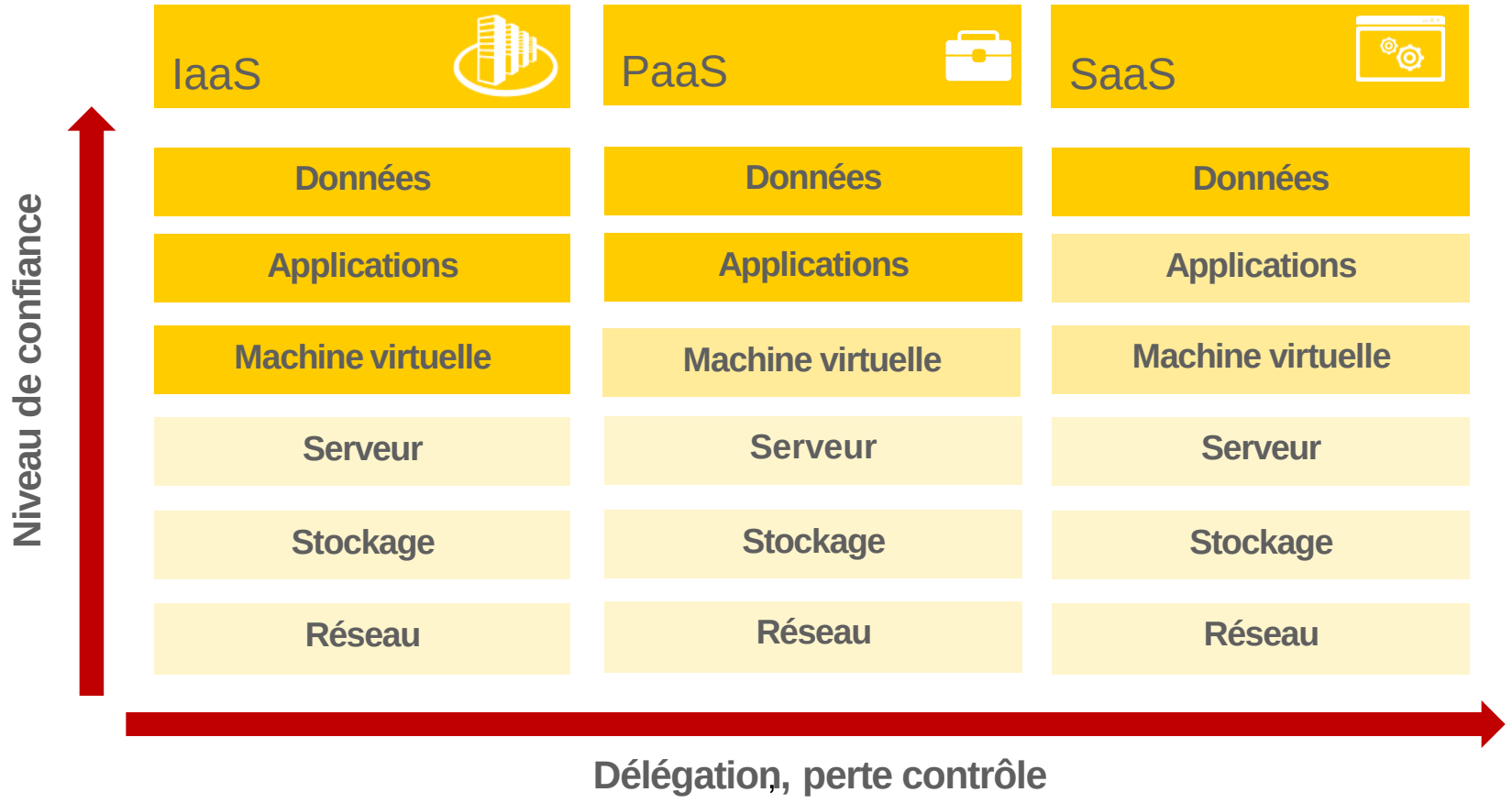
# Sommaire

# Le passage de l'entreprise étendue vers l'entreprise virtuelle

- Prolifération des informations et des accès (**Mobilité, BYOD**)
- Professionnalisation de la menace (cybercriminalité) et développement de sa furtivité
- Amplification des impacts d'un sinistre et Réduction des capacités de réaction
- Renforcement de la conformité sur la protection des données
- Passage du Système d'information centré sur les traitements vers le SI centré sur l'information (Big Data)

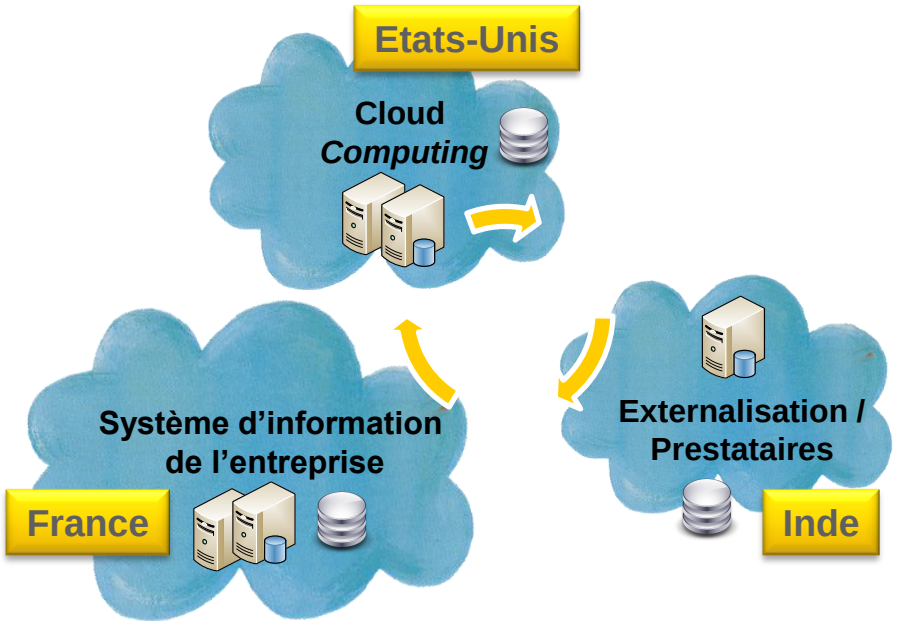


# Le Cloud Computing

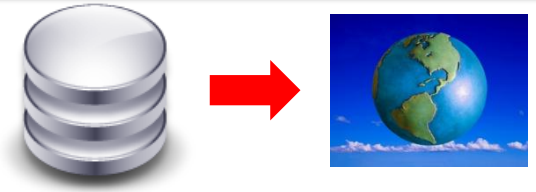


# Il est nécessaire de prendre en compte les réglementations internationale dans son SMSI

- **Exemple :** Le **USA PATRIOT ACT** est un texte voté par le Congrès des Etats-Unis, dans la suite immédiate des évènements du 11 septembre 2001. Cette loi signée le 26 octobre 2001 pour une durée limitée à quatre années, a été reconduite début 2006 puis prolongée jusqu'en juin 2015.
- Comprend notamment la possibilité de mener l'investigation en l'absence de la personne perquisitionnée, et sans son consentement. Ces dispositions sont relatives aux perquisitions qui portent notamment sur les « books, records, papers, documents and others items » des entreprises.
- Il est interdit aux personnes sollicitées d'alerter quiconque sur le fait que le FBI a recherché ou obtenu des éléments au titre de son intervention.




➢ **La dissémination des données en dehors de France peut entrainer des impacts indirects notamment dans le cadre de l'Outsourcing et du Cloud Computing.**

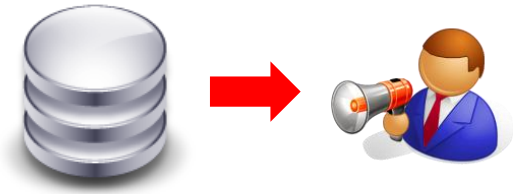


# Une obligation de notification qui se précise

## Futur règlement européen (projet).

- Le 25 janvier 2012, la Commission Européenne a dévoilé des propositions afin de réviser la Directive 95-46 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel. Ce projet prend la forme d'un règlement (avec effet direct dans les pays de l'Union Européenne) et constitue une réforme majeure de la règlementation en matière de protection des données.
- L'article 32 traite des notifications aux personnes concernées. Il prévoit que, suite à la notification à l'autorité de contrôle conformément à l'article 31, (qui devrait intervenir sans retard injustifié et, lorsque cela est possible dans les 24 heures), la notification à la personne concernée doit s'ensuivre sans retard injustifié.
- Une telle notification n'est pas requise quand l'autorité de contrôle est convaincue que «des mesures de protection technologiques appropriées […] ont été appliquées aux données concernées par ladite violation. De telles mesures de protection technologiques doivent rendre les données incompréhensibles à toute personne qui n'est pas autorisée à y avoir accès ».
- Ce règlement pourrait entrer en vigueur d'ici 2014.

➢ **Une obligation de notification qui aura un impact fort sur l'image de l'entreprise en cas de compromission de données personnelles ou médicales avec les conséquences juridiques associées.**



# Cybercriminalité en France

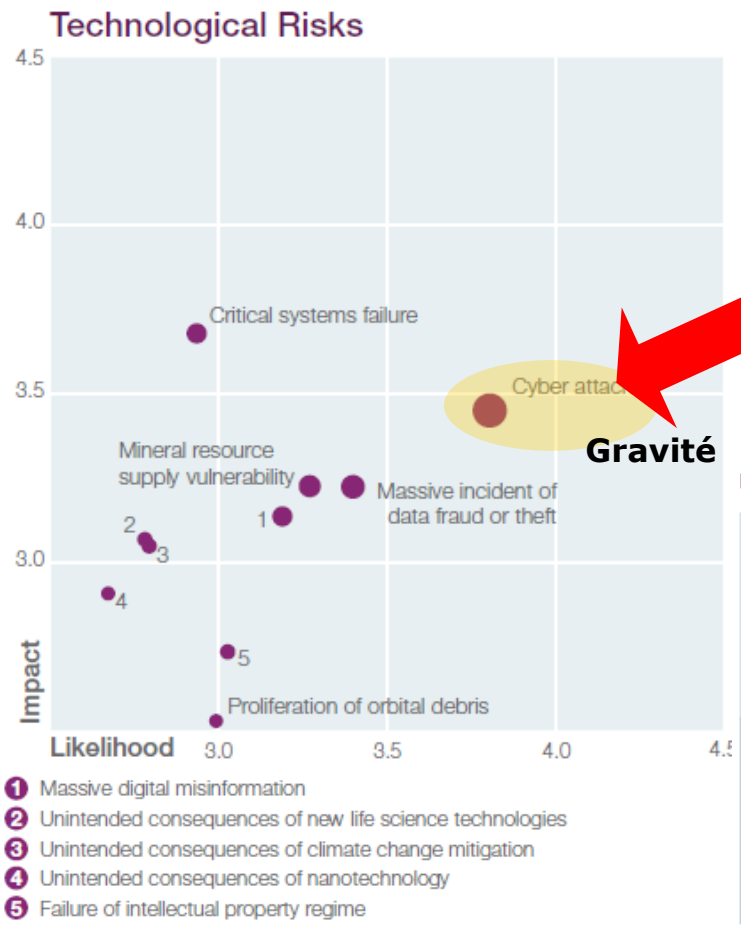
| Infraction | 2009 | 2010 | 2011 | Variations 2009/2010 (en volume et en %) |
|---|---|---|---|---|
| **Atteintes aux systèmes de traitement automatisé des données** | **419** | **626** | **1 139** | |
| *Variations en volume* | - | *+ 207* | *+ 513* | *+ 720* |
| *Variations en %* | - | *+ 49,4* | *+ 81,9* | *+ 171,8* |
| **Accès ou maintien frauduleux dans un STAD** | **416** | **617** | **1 124** | |
| *Variations en volume* | - | *+ 201* | *+ 507* | *+ 708* |
| *Variations en %* | - | *+ 48,3* | *+ 82,2* | *+ 170,2* |
| *dont* Accès ou maintien frauduleux dans un STAD avec altération ou suppression/modification de données | 165 | 241 | 458 | |
| *Variations en volume* | - | *+ 76* | *+ 217* | *+ 293* |
| *Variations en %* | - | *+ 46,1* | *+ 90,0* | *+ 177,6* |
| **Fourniture de moyen matériel ou informatique d'entrave ou d'accès frauduleux à un système informatique** | **3** | **9** | **15** | |
| *Variations en volume* | - | *+ 6* | *+ 6* | *+ 12* |
| *Variations en %* | - | *ns* | *ns* | *ns* |

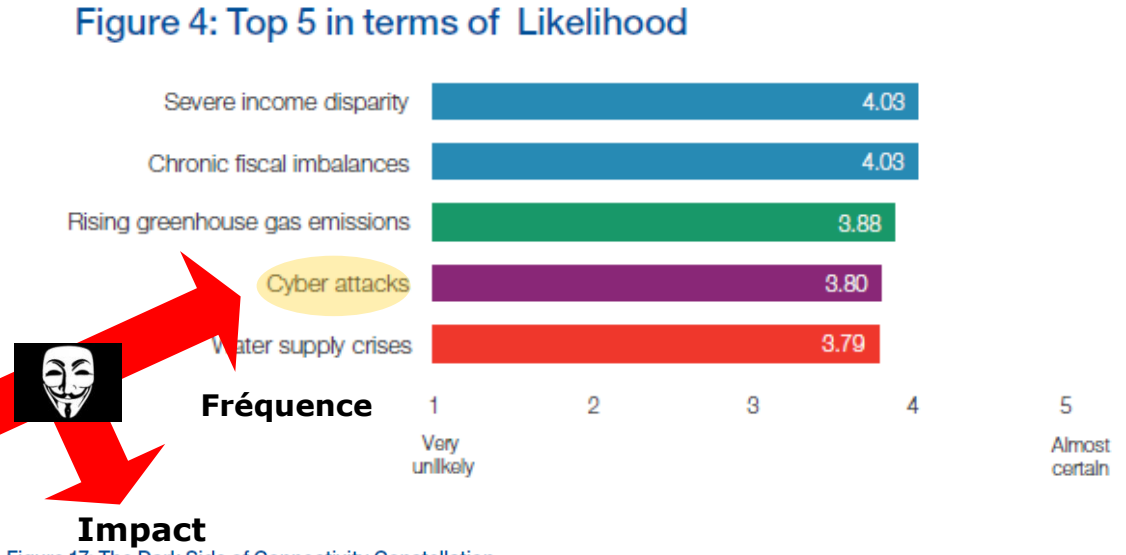
*Source : STIC-BN, DCPJ - JUDEX, DGGN - Traitement ONDRP*

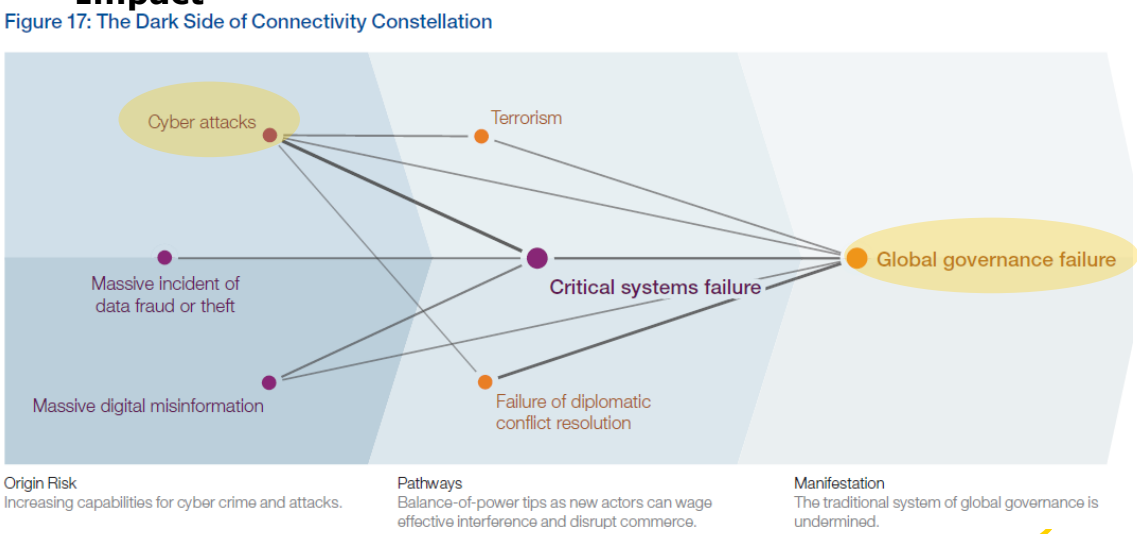
| Infraction | 2009 | 2010 | 2011 | Variations 2009/2010 (en volume et en %) |
|---|---|---|---|---|
| **Escroqueries et infractions économiques et financières commises sur Internet** | **37 357** | **33 928** | **33 944** | |
| *Variations en volume* | - | *- 3 429* | *+ 16* | *- 3 413* |
| *Variations en %* | - | *- 9,2* | *+ 0,0* | *- 9,1* |
| **Escroqueries et abus de confiance** | **28 044** | **27 225** | **27 259** | |
| *Variations en volume* | - | *- 819* | *+ 34* | *- 785* |
| *Variations en %* | - | *- 2,9* | *+ 0,1* | *- 2,8* |
| **Falsifications et usages de cartes de crédit** | **9 313** | **6 703** | **6 685** | |
| *Variations en volume* | - | *- 2 610* | *- 18* | *- 2 628* |
| *Variations en %* | - | *- 28,0* | *- 0,3* | *- 28,2* |

*Source : STIC-BN, DCPJ - JUDEX, DGGN - Traitement ONDRP*

# Les cyber attaques impactent directement la gouvernance d'entreprise (forum de Davos)



# Sommaire

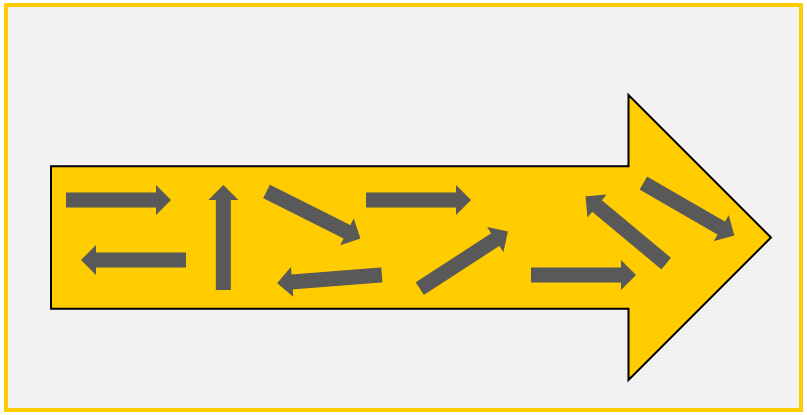
# Quelques travaux normatifs  en cours…….

- **2nd WD 27017 – Information technology – Security techniques – Information security Management -- Guidelines on Information security controls for the use of cloud computing services based on ISO/IEC 27002**

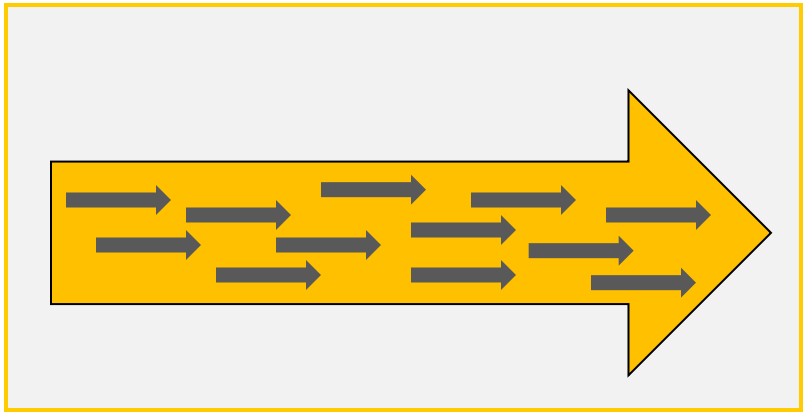
- **1st WD 27018 – Information technology – Security techniques - Code of practice for data protection controls for public cloud computing services**

- **FDIS 27032:2012(E) — Information technology — Security techniques — Guidelines for Cybersecurity.**

# Fédérer les approches au sein du SMSI



Les projets de l'organisation et les efforts humains et financiers ne sont pas orientés dans la même direction. L'atteinte des objectifs individuels ne garantit pas l'atteinte des objectifs collectifs.



Définir les objectifs stratégiques comme moteur de la politique de gestion des risques et de la gouvernance en sécurité et décliner ensuite les leviers d'atteinte de cette stratégie permet de s'assurer que l'ensemble des acteurs de l'organisation contribue à la construction de la même cible.

# Évolution de la posture vis-à-vis de la cybercriminalité (1/2)

- **Plus que jamais nécessité d'une évolution globale de la protection du Système d'Information vers la protection de l'Information**
  - Logique d'entreprise ouverte et communicante centrée sur la maitrise des risques liés à l'information.
  - Catégorisation de l'information
    - Externe/ non structurée (ex : réseaux sociaux)
    - Interne/structurée (ex : fichiers clients)

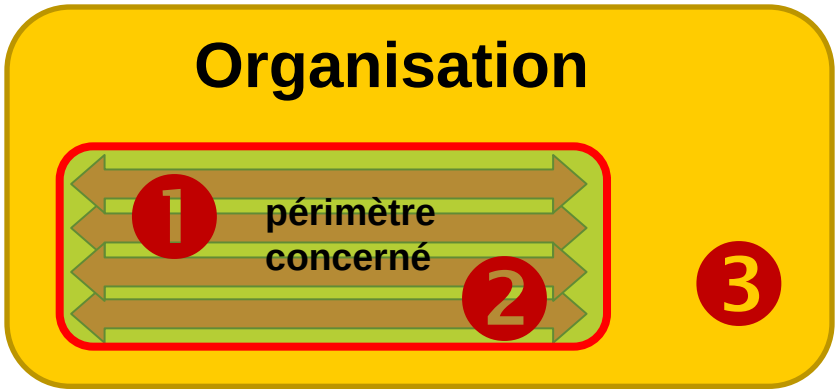
- **Approche systématique par les risques**
  - Prise en compte de l'évolution de la menace (cybercriminalité)
  - Prise en compte de l'évolution des risques des tiers (filiales, outsourcing / cloud)
  - Prise en compte de l'évolution du contexte et des parties prenantes (France , Europe, US, reste du monde)
    - Organisationnelle (filiales, partenaires, prestataires, clients)
    - Technologique (ex( BYOD)
    - Humain, (ex: parasitage commercial (statut auto-entrepreneur)

# Évolution de la posture vis-à-vis de la cybercriminalité (2/2)

- **Élargissement de la prise en compte du contexte légal, réglementaire et contractuelle dans la démarche**
  - Prise en compte de l'évolution des réglementations, lois et jurisprudence (France & Internationale)
  - Évolution des usages (BYOD)
  - Définissant un cadre de mesures vis-à-vis des relations avec les tiers.
- **Importance de la classification de la sensibilité des actifs pour l'entreprise**
  - de nature informationnels (valeurs immatériels) afin de déterminer les moyens de protection adaptés sur les bonnes informations au bon moment et au meilleur cout.
  - Plus sélective à l'heure du Big Data
  - Plus proche des métiers
- **Mise en œuvre d'un plan de traitement des risques adapté**
  - Intégrant des projets spécifiques sur la fraude lié à la cybercriminalité
    - Renforcement du traitement des incidents et de la gestion de crise
    - Identification des signaux faibles (SIEM 2.0)
  - Prenant en compte de la possibilité de s'assurer contre les cyber attaques
- **Évolution de la nature des audits**
  - Renforcement des audits Privacy (ne pas confondre avec audit CNIL)
  - Renforcement des audits de Tiers

# renforcer la relation contractuelle avec les tiers

1 Identifier les processus métiers en fonction des objectifs du SMSI




2 Identifier les actifs sensibles

3 Identifier les relations avec les tiers

4 Définir la solution adaptée

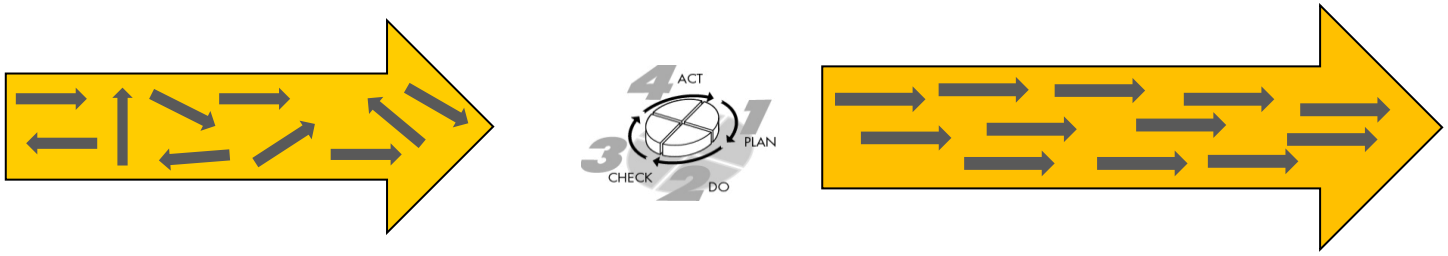
Clauses sécurité dans les contrats Cloud
Données Personnelles : Binding Corporate Rules (Outsoursing)
Conventions de services pour le Cloud privé
Audit ISAE 3402 (ex SAS70)
Audit Technique, Tests d'intrusion
Cyber Assurance (ex Beazley/)

# Renforcer la gestion des risques

- **Coordonner les différentes actions concernant la gestion des risques**
  - ✓ Apporter de la cohérence entre les différents acteurs de la maîtrise des risques (7 acteurs différents),
  - ✓ Lier les risques opérationnels et les risques système d'information.
  - ✓ Permettre la consolidation des risques jusqu'à la cartographie globale de l'entreprise

# Renforcer l'intégration des Systèmes de Management

- **Mettre en œuvre des Systèmes de Management coordonnés au sein de l'entreprise**
  - ✓ Apporter de la cohérence entre les différentes actions de sécurité (audit, tableaux de bord, planification des projets)
    - ✓ La protection de l'information s'appuie sur la norme ISO27001
    - ✓ L'IFACI préconise l'ISO9000 pour la mise en œuvre du contrôle interne
    - ✓ L'AMF recommande l'utilisation de l'ISO31000 pour la gestion des risques
  - ✓ Réduire la sollicitation des opérationnels sur le terrain
    - ✓ Outillage sur les processus communs
    - ✓ Gestion intégré des différents risques (OP,SSI)
    - ✓ Harmonisation du vocabulaire qualité dans les différentes systèmes de management
    - ✓ Mutualisation possible des audits (qualité, sécurité, Contrôle Interne,….)



# Des Questions ?

Cyber Security Consulting Team

Global Cyber Innovation Center

Biometrics Software Innovation Lab

**Thierry Jardin**
**Directeur Associé,**
**thierry.jardin@logica.com,**
**Tél: 01 57 87 45 16**

Security Operation Centre

Common Criteria, Crypto Module Lab