2008

Protection de l'information

Enjeux, gouvernance et bonnes pratiques

CIGREF

« Promouvoir l'usage des systèmes d'information comme facteur de création de valeur et source d'innovation pour l'entreprise »

Publications CIGREF 2007-2008

Pilotage de la stratégie SI
Quelques bonnes pratiques d'exécution du plan stratégique SI

Open source

Web 2.0 en entreprise

Le SI de la DSI
Permettre à la fonction SI d'opérer efficacement son cœur de métier

L'Architecture d'Entreprise
Un cadre global de coopération pour les acteurs de l'entreprise

Les dossiers du Club Achats
Synthèse des activités 2008

Poste de travail
Perspectives d'évolution

Protection de l'information
Enjeux, gouvernance et bonnes pratiques

Dynamique des relations entre les grandes entreprises et les PME innovantes
Recommandations du Cercle Innovation destinées à aider la DSI à se structurer pour favoriser l'innovation

Cahier de Recherche : Capital immatériel et systèmes d'information
Premières explorations théoriques

Ressources humaines
Facteurs d'évolution des métiers de la DSI : mesure de leur impact

Contrôle interne et systèmes d'information (en partenariat avec l'IFACI)
Guide opérationnel d'application du cadre de référence AMF relatif au contrôle interne

Dynamique de création de valeur par les SI (en partenariat avec McKinsey)
Une responsabilité partagée

Télécoms et infrastructures (en partenariat avec l'EVUA)
Perspectives d'évolution

Usage des TIC et RSE (en partenariat avec l'ORSE et l'ESCEM)
Comprendre l'impact de l'usage des TIC sur la responsabilité sociale de l'entreprise

Immatériel et innovation dans les services (en partenariat avec l'AFOPE et le MEDEF)
Bonnes pratiques

Le groupe de travail a été piloté par Jean-Pierre Gagnepain, DSI d'Air Liquide. Nous tenons à remercier toutes les personnes qui ont participé aux travaux du groupe :

- Alain Bouillé, Groupe CDC
- Philippe Colman, Sanofi-aventis
- Olivier Daloy, LVMH
- Renaud de la Porte des Vaux, France Telecom
- Alain Delboy, Air Liquide
- Jérome Galerne, Auchan
- Emmanuel Garnier, Systalians
- Gaelle Gissot, GMF
- François Gratiolet, La Poste
- Eric Grospeiller, ANPE
- Philippe Hollinger, Arkema
- Michel Jumel, Yves Rocher
- Christophe Le Caignec, Groupe Invivo
- Jean-François Montagne, EDF
- Guy Nicolas, Nexans
- Christophe Olivier, Canal +
- Alain Perraud, Renault
- Bernardo Ramos, Arkema
- Bernard Saint-Jours, SI2M
- Pascal Wagner, Nexter Group

L'étude a été rédigée par Stéphane Rouhier, Chargé de mission au CIGREF.

Table des illustrations

1. Contexte

Dans le cadre de ses groupes d'échanges de pratiques, le CIGREF a retenu un axe de travail autour de la protection de l'information, en termes d'usages des systèmes d'information. Le pilotage de ce groupe de travail a été assuré par Jean-Pierre Gagnepain, DSI d'Air Liquide.

Le CIGREF s'est intéressé cette année à ce thème car l'information est au cœur des actifs immatériels de l'entreprise. Et trop souvent le discours ambiant porte sur les aspects techniques et contenant de la sécurité au détriment de ses aspects organisationnels et contenu.

Il convient de définir au préalable ce que l'on entend par protection de l'information. En effet la protection de l'information, ce n'est pas seulement la confidentialité ou la valorisation de l'information.

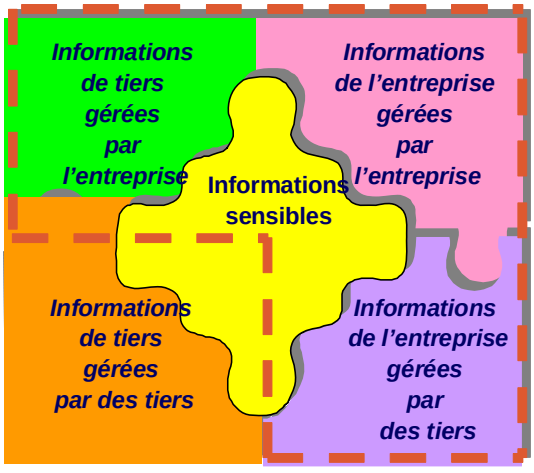
Le groupe de travail s'est intéressé au terme de protection de l'information

Définition

La protection de l'information est une démarche consciente visant à protéger, au sein de l'entreprise étendue, ce qui vaut la peine d'être protégé, tant au niveau des données que des supports d'information. Cette démarche implique un système de gestion, une identification des informations sensibles, une analyse de risques, des acteurs, avec des rôles et responsabilités et un programme de réduction des risques.

Le schéma ci-dessous définit le périmètre de l'information sensible pour une entreprise, à savoir les informations de tiers gérées par l'entreprise, les informations de l'entreprise gérées par l'entreprise et les informations de l'entreprise gérées par des tiers.

Figure 1 : Périmètre de l'information sensible



Source : CIGREF

En effet, la collecte, la valorisation et la diffusion de l'information tant interne qu'externe constituent un élément clé de la compétitivité des entreprises. Les entreprises doivent également chercher à limiter au maximum le risque de diffusion d'informations confidentielles, que cette diffusion soit volontaire ou accidentelle.

Par ailleurs, les entreprises sont de plus en plus confrontées à des exigences légales en matière de conservation de données (données personnelles, données financières, archivage légal…) à des fins de conformités ou de contrôle, ou à valeur probante.

L'ensemble de ces tendances pose, de manière sous-jacente, la question de la protection de l'information.

Confidentielle, ou ouverte, structurée ou non, maîtrisée ou libre, l'information est un actif qu'il convient de protéger techniquement, juridiquement, humainement. On entend par actif, tout ce qui a de la valeur pour l'entreprise.

Ce document vise l'ensemble des personnes concernées et en charge de la protection de l'information : dirigeants, responsables métiers, responsables sécurité, responsable intelligence économique, documentalistes, salariés.

2. Objectifs poursuivis

Les objectifs du groupe de travail ont été les suivants :

- Identifier et caractériser les enjeux liés à la protection de l'information en entreprise ;
- Comprendre les modèles d'organisation, les acteurs, les méthodes et les démarches ;
- Mieux positionner la démarche de protection de l'information au sein de l'entreprise en adoptant une approche de type gouvernance (rôles et acteurs) et en nouant un dialogue stratégique avec les métiers (implication, sensibilisation, responsabilisation, appropriation) ;
- Identifier des bonnes pratiques fortes et lister les précautions minimales à prendre ou à préparer ;
- Avoir une approche équilibrée entre les enjeux majeurs et les pratiques.

La littérature sur la protection de l'information est ancienne, riche et abondante. La démarche suivie par le groupe de travail n'a pas été de réinventer la matière mais plutôt de la simplifier, d'avoir une approche transversale, en mettant l'accent sur la démarche, la sensibilisation et les bonnes pratiques.

Ce groupe de travail a cherché également à capturer les retours d'expérience les plus pertinents et à l'intérieur de ceux-ci, les « invariants », les éléments communs aux entreprises, notamment sur les aspects gouvernance, classification de l'information et sensibilisation.

Ce groupe de travail n'a pas cherché à être exhaustif mais plutôt à être pertinent, en fournissant des éléments à la fois descriptifs (les modèles d'organisation) et prescriptifs (les bonnes pratiques).

Le rapport s'est intéressé aux thèmes suivants :

- Les enjeux, les risques et les grands axes ;
- La démarche, l'organisation et la gouvernance ;
- La sensibilisation et l'implication des acteurs ;
- Les bonnes pratiques.

Ce qui parait critique (et perfectible) aujourd'hui dans une entreprise c'est :

1) de prendre conscience de ses enjeux et de ses risques ;
2) de mettre en place une démarche de gouvernance structurée et cohérente ;
3) de sensibiliser l'ensemble des acteurs et de promouvoir une culture de protection de l'information,
4) de conduire des actions concrètes et sélectives de réduction des risques.

3. Les enjeux, les risques, les grands axes

3.1. Les enjeux de la protection de l'information

L'information est aujourd'hui unanimement considérée comme un actif stratégique pour l'entreprise. En même temps, il s'agit d'un actif intangible, dont la valeur est difficilement mesurable et dont la prise de conscience pourrait être amplifiée chez les dirigeants.

On se retrouve donc face à un paradoxe dans lequel l'accès à l'information est jugé stratégique alors que sa protection est jugée non prioritaire.

Longtemps on a considéré que la démarche de protection de l'information « papier » était suffisante, que le fait de ne pas faire transiter d'information sensible par des moyens électroniques, voire de chiffrer ponctuellement les documents électroniques ou les transmissions, était suffisant. Or il n'en est rien.

Il existe en effet un certain nombre de tendances de fond et de ruptures d'ordre économique, réglementaire et sociologique, qui

obligent à repenser de façon plus globale la protection de l'information.

Parmi les évolutions internes on peut citer les tendances suivantes :

- *L'explosion des services dématérialisés et des volumes d'information* (structurée mais surtout non structurée) circulant dans les entreprises et sur Internet. Cette volumétrie croissante des contenus oblige à repenser et à industrialiser la démarche de protection de l'information ;
- *L'environnement décentralisé des entreprises et l'hétérogénéité des niveaux de « sécurité » interne* qui peuvent justifier la mise en place d'un référentiel de protection de l'information.

Parmi les évolutions externes on peut mentionner :

- La tendance à la *convergence des usages domestiques et professionnels des SI.* Wifi, messageries instantanées, réseaux sociaux, blogs, wikis…sont d'utilisations courantes dans la sphère privée mais souvent incompatibles avec les usages et les besoins dans l'entreprise. Ceci oblige à revoir les règles d'usages des SI (chartes) mais aussi à redéfinir plus précisément la valeur de ces systèmes d'information pour l'entreprise ;
- *L'émergence de l'entreprise étendue*, impliquant un changement des modèles d'affaire, des relations avec les clients, les partenaires, les fournisseurs, les salariés et conduisant à étendre le périmètre de protection de l'information au-delà des frontières traditionnelles de l'entreprise ;
- *L'exigence de transparence et de reporting* accru avec un renforcement des contraintes légales, réglementaires, contractuelles. Cette tendance conduit d'un côté à publier davantage d'informations mais d'un autre côté à contrôler en amont beaucoup plus finement leur origine, et véracité et en aval les destinataires de l'information ;
- *La complexité et l'interaction croissante avec l'environnement*, ce qui se traduit par exemple par une d*iversification et une dangerosité croissante des menaces,* obligeant les entreprises à repenser leur politique de protection de l'information et à se préparer au changement.

3.2. Les risques en entreprise

Les évolutions internes et externes examinées ci-dessus sont porteuses de nouveaux risques.

Afin d'avoir une approche globale, efficace et cohérente, il est nécessaire d'identifier et d'intégrer les risques en amont de la démarche de protection de l'information.

Les entreprises sont confrontées à des risques variés, complexes et croissants. Le CIGREF a déjà abordé la gestion des risques et la place du DSI dans la démarche dans un précédent rapport[1].

L'objectif ici n'est pas de refaire une nouvelle étude sur le sujet, mais plutôt de voir en quoi les risques impliquent d'avoir une démarche de protection de l'information. Cette démarche de protection doit s'inscrire en complément d'une politique de gestion des risques.

On distingue généralement plusieurs types de risques : les risques financiers, opérationnels, de conformité et d'atteinte à l'image.

Les risques liés aux usages IT font partie des risques opérationnels. On peut classer les risques liés aux usages IT de différentes façons, par exemple :

- Les risques informationnels ;
- Les risques liés aux applications ;
- Les risques liés aux développements ;
- Les risques liés à la maintenance ;
- Les risques liés aux infrastructures, serveurs ;
- Les risques liés aux projets ;
- Les risques liés aux fournisseurs.

Les critères pris en considération pour l'analyse des risques IT sont classiques :

- Disponibilité ;
- Intégrité ;
- Confidentialité ;
- Continuité ;
- Preuve / Traçabilité / Auditabilité.

Ce que l'on peut dire des risques aujourd'hui en entreprise, c'est qu'il est indispensable de répertorier ces risques, de les hiérarchiser, de les relier à des processus, et de mettre en place un modèle de gouvernance approprié afin de les gérer tant d'un point de vue performance financière, conformité, continuité, image et protection de l'information…

[1] Cf. le rapport « Analyse et gestion des risques dans les grandes entreprises » – 2007 – www.cigref.fr

Il est nécessaire d'avoir une démarche consciente et explicite d'évaluation et de traitement des risques.

Il faut ensuite inscrire cette démarche dans une politique de protection de l'information.

Aujourd'hui c'est l'expression des besoins qui est difficile : que protéger et à quel niveau ?

Une démarche pragmatique, et progressive de cartographie des risques est un prérequis, à la fois à une démarche de gestion des risques, mais aussi à une démarche performante de protection de l'information.

3.3. Les principales mesures de réduction des risques

Le tableau ci-dessous présente les différentes mesures de réduction des risques liés à l'information :

Figure 2 : Exemples de mesures de réduction des risques

Risques majeurs encourus	Causes	Exemples de mesures de réduction du risque
Risque de perte, fuite ou de vol de données stratégiques de l'entreprise **Impacts multiples : perte d'image, perte financières, ...** **Exemples de documents concernés : Données stratégiques d'entreprise : plans stratégiques, grille de tarification, rapports d'audit, ...**	• Vol ou perte physique d'ordinateurs portables, téléphones communiquants, agendas électroniques, etc. • Intrusion externe sur le SI • Mauvaise gestion des habilitations • Accès non autorisé par les administrateurs informatiques • Envoi par des moyens autorisés par l'entreprise (messagerie électronique, etc.) • Mauvaise classification du document • Duplication de l'information à des endroits différents du SI • Etc.	Mesures techniques ▪ **Utilisation de protocoles de communication réseaux et/ou applicatifs sécurisés (SSL, IPSec, etc.) dans les échanges électroniques** ▪ **Mise en œuvre d'une solution de chiffrement du disque dur et authentification forte au poste de travail (biométrie)** ▪ **Contrôle de l'usage des périphériques sur l'ordinateur portable** ▪ **Solution de « Data Loss Prevention »** ▪ **Contrôle d'accès aux données stockées avec authentification forte et gestion des habilitations** ▪ **Mise à disposition d'une clé USB « sécurisée » (authentification forte avec chiffrement des données).** Mesures organisationnelles et juridiques ▪ **Politique de protection de l'information, PSSI, charte d'utilisation SI** ▪ **Gestion de la sécurité avec les Tiers, etc.** ▪ **Sensibilisation / éducation / formation**

Source : La Poste / CIGREF

3.4. Les objectifs d'une politique de protection de l'information

Les objectifs que l'on peut assigner à une politique de protection de l'information peuvent être les suivants :

- Protéger les actifs immatériels de l'entreprise ;
- Définir les orientations générales et les priorités ;
- Développer, mettre en œuvre et maintenir un référentiel de protection de l'information (politiques, rôles et responsabilités, processus, normes) ;
- Sensibiliser et éduquer le management/les employés à tous les niveaux ;
- Identifier et traiter les faiblesses prioritaires ;
- Assurer la conformité et contrôler.

4. La démarche de gouvernance

Chaque entreprise a son type d'organisation, sa culture, son modèle de gouvernance et ses modes de gestion de projet. On peut néanmoins recenser quelques principes forts et universels en matière de démarche de gouvernance, tant au niveau des étapes, que des acteurs et des responsabilités. La gouvernance, autrement dit la définition des rôles et des responsabilités des acteurs, est un point clé dans la réussite d'une démarche de protection de l'information.

4.1. Les axes structurants – le fil conducteur

La démarche de protection de l'information peut se décliner de la façon suivante :

- S'appuyer sur la vision et la volonté politique et stratégique de la direction ;
- Avoir une approche globale et raisonnée (expression de besoin assise sur une analyse de risques) ;

- Avoir une démarche inscrite dans la durée (une protection durable) ;
- Axer la démarche selon trois axes :
  - Les hommes (comportements, sensibilisation, …) ;
  - Les processus (la finalité métier, intégrer la démarche de Protection de l'Information dans les processus métiers) ;
  - Les règles et les outils (pour automatiser)
- Avoir une démarche cohérente selon ces trois axes (autrement dit progresser de la même façon sur l'axe organisationnel, l'axe humain et l'axe outils) ;
- Avoir une démarche d'amélioration continue
- Ne pas chercher l'exhaustivité ni la complétude ;
- Disposer d'une politique de sécurité et d'une politique de gestion des risques structurée et explicite ;
- S'appuyer sur la maturité de l'entreprise et sur une culture partagée de ce que constitue le « patrimoine informationnel » de l'entreprise ;
- S'appuyer sur la démarche de cartographie des risques ;
- Capitaliser sur d'éventuels incidents pour ancrer la démarche.

4.2. Sept étapes

La démarche peut suivre les étapes suivantes :

1. Faire un audit, état des lieux ;
2. Définir le modèle d'organisation, les acteurs, les rôles, les responsabilités. Mettre en place un comité de pilotage transverse qui oriente, valide et supporte les actions ;
3. Définir les grandes orientations, priorités et objectifs (créer l'attention sur le sujet et engager le management) ;

4. Élaborer, mettre en place et maintenir le référentiel de protection de l'information (charte utilisateurs et administrateurs des SI, politique groupe, politique particulière de sécurité de l'information) ;
5. Sensibiliser et responsabiliser le management et les employés (sessions d'information et communication) ;
6. Identifier et assurer le traitement des sujets prioritaires (mise en place d'une cellule de gestion des vulnérabilités et des incidents, protection des communications écrites et orales, protection anti-virus, sécurité des réseaux, gestion des accès, gestion de l'information) ;
7. Evaluer et contrôler (intégration dans le programme d'audit et démarche de tests et évaluation).

La définition des objectifs peut se faire par rapport à des règles groupes :

- La protection de l'information est de la responsabilité des métiers (*business) ;*

- La protection de l'information suppose un responsable par entité ;

- La protection de l'information repose sur des outils et des processus.

Il faut aussi prendre en compte dans la démarche des données-clés telles que le volume d'information ou le facteur temps.

A propos du volume d'information par exemple : il faut faire attention à ne pas perdre de vue l'essentiel : les entreprise ont des téraoctets de données dans lesquelles seulement 1% des informations sont à protéger (et parfois seulement pendant un certain laps de temps).

La question clé est : quel est l'actif sensible par métier et à quel moment ? Pour les brevets par exemple, la phase critique a lieu avant le dépôt du brevet à l'INPI (Institut national de la Propriété Industrielle) ou l'OEB (Office Européen des Brevets). Autre exemple, pour les résultats financiers, la phase critique a lieu avant la communication publique de ceux-ci.

Il est, par conséquent, nécessaire de définir et mettre en œuvre une politique de protection adaptée à la nature des informations et à leur cycle de vie, par exemple :

- classification / marquage des documents selon leur criticité et leur nature ;
- chiffrement fort des contenus / déchiffrement transparent pour l'utilisateur ;
- conservation à valeur probante dans le temps.

De manière générale, la démarche de progrès doit se faire de manière sélective, graduelle, permanente et selon plusieurs axes.

Un axe descendant/organisationnel (*top-down*) visant à responsabiliser l'ensemble des acteurs autour des enjeux et sur la base de règles communes auditables.

Un axe montant/opérationnel (*bottom-up*), visant à renforcer la sécurité technique de façon concrète, visible et cohérente (chiffrement, classification de l'information…).

Un axe transverse, visant à favoriser la diffusion des bonnes pratiques entre départements.

Dans une démarche de protection de l'information, il ne faut pas hésiter à s'inspirer des référentiels existants, notamment le référentiel ISO 27002 et des documents issus par exemple de *l'Information Security Forum*.

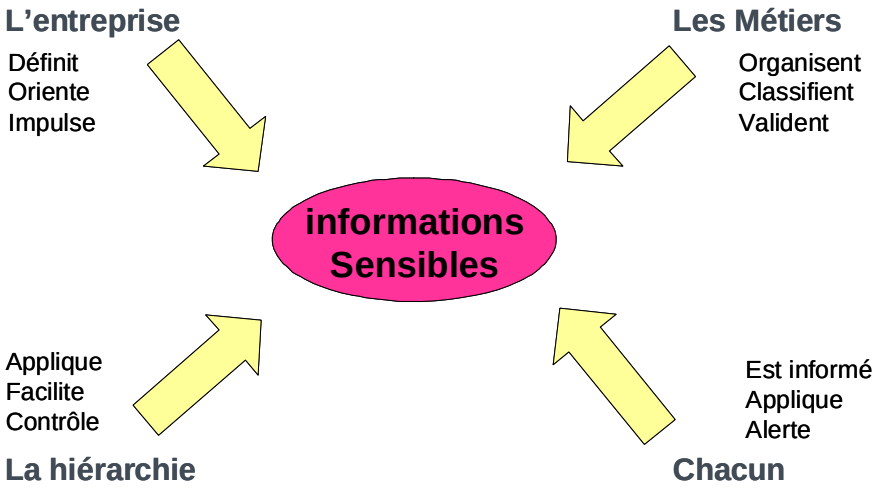
4.3. Quatre acteurs

La protection de l'information doit s'inscrire dans une démarche organisée, transversale, collaborative et dynamique.

Quatre acteurs principaux interviennent dans la protection de l'information :

- l'entreprise qui fixe les règles et met à disposition des solutions standard de protection et les consignes associées ;
- les métiers qui identifient les informations sensibles à protéger ;
- la hiérarchie qui contrôle la bonne application des règles dans son périmètre de responsabilité ;
- et chacun, qui connait le niveau de sensibilité des informations qu'il détient et les règles et procédures à appliquer.

Figure 3 : les quatre acteurs principaux de la démarche de protection



Source : Renault / CIGREF

Les fonctions RH, juridique, audit, services généraux, sont des co-acteurs importants qu'il faut impliquer complètement dans la démarche.

Ces parties prenantes peuvent aider au développement d'une démarche de protection de l'information. Par exemple :

- la direction juridique pour les chartes, les contrats, les clauses ;
- la DRH pour les chartes, les contrats de travail et la formation

- l'audit pour le contrôle interne ;
- les moyens généraux pour les outils tels que les destructeurs de documents, le papier non photocopiable, … ;
- la sécurité physique pour les contrôles d'accès aux bâtiments ;
- etc.

Il est essentiel d'intégrer pleinement la protection de l'information dans les relations d'affaires avec des tiers, notamment :

- l'intégration de mesures de sécurité dans tous les services sous-traités à des tiers ;
- la protection des échanges d'information avec les tiers ;
- la protection de l'accès à des informations appartenant à l'entreprise par des tiers. En effet, certaines collaborations peuvent nécessiter l'ouverture des SI et doivent entraîner une gestion rigoureuse des accès aux Systèmes d'Information de l'entreprise.

La démarche doit être supportée et impulsée par la Direction Générale. La démarche doit ensuite se construire en instaurant le dialogue en interne entre la DSI, les métiers et les fonctions supports. En amont, il faut impliquer les comités et fédérer les acteurs. L'idée est d'avoir une approche transversale, durable et cohérente par la mise en place d'un cadre de référence commun et partagé.

Pour cela une bonne pratique peut être de traiter la protection de l'information comme partie intégrante des processus métiers.

4.4. Les bonnes pratiques en matière de gouvernance

A titre de recommandations, parmi les bonnes pratiques, on peut suggérer les points suivants

- Avoir une politique de management de l'information basée sur un nombre limité et connu de principes ;
- Avoir une approche déclinée au niveau groupe et filiales ;
- Mettre en place au niveau des filiales, des « responsables protection de l'information » correspondants locaux métiers

responsables et propriétaires de l'information métiers (business owner), quand la taille de l'entreprise et des filiales le permet ;
- Faire tenir au DSI groupe le rôle de *business owner* au niveau des infrastructures du SI (conception, développement…) et d'accompagnateur global de la démarche ;
- Mettre en place des comités de pilotage au niveau groupe et local ;
- Faire inscrire la protection de l'information dans les « procédures groupe » obligatoires ;
- Déployer des kits de communication pour les collaborateurs.

La protection de l'information est un enjeu d'entreprise qui requiert l'engagement de la Direction Générale et du management :
- L'appropriation par les Directions opérationnelles est essentielle ;
- La politique de protection de l'information est un programme de changement qui doit s'inscrire dans la durée ;
- La dimension organisationnelle et humaine (éducation, comportements) est prépondérante.

La stratégie gagnante est de crédibiliser les actions de fond avec des résultats court-terme (*« quick win »)*, de rester pragmatique et d'apporter des solutions.

Une autre recommandation que l'on peut faire, est de lier technologies, processus et règles métiers, autrement dit, ne pas traiter la protection de l'information comme un sujet à part et ne pas avoir de solution technique sans règles *business* associées,

Enfin une dernière recommandation porte sur la communication : il faut communiquer, communiquer, encore et toujours ...

Au final la protection de l'information doit être vue comme une partie intégrante de l'activité métier et donc donner lieu à un dialogue permanent avec le business.

4.5. Les bonnes pratiques juridiques

- Impliquer le juridique dans la démarche, dans la définition, la mise en œuvre et le contrôle ;
- La démarche de protection peut se faire en synergie avec la diffusion de chartes d'usages des ressources SI ;
- Prévoir des clauses d'audit dans les contrats avec les fournisseurs et les prestataires ;
- Prévoir les moyens de traçabilité et de conservation des preuves (en cas d'action judiciaire) ;

- Associer le Correspondant Informatique et Libertés (CIL) le cas échéant (quand il est nommé) dans la démarche de protection de l'information et vérifier qu'elle est compatible avec la réglementation en vigueur (notamment la durée de conservation des données).

4.6. Les bonnes pratiques RH

- Impliquer les RH dans la démarche, dans la définition, la mise en œuvre et le contrôle ;
- S'assurer de la définition et du respect des engagements de confidentialité sur les postes clés ;
- Instiller la sensibilisation sécurité dans les fonctions et dans la démarche qualité ;
- Intégrer la sensibilisation à la protection de l'information dans l'évaluation, dans le Droit Individuel à la Formation (DIF) et dans l'intéressement ;
- Utiliser le *e-learning* (sans forcément commencer par la sécurité).

5. La démarche de classification de l'information, un élément clé de la protection de l'information

5.1. Une démarche essentielle mais complexe et risquée

La démarche de classification de l'information constitue la pierre angulaire mais aussi le point faible de la politique de protection du patrimoine informationnel de l'entreprise..

C'est une démarche complexe et risquée : complexe car il faut bien définir le périmètre et les actifs que l'on veut protéger, risquée car il ne faut pas s'engluer dans la méthode au point d'en oublier la finalité : protéger les informations essentielles et critiques pour l'entreprise.

Il faut raisonner par grandes masses et s'intéresser à l'aspect physique des données. La démarche de classification doit prendre en compte les contraintes technologiques en raisonnant de manière préférentielle sur des composants physiques car à un niveau plus fin, les données qu'elles soient critiques ou pas sont imbriquées dans des ensembles techniquement indissociables (SGBD).

La démarche existe depuis de nombreuses années dans certains secteurs (aéronautique, défense, banques…) ou au sein de certaines fonctions (direction de la sûreté) afin d'assurer la protection physique ou logique des informations.

La démarche de protection de l'information écrite existe déjà depuis de nombreuses années dans les entreprises. Ce qui est nouveau en revanche, c'est la transposition des règles écrites et orales de l'analogique dans le monde numérique. La maturité des entreprises est moins forte dans ce domaine. Un travail de fond sur les règles comportementales doit aider à progresser dans la démarche.

5.2. Retour terrain : une démarche interne vers les métiers et une démarche externe vers les fournisseurs

Ce cas concerne une entreprise membre du CIGREF qui a mené une démarche interne de protection de l'information vers les métiers ainsi qu'une démarche externe vers les fournisseurs

5.2.1. La démarche vers les métiers

A l'origine, le système de classification a été conçu fin des années 90, pour accompagner un projet informatique très spécifique et unique : le passage à l'an 2000. La méthode, conçue par des experts pour des experts, avait pour objectif de classifier selon leur criticité : les applications informatiques, les ressources techniques et processus métier associés ainsi que les flux inter-applicatifs.

Cette méthodologie, basée sur 7 échelles à 5 niveaux d'expression de besoin fonctionnel de sécurité, a permis d'identifier les applications stratégiques de l'entreprise et leurs applications connexes, soit environ 300 dans un parc applicatif de plus de 2000 applications. Cette méthode a également permis de simplifier les démarches de sécurisation en proposant pour chaque niveau des échelles de sécurité, une solution de sécurité standard « disponible sur étagère ». Coté mise en œuvre, sur une échelle allant de 0 à 4, le niveau standard a été positionné à 2. Le choix de baisser ou d'augmenter le niveau de sécurité relève d'une décision justifiée par une analyse de risques. Cette méthode est encore aujourd'hui utilisée pour classifier les applications informatiques.

Sur la base de ces résultats, au début des années 2000, il a été décidé de déployer de manière plus large cette méthodologie en l'appliquant à l'ensemble des informations quelle que soit leur forme : numérique, document papier, orale, prototype, …. Ce fut globalement un échec, pour deux raisons. La première raison est que la majorité des utilisateurs impliqués se sont avérés incapables de la mettre en œuvre sans l'assistance d'un expert sécurité, pour leur expliquer les principes de sécurité sous-tendus par les échelles. La deuxième raison est que la démarche étant une démarche terrain (*bottom-up*), une même information peut être classifiée de manière différente suivant la sensibilité du secteur concerné, à l'origine d'incohérence en matière de protection des informations.

L'entreprise a donc décidé en 2007 de faire un état des lieux des pratiques en organisant un benchmark avec un large panel d'organismes : des entreprises françaises et étrangères, à rayonnement national et international, des administrations, des banques, …

5 enseignements principaux selon les sociétés se sont dégagés :

- Dans tous les cas, une démarche de classification formalisée est nécessaire ;
- Un mode de classification simple selon trois niveaux. Pour des besoins internes à l'informatique, elle peut être combinée à 3 critères complémentaires (*Disponibilité, Intégrité, Confidentialité) ;*

- Deux approches en termes de responsabilité de la classification :
  - Par le créateur / rédacteur de l'information (non homogénéité des résultats) ;
  - Par les métiers ou instance transverse avec publication d'un catalogue des informations sensibles ;

- Deux processus de déploiement :
  - Par le haut, avec implication de l'ensemble des managers (intégration dans les objectifs) ;
  - Par le bas, avec formation et sensibilisation directe des opérationnels ;
- Processus de contrôle envisagés :
  - Sans : de la responsabilité des acteurs ;
  - Contrôle/reporting interne dans chaque métier, puis au niveau d'une organisation centrale.

Finalement l'entreprise a opté pour la démarche suivante :

- Classification simple et unique pour tous : 1 seul critère, 3 niveaux
  - **Niveau A, qualifié stratégique :**

    L'information est réservée aux personnes nommément désignées qui en ont besoin pour agir. Sa divulgation ou son altération peut entraîner des préjudices irréparables ou dont l'impact sera visible au niveau des résultats du groupe.
  - **Niveau B, qualifié critique :**

    L'information est réservée aux personnes, entités ou partenaires qui en ont besoin pour agir. Sa divulgation ou son altération peut entraîner des préjudices importants mais réparables.
  - **Niveau C, qualifié sensible :**

    L'information est accessible au personnel du groupe et aux partenaires autorisés. Sa divulgation ou son altération n'entraîne qu'une gêne au fonctionnement normal de l'entreprise, sans conséquence durable.
- Démarche impulsée par le haut, avec une Politique formalisée ;
- Des instances Métier qui dressent la liste des 20% d'information stratégique ou critique ;

- Une instance centrale qui coordonne la transversalité du déploiement et du fonctionnement du système ;
- Mobilisation via les objectifs personnels ;
- Contrôles forts.

Pour déployer cette démarche dans l'ensemble de l'entreprise, un programme « maîtrise de l'information » est en cours de mise en place. Ses principaux objectifs sont :

- D'ici à mi-2009, actualiser et compléter les normes et procédures existantes en matière de protection de l'information ;
- Organiser un plan de communication d'entreprise ;
- Mettre en place la structure de pilotage impliquant le management (un comité de pilotage par direction) ;

- Inscrire la démarche dans le cadre de la norme ISO 27001, en visant une certification pour les informations les plus critiques (première certification avant fin 2009).

5.2.2. La gestion des fournisseurs & partenaires

Le modèle de l'entreprise évolue, aujourd'hui on parle d'entreprise étendue aux fournisseurs et partenaires. Cette évolution rend plus complexe **la protection des informations dont la sécurité est de plus en plus mise entre les mains des fournisseurs et partenaires.** L'évolution des systèmes d'information et leur imbrication complexifient encore cette situation en imposant l'ouverture de ceux-ci à nos partenaires. Garder ses informations stratégiques uniquement au sein de son entreprise fait aujourd'hui partie du passé, la manière de gérer la sécurité doit évoluer pour s'adapter à ce nouveau contexte, en y intégrant la nécessité de délocaliser, y compris dans des pays qui ne partagent pas toujours les mêmes objectifs…

Pour ce faire, **l'entreprise a mis en place un PAS (Plan Assurance Sûreté),** qui reprend les principes du Plan d'Assurance Qualité qui ont fait la preuve de leur efficacité. L'objectif de ce PAS est de standardiser le modèle type de gouvernance et d'avoir une structuration du dialogue, en indiquant aux fournisseurs et partenaires ce que l'on attend d'eux, et en leur demandant de s'engager formellement sur les moyens mis en œuvre pour répondre aux exigences et les éventuels risques résiduels. L'ensemble de cette démarche est conjointement animée par la sécurité et le métier concerné qui valident le PAS. Cette démarche est aujourd'hui mise en œuvre pour tous les nouveaux contrats manipulant des informations sensibles. Le PAS est un document contractuel. Cette démarche est également mise en œuvre pour des contrats en cours, mais de manière informelle, en accord ou voire à la demande des fournisseurs et partenaires qui y voient un intérêt certain.

Le plan type comprend les points suivants : objet, formalisation des exigences, structure de gouvernance de la sécurité, mesures de sûreté mises en place par le partenaire ou fournisseur, correspondance entre les exigences du client et les mesures mises en œuvre, risques résiduels non couverts

Il y a autant de PAS que de fournisseurs. En général, c'est le fournisseur, qui le rédige, selon les exigences de l'entreprise. Des comités de pilotage et des tableaux de bord sont mis en place pour le suivi.

Finalement la méthode à suivre, en interne comme en externe, peut se résumer en trois mots : Responsabilisation, Confiance et Contrôle.

5.3. Les bonnes pratiques managériales et organisationnelles

De manière plus générale, les membres du groupe d'activité ont listé un certain nombre de bonnes pratiques en matière de classification de l'information.

5.3.1. Les bonnes pratiques en matière de management et de méthodes

- Faire impulser la démarche par la DG & impliquer les métiers ;
- Assurer une séparation des tâches (segregation of duties) ;
- Intégrer la démarche de classification de l'information dans les projets métiers
- Auditer (audit de risque, de conformité)

5.3.2. Les bonnes pratiques autour des projets

- Transposer au virtuel les règles de protection de l'information papier (cycle de vie, classement, archivage, destruction, …) ;
- Adopter une échelle simple de classification ;
- Etre sélectif : ne pas classifier toute l'information (règle des 80/20) ;
- Faire appliquer la démarche de protection de l'information aux fournisseurs, partenaires, voire clients (ex : en B2B) de l'entreprise ;
- Etre réaliste dans la séparation des tâches : dans les petites entités, la séparation des activités opérationnelles et de contrôle n'est pas évidente ;
- Auditer régulièrement.

6. La sensibilisation, la communication et l'implication des acteurs

La démarche de sensibilisation doit être orientée vers trois cibles

- Management
- Utilisateurs finaux
- Equipes informatiques

Là encore il n'y a pas de règle universelle, ni générique mais il y a tout de même quelques fondamentaux à respecter.

6.1. La démarche de sensibilisation vers le management

La démarche de sensibilisation et de communication vers le management est la plus importante et la plus délicate aussi. Elle vise à faire prendre conscience et s'approprier par les décideurs les enjeux de la protection de l'information.

Elle doit porter sur les bons messages, la bonne fréquence et intervenir tout au long du processus, tant en amont de la démarche, qu'en aval.

Sur la forme, là encore, il est recommandé d'avoir une approche différenciée selon les populations (Stratégique - DG, Tactique – Area Management, Opérationnel, …).

L'approche variera aussi selon les modèles d'organisation de l'entreprise (centralisée, fédération).

Sur le fond, il faut sélectionner les messages clés parlant métier, se focaliser, éviter les banalités, les généralités, ne pas nécessairement parler de coûts, …être simple, précis, concret.

Il est recommandé de cartographier, d'identifier et d'associer les contributeurs externes (les consultants, les commissaires aux comptes) de se référer aux actualités -ex : le cadre de référence produit par l'Autorité des Marchés Financiers-…), d'associer également les contributeurs internes (département risque, audit interne, RH, juridique). Combiner un partenaire externe, un relais interne et la communication, constitue souvent une démarche efficace.

Les messages et axes de communication peuvent porter par exemple sur les points suivants :

- sécurité : êtes-vous bien protégé ?
- risques : quels sujets couvrir et quelle priorité ?
- business : travaille-t-on sur le bon périmètre ?

Au niveau stratégique (*executive level*), la fréquence peut être d'une réunion par an et porter sur le sujet de l'année (exemple de sujet : la sécurité, l'analyse de risque…) avec les mesures associées.

Au niveau tactique (*area level*), la fréquence peut être de deux communications par an, par exemple sur les points sur lesquels les efforts doivent porter (acquisition, cession) ainsi qu'une revue des indicateurs.

6.2. La démarche de sensibilisation vers les utilisateurs

La démarche de sensibilisation vers les utilisateurs est la plus fréquente et souvent la mieux maîtrisée. Elle ne doit pas pour autant être négligée. Elle vise à expliquer et à faire évoluer les comportements.

Les campagnes peuvent être globales ou ciblées, multi-supports (web, affiches, vidéos, *quizz*, *goodies*, jeux) ou non et comporter plusieurs messages ou non.

La démarche doit, au préalable, être présentée et validée par la direction générale ou le conseil de surveillance.

L'objectif suivi n'est pas d'inquiéter mais d'informer et de responsabiliser avant de réglementer. L'information doit être vue à la fois comme un patrimoine vivant et comme un patrimoine économique dont les salariés sont co-responsables. Pour une plus grande efficacité, il est conseillé de chercher un alignement de la démarche sur les valeurs de l'entreprise.

Les campagnes de sensibilisation à la protection de l'information peuvent aussi être ludiques, humoristiques et interactives afin de renforcer l'efficacité des messages.

Ces campagnes peuvent se faire en complément d'une démarche de diffusion de chartes internes d'usages et de bonnes pratiques.

Il est indispensable en aval de mesurer l'impact des campagnes réalisées (par exemple avec des questions du type : « Avez-vous lu/vu ces campagnes ? », « Avez-vous modifié vos comportements ? »)

6.3. La démarche de sensibilisation vers les informaticiens

La démarche de sensibilisation vers les informaticiens est une démarche très largement négligée, mais néanmoins indispensable, car ce sont souvent les populations les plus exposées et les moins sensibilisées à leurs droits et devoirs et à ce genre de risque. Ce sont aussi les populations parmi lesquelles le taux de pénétration des campagnes est plus faible que la moyenne.

L'idée est de parvenir à leur faire comprendre qu'ils ont une double responsabilité, à la fois vis-à-vis d'eux-mêmes comme toute fonction d'entreprise (obligation professionnelle) et vis-à-vis de leurs collègues en tant que fonction support (exemplarité et relais interne de la démarche de protection).

Cette démarche doit venir en appui à la diffusion et signature des chartes, qu'il s'agisse de la charte utilisateur applicable à l'ensemble des informaticiens ou de la charte administrateur applicable aux administrateurs réseaux et systèmes.

« Il faut d'abord casser les mythes », nous dit un RSSI. Les informaticiens invoquent généralement la surcharge de travail, le fait que ce n'est pas leur rôle au niveau local, qu'ils risquent de prendre du retard dans leurs projets ou encore le fait que si l'on commet une erreur il vaut mieux la cacher. Ces pratiques doivent impérativement être identifiées, expliquées et contre-argumentées.

Il s'agit également de « sensibilisation » et non pas de formation. L'objectif est de changer la perception et l'attitude des informaticiens face aux risques. Il faut conduire à ce que l'informaticien puisse s'interroger et comprenne par des exemples illustrés pourquoi les règles, les outils et les processus de protection ont été mis en place.

L'ensemble des fonctions/métiers de l'informatique doit être couvert :

- Les nouveaux arrivants ;
- Les collaborateurs ;
- Les stagiaires ;
- Les CDD ;
- Tous les métiers IT : fonction support utilisateur (notamment sur le *social engeneering*, les accès et mots de passe), les équipes infrastructures & réseaux, les équipes de développement applicatif, les chefs de projets, les managers SI, les correspondants sécurité SI.

6.4. Les bonnes pratiques en matière de communication, de sensibilisation et d'accompagnement du changement

Sur la forme :

- Ne pas faire une communication spécifique sur la protection de l'information mais intégrer la protection de l'information dans la communication globale de l'entreprise (« *embedded communication* ») ;
- Viser trois populations clés avec des messages spécifiques: le management, les informaticiens, les utilisateurs finaux ;
- Prévoir des kits de communication simples et ludiques : les moyens les plus efficaces restent les jeux de rôle, les films, les outils « impliquants » ;
- Adapter la stratégie de communication en fonction de l'organisation et de vos interlocuteurs (parler des bons sujets, de la bonne manière, aux bonnes personnes, et au bon moment) ;
- Communiquer peu (un message ou deux par campagne) mais régulièrement, à propos et en capitalisant sur l'actualité ;
- Communiquer systématiquement après un incident majeur ;
- L'humour peut être un bon moyen de faire passer les messages ;
- Associer des spécialistes de la communication, internes et externes ;
- Utiliser des indicateurs et métriques partagés et lisibles ;
- Tester l'efficacité de la démarche et avoir des feedbacks.

Sur le fond :

- Partir des enjeux business ;
- Ne pas parler informatique mais information ;
- Éviter de parler « coûts » ou « technologies » ;
- Préserver sa crédibilité en fournissant une lecture objective et pondérée des risques : éviter l'écueil de la surenchère ;
- Expliquer plutôt que moraliser ;
- Ne pas culpabiliser les utilisateurs (« ça arrive à toutes les entreprises, à notre entreprise, à tous les salariés ») ;
- S'appuyer sur les valeurs et la culture de l'entreprise ;
- Passer d'un mode réactif à un mode préventif ;
- Indiquer que l'information est un patrimoine vivant pour les salariés, dont ils sont co-détenteurs et coresponsables ;
- Indiquer que l'information est un patrimoine économique pour les actionnaires.

7. Les bonnes pratiques techniques et en termes d'outils

Bien que le groupe n'ait pas focalisé sur les outils, il est ressorti un certain nombre de bonnes pratiques en matière d'architecture, de supervision, d'administration et de contrôle. Ces bonnes pratiques sont résumées ci-dessous.

Ces outils ne sont rien sans des processus et des ressources pour les soutenir.

Architecture de protection :

- Créer des espaces de confiance (mise en place de coffres forts électroniques …) ;
- Les solutions « périmétriques » ne sont plus suffisantes, il faut avoir en plus une approche « poste de travail » (VPN, pare-feu personnel, anti-virus, chiffrement, authentification forte, *reboot* à distance), et des plans de restauration des données ;
- Gestion fine des droits d'accès utilisateurs (cycle complet, habilitation, exception, révocation …) en lien avec le cycle de vie de l'information.

Supervision, administration et contrôle :

- Cartographier les flux ;
- Supervision (revue des logs…) ;
- Audit & tests d'intrusion comme « sonnette d'alarme » et vecteur d'amélioration.

Les bonnes pratiques autour des outils :

- Standardiser (les postes de travail, master unique…) ;
- Faire des mises à jour régulières des anti-virus et appliquer les correctifs de sécurité (patchs) ;
- Eviter les droits d'administrateur locaux sur les postes de travail ;
- Identifier le « hors zone » et le gérer (les comportements non couverts par le SI – exemple les feuilles Excel) ;
- Avoir une démarche proportionnée (entre l'outil utilisé et le risque couvert) ;
- Avoir un lien clair entre l'outil, le processus et l'objectif visé
- Avoir une approche transverse.

Sans oublier les outils de sécurité physique, tels que des broyeurs, des armoires à clés, des moyens de contrôle d'accès aux bâtiments …

8. Sources

Les sources sont nombreuses et variées. Ci-dessous quelques sources citées le plus fréquemment par les membres du groupe :

- http://www.ssi.gouv.fr/fr/index.html
- www.isiq.ca
- http://staysafeonline.org/index.html
- http://www.clusif.asso.fr/
- http://www.ssi.gouv.fr/fr/index.html
- http://www.cnil.fr/

9. Annexes

9.1. Annexe 1 – Exemple de règles et devoirs par acteur

Ci-dessous à titre d'illustration un document recensant les 7 devoirs et règles par acteur. Ce document a été développé et mis en œuvre au sein d'une grande Entreprise française.

Les 7 devoirs et règles de l'Entreprise :

1. Définir et organiser la maîtrise des risques de l'Information.
2. Définir les règles et consignes à appliquer, en complément des législations et règlements.
3. Proposer, via ses pairs techniques métier, des solutions standard de protection et les consignes de sécurité associées (ex : charte de confidentialité).
4. Définir les bonnes pratiques comportementales à appliquer en toutes circonstances (ex : fiches réflexes).
5. Sensibiliser et assister l'ensemble des acteurs.
6. Vérifier périodiquement la bonne application des règles, des consignes et bonnes pratiques comportementales, ainsi que l'efficacité des solutions techniques.
7. Engager une action appropriée à l'encontre de tout membre du personnel qui enfreint les règles de l'Entreprise.

Les 7 devoirs et règles des Métiers :

1. Définir les critères « Métier » permettant de mettre en œuvre facilement la protection de l'information.
2. Classifier les informations du Métier au regard des critères Métiers et des enjeux.
3. Organiser la protection des informations les plus sensibles, en nommant pour toute information sensible un responsable de leur protection.
4. Gérer dans le cadre de la transversalité, la cohérence de la sensibilité des informations du Métier.
5. Gérer dans le temps la pertinence du niveau de sensibilité des informations du Métier.
6. Valider et contrôler la légitimité des personnes qui accèdent aux informations sensibles du Métier, et ce quelle que soit leur forme.
7. Rechercher en permanence un compromis acceptable entre impératif d'efficacité et d'efficience et impératif de sécurité de l'information : « le juste nécessaire ».

Les 7 devoirs et règles de la hiérarchie :

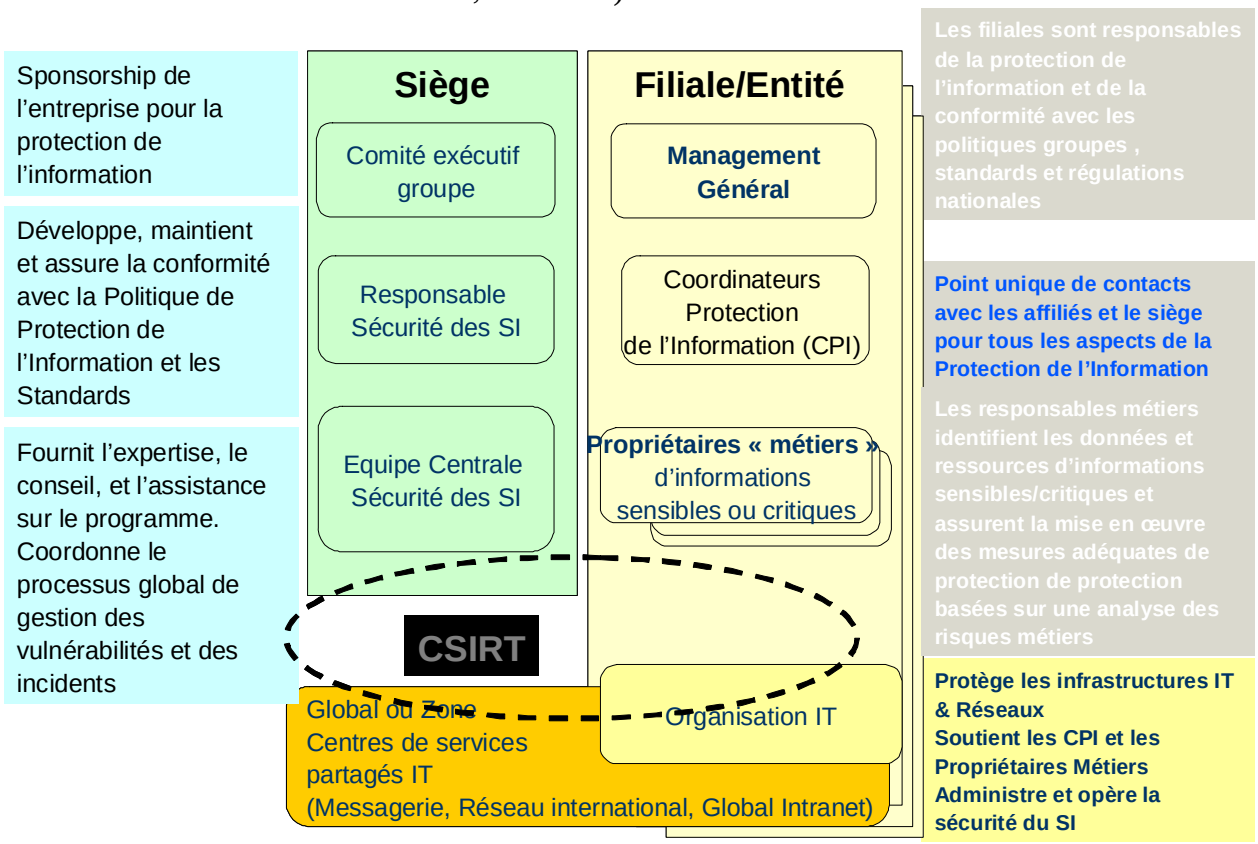
1. Montrer l'exemple.
2. Classifier dans son périmètre de responsabilité le niveau de sensibilité des informations utilisées.
3. Diffuser les règles de protection de l'information à ses collaborateurs et partenaires.
4. Doter ses collaborateurs des moyens nécessaires pour protéger l'information.
5. Valider, pour son périmètre de responsabilité, les demandes d'accès à des informations sensibles.
6. Contrôler la bonne application des règles de protection dans son périmètre de responsabilité.
7. Remonter à l'équipe en charge de la Protection et de la Sécurité du Groupe, les besoins non couverts par les règles et solutions existantes.

Les 7 devoirs et règles de chacun :

1. Connaître le niveau de sensibilité des informations détenues.
2. Connaître les règles et procédures à appliquer.
3. Définir le niveau de classification des documents rédigés.
4. Transmettre des informations confidentielles ou secrètes uniquement aux personnes habilitées et qui en ont besoin pour réaliser leur mission.
5. Respecter un devoir de réserve en tout lieu et toute circonstance. Le fait qu'une information confidentielle soit connue à l'extérieur de l'Entreprise ne nous décharge pas de notre devoir de réserve sur le sujet.
6. En cas de situation exceptionnelle, faire appel à son bon sens pour garantir la protection des informations de l'Entreprise.
7. Intervenir et alerter en cas d'anomalie.

9.2. Annexe 2 – Exemple de schéma de gouvernance

Ci-joint un schéma résumant le modèle de gouvernance d'une entreprise en matière de protection de l'information (rôles, acteurs, structures).



Source : CIGREF

Le CIGREF, Club Informatique des Grandes Entreprises Françaises, est une association d'entreprises. Sa mission est de promouvoir l'usage des systèmes d'information comme facteur de création de valeur et source d'innovation pour l'entreprise.

Le CIGREF regroupe des grandes entreprises de tous secteurs (assurance, banque, distribution, énergie, industrie, services, services sociaux et santé et transport).

Le CIGREF favorise le partage d'expériences et l'émergence des meilleures pratiques. C'est un interlocuteur des pouvoirs publics français et européens sur les domaines des technologies de l'information.

Le CIGREF fait valoir les attentes légitimes des grands utilisateurs d'informatique et de télécommunications. Les thématiques d'échanges du CIGREF sont *le SI au service des métiers de la DG, la performance durable du SI* et le *management de la fonction SI*.

CIGREF
21, avenue de Messine
75008 Paris

Tél. 01 56 59 70 00
Fax 01 56 59 70 01

E-mail : cigref@cigref.fr
www.cigref.fr