Les synthèses du CLUSIF

RSSI-CIL, deux fonctions, un seul objectif

Synthèse de la conférence thématique du CLUSIF du 25 octobre 2012 à Paris

Olivier Caleff de Devoteam introduit cette conférence commune « Clusif – AFCDP ». Dans un contexte qui voit parfois se rencontrer la prise en compte des risques informatiques et ceux liés à la protection de la vie privée, l'objectif de cette conférence est d'identifier les points de contact des problématique du RSSI et celles du CIL, afin de montrer comment ils coopèrent pour faire converger leurs objectifs qui ne sont pas nécessairement complètement convergents.

Mireille Deshayes, Adjointe au CIL Groupama

Mireille Deshayes donne le point de vue d'un CIL sur la synergie CIL-RSSI : « ami » ou « ennemi » ?

Groupama est un groupe multimarques qui compte 38 000 collaborateurs en France et à l'étranger. Groupama a décidé de nommer un CIL en 2006.

Chez Groupama, les fonctions CIL et RSSI sont positionnées de la façon suivante :

- Le CIL occupe une place au Secrétariat Général de Groupama, au plus haut niveau du groupe. Il a une équipe de trois personnes, des juristes et des informaticiens. Il s'appuie sur un réseau de relais présents dans chacune des entreprises du groupe. Le CIL les forme et les anime. Son périmètre s'étend à toutes les filiales et tous les traitements.
- Le RSSI fait partie d'un GIE. Le RSSI est rattaché à la Direction de la stratégie de la performance et de la maîtrise de la sécurité des risques et de la qualité. Son périmètre s'étend à tout le groupe également mais seulement à la demande des filiales quand elles décident de faire appel au GIE.

Le CIL et le RSSI répondent à des problématiques communes sur lesquelles ils s'entendent :

- Sur la sécurité et confidentialité des informations : les articles 34 et 35 de la loi informatique et liberté et les réglementations qui impactent le secteur de Groupama.

➢ Le CIL et le RSSI définissent les mesures adéquates en fonction de la nature des données. Ils tiennent le même discours sur la formation et la sensibilisation des personnes concernant la sécurité. Ils ont contribué également ensemble à la révision de la PSSI du groupe.

- sur la violation des données à caractère personnel.

➢ Le CIL et le RSSI s'entendent pour que chacun remonte à l'autre les atteintes sur les données personnelles dont il a connaissance. Ils gèrent ensemble les incidents.

- Sur la conservation des informations et le droit à l'oubli, la numérisation des informations.

➢ Le CIL et le RSSI ont défini des politiques d'archivage communes, ont mis en place

des outils de détection des mots interdits, ont travaillé à la réduction des espaces de stockage et de coûts.

- Sur tous les usages nouveaux qui s'imposent à l'entreprise comme l'utilisation de l'ordinateur personnel du salarié dans l'entreprise.

➢ Sur ces points, le CIL et le RSSI travaillent de concert.

Pour mener tous ces chantiers, le CIL et le RSSI organisent des réunions mensuelles. **Chacun « forme » l'autre, les RSSI apportent aux CIL leur savoir technique et les CIL sensibilisent les RSSSI aux aspects juridiques et aux problématiques informatique et liberté.** Par ailleurs, le CIL participe à la Commission Sécurité Groupe et le RSSI aux journées d'animation des CRIL. Ils mutualisent leur documentation et montent des groupes de travail sur les problématiques communes.

Un point de rencontre particulièrement important entre le CIL et le RSSI est l'audit sur site. En effet, le CIL remplit des missions d'audit : il procède soit par questionnement soit directement dans l'entreprise. Dans ce dernier cas, venir avec le RSSI permet d'associer les compétences. Chacun fait son rapport d'audit puisque les plans d'actions doivent être déclinés soit par les directions informatiques soit par les autres directions.

Et enfin, afin que le RSSI s'ouvre plus facilement aux problématiques CIL, il est aussi CRIL de son entreprise dans le groupe.

Mais, sur certains sujets la synergie CIL-RSSI est plus difficile. Par exemple, le RSSI étant dans un GIE, il a fallu formaliser les relations contractuelles entre les entreprises du groupe et le GIE informatique. Un autre sujet qui pose problème est la difficulté pour le CIL d'exploiter la documentation générée par le RSSI, volumineuse et très technique. De manière plus générale, les manières de concevoir la sécurité diffèrent souvent. Le RSSI traite la sécurité dans sa globalité et le CIL se focalise sur les données personnelles. Ce dernier doit faire l'effort de considérer les données personnelles dans un cadre plus large.

Enfin, CIL et RSSI sont confrontés à la lourdeur d'un grand groupe, notamment à la suite d'audits qui impliquent des demandes de modifications. Ils sont tous les deux contraints de respecter un budget limité. Et ils n'ont pas de pouvoir hiérarchique sur leurs relais respectifs. Sur ce dernier point, le CIL dispose d'armes en cas de problème : son droit d'alerter la CNIL en cas de difficulté à exercer sa mission, et son indépendance, qui sont prévus par la Loi

CIL et RSSI ont chacun leurs prérogatives :

- Le CIL, positionné au Secrétariat Général du Groupe, a accès aux comités de direction des entreprises du groupe. Ses missions sont fixées par les textes et il peut donc s'y référer pour intervenir. Il dispose de moyens humains avec les relais. Il a une bonne vision des traitements parce qu'ils passent tous par les CIL. Le CIL est utilisé comme un vecteur de confiance : il est sollicité par les salariés et les institutions représentatives du personnel. Il est accompagnateur et facilitateur de projet.

- Le RSSI connaît tous les nouveaux projets informatiques des entreprises du groupe. Il dispose de toutes les connaissances techniques et avancées technologiques. Il bénéficie d'un réseau de responsables sécurité dans toutes les entreprises. Enfin, il a une vision internationale du groupe puisqu'il héberge toutes les applications des filiales étrangères.

En conclusion, si au début, le CIL et le RSSI travaillaient ensemble en fonction des sujets, une collaboration régulière s'est installée. Ces deux fonctions sont complémentaires pour augmenter le niveau de sécurité.

Thierry Autret, RSSI et CIL adjoint, Groupement des Cartes Bancaires

Thierry Autret rappelle que le rôle du Groupement des Cartes Bancaires est d'assurer l'interbancarité en France, ce qui signifie l'acceptation de toute carte sur tout terminal dans le respect des règles interbancaires. Alors que le nombre de cartes bancaire atteint 60 millions et qu'1 million de commerçants acceptent la carte, la société compte un peu moins d'une centaine de personnes soit la taille d'une PME.

Cet effectif restreint explique que le RSSI, nommé en 2005, assurait déjà, en plus de ses fonctions, le rôle de responsable sécurité (des locaux, des personnes etc.), puis de responsable des plans d'activités et de continuité.

En 2011, la société fait le choix de nommer un CIL et c'est la Directrice des affaires juridiques et bancaires qui prend cette fonction. Comme elle a l'habitude de travailler en étroite collaboration avec le RSSI, celui-ci devient son adjoint cette année.

Le « cumul des mandats » est souvent nécessaire dans une petite société qui ne peut pas nommer des salariés à temps plein sur des fonctions pourtant nécessaires. Au sein du Groupement des cartes bancaires, le RSSI détient les compétences pour exercer la mission d'adjoint au CIL mais le cumul des compétences ne se trouve pas forcément au sein de toutes les entreprises.

L'avantage du cumul des fonctions de RSSI et d'adjoint au CIL est que le RSSI a la connaissance de l'historique en terme de données et qu'il a donc plus facilement accès aux informations quand il joue le rôle de CIL.

Cela dit, la double compétence ne suffit pas et la fonction de CIL ne saurait être imposée à un RSSI qui ne le souhaite pas. Une affinité avec cette nouvelle attribution est nécessaire pour qu'elle soit remplie en totale complémentarité avec celle de RSSI.

Comme l'exige la CNIL, les tâches du CIL doivent être clairement identifiées dans sa fiche de fonction. Au Groupement des Cartes Bancaires, la même chose a été faite pour l'adjoint. La fiche de fonction doit être mise à jour afin que la fonction CIL, ou adjoint CIL, ne soit pas un simple ajout aux fonctions précédentes.

Le profil des fonctions :

- Le RSSI doit pouvoir formaliser de manière précise des objectifs de sécurité. Il peut être un « geek » mais pas forcément : au Groupement des Cartes Bancaires, le RSSI s'appuie sur des spécialistes très techniques. Il est fortement sensibilisé à la protection des données, au delà même de celle attendue par le CIL : il assure l'analyse de risques selon les critères « DICP » (disponibilité, intégrité, confidentialité et preuve), la protection du patrimoine informationnel, etc. Doté d'un très bon relationnel il forme et sensibilise les équipes opérationnelles et supervise les comptes rendus à la Direction Générale. Enfin, il veille à entretenir une relation partenariale avec la DSI et, même s'il n'est pas juriste, il connaît les aspects juridiques du SI et des données.
- Le RPCA (Responsable des plans de continuité d'activité), doit avoir une bonne connaissance des métiers et de leurs besoins. Il a connaissance des applications, des processus, des flux et des données.
- Sur le CIL, l'article 22 de la loi dit : « le correspondant est une personne bénéficiant des qualifications requises pour exercer ses missions ». Rien d'autre n'est spécifié. Le guide du CIL donne plus d'informations. Il indique que les compétences du CIL doivent porter sur :
  - L'informatique et les nouvelles technologies.
  - La réglementation relative à la protection des données à caractère personnel.
  - Le domaine d'activité dans lequel il exerce ses fonctions et la législation applicable.

Afin de concilier les compétences informatiques et juridiques nécessaires à la fonction de CIL, la directrice des affaires juridiques et bancaires a été nommée CIL et le RSSI, adjoint CIL. La CNIL, les filiales et le comité d'entreprise ont été avisés de ces nominations comme il se doit. A noter que la CNIL ne reconnaît que le CIL. L'adjoint CIL par exemple ne dispose donc pas d'accès à l'intranet de la CNIL.

Concernant la légalité du cumul des fonctions, l'article 46 dit simplement qu'il est possible d'effectuer les deux fonctions

dès lors qu'il n'y a pas de conflits d'intérêts dans l'exercice de la mission.

Les compétences du RSSI sont un atout pour l'exercice de la fonction CIL. Il doit cependant veiller à faire la part des choses, notamment dans l'utilisation de ses outils de scrutation. Il doit enfin gérer son temps afin de faire les deux métiers et de ne pas privilégier naturellement sa mission première de RSSI.

***

Bruno Rasle, Délégué Général de l'AFCDP

Pour commencer, Bruno Rasle choisit deux articles de presse qui révèlent des failles sur les sites web de la CNIL et de l'AFCDP. Ces failles prouvent que la question n'est pas de savoir si un incident à notifier va survenir mais de savoir quand il va survenir.

La conséquence est qu'il faut absolument s'y préparer. Et il apparaît logiquement que c'est au CIL d'initier ce projet. Il a le choix d'attendre d'être dans l'obligation d'appliquer le projet en cours de règlement européen sur les données personnelles, mais le chantier étant considérable, il a intérêt à le lancer le plus rapidement possible.

L'AFCDP travaille sur ce sujet depuis 2009. Les RSSI s'étonnaient alors d'avoir à faire un jour des notifications de violations aux traitements de données à caractère personnel. Et ils furent surpris d'apprendre que ça se faisait à l'étranger depuis plusieurs années.

L'AFCDP décide alors de constituer un groupe de travail constitué de RSSI et d'autres profils, des juristes notamment. Elle auditionne à plusieurs reprises des « Chief Privacy Officer » américains qui obéissent à des lois différentes selon les Etats. Elle auditionne également le chef de l'expertise technique de la CNIL dans un contexte où le Paquet Telecom impose aux opérateurs déclarés à l'ARCEP de remonter à la CNIL tout incident de sécurité sur les données personnelles. Et enfin, le réseau social interne de l'AFCDP crée un groupe « Notification » très actif.

En mars 2010, la loi Détraigne -Escoffier était votée par le Sénat. Mais aucun décret d'application n'est encore publié et elle n'est toujours pas obligatoire. Elle prévoyait non seulement le CIL obligatoire dans l'entreprise mais également la notification à la CNIL en cas de perte de données personnelles pour tous les secteurs d'activité. Elle présente le mérite, en attendant, d'être un galop d'essai qui sert de bases aux travaux sur le sujet.

Des législations similaires existent déjà dans d'autres pays. Par exemple en Californie, pionnier du domaine, depuis 2003. Et en Allemagne, qui est soumis à cette obligation depuis 2009 dans tous les secteurs.

En France, en août 2011, la directive européenne Paquet Telecom est transposée dans le droit français : elle encadre l'implantation des cookies, impose la notification en cas de violation des données à caractère personnel par les opérateurs et le projet de règlement étend cette obligation à l'ensemble des secteurs. Concernant les opérateurs, le schéma prévu par la loi est le suivant :

Tout en haut, le responsable de traitement prend connaissance de l'incident (souvent signalé par l'extérieur). Il se pose alors la question de savoir si les mesures techniques appropriées ont été prises pour protéger les données.

- S'il estime que ces mesures ont été prises, il ne notifie pas.
- S'il estime que les précautions prises ne sont pas suffisantes, il évalue l'opportunité de faire une analyse de risque. Non pas une analyse de risque pour l'entreprise mais une analyse de risques pour les personnes concernées par la violation des données.
  - Si les personnes sont atteintes, il doit notifier à la fois à la CNIL et aux personnes concernées.
  - S'il pense au contraire qu'il n'y a pas de risques pour les personnes concernées, il doit notifier à la CNIL seulement.
  - Et la CNIL se pose alors elle-même la question de savoir s'il y a un risque pour les personnes. Si son avis est différent, elle met en demeure le responsable de traitement de notifier aux personnes concernées.

Pour l'AFCDP, le CIL joue un rôle central. Outre ses comptes rendus à la direction et sa collaboration avec le RSSI, il doit

communiquer avec les syndicats et les actionnaires. Il doit aider les commerciaux qui ont à répondre aux clients dont les données ont été atteintes. Le CIL répond aussi à la presse. Et enfin, il doit rédiger la lettre de notification, se demander qui va la signer, si elle doit donner les origines de l'incident ou pas etc.

Les questions qui se posent sont nombreuses. Par exemple :

- Qui prendra la décision de notifier ?

➢ C'est toujours le responsable de traitement qui prend la décision mais il la prend sur des raisons motivées qu'on lui fournit.

- Peut-on s'assurer contre les frais d'une notification ?

➢ Ca se fait beaucoup aux Etats Unis.

- Doit-on s'intéresser uniquement aux incidents qui devraient déboucher sur une notification ou également aux « near miss » (les incidents évités de justesse) ?

➢ La CNIL Britannique recommande aux responsables de traitement de traiter les « near miss » afin qu'ils ne deviennent pas de vrais incidents une autre fois.

En 2011, l'AFCDP et ses homologues allemands, néerlandais et espagnols créent une confédération des associations professionnelles de la protection des données personnelles : CEDPO (Confederation of european data protection organisations).

CEDPO a pour objet de promouvoir le rôle du CIL (DPO en anglais). Par exemple, le projet de règlement européen prévoit l'obligation de nommer un CIL. **CEDPO propose d'aller plus loin en faisant jouer un rôle plus important au CIL dans la gestion des éventuelles notifications de violations.**

La proposition de CEDPO est la suivante : en cas d'incident, le CIL analyse l'incident en prenant en compte le contexte et rend son conseil au responsable de traitement sur :

- La notification à l'autorité de contrôle,
- la notification à l'autorité de contrôle et aux personnes concernées ou,
- la simple documentation de l'incident.

Le CIL donne un conseil mais le responsable de traitement reste le seul responsable.

Outre la notification des violations, le projet européen intègre bien d'autres axes d'améliorations :

- Privacy by Design (technologies qui intègrent la protection des données personnelles dès leur conception)
- Security by design (applications web sécurisées dès leur conception)
- Privacy Impact Assessment (étude d'impact sur la vie privée)
- « Near Miss »
- Validation des sous-traitants, etc.

C'est un texte découpé en articles qui peut faire oublier la nécessité d'une vision globale. Or la protection des données implique d'agir en synergie avec l'ensemble de ces axes de progression.

***

Eric Grospeiller, Fonctionnaire de Sécurité des Systèmes d'Information (FSSI) des ministères des affaires sociales.

Eric Grospeiller prévient : si la loi informatique et liberté est un renfort pour la mission du RSSI, elle peut aussi présenter un risque, celui d'oublier les autres facteurs de sécurité. A titre d'exemple : la loi HPST (Hôpital patients santé territoires) met l'accent sur la confidentialité. Or il peut arriver que la sauvegarde de la vie humaine impose de négliger, pour un instant tout au moins, les questions de confidentialité.

Afin de concilier la CNIL et le RSSI, une comparaison de leurs objectifs s'impose.

- L'objectif de la CNIL est la protection des libertés à l'heure du numérique en garantissant l'anonymat, en préservant l'identité humaine, en garantissant la transparence et en préservant la vie privée.
- L'objectif du RSSI est la garantie de la sécurité des systèmes d'information et des données en fonction d'un besoin exprimé. Sa mission doit s'effectuer selon une classification DICP (disponibilité, intégrité, confidentialité et preuve) et en utilisant des méthodes standardisées ou imposées.

L'objectif du RSSI est donc plus encadré.

La CNIL est un organisme de définition d'obligations, de moyens et d'organisation. Elle recommande, contrôle et sanctionne. La loi informatique et liberté fixe le cadre des traitements des données à caractère personnel.

Pour la CNIL, les exigences en matière de sécurité des systèmes d'information concernent :

- la sécurité des fichiers,
- la confidentialité des données,
- la durée de conservation des informations.

La CNIL détaille chacune de ces exigences. Elles sont un atout pour le RSSI. En effet, quand il doit traiter des données à caractère personnel, il peut y faire référence pour mettre en place des plans d'action qui soient respectés.

En matière méthodologique, la CNIL adoptait en 1981, une recommandation qui prévoyait « que l'évaluation des risques et l'étude générale de la sécurité soient entreprises systématiquement pour tout nouveau traitement informatique, et réexaminées pour les traitements existants ».

Aujourd'hui la démarche standard consiste à analyser les risques, définir ce qui doit être couvert, mettre en place des solutions et accepter le risque résiduel. Elle est cohérente avec l'approche ISO.

Cette démarche est cohérente également avec le RGS (Référentiel Général de Sécurité) qui définit un ensemble de règles de sécurité qui s'imposent aux autorités administratives dans la sécurisation de leurs systèmes d'information. Le RGS va plus loin que l'ISO en imposant l'homologation.

L'analyse de risque commence la plupart du temps par une classification. La classification qui sert souvent de référence, celle de l'OTAN, est partagée en 5 niveaux : « non classifiée », « restreint », « confidentiel », « secret », « très secret ».

En haut de la classification, les niveaux « confidentiel », « secret » et « très secret » sont classifiés défense. Ils sont régis par des lois et pour y accéder deux conditions sont nécessaires : l'habilitation et le droit d'en connaître. Ces deux conditions se retrouvent dans la loi informatique et liberté.

En bas, les niveaux « non classifié » et « restreint » sont non classifiés défense. L'objectif était d'en tirer une classification pertinente et qui puisse être dupliquée. Des FFSI, qui travaillent sur le document de la politique de sécurité des systèmes de l'information de l'Etat, ont proposé d'ajouter 4 sous catégories à la catégorie « restreint » (« public », « confidentiel », « restreint » et « secret ») dans le volet classification. Cette classification sera reprise dans la politique générale de sécurité des systèmes de santé (PGSSI) et devrait être déclinée dans d'autres secteurs.

Par ailleurs, un groupe de travail, composé de RSSI et de CIL de la sécurité sociale, a travaillé à l'élaboration d'un tableau qui reprend cette classification en l'appliquant aux données à caractère personnel. L'objectif était que les RSSI et les CIL s'entendent sur des idées et des dénominations communes. Cette classification, cohérente avec la loi informatique et liberté, prouve que cette loi constitue un réel apport pour le RSSI.

Cependant la CNIL écrit « qu'il convient d'adopter une vision globale qui dépasse le seul cadre de l'activité de l'organisme et des finalités prévues pour ces traitements, et qui permette d'étudier les impacts sur les personnes que ces données concernent ». Or cette vision globale peut se retourner contre la protection des données à caractère personnel. Ce problème a été évoqué lors de la rédaction de la PGSSI à laquelle participe la CNIL. En effet, les données de santé sont des données très sensibles et dans la majorité des cas il convient de les privilégier. Mais il peut arriver par exemple que la nécessité d'accéder rapidement à une information prime sur la confidentialité. De la même façon il peut arriver qu'un patient ne soit pas en mesure de donner son consentement à l'accès de son dossier médical (patient dans le coma par exemple). **Dans le domaine de la santé, le RSSI compense la possibilité de désactiver la protection en augmentant le niveau de traçabilité.** On saura ainsi qui a accédé à l'information.

Amandine Jambert, Ingénieur expert, CNIL

Amandine Jambert traite le sujet de la gestion des risques sur les libertés et la vie privée.

La CNIL est une autorité administrative indépendante chargée de veiller à la protection des données personnelles. Elle compte environ 160 agents qui ont le pouvoir d'informer et de conseiller, de contrôler et de sanctionner si nécessaire.

La donnée personnelle est au cœur de la loi informatique et liberté. C'est une donnée relative à une personne physique identifiée ou identifiable de manière directe ou indirecte. La CNIL s'intéresse au traitement, donc à n'importe quelle action effectuée sur des données à caractère personnel.

I. Les raisons de gérer les risques sur les libertés et la vie privée sont :

- Assurer la sécurité des données : l'article 34 de la loi informatique et liberté dit que le responsable de traitement doit prendre toutes les précautions pour assurer la sécurité des données.
- Assurer la maîtrise par les personnes concernées : le responsable de traitement doit garantir aux personnes concernées la possibilité d'exercer leurs droits. Droits d'opposition, de rectification, de suppression et d'accès.
- Assurer le respect de la Loi Informatique et Libertés.

➢ Le non respect de ces obligations peut entraîner des sanctions administratives ou pénales.

- Préparer l'avenir : le nouveau règlement va introduire de nouveaux points dont la nécessité d'effectuer une analyse d'impacts sur la protection des données. La sanction financière prévue en cas d'absence d'analyse d'impacts pourrait atteindre un million d'euros ou 2 % du chiffre d'affaire mondial consolidé.

II. Les manières de gérer les risques sur la vie privée.

La sécurité des systèmes d'information et la protection de la vie privée se rencontrent sur de nombreux points. Mais leurs objectifs ne sont pas les mêmes.

- La sécurité des systèmes d'information doit protéger l'organisme. Le RSSI regarde toutes les informations manipulées au sein de l'organisme et étudie les impacts juridiques, financiers et d'image.
- La protection de la vie privée doit protéger les personnes concernées. Le CIL regarde uniquement les données à caractère personnel et les processus légaux.

➢ Le RSSI et le CIL travaillent à diminuer les impacts sur la vie privée ou les libertés publiques. Les deux réflexions sont donc complémentaires.

Pour gérer les risques sur la vie privée, la solution est donc d'utiliser la méthode de SSI habituelle tout en prenant en compte les spécificités de la vie privée. C'est à dire étudier les risques et les impacts sur les personnes concernées et choisir des mesures respectueuses de la vie privée.

Une autre solution est d'utiliser les guides de la CNIL :

I. Une méthode « Gérer les risques sur les libertés et la vie privée ».

Le principe de la méthode consiste à :

1. Etudier le contexte : quelles sont les données à caractère personnel, quelles sont les références applicables, quels sont les supports et quelles sont les sources de risques.

2. Etudier les évènements redoutés : se demander quels seraient les impacts sur la vie privée si le traitement était modifié, les processus légaux plus disponibles, si une personne non autorisée accédait à un ordinateur personnel, si les données personnelles étaient modifiées et si elles disparaissaient. Et pour répondre à ces questions, il faut savoir quel est le caractère identifiant d'une donnée à caractère personnel.

Une fois qu'on dispose du caractère identifiant et l'impact prévu (négligeable, limité, important ou maximal), on est capable d'évaluer la gravité des évènements redoutés.

3. Etudier les menaces (si la gravité est élevée).

4. Etudier les risques (si la gravité est élevée).

5. Etudier les mesures.

Si on reprend cette méthode les responsables sont les suivants :

- La Maîtrise d'ouvrage (MOA) définit le traitement, identifie les évènements redoutés et réalise la cartographie des risques.
- La maîtrise d'œuvre (MOE) étudie les menaces et propose des mesures pour traiter les risques.
- Le CIL et/ou le responsable SSI sont garants de la méthode : ils s'assurent que les enjeux Informatique et liberté sont bien pris en considération.
- Le responsable de traitement approuve l'étude et accepte les risques résiduels.

II. Un catalogue de mesures « Mesures pour traiter les risques sur les libertés et la vie privée ».

L'objectif du catalogue est de mettre à disposition des mesures parmi lesquelles on choisira la plus appropriée pour éliminer un risque identifié comme important. Une fois le risque diminué, une cartographie des risques peut être établie. C'est un tableau qui présente, en abscisse la vraisemblance de survenue des risques (de « négligeable » à « maximal ») et en ordonnée, la gravité de ces risques (de « négligeable » à « maximal » également). De manière logique, un risque très grave et très vraisemblable devra être traité : il faut diminuer soit sa gravité soit sa vraisemblance. Bien évidemment les décisions peuvent être nuancées, en cas de mise en cause de la vie humaine par exemple.

Les deux guides sont disponibles sur le site web de la Cnil.

Conclusion de Lazaro Pejsachowicz, Président du Clusif.

Lazaro Pejsachowicz conclut en faisant remarquer que c'est le débat contradictoire qui apporte la vérité. Or, la présence d'un CIL et d'un RSSI dans l'entreprise permet de mener ce débat contradictoire, souvent fort intéressant par ailleurs. L'entreprise qui se prive de ce débat se prive de choses importantes. Quelle que soit la situation, elle doit trouver le moyen de le provoquer. C'est la finalité et la culture de l'entreprise qui indiquent de quelle manière maintenir ces rôles contradictoires et comment monter la coopération RSSI-CIL de telle façon que maintenir les rôles contradictoires ne signifie pas « refaire deux fois le même travail ».

Questions et Réponses avec l'assistance.

Cette conférence comportait également une table ronde animée par M. Jean-Marc Grémy (CLUSIF) et à laquelle ont participé Mme Amandine Jambert (CNIL) et MM. Thierry Autret (GIE Cartes Bancaires) et Paul-Olivier Gibert (AFCDP), ainsi qu'un débat avec la salle, non retranscrits dans ce document mais disponible en vidéo, sur le site web du CLUSIF, à l'adresse suivante : http://www.clusif.fr/fr/production/videos/#video121025.

Retrouvez les vidéos de cette conférence et les supports des interventions sur le web CLUSIF http://www.clusif.fr/fr/infos/event/#conf121025.