



Internet Security Day, 8 mai 2008

La fonction de sécurité de l'information dans l'entreprise

Cyril Pierre-Beausse, Allen & Overy Luxembourg

ALLEN & OVERY

La fonction de sécurité de l'information

Vulnérabilité

La dépendance à l'information

Risque

Economique, commercial/réputationnel, juridique

Obligation

La loi prévoit une véritable obligation de sécurité

Fonction

La fonction de RSSI, sa place dans l'entreprise

Prévention

Outils et arguments du RSSI

Perspectives

Nécessité d'une prise de conscience

Vulnérabilité: La dépendance à l'information

L'information est à la base de l'activité de l'entreprise

La collecte et le traitement de l'information forme de plus en plus souvent l'essence de l'activité de l'entreprise

L'entreprise est dépendante de l'information

Les entreprises sont de plus en plus dépendantes de l'information et des systèmes utilisés pour leur traitement

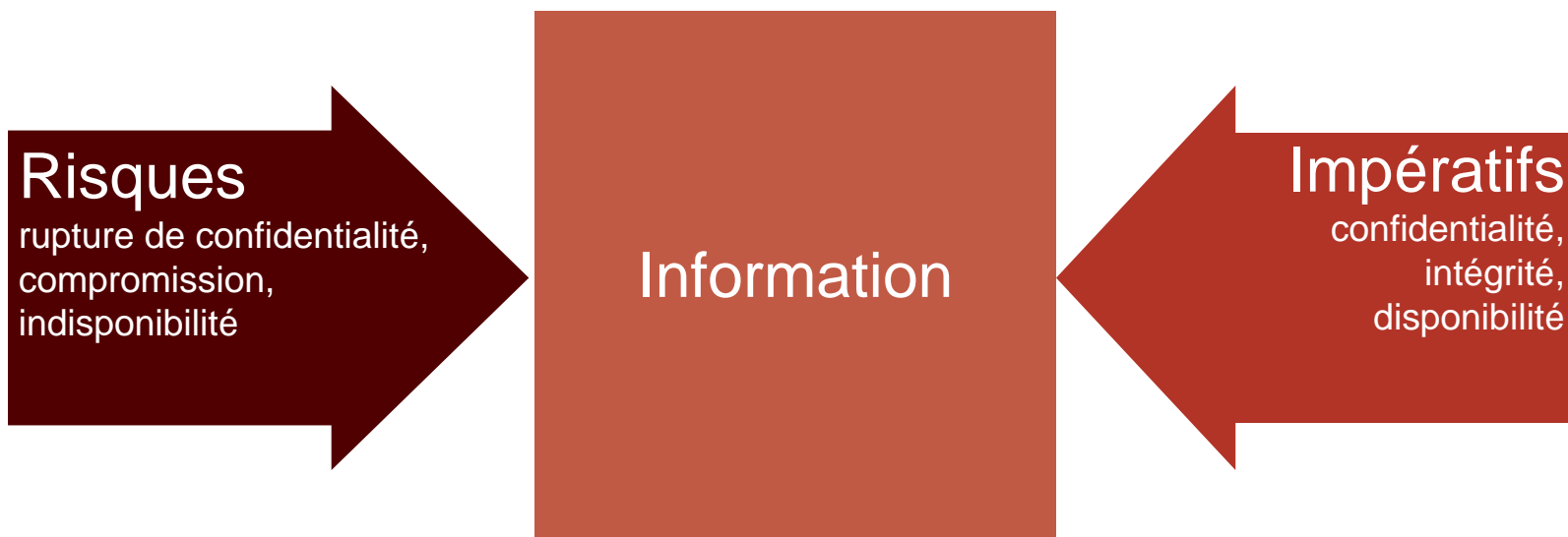
L'information est un point de vulnérabilité de l'entreprise

L'information est fragile (facile à altérer) et volatile par nature

L'insécurité de l'information est un phénomène croissant

Un moyen économique, rapide et relativement sans danger de porter préjudice à une entreprise –parfois de manière inconsciente

Vulnérabilité: La valeur à protéger



Vulnérabilité: La valeur à protéger

Risques

Attaques
informatiques

Mise en
réseau
/Internet

Technologies
nomades

Externalisation
/outsourcing

Comm.
électroniques

Information

bases de données,
documents informatiques,
communications
électroniques
archives papier,
savoir-faire,
connaissances

Risque

Economique

Coût de la reconstitution des données perdues, inefficacité liée à l'indisponibilité des données, dommages résultant d'une rupture de confidentialité

Réputationnel

Préjudice peut être total (disparition de l'entreprise dans certaines activités sensibles), perte de confiance des clients et partenaires

Juridique

Responsabilité civile (dommages & intérêts), risque de sanctions administratives (CNPD, CSSF) et pénales

Obligation de sécurité : Disponibilité, intégrité

Disponibilité, intégrité

La loi oblige les entreprises à garantir la disponibilité de certaines informations (et donc à les protéger)

Protection des données personnelles

Code de commerce

Loi fiscale (TVA)

Lois spéciales, textes réglementaires

Circulaires CSSF

Obligation de sécurité : Confidentialité

Confidentialité

L'entreprise doit garantir la **sécurité** et la **confidentialité** des données qu'elle traite

(art. 22 et 23, loi du 2 août 2002)

Sanctions

La loi prévoit des sanctions en cas de manquement.
Une attaque réussie et/ou une divulgation non autorisée de données peut suffire à constituer l'infraction

Administratives

avertissement, verrouillage, effacement des données, interdiction temporaire ou définitive du traitement, publication de la décision

Pénales

8 jours à 1 an de prison, EUR 251 à EUR 125 000 d'amende, cessation du traitement (astreinte)

Civiles

responsabilité civile (dommages & intérêts), préjudice ?



Secret professionnel
Secret bancaire...

Obligation de 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'introduction non autorisée de données, que toute prise de connaissance, modification ou effacement non autorisés des données)
: restriction d'accès au système



Obligation de 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 transmission de données)
: protection réseau (firewalls)

Contrôle de l'accès

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

Contrôle de la transmission

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



Obligation de sécurité: nature des mesures (3/3)



Contrôle de l'introduction

(garantir que puisse être vérifié et constaté a posteriori l'identité des personnes ayant eu accès au système et garantir le traçabilité des accès)

: autre traitement? surveillance?

Contrôle du transport

(empêcher que, lors de la communication/transport de supports, les données puissent être lues, copiées, modifiées ou effacées sans autorisation)

: cryptage des supports

Contrôle de la disponibilité

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

Obligation de sécurité: niveau de sécurité à atteindre

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)

Rôle des auditeurs

Des coûts
liés à leur mise
en oeuvre

**D'autres pays songent à suivre l'exemple du Luxembourg
(ex. Royaume-Uni/ICO)**

Obligation de sécurité: conformité

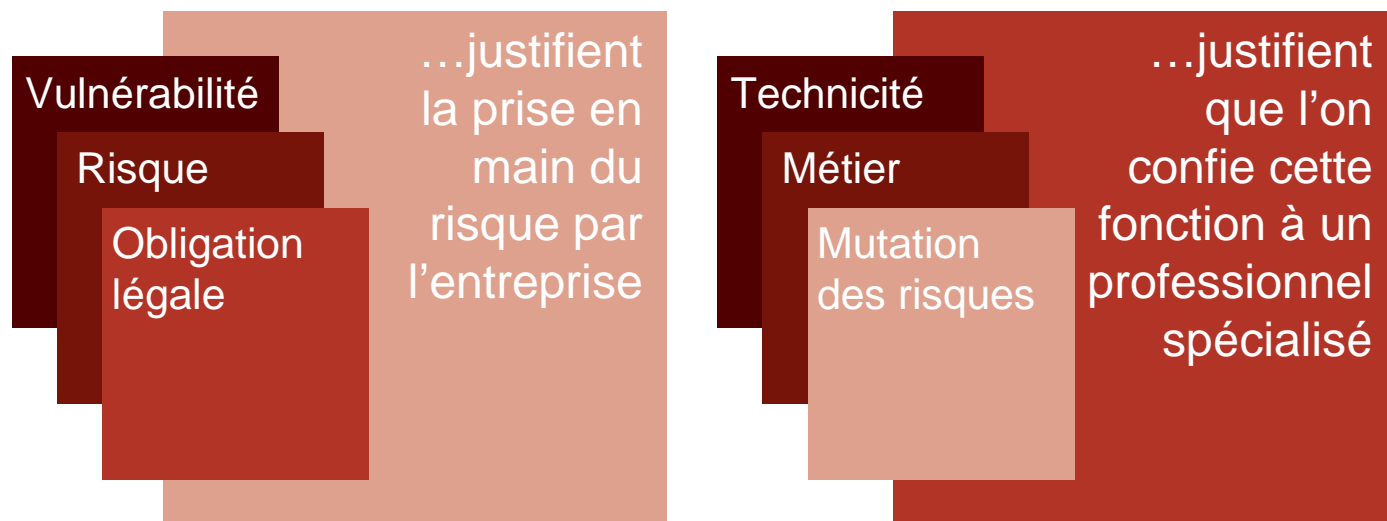
Mise en conformité initiale

Notification
Autorisation préalable
Information des personnes

Maintien en conformité (conformité dynamique)

Respect des finalités
Principe de qualité des données
Mise à jour de la sécurité

Fonction: la fonction du RSSI



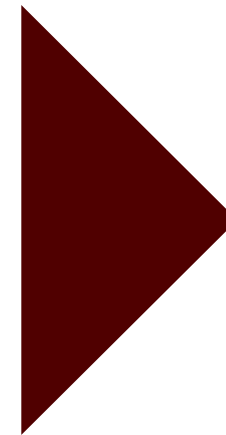
Fonction: la fonction du RSSI

Définir et faire évoluer la politique de sécurité

Coordonner la classification des informations

Assurer la continuité de l'activité

Sensibiliser les parties concernées



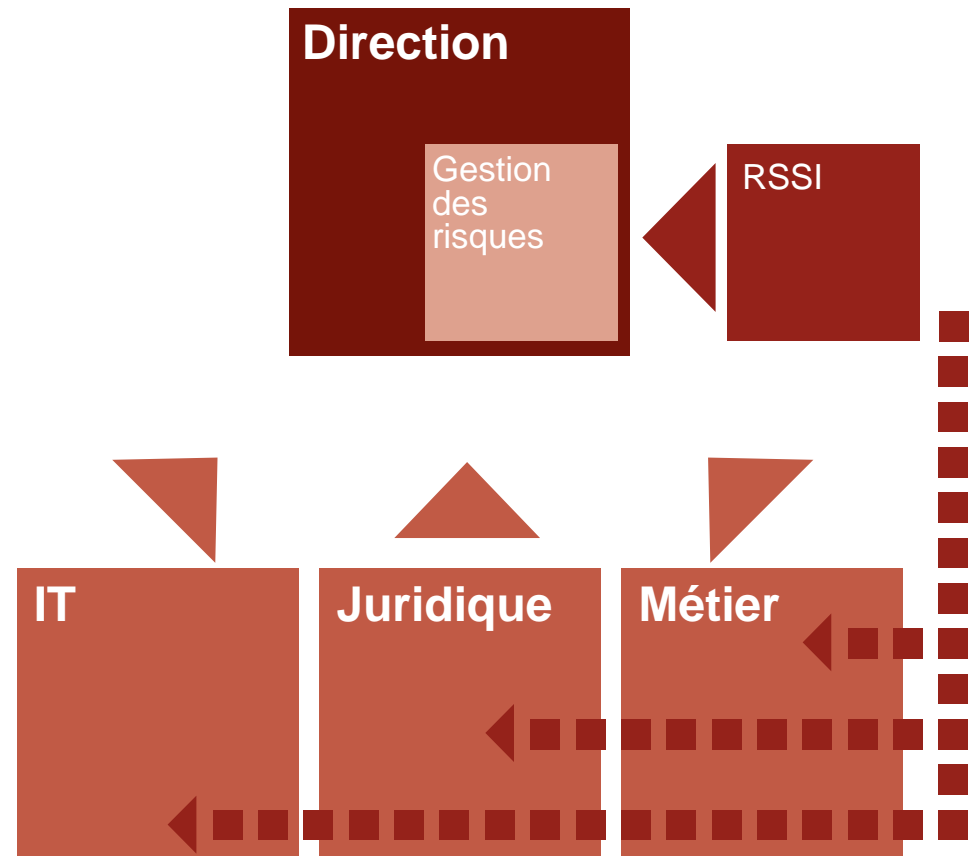
Fonction: la position du RSSI dans l'entreprise

Transversalité

Le RSSI doit s'intéresser à tous les aspects de sécurité (y inclus les aspects juridiques) et se faire aider au besoin

Indépendance

Le RSSI doit être indépendant de la fonction IT (risque de conflit d'intérêts)



Prévention :

Les moyens du RSSI

Politique de sécurité

...doit être précise, complète et adaptée à l'activité de l'entreprise et à la criticité de l'information (classification)

Politique interne

Les éléments clés de la politique de sécurité doivent être déclinés en une politique interne (par exemple, sous forme de «Charte IT») connue et respectée par le personnel

Sensibilisation du personnel

...et notamment des employés et collaborateurs ayant accès à des ressources ou infrastructures sensibles

Prévention : Sensibilisation à 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)

Exemple:
Attaque Trojan

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

2 mois
à 2 ans de prison

EUR 500 à 25 000
d'amende

Prévention : Sensibilisation à 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

Prévention : Sensibilisation à 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

Eléments 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

Prévention : Sensibilisation à 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

Prévention : Sensibilisation à la criminalité informatique

Accès, maintien, entrave,
altération d'un STAD
+transfert d'argent ou de
valeur monétaire

Article 509-4 du Code pénal

Suppose :

1. une des infractions de 509-1 à 509-3
2. transfert d'argent
3. perte de propriété
4. avantage économique pour l'auteur ou un tiers

Eléments indifférents:

1. attaque externe ou interne
2. méthode choisie pour l'attaque

Exemple:
Détournement de
fonds

4 mois
à 5 ans de prison

EUR 1 250 à 30 000
d'amende



Mêmes peines pour ceux qui auront fabriqué, reçu, obtenu, détenu, vendu ou cédé à un tiers des logiciels ayant pour objet de rendre possible cette infraction.

Prévention : Sensibilisation à 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

Prévention : Sensibilisation à la criminalité informatique

Divulgarion 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:

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

3 mois
à 3 ans de prison

EUR 251 à 12 500
d'amende

Prévention : Sensibilisation à 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

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

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

8 jours
à 1 an de prison

EUR 2 500 à 50 000
d'amende

Prévention : Sensibilisation à la criminalité informatique

Faux en écritures électroniques

Article 196 du Code pénal

Suppose (art. 460) :
1. commettre un faux
d'un écrit protégé
2. par fausse signature
3. (ou) contrefaçon ou
altération
4. (ou) fabrication de
conventions

Vise les éléments
préparatoires à une
attaque informatique
(falsification d'un
certificat électronique)

Vise également le
résultat de l'infraction
(modification de
données en vue de se
procurer un avantage
illicite)

5 à 10 ans de prison

EUR 2 500 à 50 000
d'amende

Prévention : Sensibilisation à 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

***La sensibilisation du personnel
est un puissant moyen de prévention.
C'est une mission essentielle du RSSI.***

Conclusions & perspectives

La fonction de sécurité doit être “dimensionnée” en fonction de la taille et de l’activité de l’entreprise

Faut-il imposer (au moins dans les secteurs régulés) la mise en place d’un RSSI ayant une formation ou expérience suffisante



Questions?

These are presentation slides only. The information within these slides does not constitute definitive advice and should not be used as the basis for giving definitive advice without checking the primary sources.

Allen & Overy means Allen & Overy LLP and/or its affiliated undertakings. The term partner is used to refer to a member of Allen & Overy LLP or an employee or consultant with equivalent standing and qualifications or an individual with equivalent status in one of Allen & Overy LLP's affiliated undertakings.