



Internet Security Day 2007

## Criminalité informatique: Répression & risques juridiques pour les entreprises

Cyril Pierre-Beausse, Avocat à la Cour



## Sommaire

# Introduction

Répression de la criminalité informatique

Risques pour les entreprises

Conclusion: prévention du risque informatique



# Conséquences d'une attaque informatique



Responsabilité  
de l'auteur de  
l'attaque

Responsabilité de  
l'intermédiaire de  
l'attaque

Responsabilité de  
la victime de  
l'attaque



# Sanctions pénales applicables (amendes)

EUR 125 000

...

...

EUR 50 000

EUR 40 000

EUR 30 000

EUR 20 000

EUR 10 000

Accès frauduleux

Accès frauduleux  
+modification  
/suppression de  
données ou entrave  
au fonctionnement

Entrave au  
fonctionnement

Introduction,  
altération,  
modification de  
données

Divulgence de  
secrets d'affaires  
ou de fabrique

Faux en écritures  
électroniques



Manquement à  
l'obligation de  
sécurité /données  
personnelles

## Sommaire

Introduction

# Répression de la criminalité informatique

Risques pour les entreprises

Conclusion: prévention du risque informatique



# Répression de la criminalité informatique



Infractions  
informatiques  
proprement dites

Infractions  
connexes

# Répression de la criminalité informatique



Accès ou maintien  
frauduleux dans un  
système de traitement  
automatisé de données

Article 509-1 du Code pénal

Suppose :

1. l'accès ou le maintien dans un STAD
2. intention frauduleuse (agir en connaissance de cause)

Éléments indifférents:

1. préjudice pour la victime
2. attaque externe ou interne
3. méthode choisie pour l'attaque
4. mobile

Exemple:  
Attaque Trojan

2 mois  
à 2 ans de prison

EUR 500 à 25 000  
d'amende

# Répression de la criminalité informatique



Accès ou maintien  
frauduleux dans un  
système de traitement  
automatisé de données  
+ modification/suppression  
de données ou altération  
du fonctionnement du  
système

Article 509-1(2) du Code pénal

Suppose :  
Même éléments  
constitutifs que 509-1  
(circonstance  
aggravante)

Éléments  
supplémentaires:  
1. «mépris des droits  
d'autrui»  
2. modif. ou suppr.  
de données ou altér.  
du fonctionnement du  
STAD

Éléments indifférents:  
1. attaque externe ou  
interne  
2. méthode choisie  
pour l'attaque  
3. mobile

4 mois  
à 2 ans de prison  
  
EUR 1 250 à 25 000  
d'amende

# Répression de la criminalité informatique



## Entrave au fonctionnement d'un système de traitement automatisé de données

Article 509-2 du Code pénal

### Suppose :

1. entraver ou fausser le fonct. du STAD (plus grave que simple altération)
2. intention de l'auteur
3. «mépris des droits d'autrui»

Exemple:  
Attaque DOS

### Éléments indifférents:

1. accès ou maintien dans le STAD
2. attaque externe ou interne
3. méthode choisie pour l'attaque
4. mobile

3 mois  
à 3 ans de prison

EUR 1 250 à 12 500  
d'amende

# Répression de la criminalité informatique



## Introduction, altération, modification de données

Article 509-3 du Code pénal

### Suppose :

1. introd., suppr. ou modif. des données ou leur mode de trait. ou de transmission
2. intention de l'auteur
3. «mépris des droits d'autrui»

### Eléments indifférents:

1. accès ou maintien dans le STAD
2. attaque externe ou interne
3. méthode choisie pour l'attaque
4. mobile

### Exemple:

Attaque de site Web

3 mois  
à 3 ans de prison

EUR 1 250 à 12 500  
d'amende

# Répression de la criminalité informatique



Complicité, tentative

Article 509-6 du Code pénal

Suppose :

1. complicité ou tentative d'une des infractions précédentes
2. commencement d'exécution (tentative)

Éléments indifférents:

1. échec (tentative)
2. mobile

Sanctions identiques

# Répression de la criminalité informatique



Association de malfaiteurs  
en vue des mêmes  
infractions

Article 509-7 du Code pénal

Peines encourue  
pour l'infraction  
ou l'infraction la plus  
sévèrement réprimée

# Répression de la criminalité informatique



## Divulgation de secrets d'affaires ou de fabrique

Article 309 du Code pénal

Suppose :

1. être un employé
2. agir dans un but de concurrence/nuisance ou pour obtenir un avantage illicite
3. divulgation d'un secret d'affaires

Vise aussi:

1. ceux qui utilisent les secrets d'affaires ainsi divulgués
2. ceux qui utilisent des secrets confiés pour l'exécution d'une commande

Exemple:

Divulgation d'informations confidentielles (ex. au moyen d'un e-mail)

3 mois  
à 3 ans de prison

EUR 251 à 12 500  
d'amende

# Répression de la criminalité informatique



## Violation du secret des correspondances /vie privée

Article 460 Code pénal,  
loi du 11 août 1982

Suppose (art. 460) :  
1. supprimer une lettre  
confiée à la poste (ou)  
l'ouvrir pour en violer  
le secret

Suppose (loi 11/8/82):  
1. ouvrir un message  
sous pli fermé  
2. prise de  
connaissance par un  
moyen technique  
3. sans l'accord du  
destinataire/auteur

Exemple:  
Interception et/ou  
consultation et/ou  
suppression d'un  
e-mail privé

8 jours  
à 1 an de prison

EUR 2 500 à 50 000  
d'amende

# Répression de la criminalité informatique



Mise en place d'un  
appareillage en vue de la  
violation du secret des  
correspondances  
/vie privée

Loi du 11 août 1982

Suppose:

- 1.mettre en place un moyen technique pour prendre connaissance de messages sous pli fermé
- 2.sans l'accord du destinataire/auteur

Exemple:

Mise en place d'un système d'interception (filtrage?)

8 jours  
à 1 an de prison

EUR 2 500 à 50 000  
d'amende

# Répression de la criminalité informatique



Commercialisation  
d'appareillages en vue de  
la violation du secret des  
correspondances  
/vie privée

Loi du 11 août 1982

EUR 2 500 à  
1 000 000 d'amende

# Répression de la criminalité informatique



## Recel (d'informations)

Article 505 du Code pénal

Suppose:

1. receler les biens /incorporels détournés à l'aide d'un crime /délit
2. bénéficiaire de biens recelés

Exemple:

Conservation de données obtenues au moyen d'une violation de secrets d'affaires ou de correspondance

15 jours  
à 5 ans de prison

EUR 251 à 5 000  
d'amende

# Répression de la criminalité informatique



## Fausses clés électroniques

Article 488 du Code pénal

Suppose (art. 460) :  
1. contrefaire ou altérer  
des clés électroniques  
2. intention frauduleuse

3 mois à 2 ans  
de prison

EUR 251 à 2 000  
d'amende

# Répression de la criminalité informatique



## Problèmes pratiques:

Chiffre noir  
considérable

Opportunité des  
poursuites  
(attaquant offshore)

Risque  
réputationnel  
+juridique  
pour la victime

Poursuivre l'auteur  
rend publiques les  
faiblesses de  
l'entreprise

**>Sentiment d'impunité**

## Sommaire

Introduction

Répression de la criminalité informatique

# Risques pour les entreprises

Conclusion: prévention du risque informatique

# Rôle de l'entreprise dans l'attaque



## Intermédiaire

Systemes de l'entreprise utilisés pour attaquer un tiers

## Victime

Attaque visant les systemes de l'entreprise

# Responsabilité de l'intermédiaire de l'attaque\*



## Responsabilité pénale

A priori exclue  
(sauf agissement en  
connaissance de cause)

## Responsabilité civile

Ne peut être exclue, si l'attaque  
sur le tiers a été rendue  
possible ou facilitée par  
l'insuffisance de la sécurité  
informatique de l'intermédiaire.

Faible dans la sécurité équivaut-elle  
toujours à faute ou la mise en place d'un  
niveau «raisonnable» de sécurité peut-  
elle entraîner l'exonération?

# Responsabilité de la victime de l'attaque

**Loi du 2 août 2002**

**protection des données personnelles**

Le responsable du traitement doit garantir la sécurité et la confidentialité des données



Sanctions pénales possibles  
en cas de rupture  
de sécurité/confidentialité



# Obligation de sécurité



Le niveau de sécurité doit être fonction...

Du risque d'atteinte  
à la vie privée

De l'état de l'art  
(obligation de  
mise à jour)

Des coûts  
liés à leur  
mise en  
oeuvre

# Sécurité: nature des mesures (1/3)



**Contrôle à l'entrée des installations**  
(empêcher toute personne non autorisée d'accéder aux installations utilisées pour le traitement de données)  
: accès sécurisés, surveillance

**Contrôle des supports**  
(empêcher que des supports de données puissent être lus, copiés, modifiés ou déplacés par une personne non autorisée)  
: supports conservés sous clé

**Contrôle de la mémoire**  
(empêcher l'introd. non autorisée de données, que toute prise de connaissance, modif. ou effacement non autorisés des données)  
: restriction d'accès au système



# Sécurité: nature des mesures (2/3)



## Contrôle de l'utilisation


(empêcher que les systèmes puissent être utilisés par des pers. non autorisées à l'aide d'installations de transmiss. de données)  
: protection réseau (firewalls)

## Contrôle de l'accès

(garantir que, pour l'utilisation d'un système de traitement automatisé de données, les pers. autorisées ne puissent accéder qu'aux données de leur compétence)  
: gestion des comptes, suivi

## Contrôle de la transmission

(garantir que puisse être vérifié et constaté l'ident. des tiers auxquels des données peuvent être transmises par des install. de transmission)  
: cryptage, signature électronique



# Sécurité: nature des mesures (3/3)



## Contrôle de l'introduction

(garantir que puisse être vérifié et constaté a posteriori l'identité des pers. ayant eu accès au système et garantir le traçabilité des accès)  
: autre traitement? surveillance?

## Contrôle du transport

(empêcher que, lors de la communic./transport de supports, les données puissent être lues, copiées, modifiées ou effacées sans autoris.)  
: cryptage des supports

## Contrôle de la disponibilité

(sauvegarder les données par la constitution de copies de sécurité)

+ Rapport annuel sur la sécurité des systèmes

# Obligation de sécurité: sanctions



Manquement à l'obligation de sécurité en relation avec un traitement de données personnelles

Article 24 de la loi du 2 août 2002

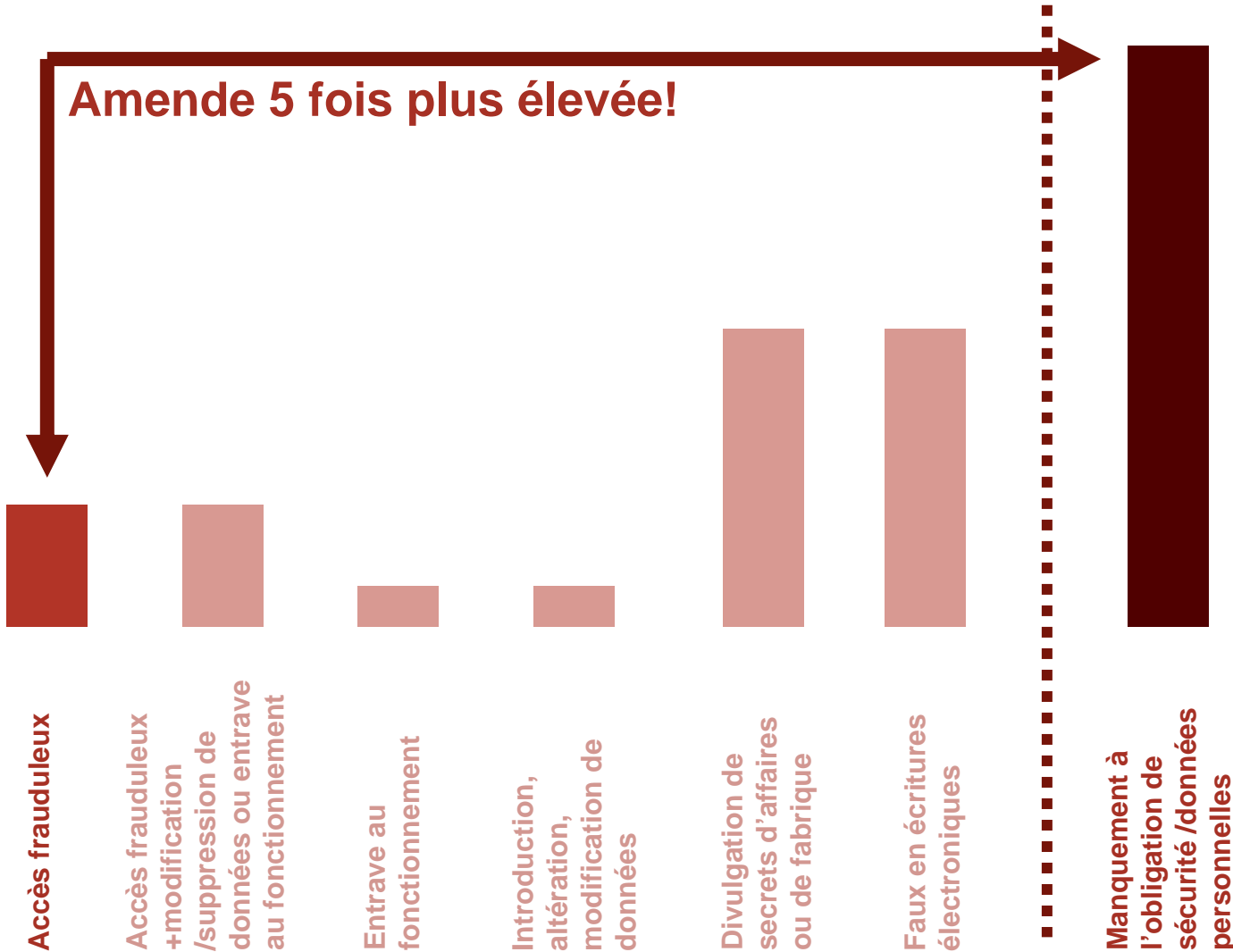
Suppose :  
1. Manquement à l'obligation de sécurité (ex. attaque réussie)

8 jours à 1 an de prison

EUR 251 à 125 000 d'amende

# Sanctions pénales applicables (amendes)

EUR 125 000  
...  
...  
EUR 50 000  
EUR 40 000  
EUR 30 000  
EUR 20 000  
EUR 10 000



# Autres risques



## Autres risques juridiques

Sanctions administratives

Responsabilité civile



Risque économique /opérationnel  
Perte de données, d'activité, de marché

Risque réputationnel  
Encourage le chiffre noir et donc augmente le sentiment d'impunité

..... Risque ressenti .....

————— Risque réel —————

# Sommaire

Introduction

Répression de la criminalité informatique

Risques pour les entreprises

# Conclusion

# Conclusion: prévention du risque



## Prévention technique

*Cf. Internet Security Day*

## Prévention «culturelle»

Informer les attaquants potentiels sur les risques associés à leur comportement

Sensibilisation des tiers

Ex. actions dans les écoles

Sensibilisation interne

La majorité des menaces est d'origine interne!



Internet Security Day 2007

## Criminalité informatique: Répression & risques juridiques pour les entreprises

Cyril Pierre-Beausse, Avocat à la Cour

