TIC :
QUELS RISQUES JURIDIQUES POUR L'ENTREPRISE ?
COMMENT LES LIMITER ?

Présentation 9 Avril 2015

S.D.I.
TELECOMS - INFORMATIQUE - CLOUD

Le réseau informatique de l'entreprise

- Coexistence de risques d'origine interne et externe
- Comment les adresser au niveau juridique?

1ère Partie

Les risques externes

1. Le contexte actuel
2. Des coûts engendrés par la cybercriminalité qui restent lourds pour les entreprises victimes
3. Comment poursuivre les responsables ?
4. Des risques juridiques significatifs pour entreprises et dirigeants
5. Quelles solutions ?

Le contexte actuel : quelques chiffres

* 2013 : La cybercriminalité représente 28% des fraudes déclarées par les sociétés françaises
* 31% des attaques informatiques visent les entreprises de moins de 250 salariés (2012)
* De 2010 à 2012 la BEFTI enregistre 120 plaintes pour détournement de lignes téléphoniques
* Paradoxe : en 2014 le nombre moyen d'incidents de sécurité augmente de 30% dans les entreprises, qui réduisent malgré tout leur budget sécurité de 3% sur la même période (source PWC)

Le contexte actuel : exemples récents

* TF1 : vol de données personnelles de 2 millions d'abonnés (dont les coordonnées bancaires et les profils d'accès)
* Sony : vol des données personnelles des 50.000 employés de Sony (dont des fichiers confidentiels et des correspondances privées)
* Banque Morgan Stanley : vol des données personnelles de 350.000 clients de la banque et publication sur le net de certaines de ces données
* Target : vol de 40 millions de coordonnées clients et des codes PIN des CB associées
* Snapchat : vol de données personnelles de 4,6 millions d'utilisateurs
* Ebay : vol de données personnelles de 150 millions d'utilisateurs
* Orange : vol de données personnelles de 1,3 millions de clients/prospects

Le contexte actuel : une évolution inévitable

* Taille des systèmes d'information
* Informatisation totale des processus de production et de fonctionnement des entreprises
* Recours au cloud en augmentation constante
* Mobilité grandissante des salariés et des clients
* Dématérialisation de la vie des entreprises

Les risques externes

1. Le contexte actuel
2. Des coûts engendrés par la cybercriminalité qui restent lourds pour les entreprises victimes
3. Comment poursuivre les responsables ?
4. Des risques juridiques significatifs pour entreprises et dirigeants
5. Quelles solutions ?

Coûts directs engendrés pour l'entreprise : le cas particulier du détournement de ligne

* Différents types d'attaques malveillantes : destruction d'informations, blocage du SI de la cible, écoute de conversations, fraude financière
* Coûts directs pour l'entreprise dans le cas de la fraude financière :
  * Appels gratuits vers l'international
  * Appels en masse vers des numéros surtaxés pour générer du revenu
  * Revenue des capacités de communication détournées

Coûts directs engendrés pour l'entreprise : le cas particulier du détournement de ligne

* ***Jurisprudence Cour d'Appel de Versailles 25.03.2014***

  * Opérateur réclame à l'entreprise +21K€ de télécommunications passées vers le Timor oriental…
  * Installateur : exonéré de toute responsabilité
  * Société de maintenance : responsabilité engagée pour manquement à ses obligations d'information et de conseil
  * Résultat pour l'entreprise : facture de 21K€ quasiment totalement prise en charge par la société de maintenance finalement condamnée à lui verser 20K€

Coûts indirects souvent lourds à la charge de l'entreprise

* Frais informatiques :
  * Investigations nécessaires pour comprendre d'où vient la faille de sécurité
  * Investigations nécessaires pour mesurer l'étendue des dégâts causés
  * Remise en état du SI
  * Sécurisation et prévention des attaques futures
* Frais de notification
* Frais de communication de crise

Les risques externes

1. Le contexte actuel
2. Des coûts engendrés par la cybercriminalité qui restent lourds pour les entreprises victimes
3. Comment poursuivre les responsables ?
4. Des risques juridiques significatifs pour entreprises et dirigeants
5. Quelles solutions ?

Comment poursuivre les responsables ?

* Dépôt de plainte contre X : indispensable pour engager des poursuites
* Code Pénal : 1 chapitre entier consacré aux atteintes aux systèmes de traitement automatisé de données introduit initialement par la Loi du 5 Janvier 1988 relative à la fraude informatique
* Loi du 27 Mars 2012 : **article 323-1 Code Pénal**

  *« Le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données est puni de **deux ans d'emprisonnement et de 30 000 euros d'amende**.*

  Lorsqu'il en est résulté soit la suppression ou la modification de données contenues dans le système, soit une altération du fonctionnement de ce système, la peine est de trois ans d'emprisonnement et de 45 000 euros d'amende. »

Comment poursuivre les responsables ?

* Loi du 27 Mars 2012 : **article 323-2 Code pénal**

  *« Le fait d'entraver ou de fausser le fonctionnement d'un système de traitement automatisé de données est puni de **cinq ans d'emprisonnement et de 75 000 euros d'amende.** »*

* Loi du 13 Novembre 2014 : **article 323-3 Code Pénal**

  *« Le fait d'introduire frauduleusement des données dans un système de traitement automatisé, d'extraire, de détenir, de reproduire, de transmettre, de supprimer ou de modifier frauduleusement les données qu'il contient est puni de **cinq ans d'emprisonnement et de 75 000 euros d'amende.** »*

Comment poursuivre les responsables ?

* Peines complémentaires prévues par le Code Pénal : fermeture de l'établissement, exclusion des marchés publics, confiscation des matériels, publication de la décision…
* Condamnations des personnes morales : les peines d'amende sont multipliées par 5
* D'autres types de condamnations sont possibles sur des motifs plus traditionnels du droit français (ex: abus de confiance)

Les limites aux poursuites judiciaires

* Des tribunaux longtemps frileux à reconnaitre le vol d'informations indépendamment du support matériel (ex: ordinateur portable, PDA, clé USB)
* Des plaintes classées sans suite dès lors que les montants sont estimés minimes…
* Des hackers opérant depuis l'étranger ou impossibles à identifier
* Des preuves souvent difficiles à rassembler pour incriminer les réels commanditaires (ex: affaire EDF/Greenpeace de 2013)

Les risques externes

1. Le contexte actuel
2. Des coûts engendrés par la cybercriminalité qui restent lourds pour les entreprises victimes
3. Comment poursuivre les responsables ?
4. Des risques juridiques significatifs pour entreprises et dirigeants
5. Quelles solutions ?

Des risques juridiques significatifs

* Des risques juridiques pour l'entreprise :
  * L'entreprise est responsable des atteintes aux droits de la personne
  * L'entreprise doit assurer et garantir la sécurité et la confidentialité des données qu'elle stocke et qu'elle traite
* Des risques juridiques pour le dirigeant :
  * Le DG est en charge de fixer la stratégie concrète de sécurité des SI de l'entreprise et de protection contre les cyber-attaques
  * Une responsabilité managériale qui peut aboutir à la destitution du dirigeant (ex: Target)

Obligation générale de sécurité à la charge des entreprises et de leurs dirigeants

* **Loi Informatique et Libertés (art.34)** : « *Le responsable du traitement est tenu de prendre toutes précautions utiles, au regard de la nature des données et des risques présentés par le traitement, pour préserver la sécurité des données et, notamment, empêcher qu'elles soient déformées, endommagées, ou que des tiers non autorisés y aient accès.* »
* Responsable des traitements sanctionné ⇔ traduit en justice pour négligence
* Quelle défense pour l'entreprise et le dirigeant ?
  * apporter la preuve d'une gestion saine et de l'anticipation des risques ⇔
  * la responsabilité peut être engagée du seul fait de la mauvaise identification des précautions à mettre en œuvre

Obligation générale de sécurité à la charge des entreprises et de leurs dirigeants

* Droit de contrôle de la CNIL concernant les données personnelles stockées et traitées par l'entreprise
* Sanctions possibles : avertissement, amende (150K€ et jusqu'à 300K€ en cas de récidive dans les 5 ans), injonction de cesser le traitement en cause , publication de la décision
* Effet très négatif en terme d'image (ex: Free en 2006)

Autres types de risques juridiques encourus

* Manquement à une obligation de confidentialité :
  * Contrat signé : réparation pour les pertes subies et le manque à gagner du cocontractant
  * Hors lien contractuel : droit commun de la responsabilité ⇔ **article 1382 du Code Civil**

    « Tout fait quelconque de l'homme, qui cause à autrui un dommage, oblige celui par la faute duquel il est arrivé à le réparer. »

* Données couvertes par le secret bancaire : délit de violation du secret bancaire **art 226-13 du Code Pénal** :

  *« La révélation d'une information à caractère secret par une personne qui en est dépositaire soit par état ou par profession, soit en raison d'une fonction ou d'une mission temporaire, est punie d'**un an d'emprisonnement et de 15 000 euros d'amende.** »*

Autres types de risques juridiques encourus

* Information commercialement sensible au regard du droit de la concurrence (poursuites par le Conseil de la Concurrence)
  * Atteinte à une concurrence loyale
  * Manquement à obligation réglementaire
  * Violation du droit de la concurrence (entente, concentrations)
* Données représentant des informations privilégiées au sens de la réglementation des marchés financiers (poursuites par l'AMF)

Les risques externes

1. Le contexte actuel
2. Des coûts engendrés par la cybercriminalité qui restent lourds pour les entreprises victimes
3. Comment poursuivre les responsables ?
4. Des risques juridiques significatifs pour entreprises et dirigeants
5. Quelles solutions ?

Quelles solutions ?

4 façons de gérer les risques :

* L’arrêt d’une activité trop risquée
* La prise de risques volontaire
* La gestion du risque
* La sous-traitance du risque

Quelles solutions ?

La question de la protection du patrimoine informatique de l'entreprise se pose du point de vue :

* Technique/technologique : gestion des accès, cryptage, outils de contrôle, firewalls…
* Opérationnel : processus de gestion de l'information, gouvernance des sous-traitants…
* Juridique : Loi Informatique et Libertés, clause de confidentialité, non-concurrence…

Quelles solutions ?

* Mettre en place une politique de sécurité informatique
  * adaptée aux besoins de l'entreprise et aux traitements qu'elle effectue
  * intégrant tous les paramètres du SI dans la politique de sécurité informatique de l'entreprise (éléments physiques, téléphonie, règles d'accès…)
* Prévention interne : sensibiliser les collaborateurs aux risques, auditer la sécurité informatique régulièrement
* Assurance : des solutions très différentes offertes par les assureurs mais qui présentent toutes des lacunes
* Juridique : mettre en place des délégations de pouvoirs ?

2ème Partie

Les risques internes

1. Enjeux et contexte
2. Objectifs de la Charte Informatique
3. Quel format choisir ?
4. Un contenu très large et adapté à chaque entreprise
5. Charte Informatique et CNIL
6. Charte Informatique : un outil indispensable ?

De nouveaux enjeux avec la généralisation des TIC dans les entreprises

* Usage des NTIC dans l'entreprise : une source de productivité, d'efficacité et d'innovation

* Usage des NTIC dans l'entreprise : une nouvelle source de risques avec du temps perdu et la possibilité accrue de se livrer à des activités illégales (Affaire Lucent/Escota 2006)

=> nécessité de trouver des parades pour les employeurs

De nouveaux risques pour l'entreprise

* De nombreux comportements sur internet sont passibles de sanctions civiles et pénales lourdes (utilisation de copies illicites, intrusion dans un système automatisé de données, dénigrement (Affaire Sté Giraud et Migot 2009), diffamation…)
* Ces comportements peuvent se dérouler à partir des postes de travail mis à la disposition des salariés
* Quid de la responsabilité de l'employeur ?

De nouveaux risques pour l'entreprise

* Principe général de responsabilité de l'employeur prévu par l'**article 1384 du Code Civil** :

  « On est responsable non seulement du dommage que l'on cause par son propre fait, mais encore de celui qui est causé par le fait des personnes dont on doit répondre… »

* De nouvelles responsabilités avec l'évolution de la législation : **loi HADOPI** qui introduit l'**article L336-3** dans le **Code de la Propriété Intellectuelle :**

  «La personne titulaire de l'accès à des services de communication au public en ligne a l'obligation de veiller à ce que cet accès ne fasse pas l'objet d'une utilisation à des fins de reproduction, de représentation, de mise à disposition ou de communication au public d'œuvres ou d'objets protégés par un droit d'auteur ou par un droit voisin sans l'autorisation des titulaires des droits prévus aux livres Ier et II lorsqu'elle est requise. »

⇔ notion de négligence caractérisée qui pèse sur l'employeur dès lors qu'il est le titulaire de l'accès

Le droit du travail

* Il reconnait certaines prérogatives à l'employeur : surveillance et contrôle des salariés sur leur lieu de travail pendant leur temps de travail
* Des prérogatives qui découlent du contrat de travail et du lien de subordination
* Des prérogatives qui permettent à l'entreprise de fixer les modalités d'utilisation des moyens fournis aux salariés, de mettre en place une surveillance et de contrôler et sanctionner les abus

Le respect de la vie privée des salariés

* Principe du respect de la vie privée des salariés qui atténue les prérogatives reconnues à l'employeur
* Droit à la vie privée du salarié défini dans le **Code Civil (art 9)**

  « Chacun a droit au respect de sa vie privée. »
* Principe initial complété par :
  * le respect des correspondances privées (**Loi 10.07.1991**), et
  * la sanction de l'interception des messages électroniques : **Loi du 18.12.2013 ⇔ art 226-15 du Code Pénal**

    « Le fait, commis de mauvaise foi, d'ouvrir, de supprimer, de retarder ou de détourner des correspondances arrivées ou non à destination et adressées à des tiers, ou d'en prendre frauduleusement connaissance, est puni d'un an d'emprisonnement et de 45 000 euros d'amende.

    Est puni des mêmes peines le fait, commis de mauvaise foi, d'intercepter, de détourner, d'utiliser ou de divulguer des correspondances émises, transmises ou reçues par la voie électronique ou de procéder à l'installation d'appareils de nature à permettre la réalisation de telles interceptions. »

Application de ces principes aux NTIC

* Présomption d'utilisation professionnelle pour tous les moyens informatiques mis à la disposition des salariés : concerne les fichiers créés, les connexions à internet, l'utilisation de disques durs, les messages électroniques… => droit de consultation de l'employeur
* Présomption renversée dès lors que les documents sont désignés « personnels » ou « privés » (Affaire Association Relais Jeunes Charpennes 2010)

Comment organiser la coexistence de ces principes parfois contradictoires ?

* Adoption d'une Charte Informatique qui :
  * permet d'encadrer l'utilisation des moyens de communication
  * permet d'encadrer l'utilisation du matériel informatique fourni par l'entreprise
  * permet d'informer les salariés sur les règles applicables dans l'entreprise (Affaire Helvetia 2012)
  * rappelle aux salariés que le non-respect des dispositions prévues engage leur responsabilité
  * règle le problème de la preuve

Les risques internes

1. Enjeux et contexte
2. Objectifs de la Charte Informatique
3. Quel format choisir ?
4. Un contenu très large et adapté à chaque entreprise
5. Charte Informatique et CNIL
6. Charte Informatique : un outil indispensable ?

Objectifs de la Charte Informatique

* Établir un cadre clair et transparent des règles d'utilisation de l'informatique et d'internet au sein de l'entreprise
* Sensibiliser les salariés aux risques inhérents à l'utilisation des ressources informatiques de l'entreprise
* Apporter la preuve que l'entreprise à mis en place des actions de prévention et d'information en cas d'infractions commises par un salarié
* Rappeler la possibilité de sanctions en cas de non-respect des principes d'utilisation établis

Les risques internes

1. Enjeux et contexte
2. Objectifs de la Charte Informatique
3. Quel format choisir ?
4. Un contenu très large et adapté à chaque entreprise
5. Charte Informatique et CNIL
6. Charte Informatique : un outil indispensable ?

Quel format choisir ?

* Simple note de service ou partie du règlement intérieur?
* Si la Charte comporte un volet disciplinaire elle doit être annexée ou intégrée dans le règlement intérieur
* 4 conditions à remplir pour qu'elle ait une force contraignante :
  1. Être soumise à l'avis du CE (ou à défaut des DP)
  2. Être communiquée aux salariés (affichage)
  3. Être déposée au greffe du Conseil de Prud'hommes
  4. Être communiquée à l'inspecteur du travail

Les risques internes

1. Enjeux et contexte
2. Objectifs de la Charte Informatique
3. Quel format choisir ?
4. Un contenu très large et adapté à chaque entreprise
5. Charte Informatique et CNIL
6. Charte Informatique : un outil indispensable ?

Quel contenu ?

1. Rappeler le cadre légal
2. Ne pas omettre les définitions
3. Indiquer les règles d'utilisation des ressources informatiques
4. Définir les droits accordés ou pas aux syndicats et instances représentatives du personnel (Affaire Generali 2009)
5. Mentionner les contrôles mis en place
6. Ne pas oublier d'indiquer la date d'entrée en vigueur ainsi que celle de présentation aux IRP et à l'inspecteur du travail

Rappel du cadre légal

* La Charte Informatique est avant tout un outil pédagogique
* Rappels à mentionner :
  - des interdictions légales à respecter ⇔
    * Téléchargement de contenus en violation des droits d'auteur
    * Diffamation
    * Dénigrements
    * Atteinte à l'ordre public ou à la dignité humaine…
  - l'obligation de loyauté du salarié ⇔
    * Atteinte aux intérêts de l'entreprise : réputation, confidentialité des données, SI…
  - la responsabilité personnelle du salarié peut être engagée

Règles d'utilisation des ressources informatiques

* Concerne matériel informatique, internet, réseau interne, messagerie
* Ressources mises à disposition destinées à un usage professionnel
* Mais impossible d'interdire aux salariés tout usage personnel de ces ressources informatiques => usage raisonnable + ne pas altérer le bon fonctionnement de l'entreprise
* Mesures adaptées aux impératifs de sécurité particuliers de l'entreprise (ex: Keyloggers)

Règles d'utilisation des ressources informatiques

Introduction de règles relatives :

* Aux comptes utilisateurs : identifiants et MDP, confidentialité
* Aux accès internet : restriction d'accès possible aux réseaux sociaux, forums, sites pornographiques (Affaire Peugeot Citroën 2009), sites de jeux d'argent…
* A l'installation de nouveaux périphériques (y compris clé USB, lecteurs de musique) ou nouveaux programmes

Contrôles mis en place

* Obligation d'informer les salariés :
  * Des finalités du contrôle
  * Des informations collectées
  * Des destinataires des informations collectées
  * Des durées de conservation des informations collectées
* Quels types de contrôles :
  * Internet : temps de connexion, sites visités…
  * Messagerie : nombre de messages reçus et envoyés, volume, fréquence, pièces jointes…
  * Contenus ?

Des contrôles pour quelles sanctions?

2 principes à respecter :

- Des sanctions conformes au code du travail
- Le respect du principe de proportionnalité

Les risques internes

1. Enjeux et contexte
2. Objectifs de la Charte Informatique
3. Quel format choisir ?
4. Un contenu très large et adapté à chaque entreprise
5. Charte Informatique et CNIL
6. Charte Informatique : un outil indispensable ?

Charte Informatique et CNIL

* Principe : Déclaration CNIL indispensable dès lors qu'il y a « traitement automatisé d'informations nominatives »
* Exception : présence d'un CIL
* Déclaration CNIL : simplifiée ou normale ?
* Sanctions pénales : emprisonnement 5 ans + 300K€ d'amende
* Sanction sociale : les preuves collectées ne peuvent pas être produites en justice

Les risques internes

1. Enjeux et contexte
2. Objectifs de la Charte Informatique
3. Quel format choisir ?
4. Un contenu très large et adapté à chaque entreprise
5. Charte Informatique et CNIL
6. Charte Informatique : un outil indispensable ?

La Charte : un outil indispensable?

OUI car elle :

* Définit les règles relatives à l'utilisation des nouvelles technologies
* Encadre leur usage
* Réduit les abus
* Informe les salariés sur les moyens de surveillance
* Permet d'assurer la sécurité du réseau informatique de l'entreprise
* Permet de sanctionner les éventuels abus

MAIS…

La Charte : un outil indispensable?

MAIS

* Elle doit respecter le principe de proportionnalité qui permet de concilier l'intérêt de l'entreprise et celui du salarié
* En mettant en place des mesures justifiées et proportionnées au but poursuivi

Le contrôle est possible s'il reste loyal, transparent et proportionné!

valerie.parot@sfr.fr

Valérie **Parot**
AVOCAT

04 56 09 99 40
06 07 79 94 10

49, Cours Mirabeau
13100 Aix en Provence

S.D.I.

TELECOMS - INFORMATIQUE - CLOUD