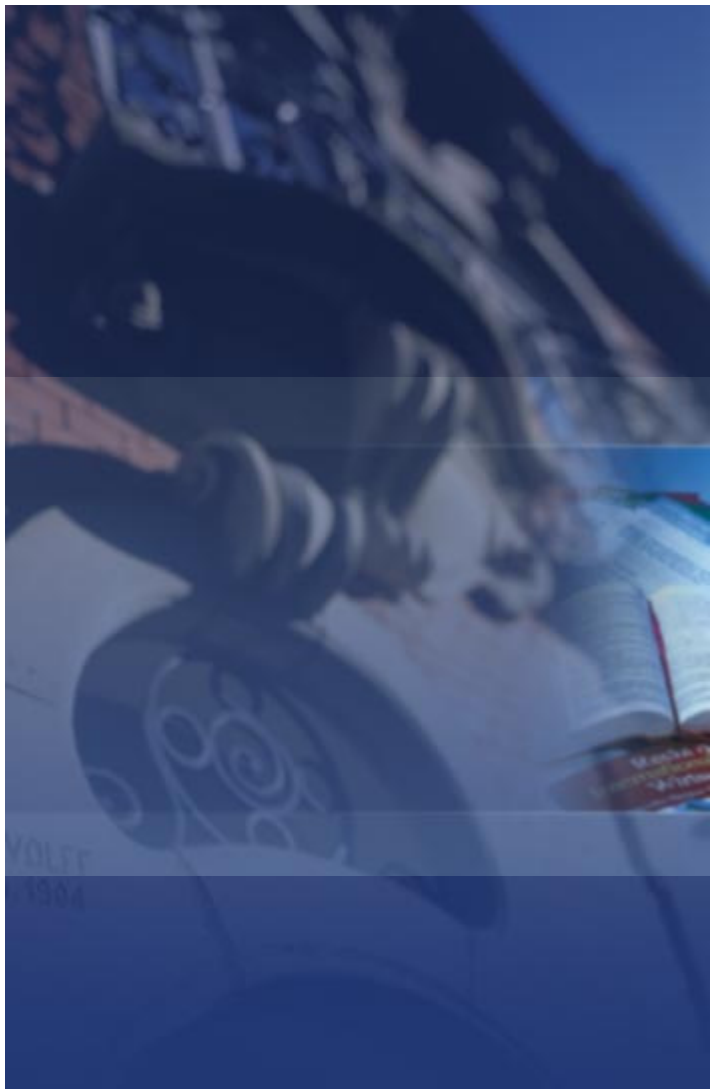

Etat des lieux de la réglementation (sécurité des systèmes d'information)

CLUSIF – 7 Novembre 2007

Garance Mathias

Avocat à la Cour

9 rue Notre Dame de Lorette – 75009 Paris

Tel : +33 (0)1 43 80 02 01

Gsm : +33 (0)6 15 91 44 07

Fax : +33 (0)1 42 12 02 22

Email: garance@gmathias.ath.cx

Plan

I. *Introduction : définition de la problématique*

II. *Evolution des menaces & Protection du patrimoine de l'entreprise*

III. *CNIL / CIL / données de connexion*

IV. *SOX / BALE II*

La sécurité interne d'une Entreprise est un enjeu collectif et partagé, pris en charge à tous les niveaux.

La définition des objectifs de sécurité et les résultats à atteindre sont de l'exclusive responsabilité de la Direction Générale.

Dans la limite des ressources qui lui sont affectées et de la Politique de sécurité, la responsabilité du Directeur Sécurité de l'Information est engagée face à toute attaque – intrusion – contre l'environnement informatique de l'Entreprise.

In fine :

• la responsabilité sur les informations accessibles est du ressort de la Direction Générale, des métiers et des fonctions supports.

• la responsabilité du contrôle de accès aux informations est du ressort de solutions et procédures de sécurité informatique, donc du Directeur Informatique.

Problématique

Le directeur informatique est le cadre chargé du fonctionnement et de l'évolution des systèmes d'information de l'entreprise.

Ses missions sont multiples et il doit faire face à différentes responsabilités :

- *d'ordre fonctionnelle*
- *d'ordre hiérarchique*
- *d'ordre sécuritaire*
- *pour le compte de tiers (hébergement, outsourcing)*
- *de gestion*

Et ce selon l'ampleur de leurs délégations de pouvoirs et leur position hiérarchique membre du Comité de direction ou rattaché à la direction administrative et financière.

Problématique

Le directeur informatique est le cadre chargé du fonctionnement et de l'évolution des systèmes d'information de l'entreprise.

Ses missions sont multiples et il doit faire face à différentes responsabilités :

- *d'ordre fonctionnelle*
- *d'ordre hiérarchique*
- *d'ordre sécuritaire*
- *pour le compte de tiers (hébergement, outsourcing)*
- *de gestion*

Et ce selon l'ampleur de leurs délégations de pouvoirs et leur position hiérarchique membre du Comité de direction ou rattaché à la direction administrative et financière.

Problématique

En d'autres termes , le directeur informatique ne peut donc échapper aux contraintes réglementaires ou salariales ni se soustraire à ses obligations.

En conséquence, il se voit dans l'obligation d'étudier les risques inhérents à son activité, en particulier le risque d'intrusion.

Il est impératif que le directeur de la sécurité dresse préalablement une cartographie des risques et de leurs conséquences tant sur les hommes, l'entreprise et les biens tant en interne qu'externe.

Il est impératif que ce dernier assure une gestion « en bon père de famille » du système d'information

Problématique

Responsabilité :

- *délégation de pouvoirs / écrite ?*
- *Responsabilité civile*
  - *engagée pour des dommages causés à la société ou aux tiers*
- *Responsabilité pénale:*
  - *Infraction commise personnellement par le dirigeant*
  - *Infraction commise par le préposé*

Problématique

Le contexte est le suivant :

- le DSI doit faire face à un fort impératif de sécurité, à des progrès technologiques de plus en plus complexe et en constante accélération

- l'environnement devient fortement dématérialisé

- A contrario, le droit demeure lent (et est rythmé par des procédures)

- Nous sommes dans un monde de globalisation qui peut entrer également en conflit avec des règles de droit (champ de compétence territoriale, etc.).

Problématique

En d'autres termes, il y a une recherche permanente d'un équilibre entre :

- *impératifs de sécurité interne / externe*
- *la protection du patrimoine de l'entreprise, des salariés*
- *la protection de la vie privée et des données personnelles*

L’évolution des menaces & protection du patrimoine de l’entreprise

Le patrimoine de l'entreprise

- Ses hommes, leurs idées, leurs savoir-faire, leurs réseaux relationnels et commerciaux
- Des informations juridiques, financières, commerciales et scientifiques, techniques, économiques ou industrielles

- Actuellement, le patrimoine de l'entreprise tend à être protégé par un ensemble de textes :

  - Loi dite Godfrain, loi sur le droit d'auteur, brevets (qui ne protége pas les méthodes, le savoir-faire, les idées, etc.)
  - La loi Informatique et Libertés, protection du logiciel (qui ne s'étend pas jusqu'à la protection des informations traitées par le logiciel).

- Quelle est la réaction du droit face aux menaces ?

Evolutions des menaces

- ***Le phishing / le pharming***

  - ***Le Phishing :*** *Technique de fraude visant à obtenir des informations confidentielles telles que des mots de passe ou des numéros de carte de crédit au moyen de messages ou des numéros de cartes de crédit au moyen de messages ou de sites usurpant l'identité d'institutions financières ou d'entreprises commerciales;*

  - ***Le Pharming*** *est une technique de fraude voisine du « phishing » consistant à rediriger le trafic internet d'un site internet vers un autre site dans le but d'obtenir des informations confidentielles telles que des mots de passe ou des numéros de cartes de crédit lui ressemblant*

Evolution des menaces

- ***BOTNET / BACKDOOR***

- ***Définition :***
  - *Robot qui renvoi l'adresse IP de sa victime vers un pirate*
  - *Le botnet est souvent associé avec un backdoor cad la machine victime possède un code qui ouvre une porte dérobée.*

- ***En fonction du code, la machine peut devenir :***
  - *Un site web pédophile*
  - *Un serveur de mail pour le spam*
  - *Un serveur pour du déni de service*
  - *Un serveur DNS pour du phishing ou du pharming*

Evolution des menaces

- ***Rootkit***
- ***Définition :***
  - *Code permettant de cacher tous les programmes malicieux qui pourraient être lancés sur la machine victime*
  - *Ne se réplique pas*
  - *Ne se propage pas*
  - *Ne contamine rien*
  - *Ne détruit rien*
- ***Juridiquement :***
  - ***Pas de lien de causalité entre le préjudice et l'acte incriminé (faute, dommage)….***

CLUSIF

Evolution des menaces

- ***KEY LOGGER***

- ***Définition :***

  Outil qui enregistre dans un fichier tout ce qui est taper sur le clavier de la victime. Ces informations sont envoyées au pirate par mail, etc . Les données, une fois, envoyées sont effacées de l'ordinateur de la victime

- ***Enjeux:***

  - *Programme vide,*
  - *Pas de trace*

- ***Quid de la réaction juridique et judiciaire***

CNIL & CIL

vie privée, données de connexion, charte, secret des correspondances

La protection des données personnelles au sein de l'entreprise

-Le Directeur informatique est responsable du Traitement

- Obligations au sens de la loi du 6 .01.1978 (modifiée en 2004)
- La délégation de pouvoirs

-Qu'est ce qu'une donnée à caractère personnel ?

-Comment gérer la collecte de données au sein d'une entreprise ?

- Droit d'information individuel des salariés
- Droit d'opposition, de rectification
- Droit de suppression

-Comment gérer les rapports avec la CNIL ?

- Autorisation auprès de la CNIL
- Déclaration auprès de la CNIL
- Contrôles de la CNIL

La protection des données personnelles au sein de l'entreprise

-Le correspondant Informatique et Libertés - CIL

- Mise en place en 2004
- Acteur « incontournable » dans le domaine de la protection des données
- Mission : « chargée d'assurer , d'une manière indépendante, le respect des obligations prévues par la loi » (…) « personne bénéficiant des qualifications requises pour exercer ses missions »
- Aujourd'hui plus de 1 200 organismes ont désigné un correspondant (Rapport CNIL 2007)
- Allégement des formalités
- Toutefois, le statut reste problématique : salarié protégé ou non / loyauté envers l'employeur / CNIL.

La protection des données personnelles au sein de l'entreprise

-Le correspondant Informatique et Libertés - CIL

- 1. Statut
  - Compétence
  - Indépendance
  - Information: Notification à la CNIL + aux IRP
- 2. Rôle
- 3. Responsabilité
  - Absence de sanctions de la part de l'employeur
  - Refus de communication d'informations / secret professionnel

La Politique de sécurité, édictée par la Direction Générale, s'adjoint une « Charte de bonnes pratiques » insérée au Règlement intérieur de l'Entreprise

La « ***Charte*** de bonnes pratiques » condense les règles et impératifs de sécurité propres à l'Entreprise. Elle prend valeur de Loi vis-à-vis des salariés et s'impose comme telle dans ses termes et ses sanctions.

Des transferts de responsabilités peuvent y être explicitement mentionnés et s'imposent à leurs destinataires.

Vis-à-vis des prestataires et partenaires, cette « Charte » n'a de valeur qu'informative. Ils ne sont pas tenus de s'y conformer, sauf accord contractuel.

Données de connexion

- Il n'existe pas de définition juridique : c'est une notion hétérogène

-De manière générale, ce sont les informations produites ou nécessitées par l'utilisation des réseaux de communications électroniques (téléphone, Internet, données de trafic, de localisation,..).

-L'état de la réglementation

- Adresse IP , données personnelles ou non ?
- Position de la jurisprudence (CA Paris) / Position de la CNIL
- La directive européenne
- L'état de la réglementation française
  - Durée de conservation :1 an
  - Quid de la compensation financière des opérateurs ?

- Le nécessaire équilibre entre les besoins de sécurité et la vie privée

SOX & BALE II

SARBANES – OXLEY ACT

-Loi américaine adoptée le 30.07.2002 après des scandales financiers (Enron, etc.)

-Une des réformes les plus importantes aux USA depuis la crise des années 1930

-Les objectifs poursuivis par la loi sont les suivants :

- augmenter la responsabilité de la société

- protéger de manière plus adéquate les investisseurs et redonner confiance à ces derniers et aux petits épargnants

- renforcement de la « gouvernance » d'entreprise, du principe de transparence

- critique de la section 404 de la loi : mise en place de structures et de procédures de contrôle interne sur les dispositifs de reporting financier. En application de cet article, il est imposé de documenter et de tester l'ensemble des processus et contrôles qui président à l'élaboration des états financiers.

- champ d'application : toutes les sociétés qui doivent déposer des rapports auprès de la SEC

SARBANES – OXLEY ACT (II)

En France la loi de sécurité financière du 1er.08.2003 a anticipé les normes européennes.

Toutefois, cette loi US cherche à contraindre les sociétés européennes à enfreindre tant la protection des données à caractère personnel que le secret professionnel

Par voie de conséquence, ce texte qui impacte principalement les sociétés côtées sur la place américaine, induit des réformes de procédures et de contrôles aussi draconiennes à appliquer que coûteuses à vérifier.

Bâle II

-Risque crédit : « *le risque de pertes résultant de la défaillance d'un créancier ou d'une contrepartie* »

-Risque marché : « *le risque de pertes sur positions de négociation en cas d'évolution défavorable des cours/ prix/ taux* »

-Risque opérationnel : « *le risque de pertes provenant de processus internes inadéquats ou défaillants de personnes et systèmes ou d'événements externes* »

Etant entendu que la réduction du risque opérationnel suppose une prise de mesure pour maîtriser notamment les dommages qui pourraient toucher les actifs physiques, les problèmes liés à la gestion du personnel..

Afin de maîtriser le risque, cela suppose une bonne performance en :

- sûreté de fonctionnement : fiabilité, gestion des incidents, etc.
- sécurité : protection du patrimoine et des informations
- secours et continuité : capacité à pérenniser

Conclusion