

# Intelligence économique : Sécurité et dynamique de l'entreprise

- Philippe LEMELLETIER : Avocat de sociétés, chargé de l'intelligence économique et de la contrefaçon pour les Conseillers du commerce extérieur de la France, Nouvelle Aquitaine, chargé d'enseignement (intelligence économique, droit international, ...)
- Olivier GRALL : Délégué régional de l'ANSSI (Agence nationale de la sécurité des systèmes d'information).

## Thèmes abordés :

1. L'intelligence économique

2. Sécurité informatique

# **1. Intelligence économique**

- **Maîtrise des informations stratégiques de l'entreprise :**
  - Information = une des principales richesses de l'entreprise
  - Très convoitées
  - Dès 2004, l'Etat a mis au point organisation, incitation et moyens
  
- **3 axes de la politique d'intelligence économique :**
  - Protection de l'information
  - Recherche de l'information
  - Développement de l'influence

- **Des mesures simples :**

- Déterminer les informations à protéger
- Les mesures à prendre
- Implication du personnel
- Tests, contrôles, RETEX

- **Illustration des aides apportées à l'entreprise :**

- Commission « Nouvelle Aquitaine - PME sans contrefaçon »
- CCEF / Corps de l'Etat intervenants
- Qualifie et aide les entreprises à trouver une solution

## **2. Le risque Informatique**

- **La Multiplication des systèmes connectés augmente la surface d'attaque**
  - De plus en plus d'outil de maintenance à distance
  - Des objets connectés mal sécurisés
  - Des systèmes hétérogènes difficiles à maintenir
  
- **Le cyberspace déshinibe les velléités offensives des personnes ou Etats**
  - Un Espace sans frontière
  - Anonyme
  - En dehors du champ juridique

# Le risque Cyber : premier risque en entreprise

Periode COVID “Plus de 400% d'augmentation de tentatives d'hameçonnage ont été constatées”

Jérôme Notin, DG du site [cybermalveillance.gouv.fr](http://cybermalveillance.gouv.fr)

France Inter le 31 mars 2020



Arnaque



Vol de données



Ransomware



Défiguration de site web

# Quels Préjudices ?

- Destruction ou vol de données
- Perte d'activité, arrêt de la production
- Retard de livraison
- Dégradation de l'image
- Chomage technique
- Sanctions financières (pénalité de retard , amende ,etc..)
- Coût de la réparation (matériel et prestation de service)

- Cout Moyen d'une CyberAttaque : Entre 200 000 et 1 300 000 euro

# Quelles Solutions ?

- **L'analyse de risque devient un prérequis à la Transformation Numérique:**
  - Risques liés aux choix techniques
  - Risques liés aux données à caractère personnel
  - Risques liés à la localisation des données
  - Risques liés à la sous-traitance
  - Risques liés aux interventions à distance