Le financement de la continuité d'activité par l'assurance

Spécificité de l'assurance de l'information

Adaptation des garanties aux besoins

Démarche de souscription

Appels en garantie

Pascal Lointier
Ingénieur Sécurité des S.I.

« Tech Days » Microsoft

6 février 2007

L’assurance de l’information ?

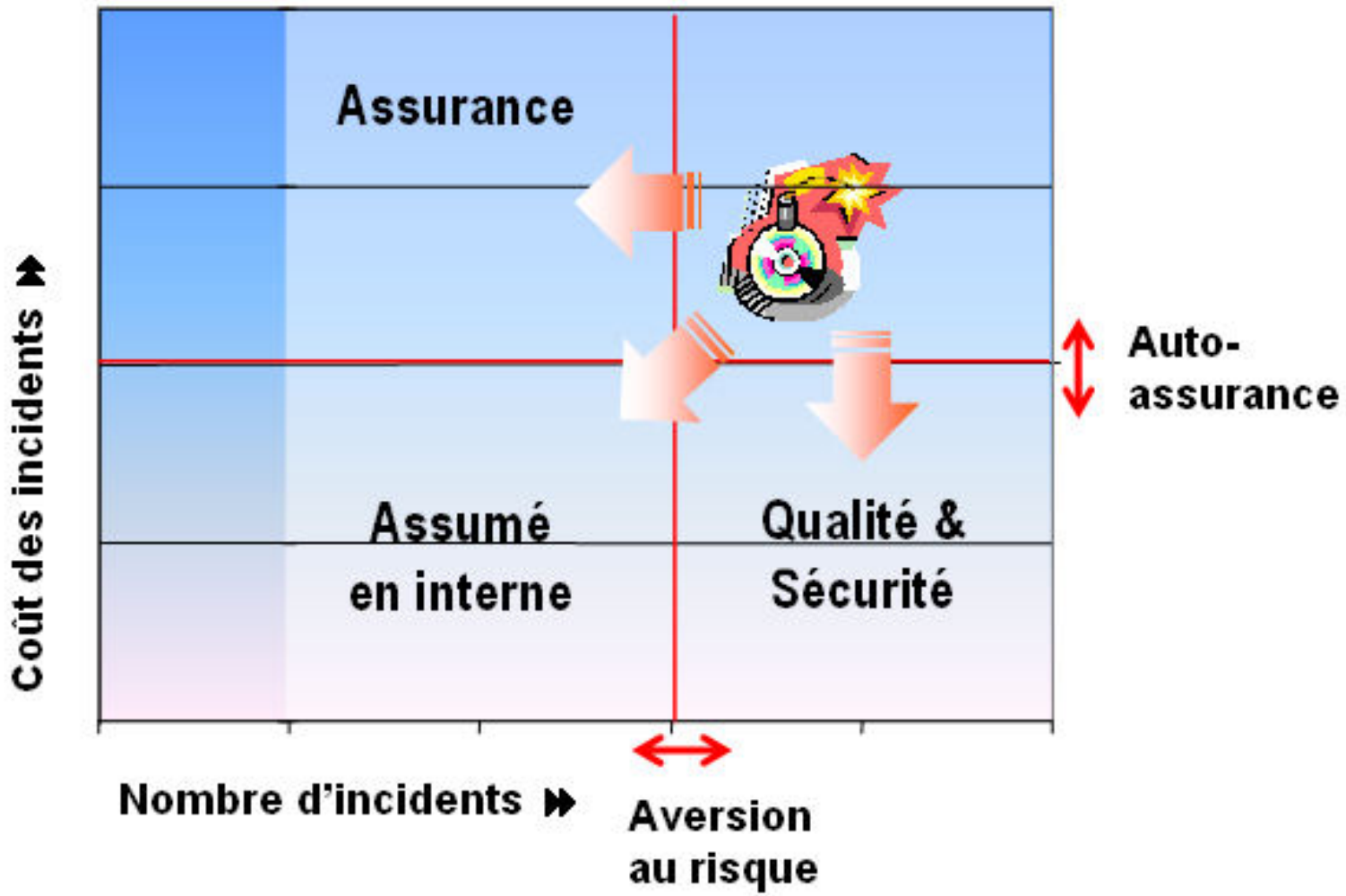
- **Un produit financier pour**
  - Remettre le système d’information en son état avant sinistre
  - Rembourser des conséquences économiques et du préjudice (charges fixes, pertes d’exploitation, bénéfice non réalisé, etc.)
  - … quelque soit (ou presque !) le fait générateur, accidentel ou malveillant

L’assurance du S.I. doit se concevoir comme…

✓**Un programme de protection de l’activité et des bénéfices de l’entreprise …**

- Qui répond au besoin du transfert du risque résiduel…
- Dans un contexte d’événement grave (risque de sévérité)…
- Et comme financement possible de l’activation du PCA (Plan de Continuité de l’Activité)

L’assurance, complémentaire à la politique de sécurité



Le contexte: essor de l'économie numérique et nouveaux risques

- ✓**Société du « tout numérique »**
  - **Marketing, gestion et comptabilité**
  - **Production**
  - **Régulation et logistique**
- ✓**Environnement à risque**
  - **Dépendance / criticité de l'activité vis-à-vis de l'information numérique**

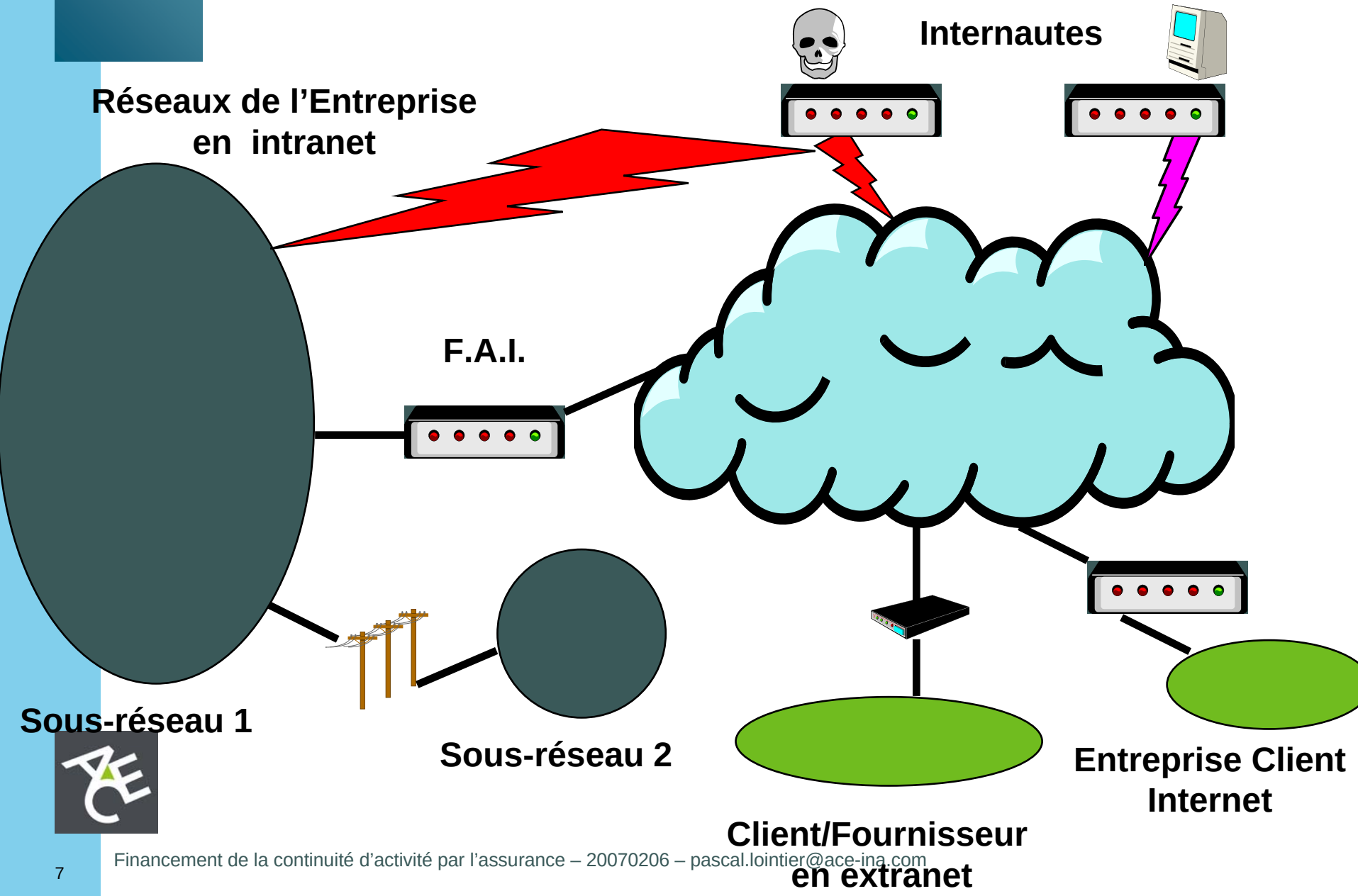
✓**Cette dépendance de plus en plus critique est parfois mal identifiée**

- **Messagerie électronique**
- **Information décisionnelle**
- **Traçabilité réglementaire (agro-alimentaire, chaîne du froid…)**

Evolution des architectures informatiques

- ✓ **Décentralisation : du terminal-hôte au client-serveur**
- ✓ **Distribution : les données brutes deviennent des informations**
- ✓ **Externalisation (des traitements)**
- ✓ **Interconnexion (des réseaux et des entreprises)**
- ✓ **Atomisation (réduction de taille des équipements)**
- ✓ **Nomadisation (mobilité et connexion à distance)**

Interconnexion des réseaux



Le patrimoine informationnel

- **Les données**
  - Données de Recherche-Développement
  - Données de production
  - Données de gestion
  - Informations nominatives
- **Les programmes (propriétaires)**
- **Les ressources (informatique et télécoms)**
  - Abus
  - Hébergement clandestin
  - Déni

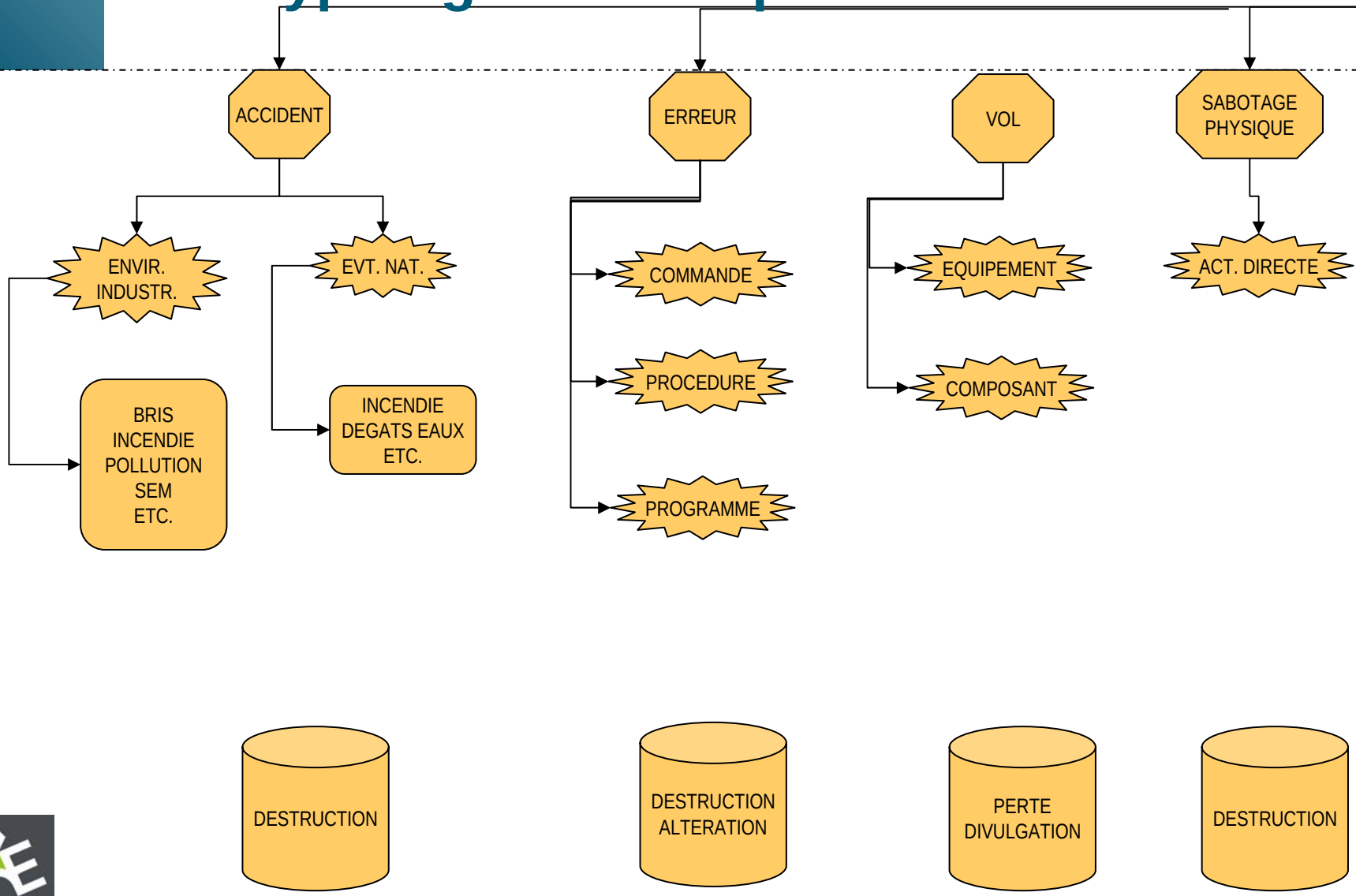
… Le patrimoine informationnel

- **La fraude financière**
  - Les détournements de fonds, la surfacturation
  - Les extorsions
  - La fraude à la vente par correspondance
- **Le vol de biens (assisté par informatique)**
  - Informatiques
  - Matières premières
  - Produits finis
- **L'image et la notoriété véhiculées *via* les réseaux**
- **La cotation financière**

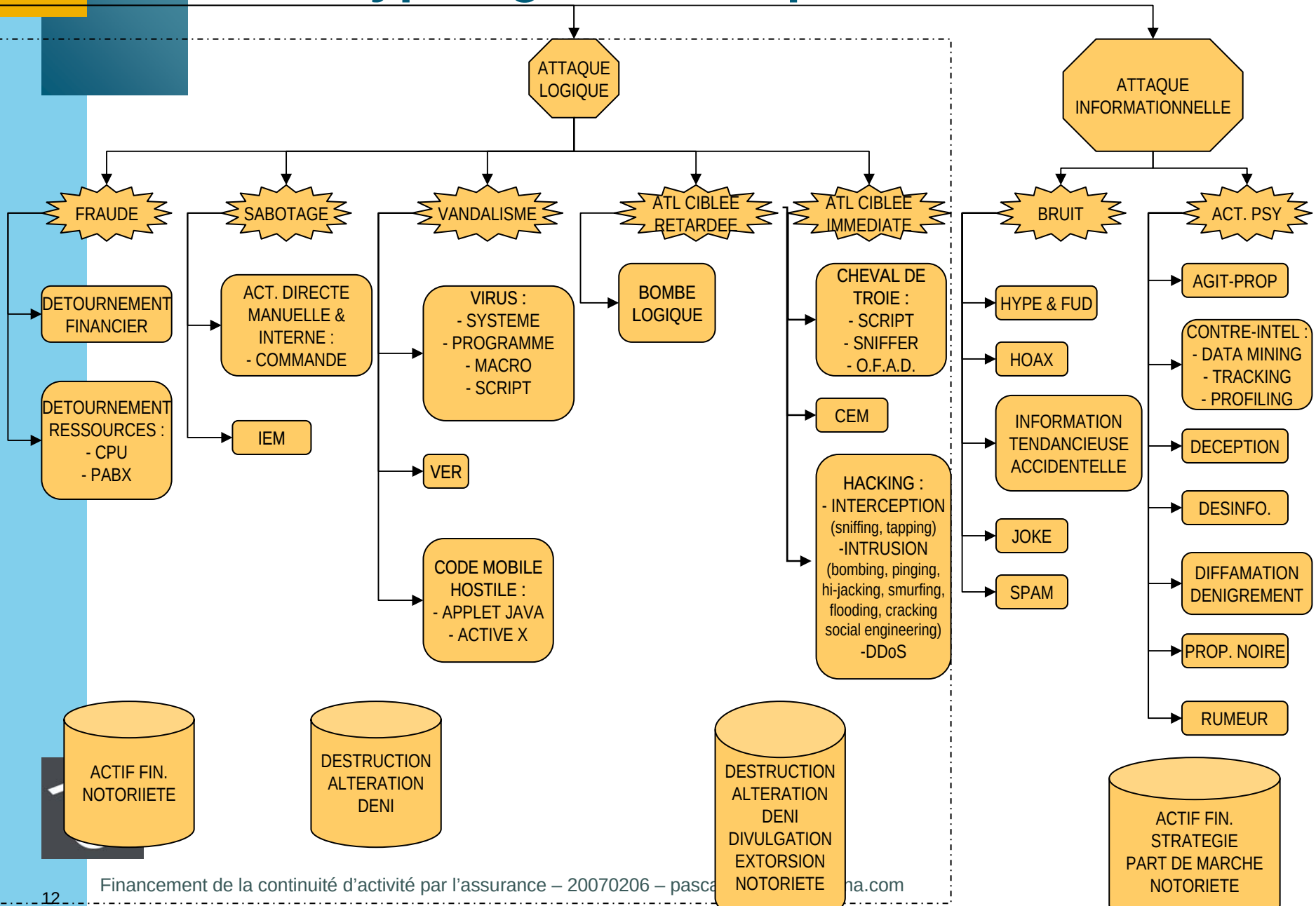
Vulnérabilités des Systèmes d'Information

- **Techniques**
  - **Faiblesses de conception (architectures, etc.)**
  - ***Bugs* (failles de sécurité) des programmes (y compris solutions de sécurité: antivirus, pare-feu)**
- **Organisationnelles**
  - **Architectures permissives**
  - **Emploi de versions non corrigées des erreurs**
  - **Administration non sécurisée de l'exploitation**
- **Humaines**
  - **Méconnaissance de la menace**
  - **Insouciance des utilisateurs… et/ou de la Direction**
  - **Internautes : connexions sans sécurité suffisante**

Typologie des risques informationnels



...Typologie des risques informationnels

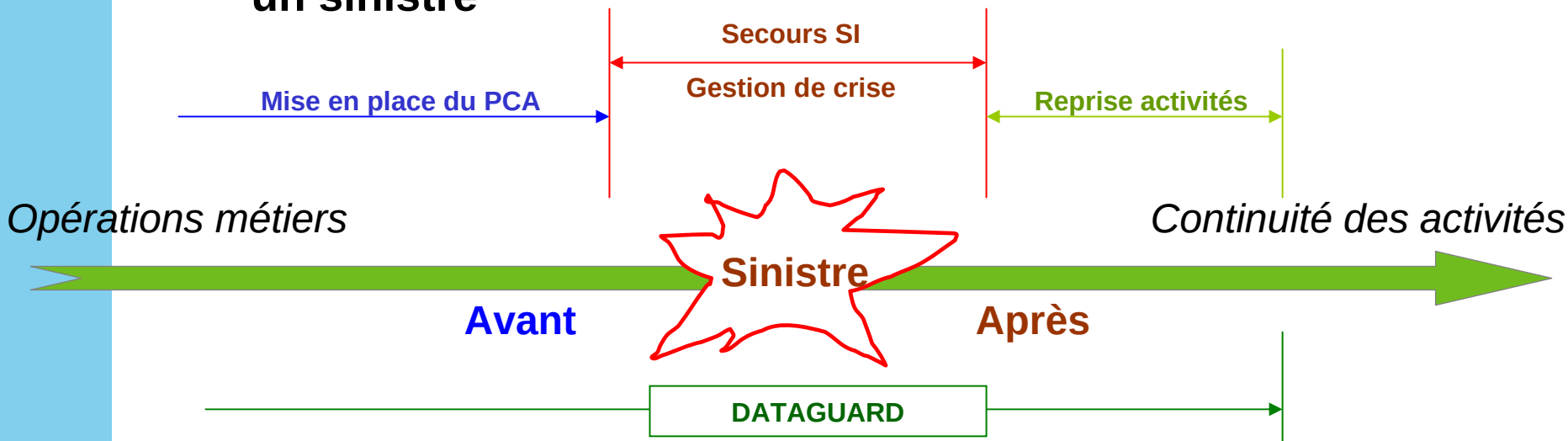


Typologie des acteurs de la malveillance

- ✓ **Personnel de l'entreprise**
- ✓ **Personnel de prestataires**
- ✓ **Mécontents**
- ✓ **Concurrence**
- ✓ ***Hackers*, *Crackers*, *Phreakers*, etc.**
- ✓ **Crime organisé (OCT, organisation criminelle transnationale), petite délinquance**
- ✓ **S.R. (service de renseignement) et S.R.P. (société de renseignement privée)**

DataGuard (ACE Europe), des ressources financières pour …

✓ **Couvrir les Frais techniques de réinitialisation du SI après un sinistre**



✓**Frais supplémentaires**

- Dépenses consenties pour éviter ou limiter l'arrêt de l'activité

✓**Pertes d'exploitation**

- Impact sur le Chiffre d'Affaires (charges fixes, profit)

✓**Perte d'image ou de notoriété**

✓**Pertes de valeurs et de biens (volet fraude)**

✓**Virus…**

Rappel sur les principes de l’assurance

✓**Existence d’un aléa**

✓**Fait générateur connu et dans le périmètre de garantie**

✓**Pas d’enrichissement de l’assuré (principe indemnitaire)**

✓**Obligation de conseil de la part du courtie d’assurances**

Le contexte d'assurance

- **A déconnecter de la TRI (Tout Risque Informatique) ou équivalent qui rembourse la remise en état et certaines conséquences à la seule suite d'un dommage physique au matériel/composants électronique**
  - Valeur à neuf ou vétusté déduite
- **Exclusion « Cyberdata » du marché de l'assurance**
  - Virus et dommages immatériels
  - Exclusions spécifiques à la compagnie

Le périmètre d'étude

- ✓**Tous les S.I. de l'entreprise**
  - Gestion
  - Production
  - Téléphonie
  - Infogérance (externalisation)
- ✓**Les filiales juridiques**
  - Sans contrainte de localisation
- ✓**Possibilité de greffe sur programmes d'assurance existants**

Les faits garantis

- ✓ **Accidentels**
  - Evénements naturels (incendie, dégâts des eaux…)
  - Evénements industriels (ex. perturbation électromagnétique)
  - Erreurs de manipulation (procédure ou exploitation)

- ✓ **Malveillants**
  - « Tout usage non autorisé du système »
    - Abus de ressource, altération, destruction
  - Programme autoreproducteur (ver ou virus)

Les faits difficilement assurables

- **La divulgation d'information**
  - Valorisation du préjudice ?
  - Engagement Responsabilité Civile (cf. conclusion): mise en cause, charge de la preuve, etc.

- **Erreurs de conception et de programmation**
  - A l'exception de la faille de sécurité lorsqu'elle est le moyen de réalisation d'une intrusion ou d'une propagation virale

Les options de couverture

- **Reconstitution de l'information**
- **Frais supplémentaires et pertes d'exploitation**
  - Reconstitution d'image
  - Ou encore pénalité de retard
- **Virus**
- **Fraude assistée par informatique**
  - Enrichissement d'un tiers, surfacturation de l'assuré,
- **Matériel (cf. TRI)**
- **D'autres extensions…**
  - Carence de fournisseur
  - Extorsion…

La démarche de souscription

- ✓ **L'entretien de souscription, véritable point de situation des enjeux et vulnérabilités**
- ✓ **4 étapes d'entretien (avec DG, DAF, DSI, RSSI)**
  - Activités générant le chiffre d'affaires
  - Dépendance vis-à-vis de l'information numérique
  - Description globale du système d'information
  - Présentation des politiques de sécurité
- ✓ **Les questionnaires**
  - Cotation indicative et/ou questionnaire principal comme aide à l'entretien et *check-list* de bonnes pratiques

La démarche de souscription

- **Modularité et flexibilité permettent**
  - L'adaptation
  - La montée en puissance
  - En complément des garanties existantes

- **Le conseil en fin de visite**

  (ce n’est pas un audit)

- **Le contact en cours d’activité**

- **La réactivité lors d’un appel en garantie**

Les éléments de discussion

- ✓**Le montant assuré (le montant total remboursé par l'assureur)**
- ✓**La prime !**
- ✓**La franchise, exprimée en euros ou en jours (heures) d'exploitation**
- ✓**Les sous-limites pour certains faits générateurs**
- ✓**Les obligations de l'assuré**

Quelques faux écueils de souscription

- ✓ **“Ce sont des pros”**
  - Ne jamais présumer du professionnalisme en sécurité de l’information…
- ✓ **“J'ai toutes les sécurités”**
  - Des sauvegardes
    - Mais sont-elles testées ? Conservées hors-site ?
  - Un antivirus
    - Mis à jour ? Par rapport à des virus à diffusion très rapide. Et les postes portables ?
  - Il y a un responsable sécurité
    - C’est un homme-orchestre. La sécurité c’est l’affaire de tous !

Quelques faux écueils de souscription

- **"J'attend d'y voir plus clair“**
  - L’assurance c’est
    - Le transfert du risque résiduel quelle que soit l’excellence des politiques de sécurité
    - Le financement de plan de continuité
    - Le remboursement du préjudice
    - … il n’y a donc pas lieu d’attendre !
  - L’incident peut survenir à tout moment…

Appel en garantie

- ✓**Reprendre l'activité normale au plus tôt**
- ✓**… en évitant le sur-accident**
- ✓**Historiser : éléments, indices permettant la reconstitution des événements, la nature du fait générateur, l'impact**
  - Tableau de bord de gestion de crise
- ✓**Possibilité d'un avis purement consultatif**

En conclusion

✓**Les produits d'assurances s'adaptent aux besoin des entreprises dans une économie dépendante de l'information numérique**

- ☞ Identifier les acteurs offrant des garanties appropriés et susceptibles de vous accompagner dans la gestion du sinistre

  D'autre garanties existantes comme la Responsabilité Civile Professionnelle adaptée à l'activité Internet

  Contexte réglementaire évolutif quant à la protection de l'activité financière