

## La gestion de la confidentialité en entreprise

L'environnement concurrentiel se durcit.

Les projets mobilisent des ressources complexes, coûteuses et de multiples sources.

La circulation des données est de plus en plus facile, opère en temps réel : c'est une donnée constitutive de la société de l'information.

L'intelligence économique s'est beaucoup développée et certaines entreprises se sont organisées pour capter, analyser et capitaliser les informations même les plus inoffensives en apparence, justement parce qu'elles s'inscrivent dans un édifice appelé à prendre du sens au détriment de l'entreprise cible.

Les grandes entreprises ont une responsabilité réglementaire et sociale de fait, de protection du patrimoine économique et industriel de leur entreprise et de leurs sous-traitant.

Les organisations étant de plus en plus ouvertes, il devient nécessaire de maîtriser les flux de données échangées. En effet, l'usage de plus en plus combatif qui peut en être fait comporte le risque qu'un échange anodin compromette un projet, un brevet, ou encore un développement.

La maîtrise des flux de données est le résultat de plusieurs éléments qui se combinent :

- l'identification des données sensibles : dans une société du savoir fondée sur la capacité à échanger des flux de données, seule une qualification des données sensibles pour l'entreprise et ses réseaux, permet de hiérarchiser et de distinguer ce qui doit faire l'objet de mesures particulières, nécessairement plus contraignantes et coûteuses ; elles doivent donc être prises à bon escient ;

Une fois les données sensibles identifiées, il devient possible de travailler sur les processus de sortie et de contrôle de ces données, car ils seront réduits en importance et dictés par une logique propre à l'entreprise.

Les processus incluent :

- l'identification des points de sortie des données (qui, modalités, situations, supports, etc)
- l'identification des comportements ainsi que des points de contact à risque
- la prise de conscience de ceux qui sont en contact avec l'extérieur de cette sensibilité et des conséquences qu'une irréflexion ou une indiscrétion peut entraîner pour eux-mêmes, leurs projets ou ceux des autres membres de l'entreprise
- un travail avec les concepteurs des vecteurs techniques afin d'améliorer la sécurité technique des réseaux
- la possibilité de modifier les comportements des « personnes-vectrices » sans que cela soit ressenti comme une inhibition ou un frein à leurs échanges normaux avec leurs interlocuteurs extérieurs, pour remédier dans des termes réellement applicables aux comportements à risque

Le fruit de notre expérience des organisations est que chaque entreprise possède ses habitudes, ses particularités, ses valeurs internes, son positionnement sur le marché ou dans la logique d'un projet, toute composante qui peut avoir une incidence directe sur la gestion de sa

confidentialité. Il s'agit donc d'élaborer une démarche ad hoc en y associant étroitement les responsables internes.

Notre approche repose sur une démarche en deux temps :

- le premier consiste à faire le diagnostic des situations à risque, en procédant aux identifications des données sensibles, des points de sortie (personnes ou vecteurs techniques) et du type de contact qui s'établissent avec l'extérieur, des règles existantes, de leur application ou des difficultés qu'elles soulèvent pour ceux censés les respecter et d'une façon générale de replacer dans leur contexte organisationnel les comportements considérés comme à risque dans cette perspective.
- le second, consiste à faire des propositions (voir détail ci-dessous) en fonction du diagnostic effectué, incluant une démarche d'amélioration qui au final s'adresse aux personnes en situation d'échanges avec l'extérieur. Le travail avec ces personnes-vectrices a le double objectif de les sensibiliser et de leur faire prendre conscience de la sensibilité des informations et des conséquences d'une information non maîtrisée. La prise de conscience est associée à un travail sur les comportements, visant en particulier à substituer à leur conduite actuelle, un attitude générale de maîtrise, par l'adoption de règles, un entraînement, des jeux de rôle, l'apprentissage de formules différentes, selon le type de données, leur support et les situations d'échanges avec l'extérieur.

Une première étape de détermination du périmètre est nécessaire en préalable au lancement de l'étude : elle doit se dérouler en étroite association avec l'entreprise afin soit d'entreprendre un diagnostic global de toute l'entreprise, soit de réserver ce travail à une activité ou une entité.

Afin de préparer le lancement d'une étude, il est possible d'organiser une rencontre avec d'autres responsables d'entreprise qui ont traité cette question afin d'échanger sur les enjeux, les difficultés, les modalités retenues, etc.

### **La phase de diagnostic**

Une fois le périmètre établi, quelques entretiens avec les responsables doivent permettre de définir quelles sont les personnes en situation de contacts avec l'extérieur ou de conception des règles ou systèmes d'information, que cela soit sous une forme directe (voyages, rendez-vous, foires, etc) ou indirecte (internet, téléphones, courriers, préparation, etc) afin de déterminer le nombre de personnes-clefs à rencontrer.

L'étude sera réalisée principalement sur la base d'entretiens et sera complétée le cas échéant, de l'analyse de la documentation existante sur ce thème (règles de sécurité et de confidentialité, rapports, le cas échéant, concernant des diagnostics précédents ou la conception de la sécurité des systèmes d'information, etc).

Les entretiens visent à cerner comment s'opèrent les contacts, le type de données échangées, les supports utilisés pour ces échanges, la connaissance et l'usage réel des modalités et des règles de sécurité existantes, les difficultés rencontrées dans les échanges ou dans l'application des règles, la conscience de la sensibilité des données ou du comportement qui leur est lié, la place qu'occupe dans l'organisation les comportements s'appuyant sur l'usage de données vis-à-vis de l'extérieur, etc.

Si des situations d'indiscrétion ont été identifiées dans l'entreprise, un retour sur cette expérience permettrait non seulement d'en cerner les mécanismes mais également de fournir un exemple tangible et compréhensible pour les participants aux formations.

**Ces entretiens donneront lieu à une analyse et une synthèse.** Les résultats seront restitués et discutés avec les commanditaires de l'étude. Des propositions seront faites en fonction des résultats, des principales difficultés constatées et des demandes des responsables internes de l'intervention. La phase de proposition peut être distincte de celle de diagnostic.

### **Les propositions**

Elles pourront porter :

- sur l'élaboration de nouvelles *règles* ou l'amélioration des précédentes,
- sur *l'organisation interne des échanges*, si celle-ci a une incidence sur l'efficacité de la gestion de la confidentialité,
- sur l'identification d'un *travail complémentaire* lié par exemple à la sécurisation de certains échanges de données transitant par des systèmes d'information ou à l'initiation de canaux distincts et déconnectés pour les informations considérées comme très sensibles,
- sur l'élaboration de *procédures* systématiques d'identification de données sensibles et de règles ad hoc d'échanges ou de comportements pour les *nouveaux projets*,
- sur l'élaboration *d'indicateurs* de suivi et d'évaluation de la gestion de la confidentialité,
- sur des séminaires de *sensibilisation*, pouvant inclure la rencontre de responsables d'autres entreprises ayant eu à s'interroger ou à gérer cette question,
- sur des entraînements en *formation* portant sur les comportements à risque afin de les modifier,
- sur la conception de *jeux* ad hoc, propres à sensibiliser les personnes-vectrices et les aider à modifier leur comportement

### **La démarche de formation**

Les éléments seront à préciser en fonction du diagnostic et des demandes de l'entreprise. Ce qui suit, constitue une trame indicative.

#### **Les objectifs de formation :**

>> permettre au personnel de comprendre ce qu'est et de qualifier une information sensible, de mesurer les risques liés à la non confidentialité, et d'acquérir les réflexes de comportement pour diminuer ces risques.

- > comprendre la qualification d'information sensible,
- > identifier les comportements risqués en terme de confidentialité,
- > mesurer les enjeux de ces comportements,
- > identifier les règles clés à respecter,
- > comprendre et intérioriser ces règles et nouveaux comportements,
- > mesurer ses forces et faiblesses,
- > s'entraîner pour acquérir les bons réflexes

**durée envisagée :**

1/2 journée

**déroulement et modalités pédagogiques :**

A définir plus précisément en fonction des résultats de l'étude et des demandes de l'entreprise.

Nous envisageons à ce jour le déroulement suivant :

- apports de l'étude et mise en perspective avec les enjeux de l'entreprise
- identification et compréhension de la qualification d'une information sensible,
- identification et compréhension des situations risquées,
- mises en situation pour acquisition de réflexes sous forme d'un jeu plateau à construire,
- synthèse, bilan, plan d'action

La pédagogie sera active et ludique. Active pour permettre l'implication de chacun sans laquelle l'appropriation ne peut se faire, ludique pour aider à prendre le recul nécessaire.

**Préparation de la formation : 3 démarches possibles :****démarche 1 : construction du module par nos soins, puis adaptation avec un responsable d'unité**

Construction du module : durée prévisionnelle 2 jours (à repreciser en fonction du diagnostic et des demandes de l'entreprise).

élaboration des outils et supports pédagogiques : de 1 à 5 jours selon les outils à concevoir.

(Cette phase a lieu une seule fois, contrairement à l'adaptation qui est nécessaire à chaque intervention pour un nouveau service)

**Adaptation de la formation à l'unité :**

pour adapter le module à l'unité, nous prévoyons un temps avec le responsable de l'unité ou avec d'autres interlocuteurs si besoin.

Il s'agira lors de cette phase de :

- > Analyser et faire comprendre ce qu'est une information sensible et ce peuvent être les comportements les plus risqués
- > Identifier des contextes les plus fréquents dans lesquels ces comportements apparaissent
- > Elaborer des réponses appropriées

ces réponses seront intégrées dans le jeu plateau pour créer des mises en situation ad hoc.

durée prévisionnelle:

1/2 journée avec le responsable de l'unité

1/2 journée pour nous

## **démarche 2 : construction du module par un groupe de travail, puis adaptation avec un responsable d'unité**

Cette deuxième démarche consiste à impliquer un groupe de personnes dans la création, puis éventuellement dans l'animation de la formation. Elle a l'avantage d'impliquer davantage le personnel, et de permettre plus aisément la démultiplication de la formation en utilisant des relais internes.

### **comment ?**

constitution d'un groupe de personnes "porteurs" de la formation

temps de travail sur 1 journée pour

> restituer les résultats de l'étude préalable

> à partir de ces résultats, identifier

- les informations sensibles
- les comportements les plus risqués propres au service ou à l'unité
- les contextes les plus fréquents
- les réponses adaptées

Les résultats fournis par le groupe de travail seront à valider par le responsable d'unité.

A partir de cette journée, nous bâtissons un module de formation "clef en main", qui pourra par la suite être porté par des animateurs internes.

Durée prévisionnelle :

Construction du module : 2 jours.

élaboration des outils et supports pédagogiques : de 1 à 5 jours selon les outils à concevoir.

mise en main du kit à l'usage des formateurs relais internes : 1 jour

## **démarche 3 : Module de formation à travers la construction d'un jeu avec une société spécialisée (AWELE-Conseil), puis adaptation avec un responsable d'unité**

Les délais de construction du jeu, d'élaboration des outils et supports pédagogiques et l'adaptation à l'unité ainsi que la formation des formateurs internes sont à préciser avec le constructeur du jeu.

Le jeu sera construit en associant le responsable de l'unité, le responsable du rapport diagnostic et des propositions, et le constructeur du jeu afin de bien préciser notamment les objectifs ainsi que les phases-clefs du contenu.

### **Retour d'expérience :**

Un retour d'expérience sera réalisé suite aux premières formations afin de les adapter et les améliorer en conséquence, au vu des résultats obtenus et des commentaires des participants.