

# Se préparer à la réponse judiciaire contre les attaques informatiques



Journée Sécurité des Systèmes d'Information  
*Paris, 16 mars 2010*

*Lieutenant-colonel Éric Freyssinet, DGGN/SDPJ*



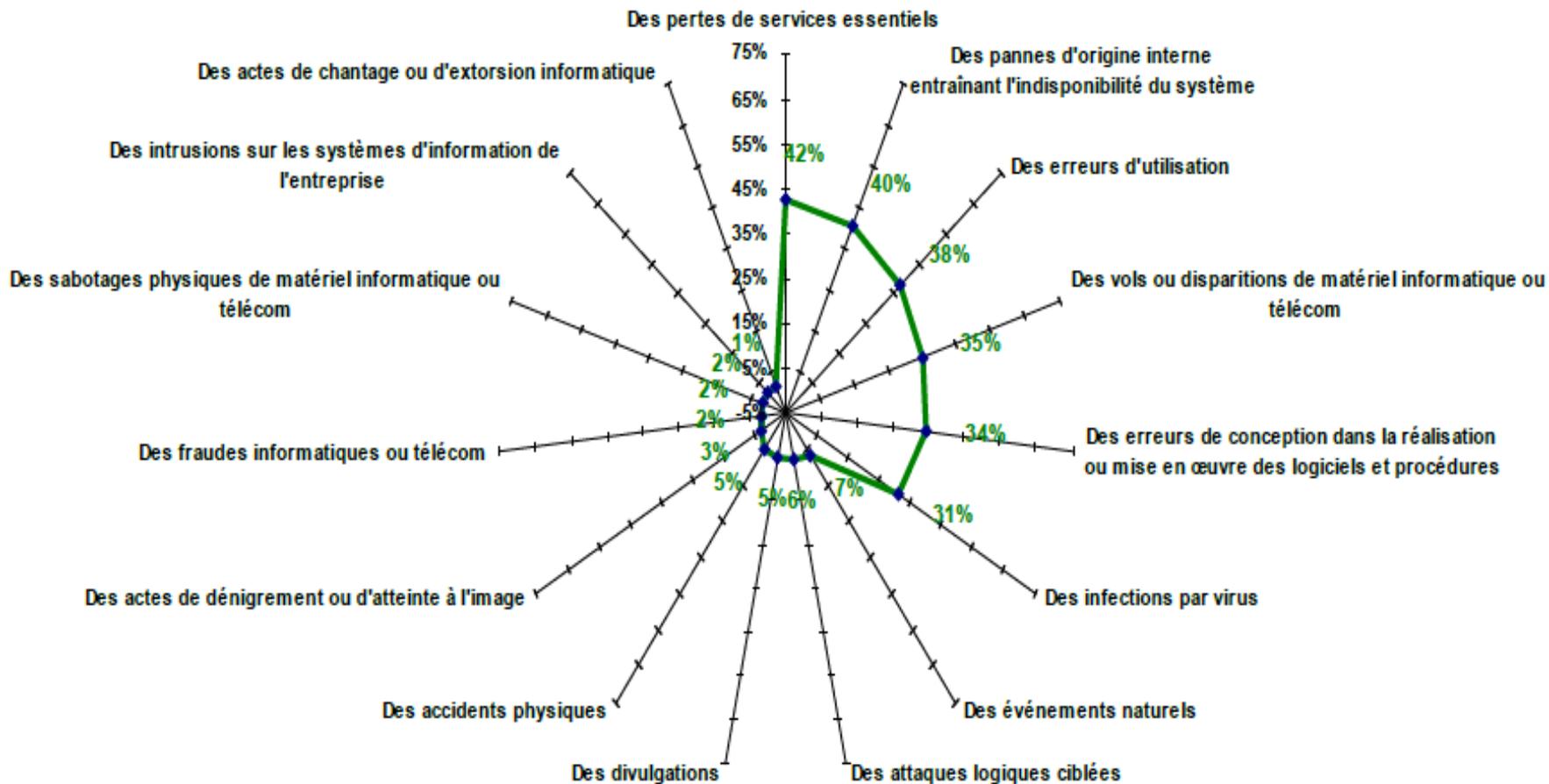
# Plan

- Pourquoi il faut agir juridiquement
- Pourquoi on peut agir juridiquement
- Comment s'y préparer
- Comment agir

# Pourquoi il faut agir

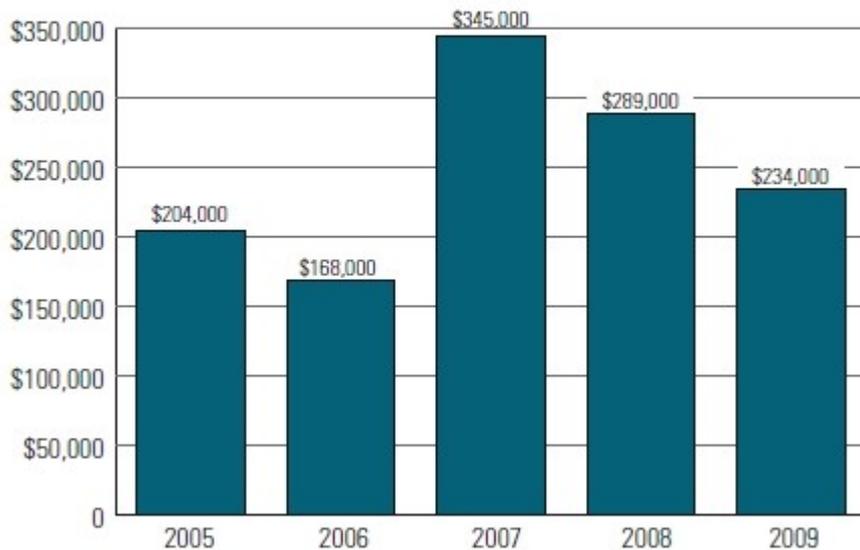
- Le nombre réel d'attaques informatiques
  - Beaucoup plus important que les chiffres publics
  - L'exemple des autres pays nous montre une autre réalité
- Si l'on veut durablement limiter le risque, il faut identifier et interpeller les auteurs. On ne peut pas les interpeller si:
  - On ne connaît pas leurs actes
  - On ne collecte pas de preuves
- Il va falloir transformer l'essai de l'obligation de notification d'incidents de sécurité

# Étude CLUSIF 2008



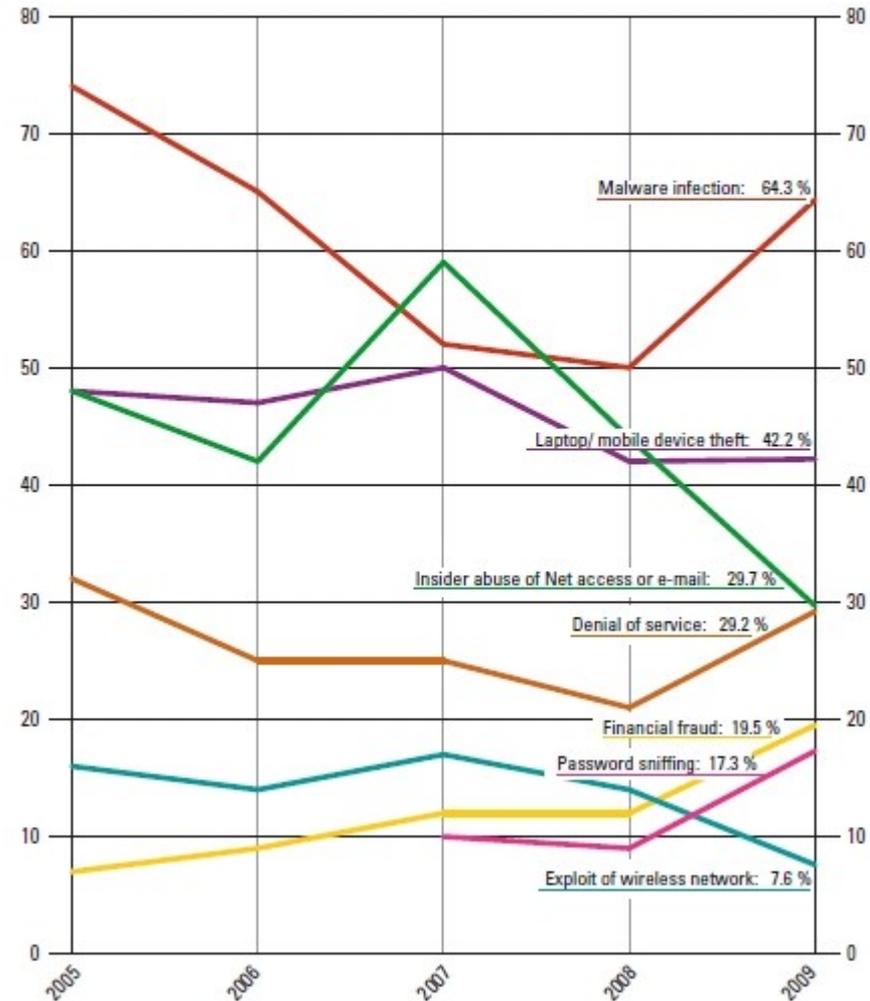
# Étude CSI 2009

## Average Losses Per Respondent



- US, 443 réponses
- <http://gocsi.com/>

## Types of Attacks Experienced By Percent of Respondents





# Databreaches.net

**OFFICE OF INADEQUATE SECURITY**  
DATABREACHES.NET

Home About Laws Contact Bills in Congress News Sections Search

You are here: [Home](#) / [Breach Incidents](#)

## S.Korea to probe huge online data leak

March 15, 2010 by admin [Leave a Comment](#)

Filed under [Breach Incidents](#), [Business Sector](#), [Hack](#), [ID Theft](#), [Non-U.S.](#), [Of Note](#)

Another contender for a future Top 10 list: South Korea said Friday it would launch a probe into security systems of major retailer Shinsegae and 24 other companies after private data on some 20 million customers was leaked. The move came a day after... [Read more...](#)

Tags:

## State leads investigation of sheriff's deputy alleged to have taken reports, data

March 15, 2010 by admin [Leave a Comment](#)

**Archived Posts**

Select Month

- Select Month
- March 2010 (89)
- February 2010 (163)
- January 2010 (166)
- December 2009 (146)
- November 2009 (148)
- October 2009 (132)
- September 2009 (119)
- August 2009 (142)
- July 2009 (141)
- June 2009 (115)
- May 2009 (144)
- April 2009 (129)
- March 2009 (152)
- February 2009 (167)
- January 2009 (210)

# Notification des incidents de sécurité

- Paquet « Télécom » voté en novembre 2009
  - Obligation qui concernera tous les opérateurs de communications électroniques
- Proposition de loi Détraigne/Escoffier
  - Débattue au Sénat le 23 mars
  - Proposent d'appliquer d'emblée cette obligation à tous les responsables de traitements de données à caractère personnel
  - Mais, il n'y a pas que les traitements de données personnelles qui ont de la valeur...



# Pourquoi on peut agir

- Parce que les partenaires judiciaires sont prêts
  - Sur le plan juridique
  - Sur le plan technique et des compétences
- Parce que cela n'implique pas forcément de révéler ses défauts
  - Ou parce que le temps judiciaire laisse le temps de les corriger

# Les instruments juridiques

- Vous les connaissez
  - Convention du Conseil de l'Europe sur la cybercriminalité (2001)
  - Décision-cadre de l'UE relative aux attaques visant les systèmes d'information (2005)
  - Loi Godfrain (1988) en France et code de procédure pénale adapté
    - Peines de prison, amendes élevées

# Les compétences sont là

- Vous connaissez les acteurs:

- Police

- DCPJ/OCLCTIC, PP/BEFTI, DCRI, ICC (ESCI)

- Gendarmerie

- IRCGN, STRJD, NTECH, C-NTECH

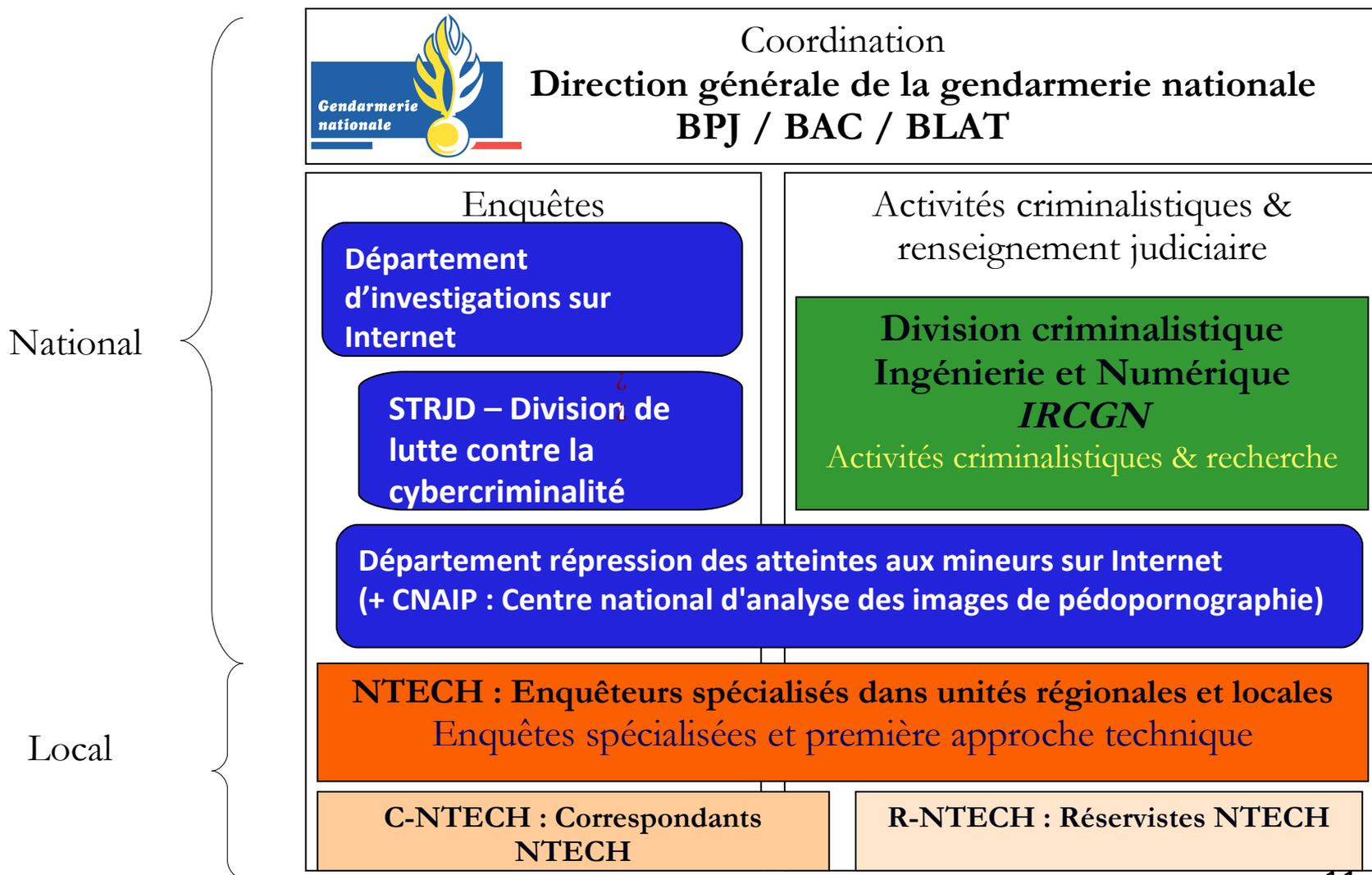
- Justice



- Chacun, dans ses zones ou territoires de compétences s'est formé, adapté, est prêt à répondre
- Les compétences se développent évidemment aussi à l'étranger, et des partenariats sont en place



# Résumé dispositif gendarmerie



# Les compétences sont là

- Vous connaissez les acteurs:

- Police

- DCPJ/OCLCTIC, PP/BEFTI, DCRI, ICC (ESCI)



- Gendarmerie

- IRCGN, STRJD, NTECH, C-NTECH



- Justice

- Chacun, dans ses zones ou territoires de compétences s'est formé, adapté, est prêt à répondre

- Les compétences se développent évidemment aussi à l'étranger, et des partenariats sont en place



# Les affaires sont traitées

- Beaucoup d'affaires se traitent dans la discrétion
- Parfois de « petites » affaires ont un impact important
  - UTOPI 62 (06/2006), HACKERs 21 (05/2008)
- Des compétences pour couvrir tout le spectre des besoins:
  - Interventions dans les entreprises, chez les opérateurs, chez les hébergeurs
  - Perquisitions chez particuliers ou entreprises



# Tous réclament une coopération intelligente

## RSA: FBI Director Calls For Action Against Cyber Threat

By Stefanie Hoffman, ChannelWeb  
2:33 PM EST ven.. mars. 05, 2010

Discuss This 

FBI Director Robert Mueller called on the U.S. security community to minimize disclosure, collaborate with governments and pursue investigations farther than appears to be a losing arms race with cyber criminals.

"We are playing the cyber equivalent of cat and mouse with thousands of IT professionals in a keynote during the RSA Conference on Thursday. "We must make the cost of doing business willing to bear,"

As part of his call to arms, Mueller pledged to work with protective orders and increased privacy for law enforcement data breaches, in order to avoid loss of reputational momentum of federal and state data breach disclosures.

"Notifying the authorities may harm your competitive advantage or the disruption into your business," he said. "Today the breadth and scope of this attack. For every incident there are hundreds that will never make the headlines because they are not the rule."



**RSACONFERENCE 2010** WEBCASTS

2 of 2

**Remarks from FBI Director Mueller**

THURSDAY, MARCH 4 | MAR 2 | MAR 3 | **MAR 4** | MAR 5

AL ZOLLAR

00:13:52

Play Mute Previous Next

**FBI DIRECTOR MUELLER**  
CA, Inc

Slide 2 of 2



# L'enquête judiciaire et la gestion des incidents de sécurité

- **Détecter** l'activité criminelle
- Recevoir les **plaintes**
  - **Collecter** les preuves, évaluer les dommages, **rétablir le fonctionnement**
  - **Identifier** et interpellier les suspects
    - Poursuivre (et obtenir **réparation**)

Nécessite: des personnels formés dans l'industrie et les services d'enquête ; en mesure de coopérer

# Comment s'y préparer

- Évidemment, sécuriser ses systèmes d'information et être en mesure de détecter les attaques
- Collecter des traces de façon préventive
- Évaluer l'ampleur des atteintes
  - Pour savoir quoi partager de façon informelle
  - Pour déterminer quand déposer plainte
- Former ses personnels
- Connaître les acteurs locaux / nationaux



# Quels critères pour un dépôt de plainte ?

- Création d'une grille d'évaluation adaptée aux risques :
  - Atteinte notable à des données personnelles
  - Atteinte à des données confidentielles
  - Préjudice financier / temps pour rétablir
  - Échanges avec les professionnels (mesurer ensemble la complexité de l'attaque, faire des rapprochements)
  - Échanges avec les services d'enquêtes

A	*
B	* * *
C	* *



# Comment agir

- Préserver les preuves
  - Disponibles et extensives
  - Admissibles (leur qualité est documentée, leur contenu éventuellement signé)
- Prévenir les autorités
  - Coordonner avec elles la reprise d'activité
  - Ainsi que la procédure de mise à disposition des preuves
  - Mesurer le préjudice
- Préparer la communication
  - A coordonner avec les autorités
  - Prévenir les victimes tierces
  - Souligner positivement la préparation et la réaction



# Préserver les preuves

- En droit français, la preuve est libre
- Mais plus on est capable de la valoriser, plus elle sera probante
  - Process de collecte documentés et propres
  - Signatures électroniques
- Privilégier des formats ouverts
- Mettre à disposition des spécialistes capables d'expliquer le fonctionnement des systèmes

# Prévenir les autorités

- Ne pas chercher à régler le problème soi-même ...
- Des interlocuteurs qu'il faut connaître par avance
- Les intervenants locaux peuvent toujours se faire assister de spécialistes si nécessaire
- Prévoir des locaux pour les accueillir
- Désigner un point de contact technique (et éventuellement un point de contact juridique)
- Prévoir une procédure d'échanges au fil de l'eau, notamment par voie électronique
- La discrétion vaut aussi pour les victimes



# Communication

- Essentielle :
  - Pour tirer le meilleur de la gestion de l'incident
  - Pour prévenir une communication négative
  - Pour se préparer au procès pénal qui est public
  - Pour expliquer les mesures correctrices apportées et rassurer les clients
  - Pourquoi ne pas communiquer sur la qualité de sa préparation à gérer ces incidents ?



# Conclusion

- Partenariat
- Impliquer les services d'enquête
- Collecter des preuves
- Se préparer et planifier !

Eric Freyssinet, lieutenant-colonel  
Direction générale de la gendarmerie nationale  
Sous-direction de la police judiciaire  
35 rue Saint Didier  
F-75775 PARIS Cedex 16  
Tél: +33 1 56 28 66 27  
Mél: [eric.freyssinet@gendarmerie.interieur.gouv.fr](mailto:eric.freyssinet@gendarmerie.interieur.gouv.fr)  
<http://blog.crimenumerique.fr/>