DEJEUNER QUALITE - 21/03/2017 - Compte-rendu

« La sécurité des informations, un enjeu stratégique »

Exposé de Monsieur Jacques ERNOUX, BUTEO-IT/E&V Partners

La sécurité des informations est de plus en plus un enjeu économique :

- Positionner l'information dans le cadre de l'intelligence économique. Les informations constituent un véritable patrimoine de l'entreprise, or celui-ci est pourtant très peu protégé.
- Protéger ses informations : veille réglementaire. Présentation des axes sur lesquels la protection des données va s'appuyer en vue d'une harmonisation de la règlementation au niveau européen (RGPD).
- Méthodologies et bonnes pratiques.

Partie 1 : l'intelligence économique.

L'information dans le cadre de l'intelligence "économique". Brevets, savoir-faire, base de données, fichiers clients,… Le patrimoine informationnel de l'organisation constitue un des pôles de l'intelligence stratégique. Quelle est sa réelle valeur ?

Le concept de l'intelligence économique : VIP = Veille + Influence + Protection.

Veille liée au secteur, en restant attentif à son environnement.

Influence : comment influencer le marché et faire parler de soi, e-réputation, que dit-on de nous ?

Protection de nos informations, de notre domaine d'expertise.

Quelle utilité de l'intelligence économique ?

- Etre informé mieux et plus vite constitue un avantage concurrentiel.
- Protéger son patrimoine informationnel (processus, savoir-faire, compétences des personnes, sécurité, brevet, réputation…).
- Préserver et augmenter l'avantage concurrentiel : conserver cette longueur d'avance par rapport aux concurrents.
- Etre crédible auprès de ses partenaires, pouvoir montrer pattes blanches par rapport à un certain nombre de bonnes pratiques.

Les risques ?

- Fuite d'informations organisée, planifiée par des hackers qui revendent les informations dérobées contre rançon.
- Perte de clé USB.
- Développement du BYOD (smartphones, tablettes…). Les employés viennent avec leurs propres matériels, se connectent au réseau de l'entreprise. Avec quoi viennent-ils et avec quoi repartent-ils ?
- Sécuriser les informations tant à l'intérieur (lieu de travail, employés, stagiaires, visiteurs, …) qu'à l'extérieur de l'entreprise (lors de déplacement, connexions au wifi public non protégé,…)
- Les occasions sensibles : l'innovation (intégrer une nouvelle version de logiciel pas encore testée), la présence à des foires et salons, la recherche de partenaires, le risque réputation et image (il n'est pas toujours bon de se retrouver en 1ère ligne).

Conclusion

- **Communiquer & sensibiliser :** 80 % des failles viennent du comportement humain. Il est donc capital de sensibiliser les gens à la valeur de l'information qu'ils utilisent, manipulent et transforment. Impliquer les gens dans cette vision de gestion des risques et de sécurité de l'information.
- **Avoir un référent sécurité** (= une imposition dans la nouvelle réglementation).
- Prendre des **mesures proportionnées :** il est tout à fait possible pour une PME de gérer la majeure partie des risques, avec des moyens accessibles.
- **Se faire aider par des experts** qui, avec leur regard extérieur et leur questionnement, permettent aux entreprises d'identifier le minimum à réaliser pour gérer la sécurité des informations. Ils n'apportent pas une solution toute faite : la culture de l'entreprise en matière de sécurité de l'information doit être internalisée.

Partie 2 : Nouveau cadre règlementaire (RGPD)

Garantir la sécurité de l'information, c'est l'affaire de tous : de la direction, de la communication interne, des pilotes de processus, de l'organisation toute entière ! → Nécessité de fixer un objectif et un cadre pour la protection des données.

Un certain nombre de balises sont prévues et obligatoires pour tous à partir de mai 2018, avec toutefois dérogation et allègement possibles pour les structures de moins de 250 personnes.

« Pour que le marché intérieur fonctionne correctement, il est nécessaire que la libre circulation des données à caractère personnel au sein de l'Union ne soit ni limitée ni interdite pour des motifs liés à la protection des personnes physiques à l'égard du traitement des données à caractère personnel.

Pour tenir compte de la situation particulière des micro, petites et moyennes entreprises, le présent règlement comporte une dérogation pour les organisations occupant moins de 250 employés en ce qui concerne la tenue de registres. »

Source: http://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32016R0679&from=FR

Pourquoi RGPD ?

- Pour combler les vides juridiques dans l'UE, en comparaison à d'autres états (USA…).
- Face à la montée en puissance des réseaux sociaux. (Exemple : même si un compte est clôturé, le réseau social reste propriétaire des données pendant 20 ans).
- Le Big data et l'arrivée de l'intelligence artificielle avec la partie *profiling* (un client est dirigé vers la partie du magasin qui lui correspondrait le mieux, compte tenu de ses préférences affichées sur les réseaux sociaux).

  Attention au profiling :

  - On en oublie la complexité du profil des gens.
  - On enferme les gens dans des stéréotypes qui ne sont pas applicables car ils peuvent changer d'avis très vite.
  - Attention à l'usage du profilage pour poser des actes légaux par rapport aux gens.

- Les objets connectés (IoT). L'internet des objets n'est plus une théorie. Les objets connectés plus nombreux que les internautes. On en est encore au tout début, toutes les failles de sécurité ne sont pas encore maîtrisées.
- Les droits des internautes. Droit à l'oubli ? Droit d'avoir une copie des informations détenues sur nous, dans un format lisible (pas binaire) ?

Le développement de l'économie numérique ne pourra se réaliser que si l'ensemble des acteurs se respectent et se font confiance (stratégie de développement économique de l'UE).

Les **principes essentiels** de la protection de la vie privée sont réaffirmés dans le texte légal : restriction d'utilisation, minimisation des données (ex : il n'est pas nécessaire de donner accès à nos mails pour pouvoir télécharger un jeu), précision, limitation du stockage (en volume d'informations stockées et limitation du stockage dans le temps), intégrité, confidentialité.

Les *data centers* sont de plus en plus présents. Le Tera stocké coûte de moins ne moins cher. Il est donc plus accessible, pour les organisations, de stocker tout sur tout le monde pendant des années. Ce qui engendre des volumes énormes d'informations à devoir gérer. Est-ce pertinent ? Est-ce nécessaire ? Par exemple, il est nécessaire de conserver les informations nécessaires au calcul des pensions. Mais il n'est pas nécessaire de conserver toutes les conversations téléphoniques filaires (règle de proportionnalité : durée et volume de stockage des informations par rapport à l'intérêt et l'utilité de ces informations).

Principales mesures

- Dès le départ, quand l'entreprise va demander des informations, puis les transmettre, une **analyse d'impact** devra être réellement effectuée (avant la mise en place d'un traitement de données) – *art. 35.*
- **Consentement explicite et clair** : il ne sera plus autorisé de jouer sur le consentement implicite (via une case déjà cochée). Le responsable du traitement doit fournir la preuve que la collecte d'informations a bien été acceptée. Ce n'est plus à la personne à qui appartiennent les données à devoir se défendre en cas d'abus – *art.7,1°* .

- **Accès facilité de la personne à ses données** : possibilité d'avoir une copie de ses informations dans un délai raisonnable, possibilité d'exiger l'effacement de ses données – *art.17.*
- **Obligation de notification des violations de données personnelles**. Un organisme qui doit se référer au RGPD devra notifier dans un délai précis qu'il a subi une fuite d'informations, qu'il a été hacké,… et devra expliquer comment cela a pu se produire – *art.33.*
- **Création et maintenance d'un registre détaillé des traitements**. Le registre doit pouvoir être remis aux autorités de contrôle à tout moment – *art.30.*
- Création de **délégués à la protection des données** = point de contact en interne – *art. 37*.
- **Transfert de données** soumis à vérification et peut être demandée par la personne (copie de l'information transférée dans un format lisible et structuré, sans qu'on ne puisse faire obstacle) – *art. 45, 49 et 20.*
- **Restriction du profilage automatisé servant de base à une décision**. De plus en plus, l'informatique algorithmique est utilisée pour le profilage à des fins commerciales. Il est possible de rendre le profilage suffisamment précis pour pouvoir identifier un tout petit groupe de personnes dans une région précise et correspondant à un profil précis – *art. 21.*
- **Recours et aggravation considérables des sanctions** – *art. 78 & 79, 82, 83.*

→ Obligation de se conformer à la réglementation : mai 2018 !

Partie 3 : Méthodologie et bonnes pratiques

Les entreprises essaient souvent de mettre des actions en place sans penser d'abord à s'inspirer de bonnes pratiques qui ont fait leurs preuves et qui ont été déployées à l'international (logique d'intégration des bonnes pratiques adaptées à l'entreprise).

(Tableau de convergence des normes)

ISO 27001 expose les exigences relatives aux systèmes de management de la sécurité des informations (SMSI). Répondre aux exigences de cette norme permet à l'entreprise d'être conforme au RGPD **et** de garantir la protection de son patrimoine informationnel.

Un SMSI, c'est quoi ?

- Un système construit selon un processus de management des risques.
- Un système qui englobe les personnes, les processus et les systèmes ICT.
- Un système qui implique complètement l'organisation interne !
- Une approche basée sur une évaluation du risque et l'acceptation des niveaux du risque.
- Mes informations = mon patrimoine !
- = des politiques, des procédures, des lignes directrices, des ressources et des activités associées.

« Un SMSI est une approche systématique visant à établir, mettre en œuvre, exploiter, surveiller, réexaminer, tenir à jour et améliorer la sécurité de l'information de l'organisme pour réaliser les objectifs de l'activité. »

Avant de construire son SMSI veiller à :

- Comprendre l'organisme.
- Délimiter le périmètre dès le départ ! « *Que voulons-nous sécuriser ?* »

Notions de risques :

« Le risque lié à la sécurité de l'information est souvent mesuré en termes de combinaison des conséquences d'un événement de sécurité de l'information et de la probabilité associée d'occurrence.

Les risques liés à la sécurité de l'information sont associés au risque que les menaces exploitent les vulnérabilités d'une information ou d'un groupe d'éléments d'information et causent ainsi un préjudice à une organisation. »

- L'analyse de risques est un élément standard présent dans toutes les méthodologies.
- Être attentif à la communication et au suivi/à l'examen du risque.

Faire des schémas ne suffit pas. Il faut les faire vivre, identifier l'occurrence du risque, prendre les mesures nécessaires pour corriger.

$$\textbf{Risque} = \frac{\text{Menace x Vulnérabilité x Impact}}{\text{Contrôles}}$$

Minimum requis pour être en phase avec une précertification ISO 27001 : voir liste des documents et enregistrements minimum requis.

Conclusions

- Les données sont un patrimoine pour toutes les organisations.

- Ces informations sont convoitées
  - par nos concurrents.
  - GAFA (Google, FB, Apple,…) : des milliards de dollars sont générés grâce à nos données privées.
  - Besoin de protéger : oui ! Les nouvelles règlementations se mettent en place. Les entreprises ont un cadre légal à respecter. Elles pourront rester opérationnelles en toute confiance dans ce cadre légal. Besoin de protéger les informations également pour garantir la satisfaction des clients.
  - Comment ? il existe des bonnes pratiques qui ont fait leurs preuves sur le terrain, qui ont été déployées et reconnues à l'international (référentiel commun).

- Auto-évaluation (inspirée d'un plan de cyber sécurité) pour établir un diagnostic : cela permet de se poser les bonnes questions de manière très terre à terre (accessible pour une PME).

Questions-réponses

1) Pour une PME : investir dans un serveur ou tout sous-traiter (cloud) ?
   3 gros blocs de coûts à évaluer et à comparer aux coûts internes (machines internes, coûts d'énergie, coûts de personnel…) :
   - Coût de migration vers le fournisseur ?
   - Opérationnel : **mes** conditions de service sont-elles bien imposées au fournisseur ?
   - Que se passe-t-il si demain on change de fournisseurs (coût de rapatriement des données ? les récupérer + les transmettre à un autre) ?

   ➔ Externaliser n'est pas toujours une bonne solution, surtout s'il s'agit d'informations stratégiques, à valeur ajoutée.

2) Quel budget pour implanter un système correct pour une PME ?
   - Cela dépend de la maturité de l'entreprise et de sa contribution.
   - S'assurer de pouvoir compter sur le sponsor clair et net de la direction, indispensable à la réussite du projet.
   - Approche conseillée : philosophie de coaching. La PME doit s'approprier la démarche. Ce n'est pas le consultant externe qui doit identifier les risques de l'organisation, il est là pour poser les bonnes questions, pour comprendre les objectifs du projet et aider ainsi l'organisation à bien définir le périmètre, et inventorier les risques. La démarche doit venir de l'intérieur de l'entreprise car le know-how doit rester en interne. La valeur ajoutée de la démarche doit profiter à l'organisation et dépend des équipes.

   ➔ Pour une PME, compter en moyenne entre 5 et 20 jours de coaching étalés sur une période de 6 à 12 mois.

3) 80% erreurs = humain. Le risque le plus important est entre le clavier et la chaise. Comment faire en sorte que le personnel n'ait pas le sentiment d'être placé sous la surveillance sévère du coordinateur du système ?
   - Travailler sur deux axes :
     - **Implication** : impliquer les équipes dans la démarche pour qu'ils comprennent le sens !
     - **Communiquer** : expliquer les choses et ne pas imposer sans expliquer pourquoi.
   - Ces 2 axes articulés correctement permettront aux collaborateurs de comprendre les enjeux. Le consultant n'a pas autorité pour descendre dans l'organisation et la transformer. Il est là pour poser les questions pertinentes qui feront réfléchir aux risques.

***

Document rédigé par V. Rossignol