



HERVÉ SCHAUER CONSULTANTS
Cabinet de Consultants en Sécurité Informatique depuis 1989
Spécialisé sur Unix, Windows, TCP/IP et Internet



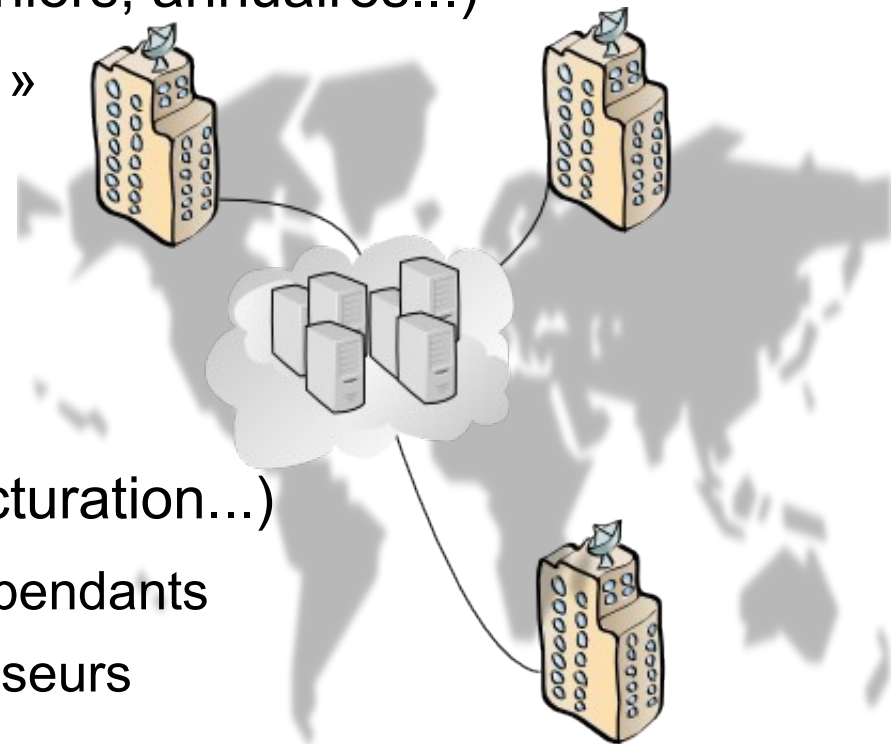
La gouvernance de la sécurité étendue

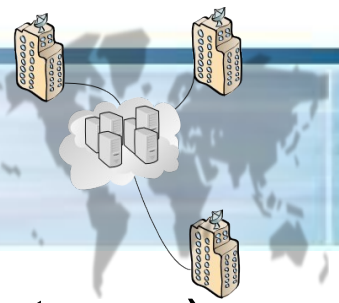
Raphaël Marichez
<Raphael.Marichez@hsc.fr>

- Besoins et typologies observés
- Quelques risques induits observés
 - Techniques
 - Organisationnels
- Pistes de réponses par l'exemple
- Conclusion
 - Evolutions
 - Quelques conseils

**Les transparents seront
disponibles sur
www.hsc.fr**

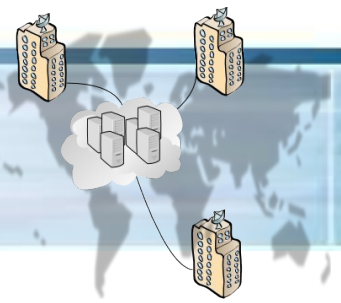
- Le SI de l'entreprise étendue (1 : au sein de l'entreprise)
 - **Fonctions dites « de siège »**
 - Centralisation de l'information (fichiers, annuaires...)
 - => Création d'intranets « Groupe »
 - => GPO Groupe
 - Besoins du métier
 - Obligations légales (logs)
 - Dématérialisation (archivages, facturation...)
 - => Interconnexions entre SI indépendants
 - => Partenaires, ou clients-fournisseurs





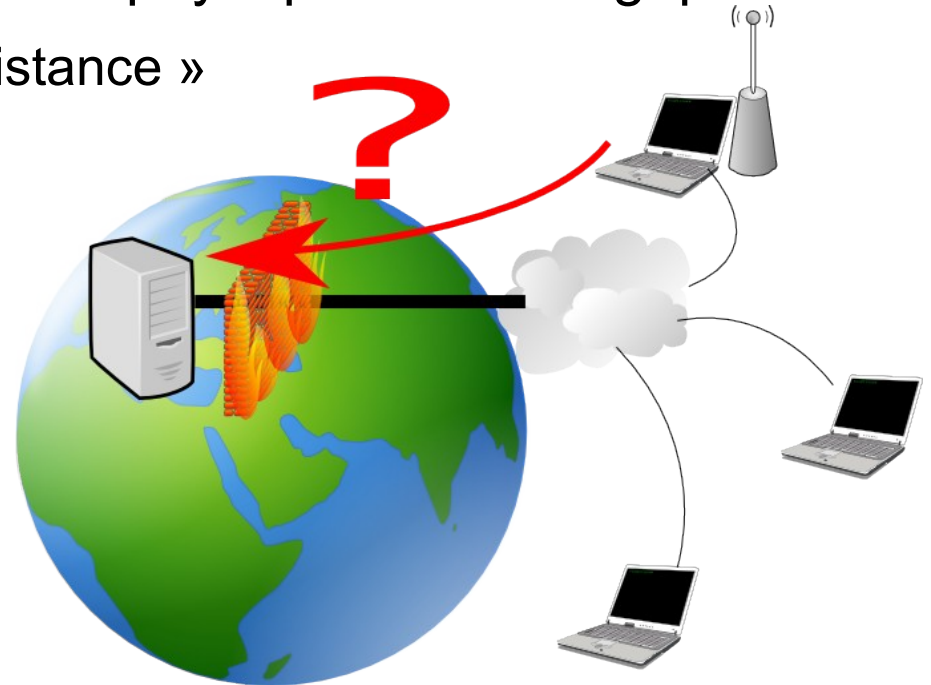
- Le SI de l'entreprise étendue (2 : mobilité des utilisateurs)
 - Sur un même site
 - => Contournement des DSI : Sans-fil, switches, clés USB, Bluetooth...
 - Entre les sites de l'entreprise
 - => Création de backbones « Groupe » (VPN/MPLS, cloisonnés)
 - Partout sur internet
 - => Points d'accès VPN
 - => Contournement des DSI : GoogleApps, GoogleCode, Blackberry...
 - Chez soi
 - => Conflit professionnel / personnel et vulnérabilité du poste de travail
 - => Contrôle d'accès se déplace du physique vers le logique



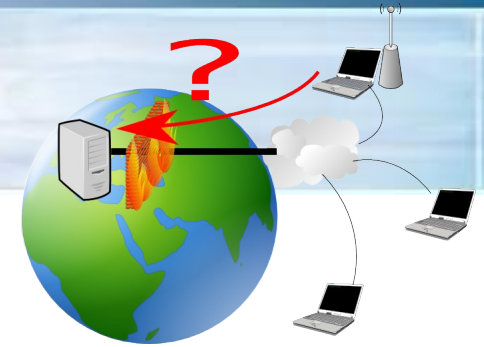


- Le SI de l'entreprise étendue (3 : sous-traitance)
 - Spécialisation du métier (hébergement, infogérance...)
 - Etre conforme aux normes de sécurité ou exigences des contrats
 - => **Externalisation**
 - Réduction du coût marginal lié à l'infrastructure (bâtiment, clim...)
 - => **Mutualisation** (voire virtualisation)
 - Principalement **trois typologies**
 - Prestations
 - Service fourni par une filiale
 - Service fourni par un GIE (centre de « services partagés »...)
 - Augmenter encore le facteur d'échelle + disponibilité
 - => **Cloud** (storage, computing)
 - **Retour sur investissement ?**

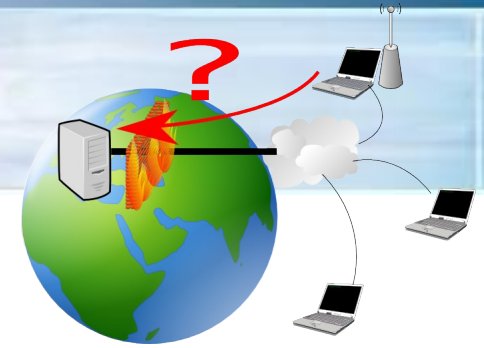
- Sécurité technique (1)
 - Déplacement du contrôle d'accès du physique vers le logique/virtuel
 - « Solutions d'administration à distance »
 - « de postes nomades »



- Poste client nomade :
augmentation des menaces
 - A cause du travail à domicile (ou dans les lieux publics)
 - Course des mises à jour
 - => Authentification forte, tokens, cartes à puce...
 - => GPO fortes sur la forêt Active Directory (penser à la hotline !)

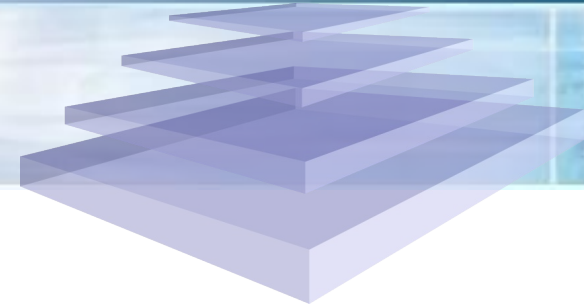


- Sécurité technique (2)
 - Déplacement du contrôle d'accès du physique vers le logique/virtuel
 - Habitudes de la sécurité physique (industries, usines, entrepôts...)
 - Sans-fil
 - Limitations des équipements (ex.: lecteurs de codes barres)
 - Terminaux non connectés, mais avec des ports USB...
 - SCADA accessibles en VPN (au mieux), RTC (au pire)
 - Virtualisation
 - Certitude du cloisonnement du système sous-jacent ?
 - Mutualisation
 - Surface d'exposition
 - Colocation : dommage colatéraux (ex. : serveurs d'envoi de mails)



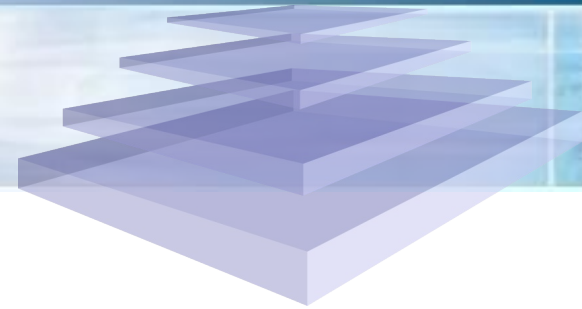
- Sécurité technique (3)
 - Déplacement du contrôle d'accès du physique vers le logique/virtuel
 - Sous-traitance
 - Télémaintenance, infogérance
 - RTC
 - Comptes partagés





- Sécurité technique (4)
 - Complexité de l'infrastructure (1)
 - Niveaux successifs d'empilement
 - Interconnexions de réseaux virtuels
 - Conflits d'adressages
 - => NAT (traduction d'adresses réseaux) partout
 - => traçabilité des accès ?
 - Continuité d'activité : retour à la normale ?
 - Flux restés ouverts sur les pare-feux
 - Tout-IP
 - Téléphonie / LAN
 - Scanneur / sécurité incendie





- Sécurité technique (5)
 - Complexité de l'infrastructure (2)
 - Demain (?) : tout HTTP
 - Contournement des filtres actuels
 - Création de protocoles de niveau 3 puis 4 dans XML/HTTP
 - Rappels TCP : débuts en 1974, dernières failles en ... 2009 (MS09-048)
 - Encore très peu audité / auditable
 - Milieux industriels surtout
 - AEX cfiXML « The potential annual savings for capital facility industries are millions of dollars [citation needed] »
 - PRODML (secteur de l'énergie)
 - => Filtrage HTTP, validation XML
 - => **Firewalls XML !!**

- Sécurité organisationnelle (1)
 - Responsabilités : qui fait quoi ?
 - Dé-responsabilisation des propriétaires des informations
 - Mutualisation
 - Au mieux : exigences de sécurité spécifiées par écrit
 - Quid des audits ?
 - Au pire : rien du tout
 - Traçabilité
 - PCA

Assurer la continuité d'activité

██████████ présente ci-après son analyse des risques liés à chacun de ses métiers et les actions envisagées pour assurer la continuité de service pendant les phases d'alerte 5B et 6.

Hébergement

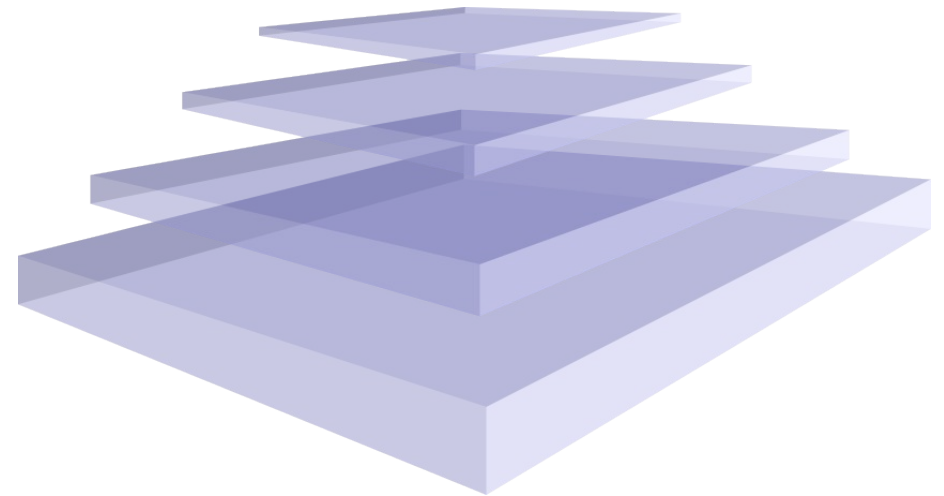
██████████ contrôlé la mise en place de Plans de Continuité d'Activité dans les ██████████ datacenters de ses partenaires ██████████ dispose d'équipements actifs.

Sur ses sites de production ██████████ gère elle-même l'ensemble des opérations liées à l'hébergement sécurisé d'équipements informatiques : mise à disposition et gestion de l'espace, de l'électricité, de la climatisation, de la sécurité anti-incendie, de la sécurité d'accès et du monitoring.

Nous avons également demandé à chacun de nos sous-traitants de confirmer la mise en œuvre d'un plan de continuité d'activité en cas de confirmation de la pandémie, afin de s'assurer d'un fonctionnement minimal en situation de crise.

- Sécurité organisationnelle (2)
 - Dilution des risques sur les intervenants
 - Facile d'être conforme aux normes ou aux contrats en externalisant
 - Titrisation du risque : contrats

- Risques portés par des tiers
- Pyramide des risques
- « Produits structurés »



```
relaismsg.minefi.gouv.fr[194.250.149.46] said: 554 Service unavailable;  
Client host [129.104.xx.xx] blocked using relays.ordb.org; ordb.org was  
shut down on December 18, 2006. Please remove from your mailserver.
```

- Sécurité organisationnelle (3)
 - Perte de maîtrise
 - Sauvegardes externalisées.... plusieurs fois
 - Scans de vulnérabilités qui ne trouvent rien

```
16:24:17 ipt: [hnpt] in drop: SRC=10.40.250.12 (...) DPT=554 (...)
16:24:17 ipt: [hnpt] in drop: SRC=10.40.250.12 (...) DPT=22 (...)
16:24:17 ipt: in accept: SRC=10.40.250.12 (...) DPT=80 (...)
16:24:17 ipt: in accept: SRC=10.40.250.12 (...) DPT=443 (...)
16:24:17 ipt: [hnpt] in drop: SRC=10.40.250.12 (...) DPT=256 (...)
16:24:17 ipt: in drop: SRC=10.40.250.12 (...) DPT=113 (...)
16:24:17 ipt: in accept: SRC=10.40.250.12 (...) DPT=25 (...)
16:24:17 ipt: [hnpt] in drop: SRC=10.40.250.12 (...) DPT=389 (...)
16:24:17 ipt: in drop: SRC=10.40.250.12 (...) DPT=9090 (...)
16:24:17 ipt: in accept: SRC=10.40.250.12 (...) DPT=53 (...)
16:24:17 ipt: in drop: SRC=10.40.250.12 (...) DPT=1723 (...)
16:24:17 ipt: in drop: SRC=10.40.250.12 (...) DPT=3389 (...)
16:24:17 ipt: [hnpt] in drop: SRC=10.40.250.12 (...) DPT=144 (...)
16:24:17 ipt: in now banned: SRC=10.40.250.12 (...) DPT=29 (...)
16:24:17 ipt: in was banned: SRC=10.40.250.12 (...) DPT=1527 (...)
16:24:17 ipt: in was banned: SRC=10.40.250.12 (...) DPT=581 (...)
16:24:17 ipt: in was banned: SRC=10.40.250.12 (...) DPT=10005 (...)
16:24:17 ipt: in was banned: SRC=10.40.250.12 (...) DPT=68 (...)
```

- Scans de vulnérabilités qui ne trouvent rien

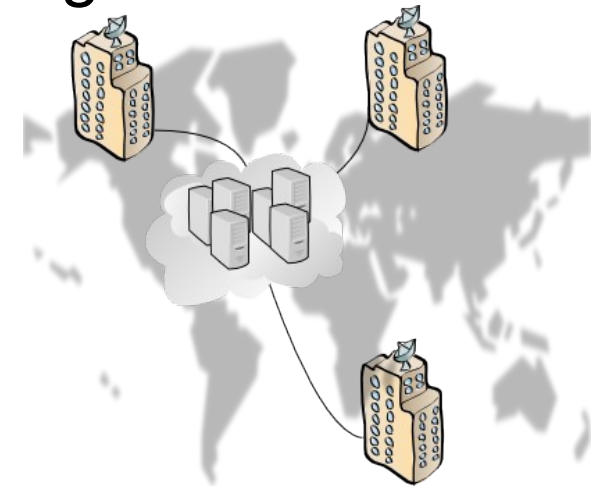
```

Interesting ports on serv.si.intra (10.20.103.12):
Not shown: 1234 filtered ports
PORT      STATE  SERVICE VERSION
25/tcp    open   smtp?
53/tcp    open   domain?
80/tcp    open   http?
443/tcp   open   https?
Too many fingerprints match this host to give specific OS details
    
```

Summary:
 No known vulnerability
 No information leak on version or OS
Excellent security level

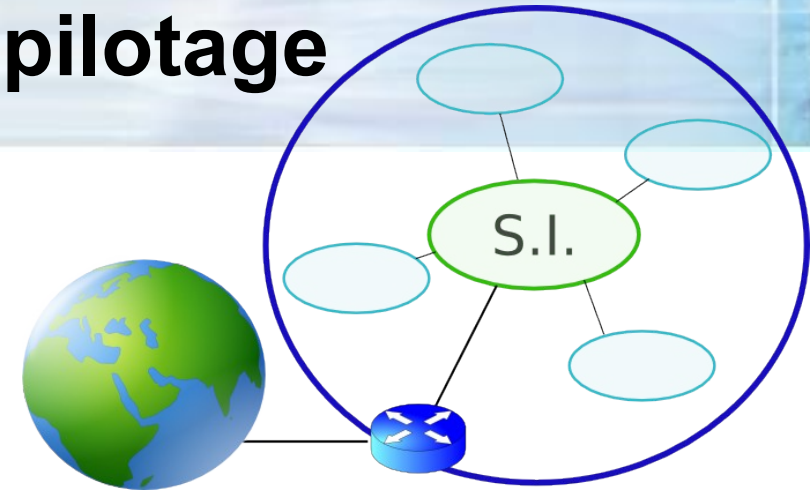
Date	Etat	Action
22/02/2009	KO http	httpd.conf: ServerTokens Prod
23/03/2009	OK	
21/04/2009	OK	
21/05/2009	OK	
22/06/2009	OK	
21/07/2009	OK	

- Sécurité organisationnelle (5) : parenthèse légale
 - Réponse aux réquisitions judiciaires
 - Recherche de la responsabilité
 - Traçabilité
 - Informatique et Libertés
 - Flux trans-frontières : déclarations obligatoires
 - Sous-traitance : contractualiser les exigences de sécurité
 - Intranets groupes et localisation des données
 - Compétences des tribunaux éloignés
 - Différences culturelles :
 - Recherche de preuves
 - ... dans des sauvegardes off-shore
 - ... chez des anciens prestataires dont on avait oublié l'existence !
Poursuites pour « destruction d'information »



- Première piste : via la gestion de risques SI
 - Gestion de risques est plus globale que « appréciation de risques »
 - Gérer les risques liés aux tiers !
 - => audits des tiers
 - => actions d'amélioration
 - => commercial, gestion de projet, conduite du changement...
 - Retour sur investissement ?
 - => **Piloter** les actions d'amélioration

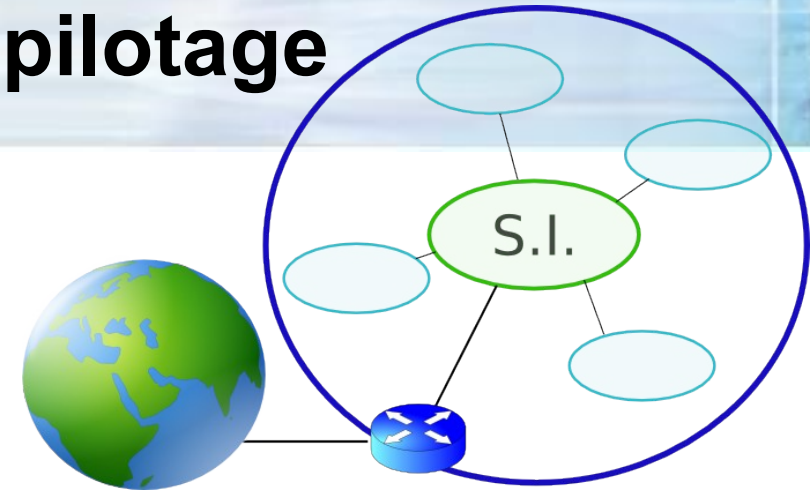
- Deuxième piste : pilotage de la SSI
- Cas 1 : Service partagé (ex. : GIE)
 - Rôle : décideur + maîtrise d'oeuvre
 - S'audite lui-même, éventuellement par un tiers (dans le meilleur des cas)
 - Audit interne = à l'initiative de l'audité ; pas d'obligation d'agir
 - Conséquences
 - Peut ne pas appliquer les règles de sécurité du Groupe
 - Si un « client » du Groupe demande un dispositif de sécurité :
 - Soit il ne se passe rien (le GIE n'étant pas moteur)
 - Soit il émet des propositions -> devis -> facturation interne
 - Relation client-fournisseur non saine



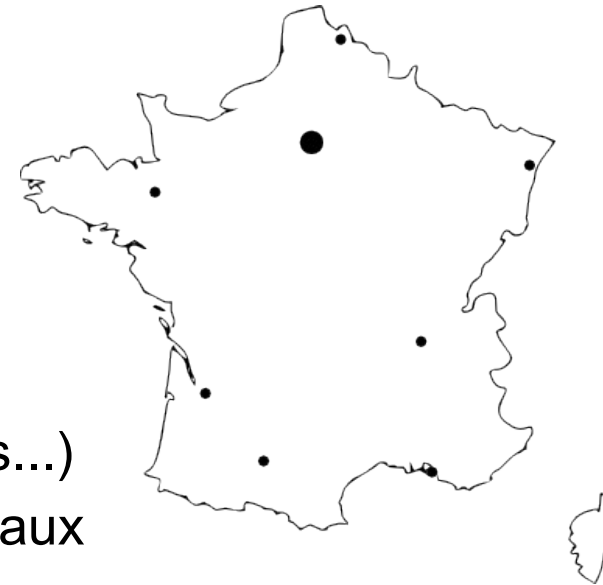
- Cas 1 : Service partagé (ex. : GIE)

- **Finalemment**

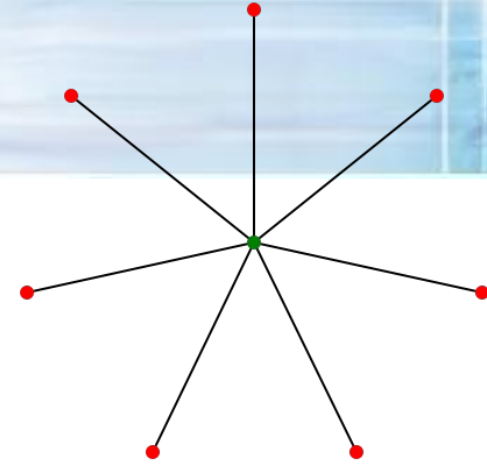
- Le GIE est-il chargé de la MoE de la SSI ?
- Si oui, est-ce normal qu'il refacture ?
- Moyens de pressions des « clients » internes au Groupe ?
 - Cas grave qui remonte au Groupe (piratage, test très démonstratif...)
 - Peu satisfaisant
 - Filialiser le GIE, voire le vendre
 - Scinder le GIE
 - Pilotage et audit *versus* MoE opérationnelle
 - Nécessite des moyens réels fournis par le groupe :
 - Moyens humains et financiers pour la MoE
 - Autorité du pilotage et de l'audit



- Cas 2 : Sites autonomes (ex. : MEN, recherche, CNRS...)
 - Forte centralisation : PSSI globale et déclinée
 - Auditeur indépendant = ANSSI (ex-DCSSI)
 - Pilotage et ressources propres à chaque site
 - Hétérogénéité :
 - des niveaux de sécurité
 - des solutions retenues (produits, fournisseurs...)
 - Coordination via des correspondants sécurité locaux

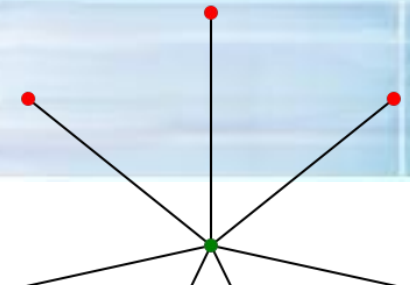


- Cas 2 : Sites autonomes (ex. : MEN, recherche, CNRS...)
 - **Risques**
 - Surcoût important (ré-inventer la roue)
 - Avantage : limitation du périmètre éventuellement compromis
 - Inconvénient : diversité
 - => plus facile de trouver au moins une faille
 - => fort risque d'atteinte à l'image de marque (institutions)
 - => une information bien protégée ici ne l'est plus ailleurs
 - => audit plus difficile
 - Manque de moyens locaux
 - Politique globale qui dévie de la réalité du terrain
 - **Solution : volonté politique SSI à haut niveau (=> secteur public)**



- Cas 3 : Groupe et filiales

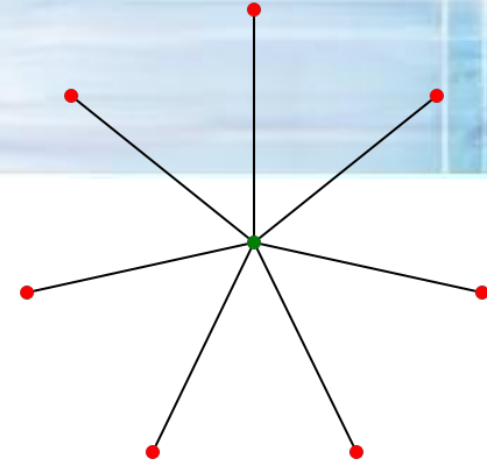
- Politique Groupe : les « bonnes pratiques SSI »
 - Idées utopiques : consultants, DG, décideurs loin de la SSI.
 - Vus dans les contrats :
 - « Le prestataire assurera 0% d'intrusions réussies »
 - « Le client validera en amont toutes les habilitations pour l'accès à ses informations »
 - « Tous les mots de passe seront changés tous les deux mois »
 - « Le prestataire assurera la traçabilité de tous les accès aux SI »
 - « ... assurera 100% de disponibilité »
 - Part pour validation à DG Groupe
 - Validation refusée et on recommence...



- Cas 3 : Groupe et filiales
 - **Finalemment** : politique jamais appliquée
 - Entités locales agissent indépendamment (cf cas 2)
 - Résultat : « best-effort »
 - Risques
 - Mise en oeuvre PCA en faisant appel aux autres entités
 - avec des niveaux de sécurité différents

© NEA, Inc.





- Cas 3 : Groupe et filiales
 - **Solution :**
 - Trouver le « plus petit dénominateur commun » des règles locales
 - Améliorer progressivement si nécessaire (suite à appréciation de risque)
 - = Plan de traitement du risque
 - qui doit déjà planifier les ressources

- Evolutions
 - Implication de tiers
 - MoE déléguée
 - Gestion (ou management, pilotage...) des tiers nécessaire !
 - Britanniques et japonais en avance
 - Modèle également appliqué :
à la continuité d'activité, aux données personnelles, à la qualité, l'environnement, la santé/sécurité au travail...

- Quelques conseils
 - **Prenez connaissance** de ce qu'offrent les référentiels existants
 - Même si ce n'est pas pour les mettre en place
 - Systèmes de gestion de ... / Systèmes de management de ...
 - Continuité d'activité : future ISO 22301
 - Données personnelles : BS 10012
 - Qualité : ISO 9001, environnement : ISO 14001
 - Sécurité et santé du personnel au travail : OHSAS 18001
 - Bien sûr la SSI, ISO 27001
 - Pour des bonnes pratiques / pour un tableau de bord
 - **Echangez**, partagez vos expériences, faites-vous aider
 - **Etudiez** le positionnement du RSSI
 - Ses responsabilités pénales en dépendent :
 - Autorité, moyens, compétence

- Quelques conseils
 - **Besoin d'adhésion de la DG : trois pistes**
 - Rattachement du RSSI à la DG
 - Tableaux de bord (ISO 27001/27002 étant standard)
 - Sensibilisez : attendre un incident grave, tests d'intrusion démonstratifs...
 - **Elaborez les objectifs de sécurité avec la DG**
 - S'appuyer sur l'éventuel PCA (analyse d'impacts déjà réalisée)
 - **Déduisez-en une appréciation de risques (réaliste)**
 - Préalable : étude des vulnérabilités
 - Audit technique et organisationnel qui ne porte pas son nom
 - Ne pas oublier les tiers !
 - **Proposez un plan de traitement des risques (réaliste) avec charges**
 - **Soyez vigilants avec les tiers : tant en tant que client que fournisseur**

Questions ?

Raphael.Marichez@hsc.fr www.hsc.fr

HSC à Strasbourg : prochaine formation

ISO 27001 Lead Implementer du 22 au 26 février 2010