FRC 2013 "Agir ou subir !"

FRC 2013 "Agir ou subir !"

Agir ou subir...

Voilà la question !

par le général d'armée (2s)
Marc WATIN-AUGOUARD
Anc. inspecteur général des armées – gendarmerie
Directeur du Centre de recherche de l'école des officiers de la gendarmerie nationale

FRC 2013 "Agir ou subir !"

Les déficits chroniques des entreprises face aux nouvelles menaces

Apport des sciences du danger et des systèmes à la cybersécurité

par Daniel GUINIER

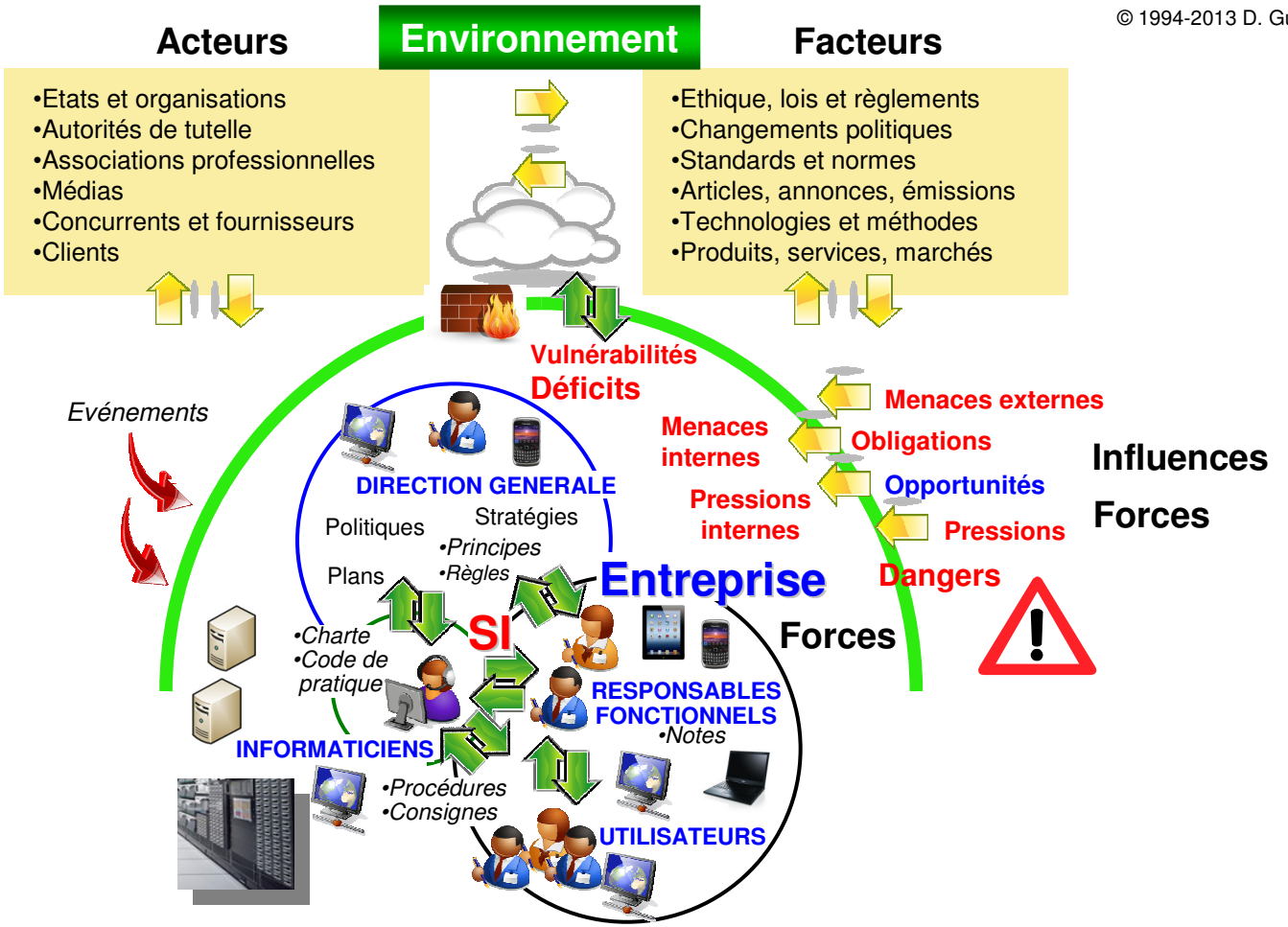
Dr. ès Sciences, Certifications CISSP, ISSMP, ISSAP, MBCI

Expert judiciaire honoraire près la Cour d'appel de Colmar

Expert près la Cour Pénale Internationale de La Haye

Lieutenant-colonel (RC) de la gendarmerie nationale

L'entreprise et les forces influentes...

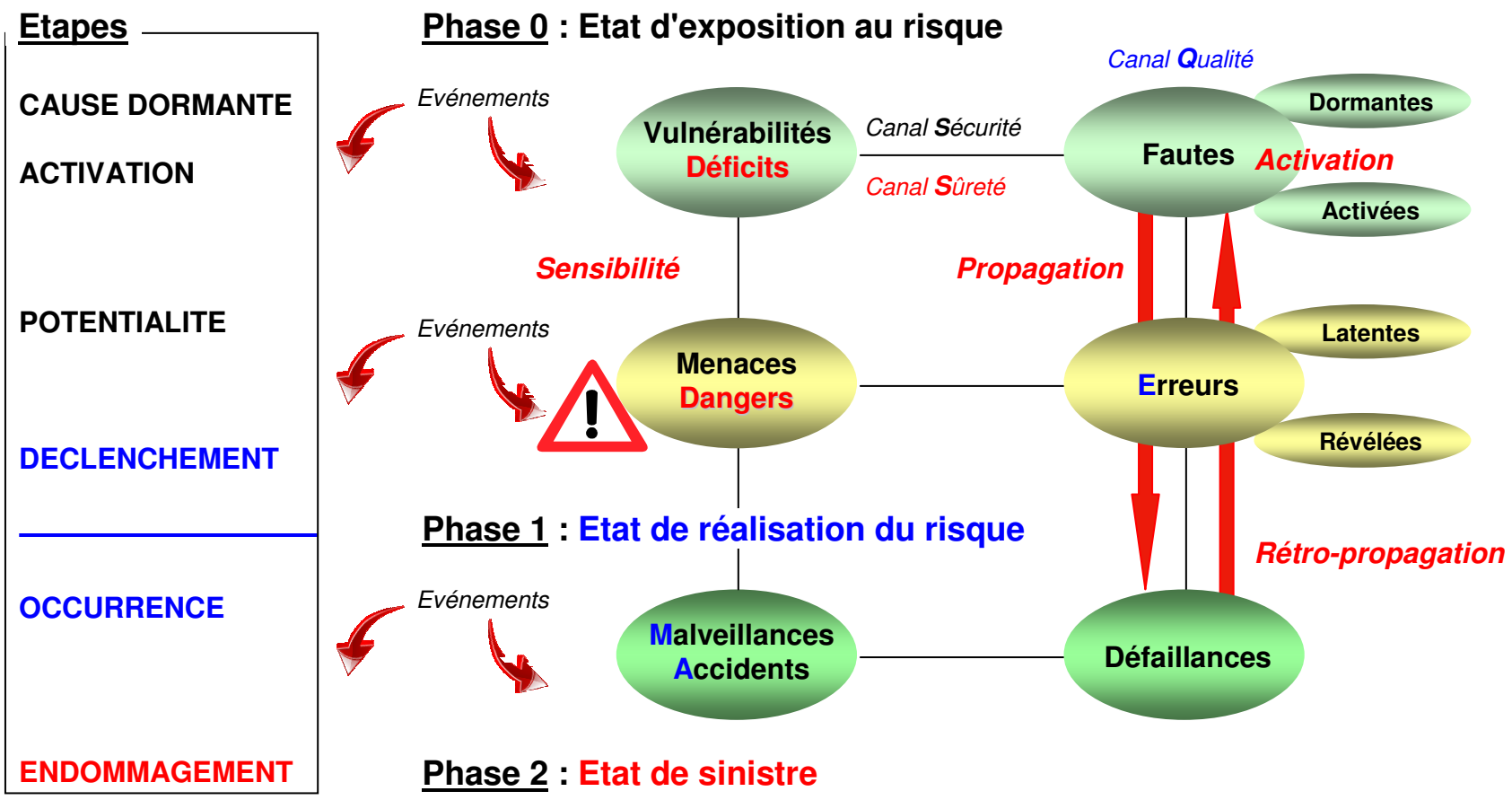


...un écosystème complexe avec des acteurs et des facteurs d'influence, auxquels on peut attribuer un hyperespace cindynique.

(G.-Y. Kervern (1995) : Eléments fondamentaux des cindyniques, Ed. Economica).

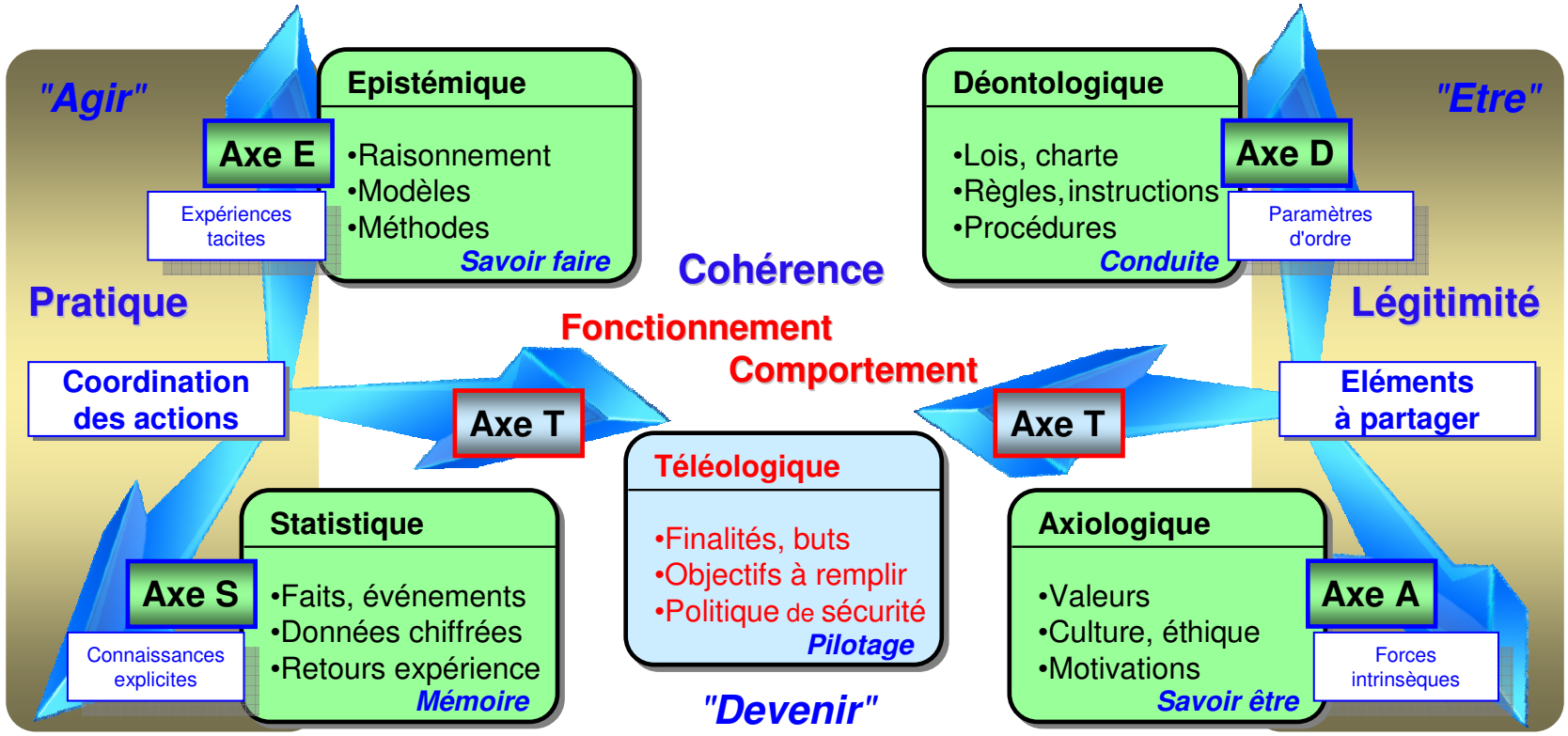
Dynamique du risque- Déficits & Dangers

Guinier D. (1994) : Oriented-scenario dynamics in information systems safety, ACM SIGSAC Review, Vol.12 , n°3, pp. 6-11,
*modèle général développé pour **S**écurité / **Q**ualité / **S**ûreté (**SQS**)*
Stoneburner G. (2006) : Toward a Unified Security / Safety Model, IEEE Computer, pp. 96-97, *modèle développé pour **S**écurité / **S**ûreté (**SQ**)*



La dynamique du risque s'exprime sur plusieurs phases par divers canaux au vu d'événements et d'états du SI ou de l'entreprise.

Modèle d'hyperespace cindynique



Ce modèle permet de dégager des absences et insuffisances mais aussi des états de divergence entre axes, la désorganisation des axes et des blocages par manque de régulation ou de coordination de sous-ensembles d'un tel hyperplan appliqué au SI.

Déficits chroniques par catégorie

Déficits managériaux

"L'origine du désastre"

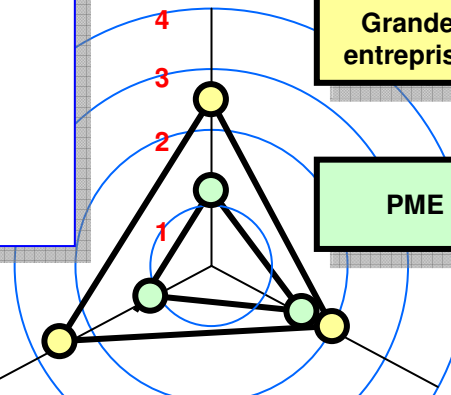
Ignorance
- Peu d'attention est portée aux incidents précurseurs
- Il n'existe ni veille, ni formation adéquate en SSI

Désengagement
- Il n'existe aucune sensibilisation relative à la SSI
- La direction n'a formalisé aucune politique PSSI

Planification
- Il n'existe aucun plan en matière de SSI
- Il n'y a pas de manuel des procédures d'urgence

4 : Sans déficit
3 : Déficit faible
2 : Déficit significatif
1 : Déficit important

SI Système d'information
SSI Sécurité des SI
PSSI Politique de la SSI



Grandes entreprises

PME

Les 3/4 des entreprises affirment l'absence d'attaque lors de l'année précédente. Elles pensent ne pas en être victime dans l'année en cours.

(Source : Information Week Analytics Strategic Security Survey of business Technology and Security Professionals (1002 répondants))

Déficits organisationnels

"L'habitude au quotidien"

Subordination
- La fonction sécurité est rattachée à la DSI
- Le RSSI est un collaborateur dépendant de la DSI

Dilution
- L'action spontanée est privilégiée sans formalisme
- Il n'existe pas de responsable RSSI nommé et formé

Rigidité
- La structure actuelle est déclarée comme satisfaisante
- La fonction sécurité est vue comme source de désordre

Déficits culturels

"L'aveuglement héroïque"

Infaillibilité
- Le SI est dit garanti contre toute défaillance technique
- L'entreprise n'a pas été victime d'attaque par le passé

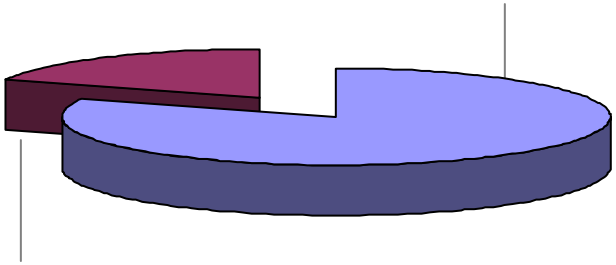
Simplisme
- Le SI est considéré comme très peu complexe
- Le recours à des méthodes est vu comme plutôt négatif

Nombrilisme
- L'entreprise n'est pas prête à se remettre en question
- L'entreprise est cloisonnée et peu ouverte à l'extérieur

Ces déficits chroniques par catégorie : culturels, organisationnels et managériaux sont observables avec plus d'ampleur pour les PME. Ils relèvent de l'ensemble des axes de d'hyperespace cindynique.

Ex. Déficit lié à l'espace "Agir"

Mode informel : discussion au niveau de l'entreprise mais aucune analyse pour 81%



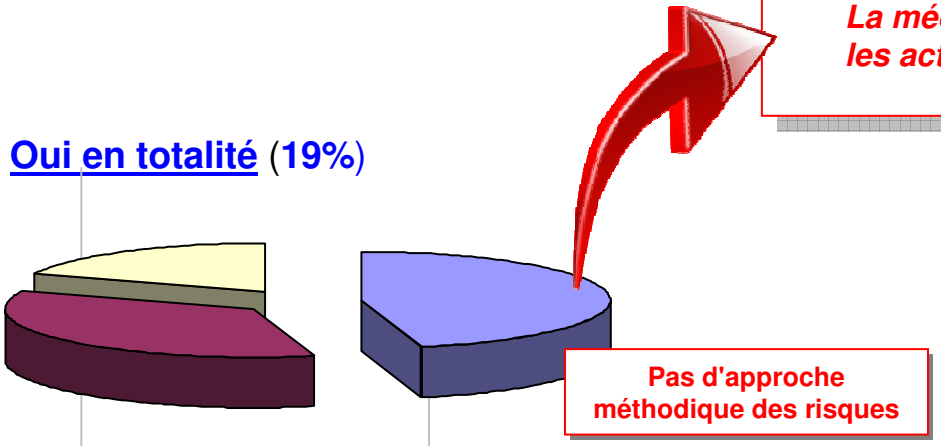
Mode formel : référentiel ISO 27005 ou méthode d'analyse : EBIOS (7%), MEHARI (5%), autres (32%)

Estimation des risques

- L'estimation doit reposer sur la connaissance des menaces et des vulnérabilités du SI
- Pour **81%** des entreprises : la formalisation des risques est peu répandue

Un déficit de l'entreprise conséquent pour *"Agir"* :

La méconnaissance des risques ne permet pas les actions sur les expositions les plus graves



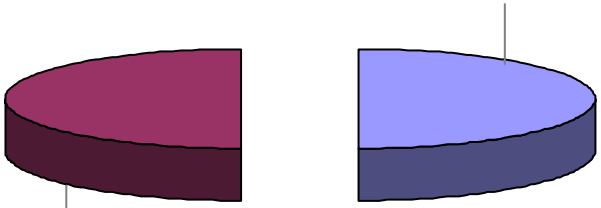
Etat des lieux

- Pour **19%** des entreprises : les risques sont évalués
- Pour **45%** des entreprises : aucun emploi de méthode pour l'analyse des risques

Source : Clusif (2012) : Menaces informatiques et pratiques de sécurité en France *(Etude sur 351 entreprises)*

Ex. Déficit lié à l'espace "Etre"

Mode informel : publication et diffusion d'informations sous diverses formes via l'Intranet ou par messagerie



Mode formel : plan de sensibilisation périodique et de formation spécifique de certaines catégories de personnels

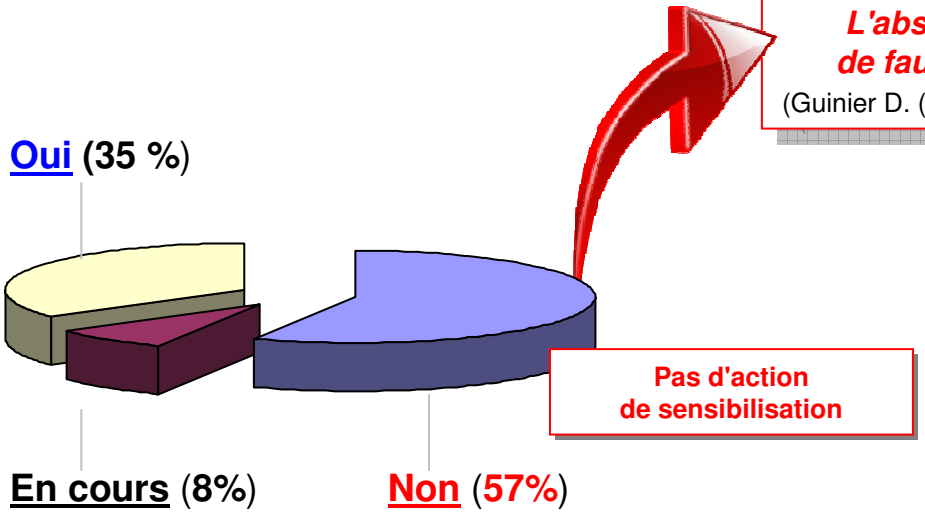
❑ Base de sensibilisation

- Les SI sont de plus en plus complexes, ouverts et mobiles et les utilisations variées
- Pour **69%** des entreprises : pas de mesure d'efficacité des programmes de sensibilisation

Un déficit de l'entreprise conséquent pour *"Etre"* :

L'absence de sensibilisation est susceptible de fautes remettant en cause la sécurité des SI

(Guinier D. (1991) : Sécurité et qualité des SI – Approche systémique, Masson)



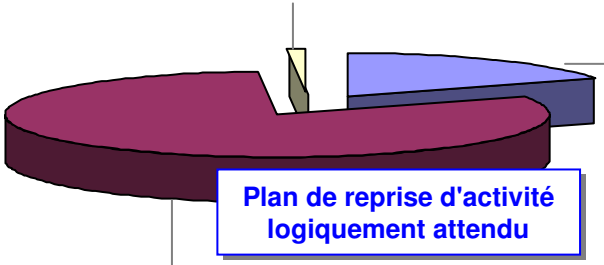
❑ Etat des lieux

- Pour **43%** des entreprises : diverses actions sont menées
- Pour **57%** des entreprises : il n'existe aucune sensibilisation prévue

Source : Clusif (2012) : Menaces informatiques et pratiques de sécurité en France *(Etude sur 351 entreprises)*

Ex. Déficit lié à l'espace "Devenir"

Dépendance faible : Indisponibilité, même de longue durée, perçue sans conséquence grave (**1%**)



Dépendance modérée : Indisponibilité tolérable jusqu'à 48h (**18%**)

Dépendance forte : Une indisponibilité de moins de 24h a des conséquences graves sur l'activité (**81%**)

❑ Dépendance au SI

- Place du SI de plus en plus cruciale pour les activités dans tous les secteurs
- Pour **99%** des entreprises : la dépendance est pressentie comme modérée à forte

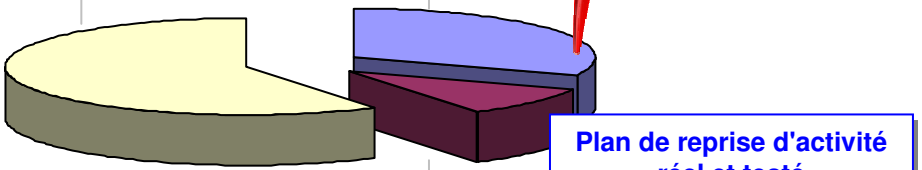
Un déficit de l'entreprise conséquent pour *"Devenir"* :

7% de chance de survie suite à un désastre s'il n'existait aucun plan de recouvrement !

(Guinier D. (1995) : Catastrophe et management, Masson)

En partie (**59 %**)

Non (**31%**)



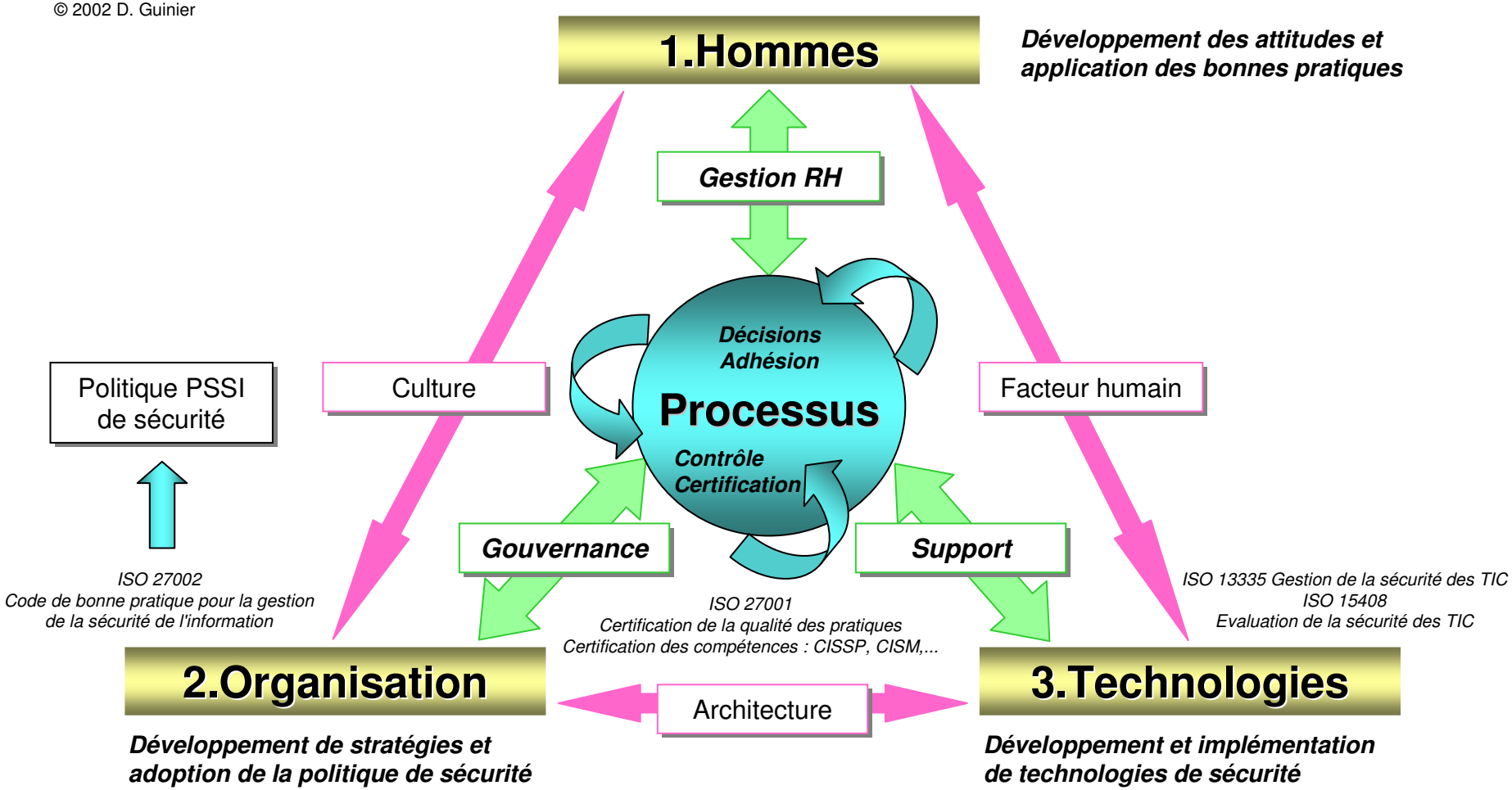
Oui en totalité (**10%**)

❑ Etat des lieux

- Pour **90%** des entreprises : pas de réel plan de reprise d'activité (PRA)
- Pour **31%** des entreprises : aucun processus de continuité est en place

Source : Clusif (2012) : Menaces informatiques et pratiques de sécurité en France *(Etude sur 351 entreprises)*

Vision systémique de la sécurité



Les trois dimensions essentielles sont reliées par des tenseurs et la régulation est assurée par des processus dynamiques.

Vision "néoréaliste" de la sécurité

1.Hommes

70% des utilisateurs reconnaissent enfreindre la sécurité au motif de faciliter les tâches

3. **La technologie** :

LE DISPOSITIF FERME LA PORTE DE FACON SYSTEMATIQUE

2. **La règle affichée** :

CETTE PORTE DOIT TOUJOURS RESTER FERMEE

Culture

Facteur humain

1. **Le contournement** :

LA CALE EMPECHE LA FERMETURE DE LA PORTE

2.Organisation

Architecture

3.Technologies

Le paradigme de la porte ouverte illustre une attitude courante impropre à la sécurité vu comme un symptôme relevant de déficits.

Conclusion

- **Devant les déficits chroniques**, malgré les efforts des entreprises au vu de cyberrisques, **d'autres approches s'imposent** à la compréhension **pour mieux *agir*** *!*
- **L'approche par les sciences du danger**
  - pour mettre en évidence des situations déficitaires ou dangereuses
  - pour déceler des carences, des contradictions, des désorganisations et des blocages
- **L'approche systémique**
  - pour prendre en compte les interactions de différente nature
  - pour disposer d'une cybersécurité ajustée mais plus en profondeur

Kervern G.-Y. et Rubise P. (1991) : L'Archipel du danger : introduction aux cindyniques, Economica
Kervern G.-Y. (1995) : Éléments fondamentaux des cindyniques, Economica
Kervern G.-Y. et Boulanger P. (2007) : Concepts et modes d'emploi, Economica

Guinier D. (1991) : Sécurité et qualité des systèmes d'information – Approche systémique – *La part de l'homme*, Masson

Introduction

De la sphère cognitive à l'action

L'anticipation des menaces majeures envers les PME — **par M Joël FERRY**
La prise en compte des risques liés aux périphériques USB — **par M Ludovic HAYE**
Prévenir la divulgation, par les nouvelles technologies, du informationnel des entreprises — **par Me Cécile DOUTRIAUX**

par M Gilbert GOZLAN

Directeur opérationnel sûreté
La Poste Nord Est
Chef d'escadron (RC) de la gendarmerie nationale

De la sphère cognitive à la sphère des actes

La démarche classique

- Informer / Convaincre
- Donner l'ordre
- Contrôler / Sanctionner

Nécessaire mais pas suffisant

il ne suffit pas d'avoir les bonnes idées pour avoir les bons comportements

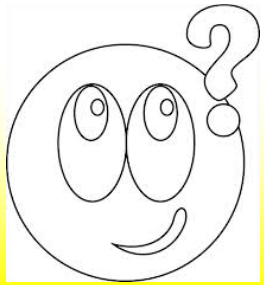
Passer des bonnes idées aux bons comportements ?

Psychologie de l'engagement

- à faire telle ou telle chose
- à ne pas faire telle ou telle chose

→ Placer l'engagement au cœur de la démarche

Comment préparer l'engagement ?



Acte préparatoire → Obtenir un premier pas « peu coûteux » allant dans la bonne direction

Exemple
si on demande à des fumeurs de s'arrêter de fumer pendant 24h, 4% acceptent
Si on commence par une privation de 2h seulement
40% acceptent = dix fois plus

Les conditions de réussite des actes préparatoires et des engagements

Se reconnaître dans les engagements → Tisser un lien entre ce que la personne fait et ce qu'elle est

3 conditions

1. Librement décidés
2. Réalisés en groupe
3. Identifiés à un haut niveau

exemple
"je pose une pierre"
"je fais un mur"
"je bâtis une cathédrale"

RV Joule & JL Beauvois : Petit traité de manipulation à l'usage des honnêtes gens (PUG)

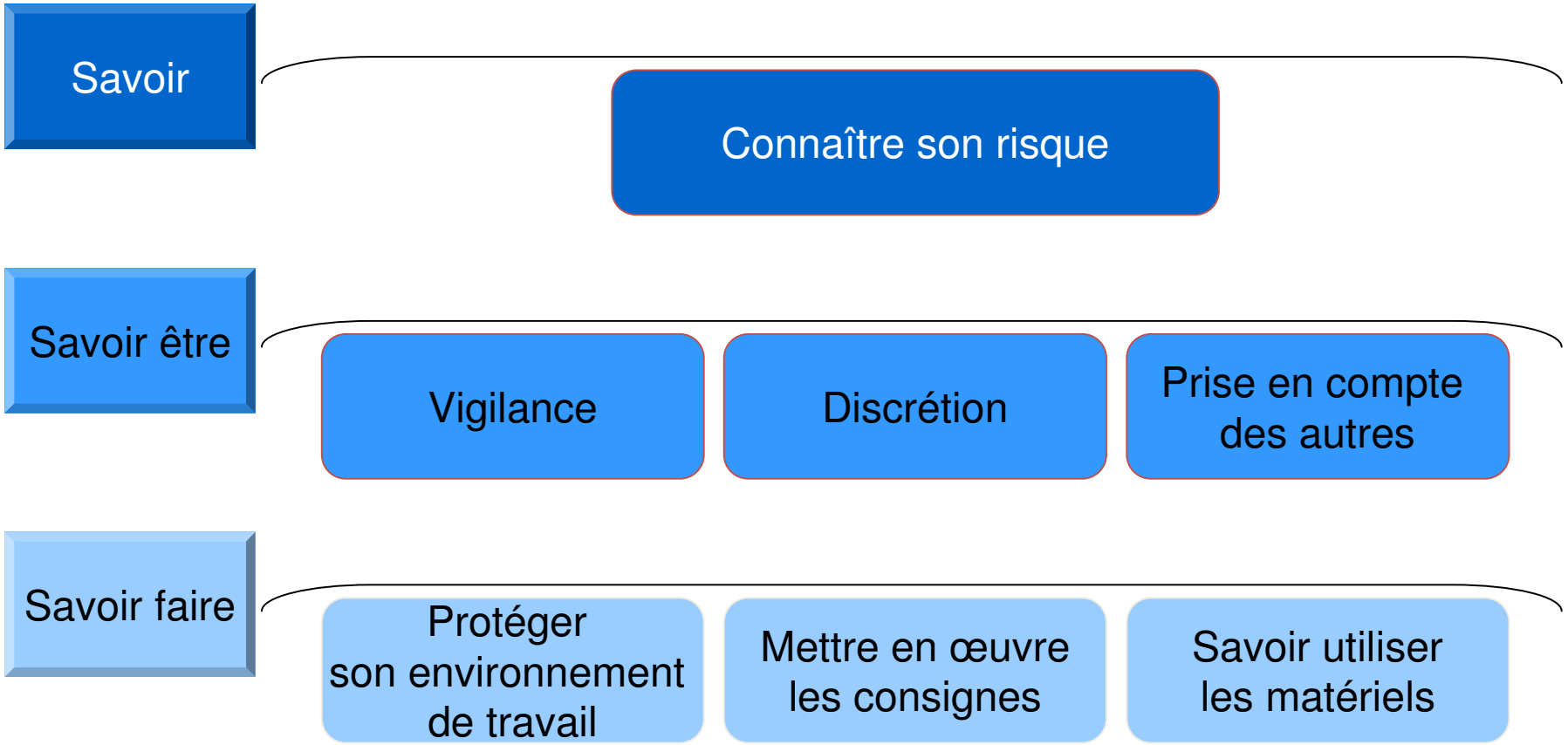
Les résultats

Résultat de l'engagement → De récepteurs passifs à acteurs et même acteurs engagés

Les équipes sont fières de ce qu'elles ont fait
Ce sont des partenaires, nous partageons les mêmes valeurs et la même ambition :

la sûreté de toutes et de tous

De la sphère cognitive à la sphère des actes



L'anticipation des menaces majeures envers les PME

1. - Les atteintes aux systèmes de traitement automatisés de données
2. - Les atteintes aux données de l'entreprise
3. - L'augmentation des infractions astucieuses

par M Joël FERRY

Conseiller Deveryware
Anc. Chargé de projets à la SDPJ – DGGN
Colonel (ER) de la gendarmerie nationale

La prise en compte des risques liés aux périphériques USB

1. – Le phénomène "USB"

2. – Les risques

3. – Les moyens simples pour se protéger

par M Ludovic HAYE

Responsable production SAP,
PSA Peugeot Citroën
Chef d'escadron (RC) de la gendarmerie nationale

Prévenir la divulgation, par les nouvelles technologies, du patrimoine informationnel des entreprises

par Maître Cécile DOUTRIAUX

Avocate au Barreau de Strasbourg
Chef d'escadron (RC) de la gendarmerie nationale
Membre de la Chaire Cyberdéfense & Cybersécurité des écoles de Saint-Cyr Coëtquidan

Questions

Introduction

Les enjeux de la lutte pour les victimes de la cybercriminalité

Essai de typologie des cybervictimes — **par Mme Myriam QUEMENER**
Le temps de l'enquête est il celui de l'internet ? — **par l'ADC Thierry JACQUOT**
Réparation et indemnisation des victimes de la cybercriminalité — **par le Pr Claude LIENHARD**

par Mme Chantal CUTAJAR

Directeur du GRASCO

Lieutenant-colonel (RC) de la gendarmerie nationale

Augmentation du nombre de victimes

- **Dans le monde** :
- **65 % des utilisateurs** d'Internet auraient été **victimes** d'une cyberattaque : *virus, fraude à la carte de crédit en ligne, vol d'identité, etc.*
- Soit :
  - **1,5 millions de victimes par jour**
  - **8 victimes par seconde**
- *Source : Meitomag Mai 2013*

Répartition des victimes

- **Les cybercriminels** ciblent les PME et les sous-traitants pour atteindre les grandes entreprises
- **Les consommateurs** sont vulnérables aux attaques mobiles
- **La France** se placerait au 16ème rang mondial des pays où la cybercriminalité est la plus active

- *Source : Rapport Symantec sur les menaces de sécurité Internet 2012*

Absence de cartographie

- L'ONDRP n'est pas en mesure de procéder à cette cartographie :
  - **Inadaptation** de l'état 4001
  - **Difficultés** liées à la mise en œuvre d'enquête de victimation

Conclusion

- La réalisation d'une cartographie des victimes est nécessaire pour :
  - Mieux connaître le phénomène
  - Adapter la politique criminelle de lutte contre la cybercriminalité en conséquence

Exemple de l'enquête de victimation menée en 2012 en Angleterre et au Pays de Galles auprès des entreprises marchandes

Essai de typologie des cybervictimes

1. - Majeurs, mineurs, entreprises, établissements financiers, e-commerçants, tous cybervictimes
2. - Cybervictimes sans le savoir
3. - Cyberharcelées et cyberamis, réponses judiciaires

par Mme Myriam QUEMENER

Magistrate,
Procureur adjoint au TGI de Créteil
Colonel (RC) de la gendarmerie nationale

Le temps de l'enquête est il celui de l'internet ?

1. - Constater, comprendre, réagir :
La réflexion est chronophage

2. - L'information utile disparaît rapidement

3. - Le temps de l'enquête :
Comment concilier les antagonismes

par l'adjudant-chef Thierry JACQUOT

Enquêteur N-TECH et référent IE de la région de gendarmerie d'Alsace
Master 2 en sécurité des systèmes d'information

Réparation et indemnisation des victimes de la cybercriminalité

1. - Des victimes diverses et traumatisées spécifiquement
2. - L'impératif d'indemnisation et la présomption de bonne foi
3. - Réparation, sécurité et confiance numérique

Par le Pr Claude LIENHARD

Directeur du CERDACC
Avocat spécialiste du droit des victimes

Questions

Introduction

Assurer la résilience de l'entreprise face à des cybermenaces de plus en plus virulentes

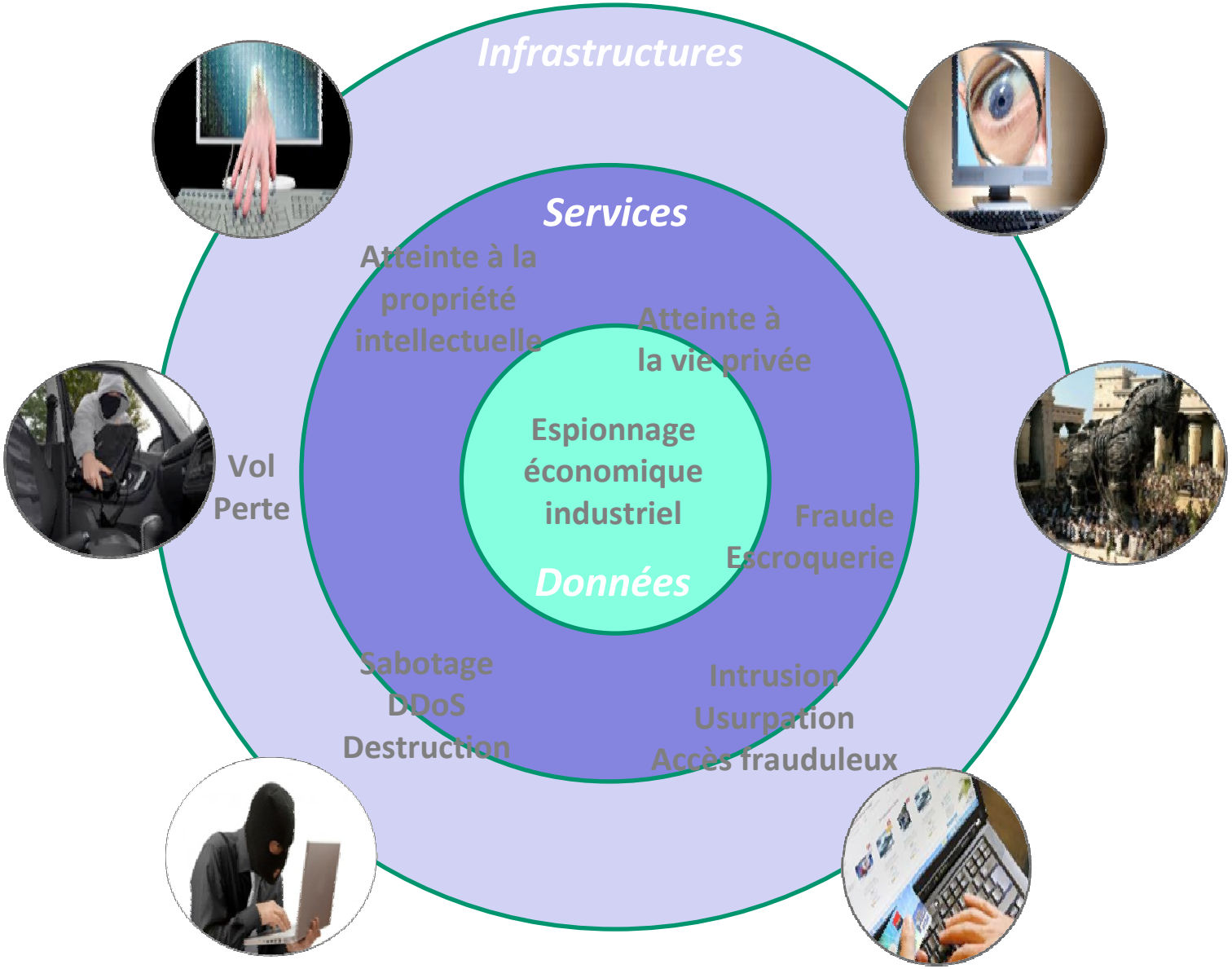
L'ANSSI, l'autorité nationale au cœur du dispositif de cybersécurité — par M Philippe WOLF
Le traitement assurantiel de réparation du cyberrisque — par M Jean-Laurent SANTONI
Les plans et moyens de secours et de sauvegarde des PME — par M Roberto GESSA

par M Stéphane JANICHEWSKI

Ingénieur général de l'armement (2s)
Vice-président de la société SOGETI

Evolution des technologies et des usages

Les cyber-risques dans la pratique



De la sécurité informatique à la sécurité globale

Complexité

Technologique

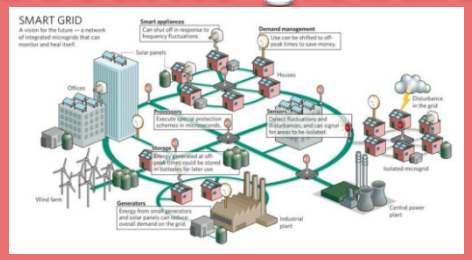
Juridique

Organisationnelle

Economique

Sociétale

Sécurité globale



Cyber-sécurité

Sécurité de l'information

Sécurité des Systèmes d'Information

Sécurité Informatique

1975 1990 1995 2000 2005 2010 2015

Nouveaux enjeux pour les entreprises / administrations

Approche plus transverse et globale

Implication des dirigeants, liens avec Risk Management, Conformité, Sûreté, RH, Finance, etc.

Choix plus stratégiques

aux plans technologique et opérationnel

Intervenir le plus en amont possible pour déclencher les bonnes décisions en termes de Sécurité « Cloud et Mobilité », SOC /SIEM, IAM, DLP, etc.

Importance accrue de l'économie

- Valeur des informations sensibles et SI critiques ?
- Impact économique des attaques / incidents (Sanctions financières des violations de données) ?
- Dépenser moins ou dépenser mieux ?
- Assurer les cyber-risques ?

Enjeux plus « Métiers »

Quelle « acculturation » (accompagnement du changement) pour une sécurité intégrée et facilitatrice de « business » (moins « contraintes ») ?

Intégration du numérique jusque dans les systèmes industriels / embarqués

L'ANSSI, l'autorité nationale au cœur du dispositif de cybersécurité

1. - Apports de l'article 15 de la nouvelle loi de programmation militaire à la cyberdéfense
2. - Après les révélations Snowden, Internet est-il cassé ?
3. - Les 10 facteurs de la cyber-insécurité. Quelle cybersécurité future ?

par M Philippe WOLF

Conseiller du directeur général
de l'Agence nationale de sécurité des systèmes d'information (ANSSI)

Le traitement assurantiel de réparation du cyberrisque

1. - Assurance des nouveaux contenants

2. - Assurance des nouveaux contenus

3. - Assurance des nouveaux responsables

par M Jean-Laurent SANTONI

Docteur en droit
Président de Clever Courtage

Les plans et moyens de secours et de sauvegarde des PME

1. - Prise de conscience et évaluation du risque en cas de sinistre
2. - Méthodologie d'implémentation d'un plan de secours
3. - Assistance au maintien du plan de secours

Par M Roberto GESSA

Consultant-architecte en stockage et plans de continuité

Questions

Discours de clôture

par Mme Catherine GROSSE
Consultante en management AUDACIS
Présidente de l'association Alsace des réservistes citoyens de la gendarmerie nationale (AARCGN)
Chef d'escadron (RC) de la gendarmerie nationale