SSI : NOUVEAUX RISQUES, NOUVEAUX ENJEUX… DES RESPONSABILITES

Florence GRISONI
Juriste SSI

RESIST 29 JANVIER 2007

SSI NOUVEAUX RISQUES, NOUVEAUX ENJEUX… DES RESPONSABILITES

PLAN

- INTRODUCTION
- LE CADRE LEGAL ET REGLEMENTAIRE
- I/- NOTION DE RESPONSABILITE
- II/- RESPONSABILITE LIEE AU SYSTEME D'INFORMATION DE L'ENTREPRISE
- III/- RESPONSABILITE LIEE AU TRAITEMENT DES DONNEES A CARACTERE PERSONNEL
- IV/- RESPONSABILITE LIEE A L'UTILISATION DU SYSTEME D'INFORMATION DE L'ENTREPRISE PAR LE SALARIE
- V/- DES POSSIBILITES DE LIMITATION ET/OU D'EXONERATION DE RESPONSABILITE
- CONCLUSION

CONTEXTE

Changement de nature des risques lié à la complexité accrue des systèmes d'information, l'ouverture aux réseaux, et au nombre de domaines complémentaires que le DSI doit traiter. Ces derniers vont des aspects juridiques à l'organisationnel, en passant par des compétences en communication interne et externe.

Textes juridiques disparates : opposition entre l'évolution exponentielle en termes de rôle et de responsabilité de la fonction de DSI et / ou de RSSI et l'absence de dispositions juridiques l'encadrant spécifiquement.

Une évolution importante dans le temps et une adaptation nécessaire du rôle et missions des responsables informatiques dans l'entreprise : « d'homme orchestre de la sécurité informatique vers homme orchestre de la sécurité du patrimoine informationnel de l'entreprise ».

INTRODUCTION

SSI : NOUVEAUX RISQUES, NOUVEAUX ENJEUX… DES RESPONSABILITES

- Traditionnellement, le DSI /RSSI a pour rôle de garantir la disponibilité et l'intégrité de l'ensemble des ressources informatiques de l'entreprise ainsi que la confidentialité des informations.
- Dans ce cadre, il est chargé de la définition et de la mise en œuvre de la politique de sécurité de l'entreprise. Il possède en outre un rôle stratégique d'information, de conseil et d'alerte de la direction générale sur les risques en matière de sécurité informatique.
- Le RSSI est en particulier chargé des choix et actions concernant :
- la sensibilisation des utilisateurs aux problèmes de sécurité
- la sécurité des réseaux et des applications
- la sécurité des systèmes et des télécommunications
- la sécurité physique
- la stratégie de sauvegarde des données
- la mise en place de moyens de fonctionnement en mode dégradé
- la mise en place d'un plan de continuité d'activité

- Importance du rattachement hiérarchique compte tenu du contexte

  Si le DSI et / ou le RSSI sont quelquefois rattachés à la Direction des Systèmes Informatiques (DSI), ils sont fréquemment rattachés à la Direction Générale (DG) de l'entreprise, compte tenu des enjeux et des risques (notamment juridiques) portés par le Système d'Information(SI).

Aperçu des risques et des enjeux

Panorama non exhaustif des risques potentiels

- Les risques peuvent être internes ou externes à l'entreprise.

  Risques internes

  exemple : risques liés à l'utilisation des outils informatiques par les salariés : utilisation d'Internet, de la messagerie

  Les outils informatiques peuvent aussi être utilisés pour nuire

  Risques externes : piratage, malveillance, intrusions, altération / vol de données confidentielles ou stratégiques…

- Les enjeux

  Pour l'entreprise

  pour la personne physique

Parmi les principaux gisements de risques figurent les traitements de données à caractère personnel, le droit d'auteur, la contrefaçon et les usages parfois illicites des outils de l'entreprise par les salariés.

Par ailleurs, il existe de plus en plus de contraintes légales en matière de sécurité (LSF, Sarbanes-Oxley, I & L …) et les nouvelles méthodes de partage de l'information (portable, liaison WiFi, port USB…) qui rendent plus perméable le SI accroissent la responsabilité du DSI et des autres préposés de l'employeur.

LE CADRE LEGAL ET REGLEMENTAIRE NATIONAL ET INTERNATIONAL

QUELQUES TEXTES…

LE CADRE LEGAL ET REGLEMENTAIRE1/2

SSI : NOUVEAUX RISQUES, NOUVEAUX ENJEUX… DES RESPONSABILITES

- Loi Godfrain du 5 janvier 1988
- Loi du 6 janvier 1978 dite Informatique et Libertés relative à l'Informatique, aux fichiers et aux libertés, modifiée par la loi du 6 Août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel
- Directive européenne du 14 Mai 1991 sur la protection des programmes d'ordinateur
- Loi du 10 mai 1994 sur la protection juridique des programmes d'ordinateur
- Directive européenne du 24 Octobre 1995 relative au traitement des données à caractère personnel
- Loi du 1er Juillet 1998 concernant la protection juridique des bases de données
- Loi du 13 Mars 2000 portant adaptation du droit de la preuve aux technologies de l'information et relative à la signature électronique

LE CADRE LEGAL ET REGLEMENTAIRE 2/2

SSI : NOUVEAUX RISQUES, NOUVEAUX ENJEUX… DES RESPONSABILITES

- Directive européenne du 12 juillet 2002 relative au traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques
- Loi américaine Sarbanes-Oxley du 29 Août 2002 visant à rétablir la confiance à l'égard de l'information financière et comptable (concerne les sociétés cotées sur un marché financier des États-unis quelle que soit leur nationalité ainsi que leurs filiales étrangères)
- Loi sur la Sécurité Financière (LSF) du 1er Août 2003
- Loi pour la Confiance dans l'Économie Numérique (LCEN) du 21 Juin 2004
- Loi du 23 janvier 2006 sur la lutte contre le terrorisme et son décret d'application du 24 Mars 2006
- ISO/IEC 17799 : 2005
- ISO/IEC 27001

NOTION DE RESPONSABILITE

NOTION DE RESPONSABILITE

Fondements possibles de la responsabilité de l'entreprise (et par délégation du DSI/RSSI/ Administrateur…)

La responsabilité civile

- **Définition**
- **Article 1383 du Code civil : responsabilité civile délictuelle ou quasi-délictuelle, contractuelle, de son fait personnel**
- **Article 1384 alinéa 5 du code civil : responsabilité du fait d'autrui**

l'employeur civilement responsable du fait de l'activité de ses préposés, notamment en cas d'utilisation malveillante des moyens informatiques et de communications électroniques.

Possibilité d'exonération par la notion d'abus de fonction.

Exemple : Arrêt d'Assemblée Plénière du 19 mai 1988 fixe les critères

La responsabilité pénale

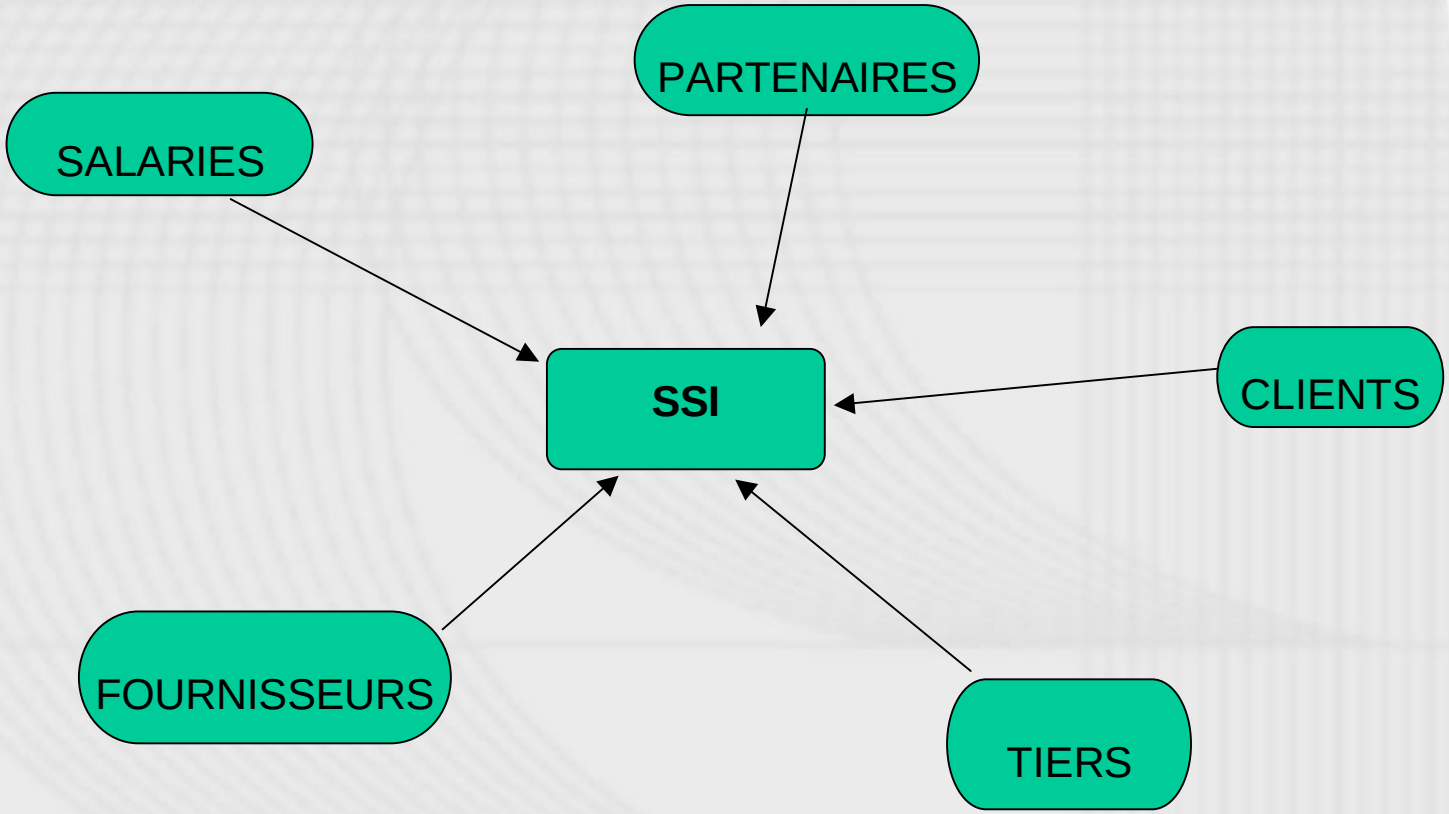
- L'article L121-2 du Code pénal pose le principe selon lequel les personnes morales ne peuvent être pénalement poursuivie que si la loi ou le règlement le prévoit de façon expresse.

- l'article 323-6 : prévoit la responsabilité pénale de la personne morale en matière de SI

  Exemple du Crédit lyonnais condamné à 45 000 euros d'amende par la CNIL, le 28 juin 2006, pour enregistrement abusif de plusieurs de ses clients dans le fichier des incidents de paiement de la Banque de France

Les titulaires de l'action :

Clients, fournisseurs, salariés, partenaires, des tiers



RESPONSABILITE LIEE AU SYSTEME D'INFORMATION DE L'ENTREPRISE

La fraude informatique et l'atteinte au système d'information

Le délit d'accès frauduleux à un système

Articles 323-1 à 323-7 du Code pénal prévoient un certain nombre d'incrimination en matière de fraude informatique

- L'article 323-1 sanctionne le délit d'accès non autorisé et le maintien frauduleux dans un système informatique par 2 ans d'emprisonnement et 30 000 € d'amende
- L'article 323-2 sanctionne le fait d'entraver ou de fausser le fonctionnement d'un système de traitement automatisé de données par 5 ans d'emprisonnement et 75 000 euros d'amende
- L'article 323-3 sanctionne par les même peines le fait d'introduire frauduleusement des données dans un système informatique ou de modifier ou supprimer frauduleusement les données qu'il contient

Exemple : l'affaire Kitetoa / Tati

- **L'incrimination de la fourniture de moyens**

  Société Lucent Technologies TGI de Marseille 11 juin 2003 : l'employeur du créateur d'un site Internet a été condamné sur le fondement de l'article 1384 du Code civil pour avoir mis à disposition de son salarié les moyens techniques nécessaires à la mise en ligne dudit site et parce qu'il n'avait pas interdit l'usage à des fins personnelles des moyens informatiques.

Les failles de sécurité

- Problèmes logiciels
- Les systèmes d'information peuvent être menacés par l'implantation d'un logiciel espion ou par la défaillance d'un antivirus.
- cas du logiciel espion introduit par l'éditeur d'un logiciel à l'insu du client : responsabilité contractuelle + manquement à l'obligation de bonne foi prévue par l'article 1134 du Code Civil en vertu duquel « les conventions doivent être exécutées de bonne foi ».
- Exemple : les révélations faites en juin 2005 au sujet d'une entreprise israélienne qui « louait » un cheval de Troie à ses clients. Cette affaire a donné lieu à l'arrestation de plusieurs dirigeants d'entreprise à travers le monde.

- cas d'un logiciel espion qui ne fonctionne pas : responsabilité contractuelle ? la question peut se poser… l'acquéreur d'un tel logiciel qui agirait en responsabilité pourrait se voir opposer la règle « nemo auditur » dans l'hypothèse d'un logiciel espion dont la légalité paraît douteuse. Même si, par principe ceux-ci ne sont pas interdits, mais leur utilisation est soumise à certaines conditions.
- Cas de l'antivirus qui est défaillant : responsabilité contractuelle / obligation de moyens et pas de résultat compte tenu de l'ampleur de la tâche. La responsabilité de l'éditeur pourra être retenue si l'on prouve qu'un autre logiciel aurait protégé le système.
- Importance ici des clauses prévues dans les contrats avec les fournisseurs et de la non-conformité d'un produit à sa destination.

RESPONSABILITE LIEE AU TRAITEMENT DES DONNEES A CARACTERE PERSONNEL

L'obligation d'information

- La loi Informatique et Libertés réglemente la collecte et l'utilisation des données nominatives. Elle prévoit un régime de déclaration préalable auprès de la CNIL et une information de la personne faisant l'objet de la collecte sur celle-ci ainsi que sur l'utilisation qui en sera faite.
- Le manquement à cette obligation constitue une infraction engageant la responsabilité pénale de l'auteur. Les sanctions sont lourdes en cas de non respect de ces formalités préalables. Elles vont jusqu'à 3 ans d'emprisonnement et 45 000 euros d'amende (article 226-16 du Code pénal).

L'obligation de sécurité

- Il existe une obligation générale de sécurité qui pèse sur le responsable d'un traitement.

- La loi Informatique et Libertés du 6 janvier 1978 modifiée par la loi du 6 août 2004 prévoit une obligation générale de sécurité. L'article 34 dudit texte précise que le responsable du traitement est tenu de prendre « toutes précautions utiles » pour protéger les données à caractère personnel sous sa responsabilité, notamment, pour « empêcher qu'elles soient déformées, endommagées ou que des tiers non autorisés y aient accès ».

- Il résulte de cette législation sur les données personnelles que le responsable d'un traitement de telles données a l'obligation d'en assurer la confidentialité et la sécurité.
- Le non respect de cette obligation est d'ailleurs sanctionné par le Code Pénal. L'article 226-17 prévoit en effet des peines allant jusqu'à 5 ans d'emprisonnement et 300 000 € d'amende pour délit de manquement à la sécurité des données.
- En cas de sous-traitance, le contrat devra préciser que le sous-traitant n'agit que sur instruction du responsable du traitement qui demeure responsable de la confidentialité des données traitées pour son compte.

- Obligation de moyen : la sécurité absolue n'existe pas, on se réfère à la notion générique de l'état de l'art.
- Il faudra justifier de la mise en place d'une politique de sécurité et de mesures variées d'ordre logique (installation d'antivirus, firewalls, cryptage…), organisationnel (accès restreint aux données en fonction des habilitations…) et physique (contrôle d'accès aux locaux).
- Ça peut aussi se traduire par des actions de sensibilisation et de formation du personnel
- La loi requiert un niveau de sécurité approprié. On raisonne ici en terme de gestion des risques
- La jurisprudence quant à elle parle d'« homme raisonnable ».
- La CNIL joue à ce propos un rôle de sensibilisation des responsables de traitements

- Exemple : perte CD Rom contenant les données personnelles d'employés
- Autre exemple : vols de PC portables contenant des données sensibles
- Problèmes d'usurpation d'identité

RESPONSABILITE LIEE A L'UTILISATION DU SYSTEME D'INFORMATION DE L'ENTREPRISE PAR LE SALARIE

Responsabilité vis-à-vis des tiers

- La duplication de logiciels sans autorisation de l´auteur ou de l´éditeur constitue, le plus souvent, une contrefaçon susceptible de poursuites et notamment de poursuites pénales. Or, les personnes susceptibles d´être poursuivies ne sont pas seulement les dirigeants légaux de la société, mais également les directeurs et notamment les DSI ayant donné des instructions claires en ce sens aux salariés.

Exemple : directeur informatique condamné le 12 avril 1996 aux côtés du Président d´une société, pour avoir donné des instructions à un technicien de son service afin qu´il reproduise en plusieurs exemplaires des logiciels acquis légalement pour les installer sur l´ensemble des micro-ordinateurs de l´entreprise.

Responsabilité vis-à-vis du salarié : les limites à l'exercice du pouvoir de direction et de contrôle de l'employeur

- Cybersurveillance et secret des correspondances

Arrêt Nikon du 2 octobre 2001 pose le principe selon lequel :

- ***« Le salarié a droit, même au temps et au lieu de travail, au respect de sa vie privée ; celle-ci implique en particulier le secret de ses correspondances ; l'employeur ne peut dès lors, sans violation de cette liberté fondamentale, prendre connaissance des messages personnels émis par le salarié ou reçus par lui grâce à un outil informatique mis à sa disposition pour son travail, et ceci même au cas où l'employeur aurait interdit une utilisation non professionnelle de l'ordinateur ».***
- Un véritable contrôle de proportionnalité qui est opéré par les juges
- Information préalable du personnel et du Comité d'entreprise en cas de mise en place d'un système de surveillance

- Arrêt Cathnet-Science du 17 mai 2005 transposant la même règle qu'en matière de fouille de placards au SI: il en résulte qu'en ce qui concerne les fichiers informatiques, les documents informatiques contenus sur le disque dur du salarié n'ont pas le caractère de correspondances privées, sauf s'ils sont identifiés comme tels par le salarié

- Arrêt Techni-Soft en date du 18 octobre 2006 : prévoit la possibilité qu'il puisse être indiqué dans le cadre d'une réglementation interne que tout fichier qui ne porterait pas la mention « personnel » a un caractère professionnel et peut par conséquent être consulté par l'employeur et la hiérarchie du salarié : employé avait été licencié pour avoir crypté des données sur son ordinateur, empêchant ainsi son employeur d'y avoir accès. Le licenciement Pour faute a été justifié.

- Les administrateurs réseaux et la loi informatique et libertés

  La CNIL a rappelé dans son rapport intitulé la « cybersurveillance sur les lieux de travail » adopté le 5 février 2002, que les administrateurs de réseaux doivent « veiller à assurer le fonctionnement normal et la sécurité des réseaux et systèmes ».

  Ayant rappelé qu´ils étaient ainsi « conduits par leurs fonctions mêmes à avoir accès à l´ensemble des informations relatives aux utilisateurs », y compris à celles qui sont enregistrées sur le disque dur du poste de travail, la CNIL a indiqué que des « prises en main à distance » des postes de travail étaient autorisées sous réserve de respecter le secret professionnel auquel ils sont tenus et ne pas « divulguer des informations qu´ils auraient été amenés à connaître dans le cadre de leurs fonctions et en particulier lorsque celles-ci sont couvertes par le secret des correspondances ou relèvent de la vie privée des utilisateurs ».

Dès lors que les fichiers stockés sur le disque dur d´un salarié peuvent présenter un caractère privé et être assimilables à une correspondance personnelle, le non-respect du secret à cet égard pourrait engager jusqu´à la responsabilité pénale du DSI.

L'obligation de conservation des données de connexion

DES POSSIBILITES DE LIMITATION ET/OU D'EXONERATION DE RESPONSABILITE

Construction d'une politique de sécurité

Rédaction de chartes, livrets de sécurité…

- Mise en place de chartes de bonne conduite concernant l'utilisation des systèmes d'information mis à la disposition des salariés
- livrets de procédure de sécurité organisant la traçabilité des incidents, le contrôle et la conservation de la preuve numérique
- L'employeur doit donc prévoir explicitement toutes les interdictions en matière d'utilisation de l'Internet sur le lieu du travail sous peine de voir sa responsabilité engagée au plan judiciaire.
- Dans un arrêt du 13 mars 2006, la Cour d'appel d'Aix en Provence a condamné un employeur pour un usage illicite d'Internet par un des ses employés, ce dernier ayant créé un site diffamant hébergé sur le serveur de l'entreprise

- **Le recours à l'externalisation**
  - **Le recours à la sous-traitance**
  - **Sécurisation des contrats informatiques**
  - Utilisation des normes et standards dans les contrats de prestations de service.
  - Rédaction de clauses adéquates pour les audits de sécurité et d'intrusion.
  - Utilisation d'une signature électronique valable juridiquement afin d'identifier les échanges de l'entreprise.
  - **Souscription de polices d'assurances adéquates :** ne pas oublier la gestion assurantielle des risques liés à la sécurité résultant notamment de la perte de chiffre d'affaires induite par des actes frauduleux ou encore les coûts engendrés par la reconstitution des données qui seraient altérées ou perdues.

Le recours par l'employeur à la délégation de pouvoir

- l'employeur peut se dégager de sa responsabilité s'il parvient à justifier de l'existence d'une délégation de pouvoir valide
- Les conditions de son admission sont cependant strictement encadrées. Ce qui laisse une possibilité aux DSI et RSSI d'être exonérés, même si pour certains ce n'est qu'un sursis, une illusion…

un DSI ou un RSSI ne pourra être valablement investi d'une délégation de pouvoir que si :

- il a les compétences nécessaires : techniques certes, mais aussi des connaissances juridiques
- il doit avoir l'autorité nécessaire
- Il doit disposer des moyens nécessaires pour accomplir sa mission
- Autres conditions :la délégation doit être précise (par exemple : mesures de sécurité liées au système d'information) et revêtir un caractère de permanence (pas de délégation à une personne occupant un poste temporaire).
- La jurisprudence exige par ailleurs que le salarié soit informé des conséquences de la délégation de pouvoir, à savoir un transfert de responsabilité pénale.

- Arrêt de la Cour de cassation du 30 octobre 1996 : admet la subdélégation, à condition que le sub-délégataire soit investi des mêmes pouvoirs que ceux énoncés précédemment.
- Difficile à concevoir entre un DSI et un RSSI, sauf dans le cas d'un très grand groupe. En effet, dans ce cas, le DSI pourrait très bien déléguer ses pouvoirs à des responsables informatiques chargés de filiales ou de départements.
- Par contre, il faudra faire attention au principe de non-cumul des délégations de pouvoir.
- Admission de la délégation verbale : attention cependant aux « notes de mission » dont disposent certains RSSI
- le refus expressément exprimé par un salarié rend invalide la délégation de pouvoir

- **CONCLUSION**

  Importance de la mise en place d'une Politique de Gestion des Risques Juridiques (PGRJ) au sein de l'entreprise.

MERCI POUR VOTRE ATTENTION !

QUESTIONS ?

SSI : NOUVEAUX RISQUES, NOUVEAUX ENJEUX… DES RESPONSABILITES

Florence GRISONI
Legal Counsel ISS
EADS France
Innovation Works